Política de Segurança da Informação - Resumo

Versão 7.0

Confidencialidade do Documento: **PÚBLICA**
Sem restrição de divulgação.

ÍNDICE

Confidencialidade do Documento: **PÚBLICA**
Divulgação livre ao público.

1. Introdução

1.1. Objetivo

No Grupo 2TM, a segurança da informação e a segurança cibernética são pilares fundamentais, visando garantir os mais elevados padrões de controle e gestão de riscos. Nossa Política estabelece as diretrizes para proteger todas as informações armazenadas, processadas e transmitidas em nossos ambientes, tanto físicos quanto virtuais. Nosso compromisso é:

- Preservar a confidencialidade, integridade, disponibilidade, sigilo e autenticidade de nossas informações.
- Orientar sobre o uso adequado de nossos ativos e proteger as atividades e a gestão do Grupo 2TM.
- Estabelecer medidas técnicas e administrativas robustas para proteger as informações, incluindo dados pessoais, contra acessos não autorizados e situações acidentais ou ilícitas, como destruição, perda, alteração, comunicação ou vazamento. Essas medidas são dimensionadas de acordo com a sensibilidade das informações, como dados de clientes e dados pessoais sensíveis, em conformidade com as exigências legais, regulatórias e de negócio.
- Nortear a definição de procedimentos específicos de controles e processos para a gestão dos riscos de segurança da informação.

A elaboração desta política considera o porte, o perfil de risco e o modelo de negócio da 2TM, bem como as legislações, diretrizes e melhores práticas aplicáveis.

Confidencialidade do Documento: **PÚBLICA**
Divulgação livre ao público.

1.2. Princípios

A gestão da segurança da informação no Grupo 2TM é norteada pelos seguintes princípios, que refletem nossos valores e compromissos para proteger nossos ativos de informação, garantir a continuidade dos negócios, a conformidade legal e a confiança de todos os envolvidos.

- **Confidencialidade:** as informações devem ser acessíveis somente a pessoas autorizadas.
- **Integridade:** as informações devem ser precisas e completas, protegidas contra alterações não autorizadas.
- **Disponibilidade:** as informações e sistemas devem estar disponíveis quando necessário para apoiar as operações do negócio.
- **Responsabilidade:** todos os colaboradores e terceiros devem assumir responsabilidade por proteger as informações sob seu controle.
- **Compliance:** cumprimento das leis, regulamentos e políticas internas aplicáveis.
- **Melhoria Contínua:** revisão e aprimoramento constante dos processos de segurança.
- **Minimização de Riscos:** identificação, avaliação e mitigação dos riscos à segurança da informação.
- **Transparência:** comunicação clara e aberta sobre políticas, responsabilidades e incidentes de segurança.

1.3 Escopo e Aplicabilidade

Esta Política aplica-se à proteção das informações do Grupo 2TM, bem como das informações de seus clientes, colaboradores, parceiros e demais partes interessadas, assegurando a confidencialidade, integridade e disponibilidade (CID) de todos os ativos de informação sob nossa responsabilidade. O escopo abrange todos os tipos de informações, eletrônicas, físicas e verbais, que são armazenadas, processadas ou transmitidas em nossos ambientes corporativos, incluindo sistemas internos, soluções em nuvem e dispositivos móveis.

Todas as menções à "2TM" devem ser entendidas como menção a todas as empresas que compõem o Grupo 2TM.

Confidencialidade do Documento: **PÚBLICA**
Divulgação livre ao público.

2. Conceitos

- **Segurança da Informação:** preservação da confidencialidade, integridade e disponibilidade da informação, protegendo-a de diversos tipos de ameaças, para garantir a continuidade de negócios, minimizar perdas e danos e maximizar o retorno dos investimentos e as oportunidades de negócio.

- **Informação:** Ativo que tem valor para a 2TM e necessita ser adequadamente protegido. Ela pode estar impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou através de meios eletrônicos, mostrada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, deve ser sempre protegida adequadamente.

- **Incidente (de segurança)** - segundo o NIST (National Institute of Standards and Technology, do português, Instituto Nacional de Padrões e Tecnologia), é uma violação ou uma ameaça iminente de violação das políticas de segurança, políticas de usos aceitáveis ou boas práticas de segurança praticadas no mercado, conforme exemplos, mas não exclusivamente, abaixo:

    - Colaboradores que compartilham arquivos corporativos com dados pessoais ou com pessoas não autorizadas, causando violações de dados e quebra de confidencialidade;

    - Um ataque externo que consiga infectar uma máquina e capturar informações confidenciais corporativas;

    - Interrupção de algum serviço após um ataque.

- **Ativos:** são todos os elementos que detém algum tipo de valor para a 2TM. Os ativos podem ser informações, documentos, hardwares (equipamentos), softwares (sistemas) e Colaboradores.

- **Dados pessoais:** informações relacionadas a uma pessoa natural identificada ou que podem levar à sua identificação (ex.: número de telefone, e-mail, CPF, data de nascimento, identificadores eletrônicos, GPS, redes WiFi, IDs de utilização de aplicações).

- **Dados pessoais sensíveis:** Dados pessoais referentes à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a 2TM de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Confidencialidade do Documento: **PÚBLICA**
Divulgação livre ao público.

- **Endpoint:** qualquer dispositivo que se conecta à rede da 2TM e que pode ser usado para acessar seus sistemas ou dados. Isso inclui computadores (desktops e notebooks), smartphones, tablets, servidores locais, dispositivos IoT, e outros equipamentos com capacidade de comunicação em rede.
- **Fornecedor:** pessoa física ou jurídica contratada para prestar serviços ou fornecer produtos à 2TM.
- **Gerenciamento de Risco de Segurança:** processo de identificação, controle e minimização ou eliminação dos riscos de segurança que podem afetar os sistemas de informação, a um custo razoável.
- **Terceiro:** indivíduo ou empresa contratada para executar atividades específicas, incluindo trabalhadores contratados como pessoa jurídica (PJ) que executam funções similares a colaboradores internos.

3. Compromisso e Responsabilidades

Todos os envolvidos com o Grupo 2TM, colaboradores, terceiros contratados, parceiros e fornecedores, são responsáveis pela proteção dos ativos tecnológicos e das informações às quais têm acesso e, por isso, precisam estar adequados. Este compromisso inclui a preservação dos ambientes físicos e tecnológicos, respeitando integralmente as diretrizes e os controles de segurança implementados.

O Grupo 2TM possui uma governança robusta, com áreas e equipes dedicadas à segurança da informação, que trabalham para assegurar a divulgação e o cumprimento desta Política, avaliar riscos, gerir projetos de segurança, e desenvolver programas contínuos de conscientização

4 . Diretrizes de Segurança da Informação

O Grupo 2TM implementou uma série de diretrizes para proteger suas informações e a privacidade dos dados pessoais.

- **Gestão de Riscos:** avaliamos e monitoramos continuamente os riscos de segurança e privacidade, considerando ameaças, vulnerabilidades, probabilidade e impacto nos ativos de informação e dados pessoais.
- **Classificação e Tratamento da Informação:** todas as informações são classificadas por grau de sigilo, e as informações contendo dados pessoais e dados pessoais sensíveis são obrigatoriamente classificadas com o mais alto grau de sigilo para garantir sua proteção.

Confidencialidade do Documento: **PÚBLICA**
Divulgação livre ao público.

- **Gestão de Acessos:** mantemos controles rigorosos de acesso físico e lógico, garantindo que usuários, sistemas e dispositivos tenham acesso apenas ao estritamente necessário para suas funções, com base nos princípios de necessidade de saber e menor privilégio. A autenticação multifator (MFA) ou Single Sign-On (SSO) é obrigatória para acessos a sistemas críticos e não críticos e a ambientes sensíveis.

- **Monitoramento de Atividades:** monitoramos continuamente, registramos e analisamos o acesso e a utilização de nossos ambientes e recursos tecnológicos para fins de auditoria, resposta a incidentes e cumprimento legal.

- **Disponibilidade de Serviços de TI:** garantimos a continuidade dos serviços de tecnologia da informação por meio de monitoramento contínuo, mecanismos de redundância planejados e testados, e planos de gestão de capacidade.

- **Gestão de Incidentes:** todos os colaboradores, terceiros contratados e fornecedores são obrigados a reportar imediatamente quaisquer incidentes de segurança. Mantemos processos documentados e formalizados para a gestão de incidentes, incluindo aqueles envolvendo dados pessoais, com um Time de Resposta a Incidentes (CSIRT) para avaliação e tratamento eficaz, bem como planos de comunicação com autoridades e clientes.

- **Gestão de Continuidade de Negócio:** realizamos análises de impacto no negócio (BIA) e mantemos Planos de Continuidade de Negócios (PCN), Planos de Recuperação de Desastre, Plano de Continuidade Operacional e Planos de Gestão de Crises, que são testados e revisados de forma recorrente para assegurar a resiliência operacional.

- **Treinamento e Conscientização:** dispomos de um programa formal e contínuo de treinamento e conscientização em Segurança da Informação para todos os colaboradores e terceiros contratados, promovendo uma cultura de proteção e prevenção de incidentes.

- **Mesa Limpa e Tela Limpa:** adotamos e exigimos práticas para proteger informações físicas e digitais em todos os ambientes de trabalho, incluindo o bloqueio automático de telas após inatividade e a guarda segura de documentos.

- **Segurança de Redes:** garantimos a segurança, integridade, disponibilidade e confidencialidade de nossas redes por meio de segregação lógica, criptografia robusta de dados em trânsito e em repouso e monitoramento contínuo para detecção de atividades suspeitas.

Confidencialidade do Documento: **PÚBLICA**
Divulgação livre ao público.

- **Uso de Endpoints e Ativos de Usuários:** dispositivos corporativos são protegidos com criptografia, antivírus e monitoramento contínuo. O uso de dispositivos pessoais para atividades corporativas é proibido.

- **Contratação e Gestão de Fornecedores e Terceiros:** todos os fornecedores e terceiros, especialmente os de tecnologia da informação e serviços em nuvem, passam por rigorosas avaliações de segurança e privacidade para ser identificado a maturidade de segurança da informação e privacidade. Essa análise ocorre antes da contratação e durante o período contratado de forma recorrente. Os contratos incluem cláusulas específicas sobre segurança da informação, privacidade de dados, propriedade intelectual, entre outras, e há um monitoramento contínuo da conformidade com a segurança da informação e privacidade.

- **Privacidade de Dados Pessoais:** o Grupo 2TM tem um compromisso firme com a privacidade dos dados pessoais, em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) e o Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR). Coletamos e tratamos apenas os dados estritamente necessários, mantemos a Política de Privacidade e de Proteção de Dados Pessoais e a Política de Tratamento de Dados Fornecedores_Parceiros específicas e contamos com um Encarregado pelo Tratamento de Dados Pessoais (DPO) formalmente designado. Nossos processos incluem o mapeamento do ciclo de vida dos dados (ROPA), a realização de Relatórios de Impacto à Proteção de Dados (RIPD/DPIA) quando necessário e implementação de medidas técnicas de segurança e privacidade, incluindo criptografia, mascaramento de dados, anonimização, pseudonimização e o descarte seguro dos dados..

- **Proteção Contra Malware:** utilizamos softwares de detecção e remoção de malware atualizados e eficazes em todos os ativos tecnológicos, com varreduras contínuas e planos documentados de resposta e recuperação a ataques.

- **Gestão de Vulnerabilidades Técnicas:** adotamos uma abordagem integrada para identificar, avaliar e corrigir vulnerabilidades através de scanners automatizados, testes de intrusão (pentests) e inteligência de ameaças.

    - **Canal Público de Reporte de Vulnerabilidades:**

Com o compromisso de garantir a segurança das informações e promover a transparência, o grupo 2TM disponibiliza um canal público exclusivo para o reporte de vulnerabilidades e problemas de segurança. Este canal é destinado a pesquisadores, parceiros, fornecedores e demais partes interessadas que desejem comunicar eventuais falhas ou riscos identificados

Confidencialidade do Documento: **PÚBLICA**
Divulgação livre ao público.

em nossos serviços. Solicitamos que as informações sejam enviadas de forma detalhada para facilitar a análise interna do problema reportado. O grupo 2TM assegura o tratamento confidencial das informações recebidas e o devido retorno sobre as ações tomadas.

Para reportar vulnerabilidades, favor utilizar o seguinte canal: security@mb.com.br

- **Desenvolvimento Seguro de Softwares:** nosso ciclo de vida de desenvolvimento de software segue princípios e práticas formais de segurança, incorporando "Security by Design" e "Privacy by Design" desde a concepção dos sistemas, com segregação de ambientes e testes de segurança antes da liberação.

- **Gestão de Backups e Restauração:** mantemos cópias de backup de informações que são regularmente testadas e armazenadas de forma segura em locais distintos e redundantes para assegurar sua eficácia e integridade.

6. Recomendações de Segurança para Clientes

A 2TM possui ações de conscientização de Segurança disponíveis publicamente para clientes e que são transmitidas através de posts nas redes sociais oficiais, *push* de e-mail ou através do site.

- https://www.mercadobitcoin.com.br/dicas-de-seguranca
- https://www.mercadobitcoin.com.br/seguranca

As ações de conscientização tem como objetivo ensinar boas práticas básicas de Segurança da Informação e alertar sobre novos tipos de golpes, de forma que nossos clientes possam ter ações preventivas em seus dispositivos pessoais e credenciais antes de acessar a nossa plataforma.

7. Canais de Comunicação

Canais de Segurança da Informação

A 2TM possui dois canais dedicados à Segurança da Informação, utilizados internamente pelos colaboradores e também abertos ao público. São eles:

security@mb.com.br - Canal público para receber denúncias sobre problemas de segurança na estrutura, sistemas e ambiente da 2TM.

abuse@mb.com.br - Canal público para receber denúncias de fraudes eletrônicas envolvendo, citando ou tentando se passar por qualquer empresa da 2TM.

Confidencialidade do Documento: PÚBLICA
Divulgação livre ao público.

Canal de Denúncias

A 2TM mantém um canal de denúncias seguro, acessível e confidencial, disponível para colaboradores, terceiros, parceiros e demais partes interessadas, com o objetivo de receber relatos sobre condutas suspeitas, violações à Política de Segurança da Informação, fraudes, uso indevido de informações, ou quaisquer comportamentos que possam comprometer a integridade, confidencialidade ou disponibilidade das informações da organização.

O canal de denúncia pode ser acessado pelo site:
https://www.mercadobitcoin.com.br/compliance

8. Conformidade e Auditoria

O Grupo 2TM realiza auditorias e verificações periódicas para assegurar a conformidade com as políticas de segurança da informação, privacidade e compliance regulatório. Os resultados são utilizados para fortalecer controles e promover a melhoria contínua.

9. Disposições Finais

Esta Política entra em vigor a partir da data de sua publicação e deve ser revisada anualmente.

10. Controle de Versões

Data de revisão	Versão	Alterações	Aprovador (es)
30/03/2026	7.0	Item 5 revisado com ajustes e inclusão de novas diretrizes; item 7 atualizado com a inserção do canal de denúncias.	Comitê de Diretoria

Confidencialidade do Documento: **PÚBLICA**
Divulgação livre ao público.