Política de Segurança da Informação e Cibernética

MARCHA LTDA
CNPJ: 58.300.812/0001-32
Avenida Paulista, Nº 1337, Bairro Bela Vista, São Paulo-SP. CEP: 01.311-200

Dados da Empresa

Razão Social	MARCHA LTDA
CNPJ	58.300.812/0001-32
Endereço	Avenida Paulista, Nº 1337, Bairro Bela Vista, São Paulo-SP.
CEP	01.311-200

Informações Gerais

Título	Política de Segurança da Informação e Cibernética
Versão	V1.0.01
Aprovador	Diretoria Executiva
Data da Aprovação	20/01/2026
Próxima Revisão	—
Responsável pela Política	Zijie Pan
Classificação da Informação	Interna

SUMÁRIO

RESUMO

A Política de Segurança da Informação e Cibernética é o documento que expressa o posicionamento da MARCHAPAY LTDA E.P.P. em relação à proteção das suas informações, dados e ativos digitais. É dever de todos os colaboradores, parceiros e terceiros seguir as orientações contidas neste documento para mantermos a elevada confiabilidade e credibilidade do nosso ecossistema de pagamentos e honrarmos nosso compromisso para garantia da Confidencialidade, Integridade e Disponibilidade (CID) da informação.

Esta política reflete o compromisso da Marcha Pay com a segurança cibernética no contexto de suas atividades como PST/Gateway, incluindo o processamento de transações, o armazenamento de dados de lojistas e a proteção de seu código-fonte e Propriedade Intelectual (PI), assegurando proteção adequada contra ameaças cibernéticas e cumprimento das melhores práticas do setor.

OBJETIVO

Estabelecer as diretrizes estratégicas para compor um programa abrangente de Segurança da Informação e Cibernética na Marcha Pay, definindo princípios, responsabilidades e controles necessários para proteger os ativos tecnológicos críticos da plataforma, dados de clientes e parceiros, bem como assegurar a continuidade e integridade das operações de pagamento digital.

ABRANGÊNCIA E ESCOPO

A Política de Segurança da Informação e Cibernética é aplicável a todos os colaboradores, fornecedores, consultores, prestadores de serviços, parceiros comerciais e demais terceiros que tenham acesso aos sistemas, tecnologias de informação, dados ou instalações da Marcha Pay. Esta política abrange todas as informações processadas, armazenadas ou transmitidas pela instituição, independentemente do formato ou meio utilizado.

É de propriedade da Marcha Pay toda a informação gerada, processada ou custodiada por meio de seus recursos, incluindo:

I. Informações Abrangidas

a. **Propriedade Intelectual e Ativos Tecnológicos:** Código-fonte do Gateway e do Software Antifraude, algoritmos, bases de dados de know-how, configurações de segurança, chaves criptográficas e demais recursos tecnológicos que configuram a PI da Marcha Pay.

b. **Dados de Clientes e Transações:** Informações cadastrais de Lojistas e Consumidores (dados pessoais), histórico transacional, documentos de identificação, informações de contas bancárias e demais dados relacionados aos serviços prestados.

c. **Informações Operacionais:** Dados sobre processamento de pagamentos, transferências, gestão de chargebacks, contratos, acordos de parceria e informações sobre contrapartes (IPs/Adquirentes).

d. **Informações Corporativas:** Estratégias de negócio, informações financeiras da instituição, relatórios gerenciais e políticas internas.

II. Princípios de Utilização

Toda informação de propriedade ou custodiada pela Marcha Pay deve observar os seguintes princípios:

a. **Finalidade Específica:** Somente deve ser utilizada pelos colaboradores ou terceiros contratados para fins profissionais relacionados às atividades de gateway ou, em outros casos, com autorização formal.

b. **Classificação Adequada:** Deve ser classificada segundo critérios de confidencialidade, integridade e disponibilidade definidos nesta política. O código-fonte e os algoritmos possuem a classificação máxima de Confidencialidade Crítica.

c. **Proteção Integral:** Deve ser protegida contra modificação, destruição, divulgação não autorizada e acesso por pessoas não autorizadas, em aderência à LGPD.

d. **Retenção Controlada:** Deve ser armazenada pelo tempo determinado pela MarchaPay e/ou legislação vigente, sendo recuperada somente quando necessário e por pessoal autorizado.

Política de Segurança da Informação e Cibernética

MARCHA LTDA
CNPJ: 58.300.812/0001-32
Avenida Paulista, Nº 1337, Bairro Bela Vista, São Paulo-SP. CEP: 01.311-200

TERMOS E DEFINIÇÕES

I. Ameaça: Fonte potencial de dano, incluindo ataques cibernéticos, fraudes, falhas de sistema ou ações maliciosas que visam comprometer a segurança.

II. Ativo de Informação: Qualquer recurso que tenha valor para a Marcha Pay e necessite proteção, incluindo o software/PI, sistemas de pagamentos, dados de clientes e reputação.

III. Colaborador: Qualquer pessoa vinculada à Marcha Pay que tenha acesso a informações ou sistemas no exercício de suas funções.

IV. Confidencialidade: Garantia de que a informação é acessível somente a pessoas com acesso autorizado, protegendo dados sensíveis de clientes e a PI contra divulgação.

V. Disponibilidade: Prevenção contra interrupções na operação dos sistemas de pagamentos, assegurando que os serviços estejam disponíveis de forma contínua.

VI. Evidência Digital: Dados eletrônicos que apoiam a existência ou veracidade de alguma transação ou atividade, mantidos de forma a preservar sua integridade e autenticidade para fins de investigação de incidentes.

VII. Incidente de Segurança: Evento adverso, motivado por violação ou falha de controle, com probabilidade de comprometer a Confidencialidade, Integridade ou Disponibilidade da informação.

VIII. Integridade: Salvaguarda da exatidão e completude da informação transacional e de liquidação, preservando sua originalidade e confiabilidade contra alterações não autorizadas.

IX. Terceiros: Entidades externas que prestem serviços para a Marcha Pay, incluindo parceiros White Label, fornecedores de infraestrutura (Cloud) ou consultores.

X. Vulnerabilidade: Brecha ou deficiência em sistemas ou processos que pode ser explorada por ameaças para comprometer a segurança da informação.

ESTRUTURA DE GOVERNANÇA

A governança da segurança da informação na MarchaPay é estruturada em níveis que asseguram implementação efetiva e gestão adequada dos controles:

I. **Políticas:** Documentos de caráter estratégico que estabelecem os princípios fundamentais e objetivos de segurança. Este documento enquadra-se neste nível, definindo o framework geral de segurança.

II. **Normas:** Documentos de caráter tático que regulamentam o uso específico de recursos tecnológicos e esclarecem responsabilidades detalhadas, orientando o uso seguro de sistemas e processos de pagamento.

III. **Procedimentos:** Documentos de caráter operacional contendo instruções detalhadas sobre execução prática de tarefas, implementação de controles e resposta a situações específicas de segurança.

DIRETRIZES DE SEGURANÇA

Os procedimentos e controles adotados contemplam as seguintes diretrizes fundamentais:

I. Programa de Segurança Cibernética

O programa abrange:

a. **Proteção Integral da PI:** Proteger o código-fonte e algoritmos contra acesso não autorizado ou modificação.

b. **Classificação Adequada:** Classificação dos dados sob critérios de CID, com níveis de proteção proporcionais à sensibilidade.

c. **Aderência ao PCI DSS:** Implementação dos controles de segurança para o ambiente que processa dados de cartão, conforme exigido pelos Adquirentes e IPs parceiras.

d. **Continuidade de Negócios:** Garantir a continuidade do processamento das transações críticas, conforme detalhado na Política de Riscos Operacionais.

e. **Comunicação de Incidentes:** Estabelecer canais efetivos para comunicação imediata de quaisquer descumprimentos ou suspeitas de incidentes.

II. Proteção do Ambiente Tecnológico

a. **Monitoramento Contínuo:** Implementação de sistemas de monitoramento 24/7 para detecção proativa de ameaças, tentativas de intrusão e comportamentos anômalos.

b. **Segurança de Redes:** Administração segura de redes de comunicação, incluindo segmentação adequada e controles de acesso na infraestrutura de Gateway.

c. **Computação em Nuvem:** Gestão segura de serviços de cloud computing, assegurando a conformidade com as diretrizes do BACEN para a contratação de serviços de processamento em nuvem.

III. Gestão de Ativos de Tecnologia da Informação

a. **Inventário de Ativos:** Manutenção de inventário atualizado de todos os ativos, incluindo software proprietário (PI), hardware e dados utilizados nas operações.

b. **Ciclo de Vida:** Gestão do ciclo de vida completo dos ativos, desde a aquisição até o descarte seguro de equipamentos e a destruição segura de dados.

IV. Notificação de Incidentes de Segurança

Todos os colaboradores devem relatar imediatamente à área de Segurança da Informação qualquer suspeita de violação ou intrusão.

a. **Situações Críticas:** Devem ser reportadas perdas de dispositivos, roubo de PI, tentativas de acesso não autorizado, suspeitas de fraude ou qualquer evento que possa comprometer a privacidade de dados de clientes (LGPD).

V. Gestão de Controle de Acesso

Os acessos aos sistemas e informações devem ser rigorosamente controlados e restritos ao princípio do menor privilégio.

a. **Revisão Periódica:** Acessos devem ser revisados periodicamente.

b. **Cancelamento Tempestivo:** Acessos devem ser cancelados imediatamente ao término do contrato de trabalho ou mudança de função (offboarding).

c. **Segregação de Funções:** Implementação de segregação adequada para prevenir fraudes.

VI. Política de Senhas e Autenticação

a. **Autenticação Multifator (MFA/2FA):** Implementação de MFA é mandatória para sistemas críticos, acessos remotos e contas com privilégios de administrador de rede ou sistemas de liquidação.

b. **Requisitos de Senhas:** Senhas devem ser complexas e únicas, com alteração periódica.

c. **Bloqueio Automático:** Configuração de bloqueio automático de sessão por inatividade.

VII. Processamento e Armazenamento de Dados

a. **Criptografia:** Implementação de criptografia adequada para dados em trânsito e em repouso.

b. **Localização de Dados:** Manter controle sobre a localização geográfica de processamento e armazenamento de dados sensíveis.

c. **Retenção e Descarte:** Políticas claras de retenção e descarte seguro de informações transacionais e pessoais, em conformidade com o prazo legal.

VIII. Gestão de Continuidade de Negócios

A Marcha Pay deve implementar planos abrangentes de continuidade de negócios (PCN), documentados, testados e revisados periodicamente, assegurando que seus serviços essenciais sejam mantidos.

a. **Testes Regulares:** Realização de Testes de Estresse nos planos de continuidade para simular cenários adversos.

IX. Programa de Treinamento e Conscientização

A Marcha Pay promove cultura organizacional de segurança através de programas abrangentes de capacitação e conscientização, visando proteger os objetivos estabelecidos nesta política e os dados de clientes.

ATRIBUIÇÕES E RESPONSABILIDADES

I. Diretoria Executiva

a. **Aprovação e Governança:** Aprovar e revisar esta Política e definir o apetite ao risco cibernético.

b. **Recursos e Apoio:** Prover recursos necessários à implementação efetiva da segurança.

II. Área de Segurança da Informação (Assegurada pela TI e Compliance)

a. **Coordenação e Supervisão:** Coordenar e supervisionar a implementação dos procedimentos de segurança.

b. **Gestão de Incidentes:** Receber, analisar criticamente e tomar medidas de resposta a incidentes.

c. **Melhoria Contínua:** Revisar esta política anualmente e garantir conformidade com mudanças regulamentares.

III. Áreas Operacionais

a. **Implementação de Controles:** Administrar a segurança operacional em seus processos e sistemas, garantindo a adesão dos colaboradores às políticas.

IV. Área de Tecnologia da Informação (TI)

a. **Infraestrutura e Sistemas:** Manter atualizada a infraestrutura tecnológica, implantar e manter controles e padrões de segurança, e tratar vulnerabilidades identificadas.

b. **Gestão de Acessos:** Conduzir gestão centralizada dos acessos e implementar MFA em sistemas críticos.

V. Área de Recursos Humanos

a. **Onboarding e Conscientização:** Garantir que novos colaboradores leiam e declarem ciência sobre esta política.

b. **Offboarding:** Coordenar com a TI para desativação tempestiva de acessos e recolher os recursos da instituição.

VI. Áreas Jurídica e de Compliance

a. **Suporte a Investigações:** Apoiar a Segurança da Informação em investigações de incidentes e garantir a aplicação de sanções cabíveis.

b. **Conformidade Regulatória:** Assegurar alinhamento desta política com as regulamentações (BACEN e LGPD).

MONITORAMENTO E AUDITORIA

I. Monitoramento Contínuo

a. **Análise de Logs:** Implementação de sistemas de análise de logs de segurança (SIEM) para detecção proativa de atividades suspeitas em sistemas críticos.

b. **Avaliações Regulares:** Realização de avaliações periódicas de vulnerabilidades e Testes de Penetração (Pentesting) anuais.

II. Auditoria Interna

a. **Programa de Auditoria:** Estabelecimento de programa anual de auditoria interna para verificar o cumprimento desta política e a efetividade dos controles implementados.

b. **Planos de Ação:** Acompanhamento de planos de ação para correção de deficiências identificadas em auditorias.

GESTÃO DE INCIDENTES

I. Classificação de Incidentes: Os incidentes são classificados conforme sua severidade (Crítico, Alto, Médio, Baixo), determinando o nível de resposta e os recursos a serem mobilizados.

a. **Níveis de Severidade**

- Crítico (Nível 1): Incidentes que podem causar interrupção significativa dos serviços de gateway, vazamento de dados sensíveis de clientes ou comprometimento do código-fonte.
- Alto (Nível 2): Tentativas de ataque frustradas, falhas de segurança em sistemas secundários.

b. **Tempos de Resposta**

- Crítico: Resposta imediata (até 15 minutos) e resolução em até 4 horas (conforme criticidade do SPB).

II. Estrutura de Resposta a Incidentes (ERI)

a. A Marcha Pay mantém uma ERI para resposta a incidentes de segurança, composta por Coordenador de Incidentes, Analista de Segurança, Especialista em TI, e Representantes de Compliance e Jurídico.

III. Procedimentos de Resposta

a. **Fase 1: Detecção e Reporte:** Registro de incidentes no sistema de gestão em até 30 minutos.

b. **Fase 3: Contenção e Estabilização:** Implementação de medidas urgentes para impedir a propagação do incidente (ex: isolamento de sistemas).

c. **Fase 4: Erradicação e Recuperação:** Remoção completa da causa raiz e restauração dos sistemas a partir de backups limpos.

IV. Comunicação Durante Incidentes

a. **Comunicação Interna:** Notificação imediata à Alta Administração para incidentes Críticos e Altos.

b. **Comunicação Externa:** Notificação às Autoridades Reguladoras (BACEN/ANPD) e ao parceiro Celcoin, conforme exigências regulamentares, especialmente para incidentes que envolvam vazamento de dados pessoais (LGPD).

CONSIDERAÇÕES FINAIS

A Marcha Pay reserva-se o direito de atualizar e modificar periodicamente esta Política, sempre que necessário para a manutenção da adequada proteção de seus ativos de informação.

I. **Vigência:** Esta política entra em vigor na data de sua aprovação pela Diretoria Executiva.

II. **Atualizações:** Revisões desta política serão realizadas no mínimo anualmente ou sempre que mudanças significativas no ambiente regulatório ou tecnológico assim exigirem.

CANAIS DE COMUNICAÇÃO E DENÚNCIAS

Para reporte de violações ou suspeitas de incidentes de segurança, os colaboradores e terceiros devem utilizar os seguintes canais:

I. Contatos Principais

a. **Segurança da Informação (Emergências Cibernéticas):** [Placeholder para email ou telefone de emergência da Marcha Pay - TI]

b. **Compliance e Ética:** [Placeholder para email de Compliance da Marcha Pay]

c. **Canal de Denúncias:** [Placeholder para Canal de Denúncias da MarchaPay]

II. Garantias de Proteção

a. A Marcha Pay garante: Confidencialidade das informações reportadas, Anonimato quando solicitado pelo denunciante e Não retaliação a denunciantes que estiverem agindo de boa-fé.