POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

Estabelecer as diretrizes e responsabilidades adotadas pela 2TM Participações S.A. (“2TM”) e suas empresas controladas (“Grupo 2TM”) assegurando os mais elevados padrões de segurança, controle e gestão de riscos e de governança no tratamento de informações armazenadas, processadas e transmitidas nos ambientes físico e virtual da 2TM.

A presente Política provê 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 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.

2. ABRANGÊNCIA

A presente Política é aplicável a todos os colaboradores, consultores, incluindo aqueles de entidades externas ou outras entidades e/ou pessoas que acedam aos sistemas e tecnologias de informação e comunicações da 2TM. Meubank Pagamentos Ltda, como parte do Grupo 2TM (https://www.2tmgroup.com/), se aplica às condições aqui descritas.
É assegurado a todos que tenham conhecimento desta política 0 acesso adequado à informação necessária para o desempenho das suas funções, sendo exigido destes o respeito pelos controles de segurança implementados e o cumprimento dos aspectos de integridade, confidencialidade e disponibilidade da informação, sendo estes, responsabilidade de todos.

É de propriedade da 2TM toda a informação gerada ou tramitada por meio dos seus recursos.

As informações poderão envolver também dados pessoais, ocasião em que deverão ser observadas, além das diretrizes aqui presentes, a Política Interna sobre Tratamento de Dados Pessoais e a legislação aplicável à proteção de dados pessoais, incluindo a LGPD.

3. DIRETRIZES

Para fins desta Política ficam estabelecidas as seguintes diretrizes gerais:

3.1. A Segurança da Informação da 2TM deve ser apoiada por um Sistema de Gestão da Segurança da Informação e Comunicações (SGSI).

3.2. Comprometimento: Todos os colaboradores, consultores e prestadores de serviço da 2TM, em qualquer vínculo, função ou nível hierárquico, são responsáveis pela proteção e guarda dos ativos tecnológicos e informações dais quais são usuários, dos ambientes físicos e tecnológicos que possuam, respeitando as Políticas e controle implantados.

3.3. Gestão de Riscos: A área de Segurança da Informação deve apoiar com recomendações de controles e proteções de segurança cibernética na avaliação de riscos, buscando identificar ameaças e impactos sobre os ativos de informação.

3.4. 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.

3.5. 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.

3.6. Política de Mesa Limpa e Tela Limpa: Todos os colaboradores da 2TM, em qualquer vínculo, função ou nível hierárquico devem seguir boas práticas de Segurança da Informação com relação à proteção de informações e seu nível de classificação, tanto em formato digital quanto físico.

3.7. Gestão de Acessos: O acesso aos ambientes físicos e lógicos 2TM deve ser controlado, registrado e monitorado, com base nos princípios da necessidade de conhecer e do privilégio mínimo para o desempenho das atividades profissionais

3.8. Gestão de Incidentes: Todos os colaboradores, consultores e prestadores de serviço da 2TM, em qualquer vínculo, função ou nível hierárquico da 2TM têm a obrigação de reportar imediatamente quaisquer incidentes de segurança que tomaram conhecimento, de modo que possam ser registrados, avaliados e tratados conforme procedimento de gestão de incidentes.

3.9. 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, consultores e prestadores de serviço em relação ao estabelecido nesta Política e na legislação aplicável.

3.10. 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.

3.11. Gestão de exceções/procedimentos de escalação: Os procedimentos de gestão de exceções reconhecem que os conflitos de Políticas são naturais e que a Empresa tem maturidade suficiente para poder geri-los. Os gestores das áreas deverão ser consultados sobre os casos omissos para que sejam estabelecidos novos procedimentos para adequar as exceções.

3.12. Desenvolvimento Seguro: Todo desenvolvimento ou manutenção de software devem ser formalmente autorizados e deve ser realizada uma análise de riscos e impacto. Alterações de escopo de desenvolvimento ou manutenção de software deve ser documentada e formalmente autorizada.

3.13. Segurança de Redes: Toda a comunicação do grupo 2TM com a Internet ou qualquer outra rede pública deve necessariamente passar por um sistema de controle de acesso de conexões, configurado com política restritiva, com monitoramento bidirecional dos fluxos de comunicação e com proteção contra-ataques, tais como negação de serviço, entre outros.

3.14. Gerenciamento de chaves criptográficas: o uso efetivo e adequado de um sistema de criptografia deve ser estabelecido com o intuito de assegurar a confidencialidade, autenticidade e integridade das informações sensíveis.

3.15. Contratação de serviços terceirizados: deve-se assegurar que a parte contratada, e eventual(is) subcontratada(s) e/ou subordinada(s) cumpram os requisitos mínimos de governança cibernética no âmbito do gerenciamento de risco operacional. Estes objetivos deverão nortear ações que serão implementadas pela contratada em etapas antes, durante e após a contratação com detalhamento em procedimento específico.

3.16. Em proteção à Privacidade, somente dados necessários conforme finalidade ou legalmente exigidos para desempenho eficaz da Empresa e cumprimento de obrigações legais são solicitados e retidos ou divulgados em atendimento à legislação específica.

3.17. A 2TM se reserva o direito de monitorar o uso de computadores, telefones fixos, smartphones, tablets, celulares, rádios e outros equipamentos disponibilizados e atividades de rede, incluindo, mas não se limitando a e-mail, correio de voz, uso da Internet e qualquer informação armazenada nestes equipamentos, sistemas ou servidores, em circunstâncias apropriadas e com vista à proteção das informações e da segurança do tráfego de informação e conteúdo.

4. TERMOS E DEFINIÇÕES

Ativos: são todos os elementos que detém algum tipo de valor para o grupo 2TM. Os ativos podem ser informações, hardwares (equipamentos), softwares (sistemas) e colaboradores.

Dados pessoais: informações relacionadas diretamente a uma pessoa física identificada (ex.: número de telefone, e-mail, CPF, data de nascimento, identificadores eletrônicos), ou

que podem levar à identificação de uma pessoa (ex.: GPS, redes WiFi, IDs de utilização de aplicações).

Incidente (de segurança): Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores. São exemplos de incidentes de segurança:

- tentativas de ganhar acesso não autorizado a sistemas ou dados;

- ataques de negação de serviço;

- uso ou acesso não autorizado a um sistema;

- modificações em um sistema, sem o conhecimento, instruções ou consentimento prévio do dono do sistema;

- desrespeito à política de segurança ou à política de uso aceitável de uma empresa ou provedor de acesso..

Informação: É um ativo que tem valor para a organização 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, é recomendado que ela seja sempre protegida adequadamente.

LGPD: Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais, que regula o tratamento de Dados Pessoais no Brasil, em meios físicos ou digitais.

Gerenciamento de Risco: processo de identificação, controle e minimização ou eliminação dos riscos de segurança que podem afetar os sistemas de informação, a um custo aceitável.

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.

5. CANAIS DE COMUNICAÇÃO

- Suspeitas de incidentes de segurança da informação? soc@meubank.com
- Recebeu algum e-mail em nome do MeuBank e achou suspeito? Encaminhe para abuse@meubank.com