MARR GESTÃO DE RECURSOS LTDA.

POLÍTICA DA SEGURANÇA E SIGILO DA INFORMAÇÃO

Julho de 2023

FOLHA DE CONTROLE

Informações Gerais

Título	Política de Segurança e Sigilo da Informação
Elaborador	Ana Carolina Paifer
Data da Próxima Revisão	31/07/2024
Área Proprietária da Política	Compliance e Riscos Operacionais
Procedimentos e Outros Documentos Relacionados	Resolução do Conselho Monetário Nacional do Banco Central do Brasil nº 4.658/2018 e CVM 612; Lei nº 13.709 de 2018 (Lei Geral de Proteção de Dados – "LGPD").

SUMÁRIO

1. INTRODUÇÃO

A Política de Segurança e Sigilo da Informação ("Política") é parte integrante do Código de Ética e Conduta ("Código") da Marr Gestão de Recursos Ltda.("MARR"), aplica- se a todos os sócios, funcionários, colaboradores, estagiários, temporários e terceiros contratados que atuem a serviço da MARR.

Fica eleita a sócia **Ana Carolina Paifer**, Diretora da MARR, como responsável pelo disposto, em atendimento do disposto na Instrução CVM nº 558, artigo 4º, inciso IV, estando este devidamente registrada no estatuto da empresa.

O Diretor de Tecnologia ("Diretor de Tecnologia") eleito e designado no estatuto social da MARR, representado pelo sócio Etore Froda, será o responsável pelas atividades de tecnologia da informação, controlador e encarregado pelo tratamento de dados pessoais (em atendimento à Lei nº 13.709 de 2018, Lei Geral de Proteção de Dados – "LGPD") e auxílio em toda e qualquer necessidade tecnológica da MARR, podendo ser representada por outros Colaboradores devidamente habilitados nos termos da regulamentação atual.

As regras descritas na integridade das Normas Internas e na legislação aplicável aos propósitos da MARR devem ser cumpridas por todos os sócios, diretores, administradores, funcionários, representantes, colaboradores, ou estagiários da MARR (definidos, resumidamente como "Colaborador" ou no seu plural "Colaboradores").

O presente regulamento está em conformidade com o disposto no item 2.7 do Ofício Circular CVM/SIN Nº 05 de 2014 e no artigo 15 da Instrução CVM nº 558 de 2015 que dispõe regras que orientam a conduta de todos os Colaboradores no exercício de suas funções.

As atividades desenvolvidas pelo Compliance não estarão subordinadas, em qualquer hipótese, à área de gestão de recursos ou área de distribuição, conforme disposto na Instrução CVM nº 558 de 2015, artigo 4º, parágrafo 3º incisos I e II.

2. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Todo Colaborador usufrui do acesso a computadores, telefones, sistemas e informações corporativas para que possa exercer sua função, o que implica na obrigação de usar tais sistemas de forma responsável e seguir as políticas da Companhia para proteger tais informações e sistemas.

Os Colaboradores receberão, no momento de sua contratação, um usuário e senha, pessoal e intransferível para acesso à rede da MARR e correio eletrônico.

Em caso de mudança de atividade, desligamento ou ausência temporária não remunerada o Colaborador ou gestor devem comunicar o Compliance que pode revogar o acesso atual das pastas, e-mails ou documentos de forma a manter a segurança das informações.

Os arquivos com dados e informações relativas a cada uma das atividades desenvolvidas pela MARR ficarão alocados de forma que apenas os Colaboradores da área relacionada à atividade terão acesso às informações confidenciais e sigilosas relativas à sua atividade. Apenas os diretores da MARR terão acesso a todas as pastas.

Os computadores e demais equipamentos disponibilizados aos Colaboradores deverão ser utilizados com a finalidade de atender aos interesses da MARR, sendo facultada a utilização, de forma moderada, para fins particulares, desde que sejam cumpridas as seguintes regras:

a) mensagens devem ser profissionais e apropriadas para comunicação empresarial;

b) não são permitidas conversações que possam ser consideradas ofensivas, chulas, vulgares, obscenas, com ameaças ou assédio (ou seja, piadas de gosto duvidoso, comentários ou imagens de conteúdo sexual, comentários que possam transmitir ofensa, inclusive os baseados em sexo, raça, idade, crença, orientação sexual, identidade sexual, deficiência ou qualquer outra base definida por lei);

c) não é permitida a distribuição de materiais licenciados ou registrados, de maneira imprópria;

d) não é permitida a transmissão correntes, anúncios ou solicitações, a não ser que tenham sido explicitamente autorizados pela companhia;

e) não é permitido o uso e, ou, download de materiais impróprios.

Cada Colaborador tem acesso aos sistemas da MARR em prol de conduzir os negócioslegítimos da Companhia e espera-se que estes sejam usados de maneira profissional e responsável. A área de Compliance se reserva o direito de interceptar, monitorar e registrar sua comunicação através de tais sistemas.

Os computadores e demais equipamentos disponibilizados aos Colaboradores deverão ser utilizados com a finalidade de atender aos interesses da MARR, sendo facultada a utilização, de forma moderada, para fins particulares.

Todo Colaborador deve ser cuidadoso com seu próprio equipamento e zelar pela boa utilização dos demais. Caso algum Colaborador identifique a má conservação, uso indevido ou inadequado de qualquer ativo, deve comunicar à área de Compliance.

Programas instalados nos computadores, principalmente via Internet (“downloads”), sejam de utilização profissional ou para fins pessoais devem obter autorização prévia do responsável pela área de informática e pela área de Compliance. Não é permitida a instalação de nenhum software ilegal (“pirata”) ou que possuam direitos autorais protegidos.

A instalação de aplicativos, bem como *Downloads* para uso profissional, podem ser realizados com prévia autorização do Compliance, podendo realizar inspeções para averiguar a utilização de acordo com a função exercida, sanções poderão ser aplicadas se tal ato possa trazer algum tipo de risco para a MARR e seus clientes ou se for caracterizado o uso impróprio dos equipamentos da MARR para fins diversos.

O correio eletrônico disponibilizado pela MARR (“E-mail Corporativo”) caracteriza-se como correio eletrônico corporativo para todos os efeitos legais, especialmente os relacionados aos direitos trabalhistas, sendo sua utilização preferencial voltada para alcançaros fins comerciais aos quais se destina. O E-mail Corporativo pode ser utilizado para fins particulares, desde que de forma moderada.

As mensagens enviadas ou recebidas através do E-mail Corporativo, os anexos relacionados e navegação através da rede mundial de computadores estarão sujeitas a monitoramento, sendo o Compliance responsável pela verificação periódica dos acessos e da utilização de mecanismos para resguardar os interesses da MARR.

O Colaborador deverá verificar o conteúdo das mensagens recebidas através do E-mail Corporativo no momento da abertura da mensagem evitando sobre qualquer hipótese a manutenção ou o arquivamento de conteúdo ofensivo, discriminatório, pornográfico ou vexatório, sendo a responsabilidade apurada de forma específica em relação ao destinatário da mensagem. Os E-mails Corporativos poderão ser inspecionados pela MARR, a critério da área de Compliance, a qualquer

tempo e sem prévia notificação.

Todos os acessos remotos serão monitorados pelo Compliance, sendo passíveis de verificação periódica e sem prévio aviso.

A MARR utiliza a tecnologia de armazenamento de dados na nuvem ("e*Cloud Computing*"). Essa tecnologia permite maior segurança no acesso aos dados, uma vez que as credenciais podem ser validadas até 2 vezes, uma ao se conectar ao computador e uma segunda ao se conectar ao servidor através da rede mundial de computadores. Adicionalmente, além do firewall de segurança nos servidores para acesso a sua rede, as informações são monitoradas 24 horas por dia, 7 dias por semana pela empresa contratada.

Os dados armazenados no *eCloud Computing* também contam com rotinas de Backup e realocação automática de servidor em casos de falha, garantindo a integridade e o acesso aos dados armazenados bem como a continuidade nos negócios.

É de responsabilidade de todos os Colaboradores a utilização responsável, a conservação e a proteção dos patrimônios da MARR. Por isso, todos os equipamentos e recursos eletrônicos devem ser manuseados pelos Colaboradores com a intenção de propiciar as ferramentas e informações necessárias ao desempenho da função e que incentivem a eficiência de cada Colaborador. O patrimônio da MARR deverá ser utilizado exclusivamente para a consecução do seu objeto social, sendo dever de todos os Colaboradores a sua preservação e utilização adequada.

A base de dados, sistemas computadorizados, controles e planilhas eletrônicas desenvolvidas internamente são de propriedade da MARR, sendo a sua reprodução, cópia e transmissão vedados nos termos da Lei 9.609/98.

O acesso remoto aos sistemas da MARR é feito de forma monitorada e controlada pelo Administrador, podendo ser verificada pelo Compliance a partir do registro gerado pelo login do usuário.

Sempre que houver a ocorrência de descumprimento ou suspeita ou indício de descumprimento de quaisquer das regras estabelecidas no Código ou aplicáveis às atividades da MARR, de acordo com os procedimentos estabelecidos, o Compliance poderá se utilizar dos registros e sistemas de monitoramento eletrônico e telefônico disponíveis para verificar a conduta dos Colaboradores envolvidos, sendo facultado o acesso pela MARR a quaisquer informações, contatos, documentos e arquivos gerados pelas atividades profissionais desenvolvidas na MARR, ou que transitem pela sua infraestrutura de TI.

3. POLÍTICA DE CONFIDENCIALIDADE E SIGILO DAS INFORMAÇÕES

As regras estabelecidas nessa política visam proteger a MARR e os seus clientes acerca da divulgação inapropriada de informações que possam representar quebra de sigilo ou uso inapropriado da propriedade intelectual da MARR e seus clientes.

Definição: serão consideradas "Informações Confidenciais" todas e quaisquer informações e/ou dados de natureza confidencial (incluindo, sem limitação, todas as informações técnicas, financeiras, operacionais, econômicas, bem como demais informações comerciais) referentes à MARR, suas atividades e seus clientes e quaisquer cópias ou registro dos mesmos, orais ou escritos, contidos em qualquer meio físico ou eletrônico, que tenham sido direta ou indiretamente fornecidos ou divulgados em razão da atividade de administração de ativos e carteiras de valores mobiliários e/ou atividades de distribuição dos fundos geridos pela MARR, ainda que tais informações e/ou dados não estejam relacionados diretamente aos serviços ou às transações aqui

contempladas.

Não serão consideradas Informações Confidenciais todas as informações de domínio público, de fácil acesso ou que tenham sido divulgadas por terceiros por boa-fé, desde queo Colaborador tenha o direito de divulgar sem obrigação de confidencialidade.

Fica estabelecido que o Colaborador é expressamente obrigado a manter o sigilo das Informações Confidenciais transmitidas, fornecidas e/ou divulgadas em função das suas atividades através da MARR ou em função do seu vínculo. A reprodução, utilização, divulgação, sem expressa autorização formal do titular é vedada a todos os Colaboradores.

Todos os materiais produzidos e utilizados pela MARR e/ou por seus clientes, é considerada material de propriedade da MARR, sendo vedada aos Colaboradores a utilização para fins próprios, cessão, alienação ou divulgação para terceiros. Os materiais incluem, mas não se limitam a: informações sobre negócios, técnicas, planilhas, formulários,projetos, desenvolvimentos de qualquer natureza, produtos e serviços, mesmo que estes possuem significativa participação ou elaboração do Colaborador.

Os Colaboradores, ao aderirem ao Código, dão ciência formal e expressa de que todo o conteúdo produzido por eles passa a ser de propriedade intelectual da MARR.

Caso o Colaborador tenha que divulgar qualquer informação confidencial, por determinação judicial ou autoridade competente, deverá comunicar imediatamente o Compliance tão logo receba a solicitação e previamente à divulgação, limitando-se a divulgar estritamente a Informação Confidencial solicitada.

A MARR, através do Compliance, poderá:

i. manter diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções dos Colaboradores através da disponibilização de login e senhas individuais e intransferíveis;

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

iii. poderá gravar as ligações telefônicas de Colaboradores realizadas ou recebidas por meio das linhas telefônicas disponibilizadas pela MARR para a atividade profissional de cada Colaborador, especialmente, mas não se limitando, às ligações da equipe de atendimento e da mesa de operações da MARR.

Caso um Colaborador tenha acesso a qualquer informação que não tenha sido previamente autorizada deverá, imediatamente:

i. abster-se de usar tal informação em seu favor, para clientes da MARR ou para terceiros, sob pena de demissão por justa causa;

ii. informar a Diretoria acerca do ocorrido indicando: a informação obtida, a forma como tal informação foi obtida e fonte da informação.

A MARR veda expressamente aos Colaboradores efetuar qualquer tipo de operação no mercado financeiro baseada em informações privilegiadas, bem como recomendá-las ou sugeri-las a terceiros. Fica ressaltado que a realização de operações no mercado financeiro mediante o emprego de informações privilegiadas fere as regras estabelecidas pela CVM, sendo punível cível e criminalmente.

Todas as Informações Confidencias recebidas devem ser analisadas pelo Colaborador atentamente, principalmente, mas não limitado a:

i. *Insider Trading:* significa a compra e/ou venda de títulos e valores mobiliários através do uso de informação privilegiada, com a intenção de conseguir benefício próprio ou terceiros;

ii. *Front Running:* significa a realização de operações de compra e/ou venda de títulos e valores mobiliários de forma a concluir e/ou obter vantagem econômica antecipadamente a outros;

iii. Qualquer outra prática que não esteja alinhada com os interesses da MARR e seus clientes conforme previsto no Código, podendo ser aplicado ao Colaborador o rigor das sanções previstas no Código.

A vigência da Informação Privilegiada deve ser observada durante todo o período de relacionamento do Colaborador com a MARR e seus clientes, inclusive após o término.

Ao final do vínculo de um Colaborador com a MARR, o mesmo deverá devolver todos os livros, registros, relações e outros materiais manuscritos, escritos à máquina, impressos ou arquivados de forma eletrônica, que contenham qualquer informação relacionada com os negócios da MARR.

O acesso às instalações físicas da MARR é restrito aos colaboradores e controlado por crachás eletrônicos. O acesso de pessoas estranhas à MARR a áreas restritas somente será permitido com a permissão expressa de Colaborador autorizado pelo Diretor de Compliance.

Sempre que houver a ocorrência de descumprimento ou suspeita ou indício de descumprimento de quaisquer das regras estabelecidas neste Código ou aplicáveis às atividades da MARR, de acordo com os procedimentos estabelecidos, o Compliance poderá se utilizar dos registros e sistemas de monitoramento eletrônico e telefônico disponíveis para verificar a conduta dos Colaboradores envolvidos, sendo facultado o acesso pela MARR a quaisquer informações, contatos, documentos e arquivos gerados pelas atividades profissionais desenvolvidas na MARR, ou que transitem pela sua infraestrutura de TI.

Caso tenham conhecimento de que qualquer Colaborador tenha violado as regras contidas neste Código da MARR, com atenção especial ao disposto nessa política, os demais Colaboradores obrigam-se a reportar tal falta ao Compliance e/ou Diretoria da MARR, sob pena de ser considerado corresponsável diante de omissão.

O Diretor de Compliance será responsável por aplicar, bem como controlar, supervisionar e aprovar eventuais exceções ao cumprimento da Política de Confidencialidade e Sigilo das Informações.

Os Colaboradores, ao firmarem ciência através do Termo de Adesão do presente Código, atestam para todos os efeitos que estão em acordo e cientes das políticas estabelecidas e possíveis sanções aplicáveis ao não cumprimento da política.

Os Colaboradores, ao firmarem ciência através do Termo de Adesão do presente Código, atestam para todos os efeitos que estão em acordo e cientes das políticas estabelecidas e possíveis sanções aplicáveis ao não cumprimento da política.

4. POLÍTICA DE SEGURANÇA CIBERNÉTICA

É de responsabilidade de todos os colaboradores observar as regras da Política de Segurançapara evitar a facilitação de possível ação criminosa a partir das informações geridas pela MARR. De todo modo, foi definido um programa de segurança cibernética com as seguintes etapas:

i. Identificação e avaliação de riscos;

ii. Ações de prevenção e proteção;

iii. Monitoramento e testes;

iv. Vigência

A responsabilidade da implementação, validação e testes caberá à área de Compliance e poderá contar com o auxílio externo especializado para melhorar a segurança do ambiente emquestão, bem como de analistas de tecnologia para avaliar e identificar potenciais riscos da estrutura empregada.

A partir da identificação dos riscos, serão analisados os princípios da confidencialidade, integridade e disponibilidade.

5. IDENTIFICAÇÃO, AÇÕES DE PROTEÇÃO E PREVENÇÃO

Foram identificados os seguintes ativos e processos relevantes para a MARR:

- **Equipamentos:** compreendem todos os computadores e periféricos, monitores, impressoras, modem, telefones e demais equipamentos destinados a uso profissional pessoal de propriedade da MARR;
- **Instalações elétricas:** compreende toda instalação elétrica, incluindo no-breaks, que permitem o funcionamento adequado dos Equipamentos;
- **Acesso a sistemas em nuvem:** compreende os links de internet para o qual são utilizados para acessar o serviço de armazenamento em nuvem, bem como serviços de e-mail.
- **Firewall:** compreende o equipamento físico e o software utilizado para proteção de tráfego de dados entre a rede interna e redes externas;
- **Senhas:** compreende o mecanismo que administra remotamente o acesso a armazenagem em nuvem e e-mails;
- **E-mails:** compreende toda a comunicação feita através das contas corporativas da MARR, realizada entre os sócios e funcionários de forma interna e externa;
- **Sistemas e base de dados:** compreende os sistemas proprietários da MARR, bem como as informações por ela utilizada e armazenada para a gestão de portfolio, controles de operações e risco, controle de clientes e dos contatos comerciais.

- **Equipamentos:** diante de situação onde o equipamento fique indisponível ou inutilizado a MARR conta com máquinas pré-configuradas para uso, bem como fornecimento de fábrica para reposição mediante compra. Atualmente também contamos com cadastro e serviço de aluguel eventual de equipamentos que possam ser rapidamente contratados.

- **Instalações elétricas:** diante de falta de fornecimento de energia, o edifício da MARR conta com gerador independente que é capaz de suprir energia para o prédio de forma autônoma. A MARR também conta com no-breaks que tem carga suficiente para a transição de faltade energia até o início da operação do gerador.

- **Acesso a sistemas em nuvem:** o acesso é feito de forma redundante, ou seja, contamos com dois links de internet que são balanceados pelo firewall de forma a garantir disponibilidade alternada de provedores de acesso.

- **Firewall:** a MARR possui um firewall que monitora todo o tráfego de informação interno e externo, também conta com anti-virus instalado em todos os desktops que possuem monitoramento de vírus e malwares, sendo a lista atualizada automaticamente.

- **Senhas:** todas as senhas possuem registro e obedecem a mesma política de acesso através de administrador virtual, tanto para salvar arquivos como para acesso a e-mail.

- **E-mails:** todos os e-mails são monitorados e contam com armazenamento, serviços de anti-

spam, anti vírus, recuperação e alertas do G-Suite.

- **Sistemas e base de dados:** todos os sistemas e base de dados têm acesso e proteção da AWS(Amazon Web Services).

6. HOME OFFICE

A MARR permite, excepcionalmente, que os Colaboradores exerçam suas atividades remotamente, através de aprovação prévia e análise casuística da eventual necessidade.

O Home Office da MARR foi desenvolvido no modelo BYOD – do inglês, *Bring Your Own Device* (traga seu próprio dispositivo). Entretanto, a MARR permite que os Colaboradores retirem dispositivos necessários para que sejam utilizados em suas respectivas residências, desde que o Colaborador se responsabilize com o uso consciente.

O conceito do BYOD surge com a concessão da faculdade para que o funcionário possa usar seus próprios aparelhos e dispositivos para acessar e modificar informações da empresa. Para isso, é necessário que todo Colaborador:

i. Não abra e-mail ilegítimos – também chamados de phishing, que é uma técnica de fraude que visa roubar dados pessoais;

ii. Utilize senhas fortes;

iii. Se limite a compartilhar informações, materiais e outras formas de propriedade intelectual apenas com os Colaboradores da MARR;

iv. Instale apenas aplicativos permitidos e, ou, recomendados pelas áreas de Tecnologia e Compliance; e

v. Não desinstale proativamente programas e aplicativos implementados pela área de Tecnologia.

7. MONITORAMENTO E TESTES

A MARR realizará testes anuais para avaliação dos riscos, fazendo essa parte integral do Relatório Anual de Controles Internos da MARR.

Os testes relacionados à tecnologia serão realizados por equipe de suporte contratada, que buscará cobrir os seguintes itens:

i. Identificação e avaliação de riscos cibernéticos que possam afetar tanto os softwares como hardwares utilizados pela MARR;

ii. Estimar, em conjunto com Compliance, eventuais impactos financeiros e reputacionais;

iii. Estabelecer medidas de proteção ou melhoria para mitigar ataques cibernéticos;

iv. Detecção de anomalias ou fragilidades oriundas da estrutura atual de equipamentos e acesso a informações;

V. Levantamento de informações para plano de resposta e recuperação de informações que possam ser incorporados nos planos de contingência da MARR.

8. CONSIDERAÇÕES FINAIS

Os modelos, rotinas internas, bancos de dados, sistemas de análise desenvolvidos, em desenvolvimento ou que venham a ser criados pelos Colaboradores constituem propriedade intelectual exclusiva da MARR, cabendo à Diretoria deliberar acerca da comercialização, reprodução e utilização desses.

É vedada a cópia, venda, uso ou distribuição de informações, planilhas de análise, relatórios internos e outros materiais que sirvam de base para a tomada das decisões de investimento que poderão fazer parte das carteiras dos fundos; e, ainda, de outras formas de propriedade intelectual.

A utilização dos ativos da MARR – como computadores, telefones, internet, programa demensagem instantânea, e-mail e demais aparelhos – se destina a fins profissionais. O usoindiscriminado dos mesmos para fins pessoais deve ser evitado, e nunca deve ser prioridade em relação a qualquer utilização profissional.

Esta Política deverá ser revisada e atualizada semestralmente, ou em prazo inferior, caso necessário, em função de mudanças legais/regulatórias ou complementações.

9. REVISÃO DESTA POLÍTICA

O Diretor de Compliance deverá realizar uma revisão da política da segurança e sigilo da informação a cada 12 (doze) meses, no mínimo, para avaliar a eficácia da sua implantação, identificar novos riscos, ativos e processos e reavaliando os riscos residuais, incluindo no relatório anual de compliance eventuais deficiências encontradas.

A finalidade de tal revisão será assegurar que os dispositivos aqui previstos permaneçam consistentes comas operações comerciais da MARR e acontecimentos regulatórios relevantes.