



**MANUAL DE SEGURANÇA
CIBERNÉTICA, SIGILO E
SEGURANÇA DAS INFORMAÇÕES**

19 de setembro de 2023

ÍNDICE

1	Introdução	3
2	Escopo	3
3	Abrangência	3
4	Identificação de Pontos Relevantes de Atenção.....	3
5	Potenciais Riscos	3
6	Tipos de Ameaças	4
7	Salvaguarda das informações: aspectos de proteção.....	4
8	Supervisão de sistemas.....	5
9	Reação em casos de ameaças	5
10	Responsável pela área de Compliance e Risco	Erro! Indicador não definido.

1 Introdução

O manual de Segurança Cibernética, Sigilo e Segurança das Informações elaborado pela MF Pepper Serviços Financeiros LTDA (MF Pepper), inscrita no CNPJ sob o nº 19.179.087/0001-34, visa delinear e especificar como tratamos das informações que estão em nosso poder, bem como mecanismos e sistemas utilizados.

2 Escopo

O Escopo deste manual de Segurança Cibernética, Sigilo e Segurança das Informações é apresentar a metodologia aplicada na guarda de informações, sistemas, conduta e tratamento das informações seja por meios eletrônicos ou voz.

3 Abrangência

O escopo de atividade da MF Pepper se concentra na administração de fundos de investimento em participações (FIPs) e Fundo de Investimentos em Cotas (FICs), sendo assim, este manual foi elaborado dirigindo-se a este espectro dentro da resolução CVM 21 e Código ANBIMA de Regulação e Melhores Práticas de Administração de Recursos de Terceiros ("Código de ART").

4 Identificação de Pontos Relevantes de Atenção

Equipamentos de voz: A linha telefônica da MF Pepper é somente acessada in-loco, dentro de nosso escritório que para acessar é necessário cracha de acesso.

Comunicações eletrônicas: Utilizamos serviço de e-mail protegido por senha, criptografado e com as informações armazenadas em nuvem, protegido de ataques externos.

Servidores: Utilizamos a salvaguarda de todas as informações da empresa na nuvem com back-up realizado em sistema de redundante em nuvem.

5 Potenciais Riscos

Perda de dados confidenciais: Perda de dados confidenciais, ou seja, informações sobre clientes, nossas carteiras, dados contábeis e comunicações

entre os colaboradores da MF Pepper e Clientes ou Cotistas.

Perda de dados operacionais: Perda de dados operacionais que resultem em perda de processamento da carteira de fundos, seu patrimônio líquido, cálculo por cotista e aspectos contábeis do fundo.

Impossibilidade de acesso à informações: Falhas em hardware, softwares e provedores de sistemas que impossibilitem o acesso à informações e atrapalhem a operação da MF Pepper.

6 Tipos de Ameaças

Ameaças internas: uso de informações internas de maneira intencional ou não intencional.

Ameaças externas: perda da integridade das informações que estão em posse da MF Pepper realizada por terceiros.

7 Salvaguarda das informações: aspectos de proteção

Manuais de Conduta: O nosso Manual de Compliance e Ética e Código de Ética, é de leitura obrigatória a todos os colaboradores e objeto de treinamento periódico. Nele há estipulado as penalidades que colaboradores que “vazam” informações podem sofrer.

Controle de informações USB: Somente disponível aos Sócio-Diretores da Empresa.

Instalação de Softwares: Somente permitida a instalação de Softwares pelos Sócio-Diretores da MF Pepper.

Acesso às Informações: Toda e qualquer informação sigilosa somente é acessada por senha em diferentes níveis e concessões de acordo com a atividade de cada colaborador.

Acesso remoto: Realizado somente pelos sócios-diretores da empresa e em ambiente controlado como sistemas operacionais da empresa com acesso via senha.

Antivirus e dispositivo de segurança de rede: Além dos acessos serem controlados, a MF Pepper também utiliza firewall e antivirus para proteção dos dados.

Acesso às informações: o acesso às informações são controlados e liberados de acordo com área de atuação de cada colaborador.



Salientamos, também, que qualquer sistema da MF Pepper é controlado e pode ser bloqueado instantaneamente em caso de ameaças ou suspeitas de mal uso de suas informações.

8 Supervisão de sistemas

Backup: As informações vitais da empresa, salvaguarda de arquivos importantes, informações de nosso sistema operacional e e-mail contam com processo de back-up periódico.

Controles Sistêmicos: Ainda, nossos sistemas possuem dispositivos que detectam ameaças externas para garantir a proteção de nossas informações.

9 Regras de acesso às informações confidenciais

Esta regra tem como objetivo definir o processo de gestão de acessos de funcionários, estagiários e prestadores de serviços aos sistemas da MF Pepper, além de estabelecer padrões para gerenciamento de contas e senhas.

Esta regra se aplica a todos os usuários da MF Pepper.

A gestão de acessos ao ambiente e sistemas da MF Pepper é de responsabilidade da área de Compliance. Caso haja exceções, estas deverão ser analisadas e documentadas.

Na MF Pepper utilizamos um controle de acessos baseado na função exercida pelo colaborador. Os acessos são baseados em análise, a cargo dos profissionais de compliance, que determina para cada cargo/função quais informações determinado usuário terá acesso. Desta maneira, são definidas as funções existentes na empresa e os perfis de acesso e operações previamente autorizadas a sistemas, pastas de rede e demais recursos sistêmicos e computacionais pertinentes à função. A análise sobre os diferentes tipos de acesso também levam em conta definições dos Gestores das áreas. Qualquer alteração nas permissões de acesso definidas deve ser autorizada pelo gestor responsável pela função. Novos perfis só podem ser definidos e implantados mediante autorização do gestor.

No caso de Admissão e Movimentação Funcional de Funcionários / Estagiários / Prestadores de Serviços as concessões de acesso deverão ser analisadas e adequadas a nova função.

No caso de prestadores de serviços deverá também ser informado o tempo em que o mesmo prestará serviço à Companhia, para que na data de seu desligamento possam também ser encerradas as atividades relacionadas ao direito de seu acesso ao sistema.

No caso de desligamento ou afastamento de funcionários, o gestor responsável pelo funcionário, estagiário ou prestador de serviço deverá comunicar o fato o mais rapidamente possível a área de Compliance os acessos internos e externos sejam revogados imediatamente.

O acesso a VPN será autorizado e liberado para que os colaboradores possam acessar de maneira remota o ambiente da MF Pepper. Todas as solicitações devem ser efetuadas pelo Gestor da área.

10 Reação em casos de ameaça

Ameaças Externas: Imediatamente é acionado o responsável por tecnologia o qual deverá imediatamente atuar a fim de impedir que a ameaça permaneça e proteger a integridade dos sistemas da MF Pepper e suas informações. Nestes casos há a possibilidade da retirada dos sistemas em operação, restauração dos mesmos e utilização de seus back-ups em nuvem.

Ameaças Internas: O Diretor de Compliance e risco é acionado para instaurar sindicância em relação ao colaborador que teve este grave desvio de conduta. Após apuração do ocorrido as medidas cabíveis, estipuladas na lei e em nosso Código de Ética e Manual de Compliance serão aplicadas.

11 Penalidades

O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações: advertência formal, suspensão, multa, rescisão do contrato de trabalho, outra ação disciplinar e/ou processo civil ou criminal.