MARIN GESTORA DE RECURSOS S.A.

("Gestor")

MANUAL DE SEGREGAÇÃO DE ATIVIDADES E SEGURANÇA DA INFORMAÇÃO

MARÇO DE 2024

MANUAL DE SEGREGAÇÃO DE ATIVIDADES E SEGURANÇA DA INFORMAÇÃO

1. Objetivo e Atividades do Gestor

Este Manual de Segregação de Atividades ("Manual") da Marin Gestora de Recursos S.A. ("Gestor") foi elaborado de acordo com os artigos 27 e 28 da Resolução CVM nº 21, DE 25 de fevereiro de 2021("Instrução CVM 21") e tem como finalidade: (i) garantir a segregação física de instalações entre as áreas relacionadas à gestão de recursos e as áreas responsáveis por *Compliance*, Riscos e PLDFT e administrativa ("*BackOffice*") do Gestor; (ii) assegurar o bom uso de instalações, equipamentos e informações comuns; (iii) preservar informações confidenciais e permitir a identificação das pessoas que tenham acesso a elas; e (iv) restringir o acesso a arquivos e permitir a identificação das pessoas que tenham acesso a informações confidenciais.

Adicionalmente, o Manual também abrange as questões relacionadas à Segurança da Informação, que contarão com prestadores de serviço especializados visando garantir a eficiência e segurança compatíveis com as necessidades do Gestor, de seus Colaboradores, investidores e demais *stakeholders*, bem como a responsabilização dos envolvidos em caso de violação (vazamentos).

Não exercício das atividades de Distribuição e Intermediação:

O Gestor atua no setor de fundos líquidos e fundo de investimento em direitos creditórios ("FIDCs"), adotando tais fundos como veículos para investimentos de seus clientes. Considerando que não serão performadas atividades de distribuição de cotas dos fundos de investimento sob gestão e, tampouco, de intermediação, este Manual terá relevância reduzida em relação aos demais players do mercado de capitais. Sem prejuízo, suas disposições serão aplicáveis a todos os sócios, Diretores e funcionários do Gestor ("Colaboradores").

Ausência de Conflito entre Gestão e *BackOffice*:

O Gestor não identificou potenciais conflitos de interesses entre o Departamento Técnico e o *BackOffice*, e/ou em relação ao gerenciamento dos recursos financeiros próprios do Gestor.

2. Estrutura

<table>
<tr><th colspan="3">MARIN GESTORA DE RECURSOS S.A
ESTRUTURA ORGANIZACIONAL</th></tr>
<tr><td colspan="3"></td></tr>
<tr><th colspan="2">Departamento Técnico</th><th>BackOffice</th></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td colspan="2">GESTÃO</td><td>COMPLIANCE, RISCO E PLDF/ADMINISTRATIVO</td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td>Antonio Luiz Fernandes Filho
(Backup Gestão)</td><td>Nelson Bulamarqui Pinheiro
(Gestão)</td><td>Sérgio Albino Bitar Pinheiro
(Compliance, Risco e PLDFT)</td></tr>
<tr><td colspan="2" rowspan="2">Comitê de Compliance, Risco e PLDFT*
(*Previsto, porém ainda não constituído)</td><td>Paulo Rogério Teixeira dos Santos
(Tecnologia, Segurança da informação/Backup, Compliance, Risco e PLDFT)</td></tr>
<tr><td>Maise Costa de Souza
(Apoio Administrativo)</td></tr>
</table>

Considerando a estrutura do Gestor, refletida no Manual de *Compliance* e no organograma acima, foram desenvolvidas regras aplicáveis à (i) segregação física entre o Departamento Técnico e o *BackOffice*; (ii) *Chinese Wall*; e (iii) à segurança da informação do Gestor.

No que se refere a ao item (iii) acima, o prestador de serviço de tecnologia da informação será contratado pelo *BackOffice* e será responsável pela implantação e racionalização de processos, manutenção dos sistemas de informática, segurança da informação com controle de acesso dos usuários e *backup* de dados.

3. Segregação física

O acesso à área utilizada pela equipe especializada na gestão de carteiras de valores mobiliários será controlado e permitido aos Colaboradores autorizados. A referida área é localizada em sala completamente apartada, comunicando-se apenas com serviços auxiliares à atividade de gestão de carteiras de valores mobiliários, de forma a manter-se fisicamente segregada de quaisquer áreas do Gestor que venham a ser responsáveis por outras atividades relacionadas ao mercado de capitais.

É limitado o acesso às instalações físicas da área de gestão de carteiras de valores mobiliários por pessoas que não sejam os Colaboradores envolvidos na atividade de gestão de carteiras de valores mobiliários.

4. Chinese Wall

Tem como finalidade estabelecer uma barreira de comunicação entre diferentes indivíduos ou setores de uma mesma entidade, visando assegurar o cumprimento das normas que exigem a segregação entre a atividade de administração de carteiras de valores mobiliários e outras atividades relacionadas ao mercado de capitais, bem como a segregação entre ativos financeiros próprios do Gestor e os ativos financeiros de terceiros.

Via de regra, as restrições de acesso às informações e aos documentos contidos na rede de computadores e sistemas do Gestor respeitam as linhas pontilhadas do organograma funcional que integra o item 2 deste Manual. Exceções, no entanto, poderão ser avaliadas pelo(a) Diretor(a) de *Compliance*, Riscos e PLDFT conforme solicitação fundamentada e avaliação de necessidade.

5. Confidencialidade, Sigilo e Segurança da Informação

Informações Confidenciais:

No exercício de suas atividades, os Colaboradores poderão ter acesso às informações de clientes do Gestor e de terceiros, podendo tais informações não ser de conhecimento do público em geral e, portanto, podem ser consideradas confidenciais ("Informações Confidenciais" ou, no singular, "Informação Confidencial"). É terminantemente proibida a divulgação de qualquer Informação Confidencial para terceiros, para benefício próprio ou

de terceiro (*tipping*), ou mesmo que não haja intenção de beneficiar ninguém. A obrigação de confidencialidade se aplica mesmo após o desligamento do Colaborador.

O Gestor e Colaboradores possuem o dever legal e profissional de manter o sigilo das Informações Confidenciais de seus clientes, de modo que pedidos, tentativas ou ações que visem a quebra do sigilo deverão ser imediatamente comunicados ao(à) Diretor(a) de *Compliance*, Riscos e PLDFT.

Informações Sigilosas:

Informações Sigilosas, além das Informações Confidenciais, são aquelas que, caso venham à tona, podem resultar em perda do nível de segurança do Gestor.

Perda, mau uso, modificação ou acesso não autorizado às Informações Sigilosas podem afetar adversamente a privacidade de um indivíduo, desfazer negócios, macular a imagem do Gestor e a continuidade de seus negócios.

O Gestor tem a responsabilidade legal de prezar pelo sigilo de seus clientes e, portanto, informações relativas aos clientes e entidades investidas por fundos de investimento geridos pelo Gestor jamais poderão ser enviadas a terceiros, com exceção das solicitações dos órgãos públicos, dos órgãos reguladores e do Poder Judiciário e, mesmo nessas hipóteses, nos estritos limites das ordens recebidas.

Segurança da Informação:

As medidas de segurança da informação têm por finalidade a proteção contra ameaças, de modo a garantir a continuidade dos negócios, minimizar riscos e maximizar os retornos aos investidores.

Tais medidas estão sob a responsabilidade dos serviços de tecnologia da informação – terceirizada para garantia de qualidade e sob responsabilidade do *BackOffice*, conforme será descrito nos próximos itens deste Manual, e devem ser observadas por todos os Colaboradores:

Causam situações de risco à Segurança da Informação:

(i) Acessar a sites não relacionados às atividades do Gestor;
(ii) Utilizar mídias ("pen-drives", CDs, entre outras) para armazenamento de arquivos digitais, com exceção das disponibilizadas pelo Gestor;
(iii) Acessar ou salvar informações sensíveis e Informações Confidenciais em pastas virtuais de acesso público;
(iv) Salvar arquivos pessoais na rede de computadores institucional;
(v) Utilizar mídias para transporte de informações não criptografadas; e
(vi) Dividir senhas.

Mais informações poderão ser encontradas no Anexo I do presente Manual, que contém algumas regras referentes ao Gerenciamento e Segurança de Informações Confidenciais.

6. Reporte, Penalidades e Responsabilidade

É dever de todo Colaborador informar ao(à) Diretor(a) de *Compliance*, Riscos e PLDFT sobre violações ou possíveis violações das disposições referentes à Segregação Física

contidas neste Manual, sendo certo que o descumprimento de qualquer regra estabelecida neste Manual implicará, a critério do(a) Diretor(a) de *Compliance*, Riscos e PLDFT nas seguintes penalidades, a depender da gravidade do descumprimento e de eventual reincidência: (i) advertência por escrito; ou (ii) desligamento.

Qualquer Colaborador que acredite ter violado este Manual ou tenha conhecimento de violação deverá notificar o fato direta e imediatamente o(a) Diretor(a) de *Compliance*, Riscos e PLDFT, sendo que eventual ação disciplinar levará o reporte em consideração. Ainda, poderão ser tomadas ações disciplinares contra Colaborador que (i) autorize, coordene ou participe de violações a esta Política; (ii) possuindo informação ou suspeita de violações, deixe de reportá-las; (iii) deixe de reportar violações ocorridas que, pelo seu dever de ofício, deveria ter conhecimento ou suspeita; e/ou (iv) promova retaliações, direta ou indiretamente, ou encoraje outros a fazê-lo.

No que se refere à Segurança da Informação, a responsabilidade pela contratação e fiscalização dos serviços de prestados será de responsabilidade do *BackOffice*, que avaliará os terceiros com potencial de contratação nos termos do Manual de *Compliance* e demais normas internas e fará o acompanhamento e avaliação qualitativa dos serviços prestados.

Acompanhamento:

Caso haja ocorrência, suspeita ou indício de descumprimento de quaisquer das regras estabelecidas neste Manual, caberá ao(à) Diretor(a) de *Compliance*, Riscos e PLDFT utilizar os registros eletrônicos disponíveis para verificar a conduta dos Colaboradores.

O(A) Diretor(a) de *Compliance*, Riscos e PLDFT terá acesso a todo conteúdo que está na rede de computadores do Gestor e poderá acessar tal conteúdo caso haja necessidade. A confidencialidade das informações será respeitada e seu conteúdo será disponibilizado somente para fins legais[1], garantindo, assim, verificação dos responsáveis por eventuais vazamentos.

7. Diretor(a) Responsável

Abaixo apresentamos informações cadastrais do(a) Diretor(a) de *Compliance*, Riscos e PLDFT responsável por *Compliance*, Gestão de Riscos e PLDFT do Gestor:

Nome	SÉRGIO ALBINO BITAR PINHEIRO
E-mail	sergiobitarpinheiro@icloud.com.br

Por fim, o Gestor atesta que o(a) Diretor(a) de *Compliance*, Riscos e PLDFT não está subordinado às demais áreas de atuação, incluindo a gestão de recursos ou a área comercial.

[1] Da mesma forma, as mensagens de correio eletrônico profissional dos Colaboradores poderão ser interceptadas e abertas para ter a regularidade de seu conteúdo verificada, computadores poderão ser auditados e conversas telefônicas poderão ser gravadas e escutadas sem que isto represente invasão da privacidade dos Colaboradores, já que se tratam de ferramentas de trabalho disponibilizadas pelo Gestor, o que poderá ocorrer em qualquer momento que o(a) Diretor(a) de *Compliance*, Riscos e PLDFT julgue necessário.

8. Atualização

Este Manual será submetido à revisão anual ou em períodos inferiores a este, sempre que o(a) Diretor(a) de *Compliance*, Riscos e PLDFT considerar necessário, com o intuito de preservar as condições de segurança para o Gestor.

Versão	Data	Responsabilidade
3	25/03/2024	SÉRGIO ALBINO BITAR PINHEIRO

ANEXO I - SISTEMA DE GERENCIAMENTO E SEGURANÃ DE INFORMAÇÕES

O Gestor considera o gerenciamento das informações um assunto de âmbito estratégico, uma vez que as decisões que permeiam a gestão de seus ativos dependem da confiabilidade, segurança e acessibilidade ao sistema de gerenciamento de informações.

Para atingir estes objetivos, o Gestor estabeleceu regras de *Compliance* e de gestão de segurança em TI.

Gerenciamento de Informações Confidenciais

Quanto aos parâmetros de C*ompliance*, o Gestor define os perfis de acesso de cada usuário da rede interna de computadores de forma que as Informações Confidenciais fiquem acessíveis somente por determinadas pessoas do Gestor, autorizadas pelo(a) Diretor(a) de *Compliance*, Riscos e PLDFT. Ficam preservadas as informações de clientes e ao mesmo tempo evitam-se problemas relacionados a conflitos de interesses ou uso indevido de Informações Confidenciais.

Além disso, o controle de tráfego de dados entre Colaboradores é realizado por meio de sistemas de "*firewall*" e controle de acessos à rede de computadores, que são responsáveis pela proteção de Informações Confidenciais e pela segregação das informações entre os grupos de Colaboradores que a elas devem ter acesso. Tais controles são estabelecidos nas autorizações de perfis de acesso e restrição de usuários da rede. Dessa forma, controla-se quem efetivamente acessou determinados dados e/ou sistemas e ficam impedidos acessos não autorizados.

Assim, foram definidos níveis de acesso para os membros da área de *Compliance* e Riscos e Departamento Técnico.

No que se refere ao gerenciamento de riscos referentes à segurança da informação, o Gestor atuará por meio de rotinas elaboradas por prestadores de serviço especializados para assegurar um ambiente resguardado de qualquer tipo de risco para as informações e para a rede interna de computadores, evitando que a qualidade da gestão seja afetada por contingências.

Estrutura de Tecnologia de Informação e *Hardware*:

Em complemento às informações contidas no item acima, o Gestor terá uma rede integrada de computadores, revisados quanto à capacidade, segurança e nível de atualização de seus componentes, com o suporte técnico de empresa terceirizada contratada. Ainda, serão realizados "*backup*" mensal de arquivos em "*Hard Disk*" ("HD") externo e *backups* semanal e diário em servidores próprios, inclusive de e-mails. Além disso, serão adotados procedimentos contínuos relacionados aos *softwares* de antivírus, responsáveis por proteger, durante 24 (vinte e quatro) horas por dia, sem interrupção, a rede interna de computadores do Gestor e o computador de cada Colaborador.

Ainda, com relação aos e-mails, o Gestor utilizará equipamentos atualizados e seu servidor de e-mails será hospedado junto a Microsoft, através do *Exchange Online*, o que garantirá alta disponibilidade e segurança e viabilizará o trabalho remoto e via computadores reserva, se e quando necessário, sem prejuízo da manutenção de registros que irá viabilizar a realização de auditorias e inspeções nos termos dos manuais e políticas do Gestor.

No que tange aos *ids* dos Colaboradores e aos computadores, sua administração ocorrerá de forma centralizada através de servidor, onde (i) usuários e suas atividades podem ser monitorados; (ii) o particionamento das pastas é viabilizado; e (iii) os perfis de acesso são configurados conforme as prerrogativas e necessidades inerentes aos cargos dos Colaboradores.

Adicionalmente, com relação à estrutura de telefonia, o Gestor terá PABX com canais na sala de gestão, linha exclusiva para uso de fax e linhas móveis corporativas (para uso dos Colaboradores sempre que necessário) como meios de comunicação.

Por fim, todos os Colaboradores do Gestor terão acesso a atendimento relacionado aos sistemas de tecnologia da informação por diferentes canais, podendo optar pelo atendimento via telefone central, via celular dos colaboradores e, ainda, por meio de visitas periódicas e/ou emergenciais.