POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

M7 IB SOLUÇÕES FINANCEIRAS LTDA.

CNPJ 60.391.854/0001-78

1. OBJETIVO

A presente "*Política de Segurança da Informação Cibernética*" ("Política"), elaborada em conformidade com o disposto na Resolução nº 161, da Comissão de Valores Mobiliários ("CVM"), de 13 de julho de 2022 ("Resolução CVM 161"), tem por objetivo estabelecer princípios, conceitos e valores que orientam a conduta de todos aqueles que possuam cargo, função, posição, relação societária, empregatícia, comercial, profissional, contratual ou de confiança com a **M7 IB SOLUÇÕES FINANCEIRAS LTDA.**, inscrita no Cadastro Nacional da Pessoa Jurídica do Ministério da Fazenda ("CNPJ") sob o n.º60.391.854/0001-78 ("M7 IB"), tais como os sócios, diretores, empregados, ou prestadores de serviço independentemente da natureza destas atividades, sejam elas direta, indireta e/ou secundariamente relacionadas com quaisquer atividades fim ou meio ("Colaboradores"), tanto na sua atuação interna quanto na comunicação com os diversos públicos.

Os Colaboradores deverão observar os padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio, de proteção legal da M7 IB e do indivíduo, de modo a minimizar ameaças no âmbito das atividades desempenhadas.

A Política de segurança da informação tem por finalidade definir os requisitos, processos e controles no que diz respeito à proteção dos dados da M7 IB, de forma a garantir a confidencialidade e integridade de tais dados.

A Política define detalhadamente todas as regras a serem seguidas, medidas de prevenção e risco, mapeamento de vulnerabilidades, controle de acessos. Adicionalmente, o Diretor de Compliance, em conjunto a área de tecnologia, realizará verificações periódicas de segurança para os sistemas de informação, a fim de:

i. minimizar preventivamente eventuais riscos operacionais e de descumprimento do disposto no Código ANBIMA, na Resolução CVM 161 e nesta Política; e

ii. garantir que a estrutura tecnológica conte com proteção a tentativas de ataques cibernéticos.

1. IDENTIFICAÇÃO DE RISCOS (*RISK ASSESSMENT*)

Para o exercício de suas atividades, a M7 IB identificou os seguintes principais riscos internos e externos aos quais estaria sujeita:

i. Dados e Informações: Informações Confidenciais, incluindo informações a respeito de investidores, clientes, Colaboradores e da própria M7 IB, operações e valores mobiliários distribuídos sob sua intermediação, e as comunicações internas e externas (e.g. e-mails e correspondências).

ii. Sistemas: Informações sobre sistemas utilizados pela M7 IB e tecnologias desenvolvidas internamente ou por terceiros, suas possíveis ameaças e vulnerabilidades.

iii. Processos e Controles: Processos e controles internos que sejam parte das rotinas da M7 IB.

iv. Governança e Gestão de Risco: A eficácia da gestão de riscos pela M7 IB quanto às ameaças e planos de ação, de contingência e continuidade de negócios.

Especificamente com relação à segurança cibernética, em linha com o disposto no Guia de Cibersegurança da ANBIMA:

i. Malware: *softwares* desenvolvidos para corromper computadores e redes (e.g. vírus, cavalos de troia, *spyware*, *ransomware*);

ii. Engenharia social: métodos de manipulação para obter informações confidenciais (*pharming*, *pishing*, *vishing*, *smishing* e acesso pessoal);

iii. Ataque de DDoS (*distributed denial of services*) e *botnets*: ataques visando negar ou atrasar acesso aos serviços ou sistemas da instituição;

iv. Invasões (*advanced persistente threats*): ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades especificas em um ambiente tecnológico.

1.1. AÇÕES DE PREVENÇÃO E PROTEÇÃO

As medidas de segurança da informação têm por finalidade minimizar as ameaças aos negócios da M7 IB e às disposições desta Política.

A coordenação direta das atividades relacionadas a esta Política ficará a cargo do Diretor de Compliance, que também é responsável por sua revisão, realização de testes e treinamento dos Colaboradores, conforme aqui descrito.

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da M7 IB e circulem em ambientes externos à M7 IB com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas como informações confidenciais. Qualquer exceção à presente regra deverá ser previamente autorizada por escrito por qualquer dos membros do Comitê de Compliance.

A proibição acima referida não se aplica quando as cópias (físicas ou eletrônicas) ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da M7 IB. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

Em consonância com as normas internas acima, os Colaboradores devem se abster de utilizar pen-drives, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na M7 IB.

A utilização dos ativos e sistemas da M7 IB, incluindo computadores, telefones, *internet*, *e-mail* e demais aparelhos se destina prioritariamente a fins profissionais. O uso indiscriminado deles para fins pessoais deve ser evitado e nunca deve ser prioridade em relação a qualquer utilização profissional.

O envio ou repasse por *e-mail* de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem e afetar a reputação da M7 IB.

O recebimento de *e-mails* muitas vezes não depende do próprio Colaborador, mas espera-se bom senso de todos para, se possível, evitar receber mensagens com as características descritas previamente. Na eventualidade do recebimento de mensagens com as características acima descritas, o Colaborador deve apagá-las imediatamente, de modo que estas permaneçam o menor tempo possível nos servidores e computadores da M7 IB.

A visualização de *sites*, *blogs*, *fotoblogs*, *webmails*, entre outros, que contenham conteúdo discriminatório, preconceituoso (sobre origem, etnia, religião, classe social, opinião política, idade,

gênero, orientação sexual ou deficiência física), obsceno, pornográfico ou ofensivo é terminantemente proibida.

A senha e *login* para acesso aos dados contidos em todos os computadores, bem como nos e-mails que também possam ser acessados via webmail, devem ser conhecidas pelo respectivo usuário do computador e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros.

Para segurança dos perfis de acesso dos Colaboradores, as senhas de acesso dos Colaboradores são parametrizadas conforme as regras determinadas pelo Departamento de Compliance, para implementação nos perfis de acesso dos Colaboradores.

Dessa forma, o Colaborador pode ser responsabilizado inclusive caso disponibilize a terceiros a senha e login acima referidos, para quaisquer fins.

Cada Colaborador é responsável ainda por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

Todo Colaborador deve ser cuidadoso na utilização do seu próprio equipamento e sistemas e zelar pela boa utilização dos demais.

Caso algum Colaborador identifique má conservação, uso indevido ou inadequado de qualquer ativo ou sistemas deve comunicar o fato a qualquer dos membros do Departamento de Compliance.

1.2. ACESSO ESCALONADO AOS SISTEMAS

O acesso como "administrador" de área de *desktop* será limitado aos usuários aprovados pelo Diretor de Compliance, que determinará os privilégios e níveis de acesso de usuários a determinados Colaboradores.

A M7 IB mantém diferentes níveis de acesso a pastas e arquivos eletrônicos, notadamente os que contenham Informações Confidenciais, de acordo com suas funções e responsabilidades, podendo monitorar o acesso dos Colaboradores a referidas pastas e documentos.

1.3. SENHA E *LOGIN*

A senha e login para acesso a dados nos computadores da M7 IB, bem como e-mails acessados remotamente, que devem ser conhecidas pelo respectivo usuário e são pessoais e intransferíveis, devendo ser mantidas em sigilo pelos Colaboradores.

Para a segurança dos perfis de acesso, as senhas de acesso são parametrizadas conforme regras determinadas pelo Comitê de Risco e Compliance, para implementação nos perfis de acesso dos Colaboradores, sendo certo que deverão ser alteradas a cada 6 (seis) meses.

1.4. USO DE EQUIPAMENTOS E SISTEMAS

Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos sob sua responsabilidade.

Os ativos e sistemas da M7 IB, incluindo computadores, telefones, *internet, e-mail* e demais aparelhos se destinam apenas para fins profissionais. O uso indiscriminado destes para fins pessoais deve ser evitado e nunca deve ser prioridade em relação ao uso profissional.

Todo Colaborador deve ser cuidadoso na utilização do seu equipamento e sistemas, bem como zelar pela boa utilização dos demais. Caso algum Colaborador identifique má conservação ou uso indevido ou inadequado de qualquer ativo ou sistema deverá comunicar ao Diretor de Compliance.

1.5. ACESSO REMOTO

A M7 IB permite acesso remoto pelos Colaboradores, desde que o acesso seja sempre feito mediante senha para acesso aos e-mails e arquivos.

Os Colaboradores são instruídos a manter *softwares* de proteção contra *malwares*/vírus nos dispositivos remotos e relatar ao Diretor de Compliance qualquer violação ou ameaça de segurança cibernética, ou outro incidente que possa afetar informações da M7 IB em ambiente remoto. Informações confidenciais não poderão ser armazenadas em dispositivos pessoais.

1.6. MONITORAMENTO E CONTROLE DE ACESSO

O acesso pelos Colaboradores nas dependências da M7 IB é realizado por meio de crachá de acesso ou chave, pessoal e intransferível, o qual é disponibilizado a cada Colaborador no momento de sua contratação pela M7 IB.

O acesso à rede de informações eletrônicas conta com a utilização de servidores exclusivos da M7 IB, que não poderão ser compartilhados com outras empresas responsáveis por diferentes atividades no mercado financeiro e de capitais.

Tendo em vista que a utilização de computadores, internet, e-mail e demais aparelhos se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos Colaboradores, a M7 IB monitora a utilização de tais meios.

Neste sentido, a M7 IB:

i. mantém diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções dos Colaboradores e pode monitorar o acesso dos Colaboradores a tais pastas e arquivos com base na senha e *login* disponibilizados;

ii. pode monitorar o acesso dos Colaboradores a sites, *blogs, fotoblogs, webmails*, entre outros, bem como os e-mails enviados e recebidos;

iii. pode monitorar as ligações telefônicas dos seus Colaboradores realizadas ou recebidas por meio das linhas telefônicas disponibilizadas pela M7 IB para a atividade profissional de cada Colaborador, especialmente, mas não se limitando, às ligações da equipe de atendimento e da mesa de operação da M7 IB.

1.7. MONITORAMENTO E TESTES

O Diretor de Compliance (ou pessoa por ele incumbida) adotará as seguintes medidas para monitorar determinados usos de dados e sistemas em um esforço para detectar acessos não autorizados ou outras violações potenciais, em base, no mínimo, semestral:

i. deverá monitorar, por amostragem, o acesso dos Colaboradores a sites, blogs, *fotologs*, *webmails*, entre outros, bem como os e-mails enviados e recebidos;

ii. deverá monitorar, por amostragem, as ligações telefônicas dos seus Colaboradores realizadas ou recebidas por meio das linhas telefônicas disponibilizadas pela M7 IB para a atividade profissional de cada Colaborador, especialmente, mas não se limitando, às ligações da equipe de atendimento e da mesa de operação da M7 IB; e

iii. deverá verificar, por amostragem, as informações de acesso ao espaço do escritório, a desktops, pastas e sistemas, de forma a avaliar sua aderência às regras de restrição de acesso e escalonamento.

O Diretor de Compliance poderá adotar medidas adicionais para monitorar os sistemas de computação e os procedimentos aqui previstos para avaliar o seu cumprimento e sua eficácia.

2. PLANO DE IDENTIFICAÇÃO E RESPOSTA

2.1. IDENTIFICAÇÃO DE SUSPEITAS

Qualquer suspeita de infecção, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da M7 IB (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer Informações Confidenciais, mesmo que de forma involuntária, deverá ser informada ao Diretor de Compliance prontamente. O Diretor de Compliance determinará quais membros da administração da M7 IB e, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados.

Ademais, o Diretor de Compliance determinará quais clientes ou investidores, se houver, deverão ser contatados com relação à violação.

2.2. PROCEDIMENTOS DE RESPOSTA

O Diretor de Compliance responderá a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos da M7 IB de acordo com os critérios abaixo:

i. avaliação do tipo de incidente ocorrido (por exemplo, infecção de malware, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;

ii. identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;

iii. determinação dos papéis e responsabilidades do pessoal apropriado;

iv. avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;

v. avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, clientes ou investidores afetados, segurança pública); e

vi. determinação do responsável (ou seja, a M7 IB ou o cliente ou investidor afetado) que arcará com as perdas decorrentes do incidente. A definição ficará a cargo do Departamento de Compliance, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

2.3. ARQUIVAMENTO DE INFORMAÇÕES

De acordo com o disposto nesta Política, os Colaboradores deverão manter arquivado todos os documentos e informações exigidos pela Resolução CVM 161, bem como toda a correspondência, interna e externa, relatórios e pareceres relacionados com o exercício de suas funções, pelo prazo mínimo de 5 (cinco) anos ou prazo superior por determinação expressa da CVM.

2.4. TREINAMENTO

O Diretor de Compliance organizará treinamento anual dos Colaboradores com relação às regras e aos procedimentos previstos nesta Política, sendo que tal treinamento poderá ser realizado em conjunto com o treinamento anual de compliance.

3. DISPOSIÇÕES FINAIS

O Diretor de Compliance deverá realizar uma revisão desta Política a cada 24 (vinte e quatro) meses, para avaliar a eficácia da sua implantação, identificar novos riscos, ativos e processos e reavaliando os riscos residuais.

A finalidade de tal revisão será assegurar que os dispositivos aqui previstos permaneçam consistentes com as operações comerciais da M7 IB e acontecimentos regulatórios relevantes.

A presente Política foi devidamente elaborado e aprovado pelo Diretor de Risco e Compliance e entrará em vigor a partir de maio de 2025.

Esta Política deverá ser revisado anualmente ou em menor periodicidade, à medida que ocorram alterações nos procedimentos mencionados acima.

Havendo quaisquer dúvidas, favor contatar:

Ricardo Abrahão Fajnzylber
Diretor de Compliance
Telefone: +55 (11) 95077-4500
E-mail: ricardo.fajnzylber@multisete.com.