Política de Segurança da Informação ↗

Versão 6.0

Mercado Bitcoin

ÍNDICE

Introdução

Objetivo

Esta Política estabelece as diretrizes e responsabilidades a serem observadas pela 2TM Participações S.A. e suas empresas controladas (“Grupo 2TM”), relacionadas a segurança da informação e segurança cibernética, visando garantir os mais elevados padrões de controle e gestão de riscos de segurança e de governança no tratamento de informações armazenadas, processadas e transmitidas nos ambientes físico e virtual do grupo 2TM, provendo orientação e apoio de acordo com os requisitos do negócio e com as leis e regulamentações relevantes, de modo a:

(i) preservar a confidencialidade, disponibilidade, integridade, sigilo e autenticidade das suas informações;
(ii) orientar quanto ao uso adequado de seus ativos e proteger as atividades finalísticas e a gestão da 2TM;
(iii) estabelecer medidas técnicas e administrativas capazes de proteger as informações, inclusive dados pessoais, contra acessos não autorizados e de situações acidentais ou ilícitas envolvendo a destruição, perda, alteração, comunicação ou vazamento de informação; e
(iv) nortear a definição de procedimentos específicos de controles e processos para a gestão dos riscos de segurança da informação. Levou-se em conta na elaboração desta política o porte, o perfil de risco e o modelo de negócio da 2TM, assim como as legislações, as diretrizes e as melhores práticas aplicáveis.

Aplicabilidade

Todos os administradores (incluindo diretores executivos), membros do Conselho de Administração e membros dos Comitês e/ou Comissões de Assessoramento ao Conselho de Administração, sócios, funcionários, estagiários da 2TM (todos, em conjunto, os “Colaboradores”), bem como a todos os terceiros que com ele se relacionem. Todas as menções à "2TM" devem ser entendidas como menção a todas as empresas que compõem o Grupo 2TM.

Diretrizes

1.1. Acompanhamento de maturidade de Segurança: Devem ser definidas métricas e indicadores a fim de controlar, auditar e aumentar o nível de maturidade e conformidade da 2TM em segurança da informação.

1.2. Comprometimento: todos os Colaboradores da 2TM, em qualquer vínculo, função ou nível hierárquico, são responsáveis pela proteção e guarda dos Ativos tecnológicos e informações das quais são usuários, dos ambientes físicos e tecnológicos que possuam, respeitando as Políticas e controle implantados.

1.3. Gestão de Riscos de Segurança: a área de Segurança da Informação deve apoiar com recomendações de controles e proteções de segurança cibernética o desenvolvimento de novos produtos e serviços da 2TM, bem como a avaliação de riscos, buscando identificar ameaças e impactos sobre os ativos de informação.

Os riscos devem ser avaliados e administrados conforme requisitos especificados em normas e nos controles de proteção. Todos os processos, produtos e serviços desenvolvidos, que possam comprometer a segurança da informação, devem ser submetidos a processo de avaliação e tratamento de riscos antes que sejam adquiridos, implementados e disponibilizados para garantir o grau de segurança adequado para a 2TM.

1.4. Gestão de Continuidade de Negócio: a 2TM deve implementar planos de continuidade dos negócios documentados, testados e revisados periodicamente, de forma que seus serviços essenciais e relevantes sejam devidamente identificados, contemplando os mecanismos de Segurança da Informação estabelecidos nos ambientes de produção.

1.5. Classificação e Tratamento da Informação: todas as informações e os respectivos recursos tecnológicos que as suportam devem ser classificados de acordo com grau de sigilo e receber o tratamento que garanta a proteção durante todo o ciclo de vida.

1.6. Gestão de Acessos: o acesso ao ambiente da 2TM deve ser controlado, registrado, monitorado e auditável, com base nos princípios da necessidade de conhecer o mínimo privilégio para o desempenho das atividades profissionais para garantir que as informações não sejam divulgadas, modificadas, excluídas ou tornadas indisponíveis indevidamente.

Na ocasião do término do contrato de um Colaborador, assegurar que os recursos disponibilizados sejam devidamente recolhidos bem como garantir que os acessos sejam desativados no prazo definido em procedimento de gestão de acessos.

1.7. Gestão de Incidentes: todos os Colaboradores da 2TM, em qualquer vínculo, função ou nível hierárquico, têm a obrigação de reportar imediatamente quaisquer Incidentes de segurança de que tomem conhecimento, de modo que possam ser registrados, avaliados e tratados pelo Time de Resposta a Incidentes (CSIRT) de acordo com o Plano de Resposta a Incidentes(PRI).

1.8. Auditoria e Conformidade: a 2TM reserva-se o direito de auditar periodicamente a prática de segurança da informação e comunicações, de forma a avaliar a conformidade das ações de seus Colaboradores em relação ao estabelecido pela Política de Segurança da Informação e Comunicações da Empresa e pela legislação aplicável.

1.9. Monitoramento: a 2TM reserva-se o direito de monitorar o acesso e utilização de recursos em seus ambientes físicos, assim como dos recursos corporativos disponibilizados aos Colaboradores de forma que ações

indesejáveis ou não autorizadas sejam detectadas proativamente e posteriormente tratadas.

1.10. Treinamento e Conscientização: um programa de conscientização, avaliação, educação e treinamento em Segurança da Informação, com o objetivo de disseminar a cultura de segurança da informação na 2TM e avaliar o nível de maturidade e conhecimento dos Colaboradores em relação aos temas ministrados, é essencial para garantir os objetivos desta Política.

1.11. Desenvolvimento Seguro: todo o ciclo de vida do desenvolvimento dos softwares da 2TM deve seguir as melhores práticas de desenvolvimento a fim de produzir softwares seguros, buscando mitigar o surgimento de vulnerabilidades de segurança.

1.12. Segurança de Redes: todos os colaboradores da 2TM devem acessar os recursos e sistemas utilizando redes privadas com autenticação. A comunicação via rede dos recursos corporativos são monitorados e podem sofrer bloqueios de ameaças via ferramentas de monitoramento.

1.13. Trabalho remoto: as diretrizes de atuação neste modelo devem ser seguidas de acordo com as orientações descritas no documento de apoio corporativo publicado na Intranet.

Recomendações de Segurança para Clientes

O MB 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 Guia de Segurança (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.

Canais de Comunicação de Segurança

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 do MB.

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