MANUAL DE SEGREGAÇÃO DE ATIVIDADES E SEGURANÇA DA INFORMAÇÃO

Novembro de 2025

FIDEM Asset

SUMÁRIO

1. OBJETIVO E ESCOPO DE ATUAÇÃO DO GESTOR

O presente Manual de Segregação de Atividades (doravante "Manual") da Fidem Asset Gestora de Recursos S.A. (doravante "Gestor") está em estrita conformidade com os artigos 27 e 28 da Resolução CVM nº 21, de 25 de fevereiro de 2021 (doravante "Resolução CVM 21").

O Manual estabelece os seguintes objetivos primários:

Objetivo Detalhamento da Segregação Funcional e segregação física das instalações entre a área de Gestão de Recursos e as áreas de Controles Internos (Compliance, Gestão de Riscos e Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo - PLDFT) e Administrativa (BackOffice).

Controle de Ativos para assegurar a utilização adequada e responsável das instalações, equipamentos e demais ativos comuns.

Confidencialidade da Informação para preservar a confidencialidade das informações sensíveis e viabilizar a identificação inequívoca dos indivíduos com acesso a tais dados.

Implementar mecanismos de restrição de acesso a arquivos e sistemas, permitindo a rastreabilidade e a identificação dos responsáveis pelo manuseio de informações confidenciais.

Adicionalmente, este Manual incorpora diretrizes de Segurança da Informação, as quais serão suportadas por prestadores de serviço especializados. Tal abordagem visa garantir um nível de eficiência e segurança compatível com as exigências regulatórias e as necessidades do Gestor, de seus Colaboradores, investidores e demais stakeholders, estabelecendo, ainda, a responsabilização dos envolvidos em casos de violação de dados ou vazamentos.

Não Exercício de Atividades de Distribuição e Intermediação

O Gestor concentra sua atividade na Gestão de fundos financeiros e Fundos de Investimento em Direitos Creditórios (FIDCs), utilizando-os como veículos de investimento para seus clientes.

Considerando que o Gestor não exercerá as atividades de distribuição de cotas de fundos de investimento sob gestão, tampouco a atividade de intermediação de valores mobiliários, a relevância de certas disposições deste Manual, relativas a conflitos de interesse inerentes à distribuição e intermediação, pode ser mitigada em comparação a outros participantes do mercado de capitais.

Não obstante, todas as disposições contidas neste Manual são de aplicação obrigatória a todos os sócios, Diretores e empregados do Gestor (doravante "Colaboradores").

2. ESTRUTURA

Diretor de Gestão	COMPLIANCE, RISCO
Luciano Corrêa Araski	Davi Cipriano (Compliance, Risco e PLDFT)

2.1. Segregação de Atividades e Segurança da Informação

Considerando a estrutura organizacional do Gestor, refletida neste Manual e no organograma societário, foram estabelecidas políticas e procedimentos aplicáveis à: (i) segregação física entre o Departamento Técnico e o Back-Office; (ii) implementação de barreiras de informação (Chinese Wall); e (iii) segurança da informação.

No que tange à segurança da informação, item (iii), a contratação de prestador de serviço especializado em tecnologia da informação será de responsabilidade do Back-Office. Este prestador será incumbido da implantação e otimização de processos, da manutenção dos sistemas de informática, da gestão da segurança da informação — incluindo o controle de acesso de usuários — e da execução de rotinas de cópia de segurança (backup) dos dados.

3. SEGREGAÇÃO FÍSICA

O acesso às instalações físicas destinadas à equipe de gestão de carteiras de valores mobiliários é estritamente controlado e restrito aos colaboradores devidamente autorizados. A referida área está localizada em um ambiente fisicamente isolado das demais dependências do Gestor, comunicando-se exclusivamente com os serviços auxiliares indispensáveis à atividade de gestão, de modo a garantir sua completa segregação de quaisquer outros setores que possam exercer atividades distintas no âmbito do mercado de capitais.

O acesso de pessoas não envolvidas diretamente na atividade de gestão de carteiras de valores mobiliários às instalações da área de gestão é vedado, salvo em circunstâncias excepcionais e previamente autorizadas.

4. BARREIRA DE INFORMAÇÃO (CHINESE WALL)

A política de Chinese Wall tem por finalidade instituir uma barreira robusta de comunicação entre diferentes áreas e colaboradores do Gestor. O objetivo é assegurar a estrita observância das normas regulatórias que determinam a segregação entre a atividade de administração de carteiras de valores mobiliários e outras atividades exercidas no mercado de capitais, bem como a separação entre os ativos financeiros próprios do Gestor e os pertencentes a terceiros.

Como regra geral, as restrições de acesso a informações e documentos, tanto em formato físico quanto digital, contidos na rede de computadores e nos sistemas do Gestor, seguem as divisões funcionais delineadas no organograma apresentado no item 2 deste Manual. Eventuais exceções a esta regra deverão ser submetidas à apreciação do(a) Diretor(a) de Compliance, Riscos e PLD/FT, mediante solicitação formal e fundamentada que demonstre a necessidade e a ausência de conflitos de interesse.

5. POLÍTICA DE CONFIDENCIALIDADE, SIGILO E SEGURANÇA DA INFORMAÇÃO

5.1. Informações Confidenciais

No exercício de suas funções, os Colaboradores poderão ter acesso a informações relativas aos clientes do Gestor e a terceiros que não sejam de domínio público, sendo, portanto, classificadas como "Informações Confidenciais".

É expressamente vedada a divulgação de qualquer Informação Confidencial a terceiros, seja para benefício próprio ou de outrem, ainda que não haja a intenção de auferir vantagem. A obrigação de confidencialidade aqui estabelecida possui caráter perene, mantendo-se vigente mesmo após o término do vínculo profissional do Colaborador com o Gestor.

O Gestor e seus Colaboradores possuem o dever legal e fiduciário de zelar pelo sigilo das Informações Confidenciais de seus clientes. Qualquer solicitação, tentativa ou ação que vise à quebra deste sigilo deverá ser imediatamente comunicada ao Diretor de Compliance, Riscos e PLDFT.

5.2. Informações Sigilosas

Para os fins deste Manual, consideram-se "Informações Sigilosas", além das Informações Confidenciais, todos os dados e informações cuja divulgação possa comprometer o nível de segurança ou a integridade operacional do Gestor.

A perda, o uso indevido, a alteração ou o acesso não autorizado a Informações Sigilosas podem acarretar prejuízos à privacidade de indivíduos, impactar negativamente transações comerciais, macular a reputação do Gestor e comprometer a continuidade de suas operações.

O Gestor reitera sua responsabilidade legal de proteger o sigilo de seus clientes. Portanto, informações relativas a clientes e às entidades investidas pelos fundos de investimento sob gestão não poderão ser compartilhadas com terceiros, excetuando-se as hipóteses de requisição formal por parte de órgãos públicos, entidades reguladoras ou do Poder Judiciário, casos em que o compartilhamento se dará nos estritos limites da ordem recebida.

5.3. Segurança da Informação

As medidas de segurança da informação visam proteger os ativos informacionais do Gestor contra ameaças, garantindo a continuidade dos negócios, a minimização de riscos operacionais e a maximização dos retornos sobre os investimentos.

A implementação e a manutenção de tais medidas são de responsabilidade do serviço terceirizado de tecnologia da informação, cuja supervisão compete ao Back-Office, conforme detalhado em seções subsequentes deste Manual. A observância das diretrizes de segurança é obrigatória para todos os Colaboradores.

Identificam-se como situações de risco à Segurança da Informação, entre outras:

(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.

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

6. MECANISMOS DE REPORTE, SANÇÕES E RESPONSABILIDADES

6.1. Dever de Comunicação e Medidas Disciplinares

É dever de todo Colaborador comunicar prontamente ao Diretor de Compliance, Riscos e PLDFT a ocorrência ou a suspeita de qualquer violação às disposições contidas neste Manual, incluindo, mas não se limitando, às regras de Segregação Física, Chinese Wall e Segurança da Informação.

O descumprimento de qualquer política ou procedimento aqui estabelecido sujeitará o infrator a medidas disciplinares, a serem aplicadas a critério do Diretor de Compliance, Riscos e PLD/FT, com base na gravidade da infração e na eventual reincidência. As sanções incluem: (i) Advertência formal por escrito; ou (ii) Desligamento por justa causa.

Qualquer Colaborador que tenha violado este Manual, ou que possua conhecimento de uma violação, deve notificar o fato de forma direta e imediata ao Diretor de Compliance, Riscos e PLD/FT. A cooperação e a comunicação voluntária serão consideradas na avaliação de eventuais medidas disciplinares.

Ações disciplinares também poderão ser aplicadas contra Colaboradores que: a) Autorizem, coordenarem ou participem de violações a esta Política; b) Deixem de reportar violações das quais tenham conhecimento ou suspeita; c) Omitam-se no dever de reportar violações que, em razão de suas atribuições funcionais, deveriam ter identificado; ou d) Promovam ou incentivem, direta ou indiretamente, qualquer forma de retaliação contra denunciantes.

6.2. Responsabilidade pela Gestão de Terceiros

No que tange à Segurança da Informação, a responsabilidade pela contratação, supervisão e fiscalização do prestador de serviços terceirizado recai sobre o Back-Office. Este departamento conduzirá o processo de due diligence para a seleção de fornecedores, em conformidade com os critérios estabelecidos no Manual de Compliance e demais normativos internos, e realizará o monitoramento contínuo e a avaliação qualitativa dos serviços prestados.

6.3. Monitoramento e Acompanhamento

Diante da ocorrência, suspeita ou indício de descumprimento de quaisquer regras estabelecidas neste Manual, compete ao Diretor de Compliance, Riscos e

PLD/FT a apuração dos fatos, utilizando-se, para tanto, dos registros eletrônicos e demais evidências disponíveis para verificar a conduta dos Colaboradores.

Para fins de investigação e auditoria, o Diretor de Compliance, Riscos e PLD/FT possui autorização para acessar todo o conteúdo armazenado na rede de computadores e sistemas do Gestor. O acesso a tais informações será realizado de forma criteriosa, respeitando a confidencialidade e utilizando os dados exclusivamente para fins legais e regulatórios, a fim de identificar os responsáveis por eventuais infrações e vazamentos de informação.

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 Davi Cipriano

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.

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
1	05/11/2025	Davi Cipriano

ANEXO I – SISTEMA DE GESTÃO E SEGURANÇA DAS INFORMAÇÕES

O Gestor reconhece o Gerenciamento das Informações como um pilar estratégico para a condução de seus negócios, dada a dependência crítica da confiabilidade, segurança e acessibilidade dos dados para o processo decisório e a gestão de ativos.

Para a consecução destes objetivos, o Gestor estabelece diretrizes de Compliance e de Gestão de Segurança da Tecnologia da Informação (TI).

1. Gerenciamento de Informações Confidenciais

No âmbito do Compliance, o Gestor implementa perfis de acesso individualizados para cada usuário da rede interna de computadores. Esta medida garante que as Informações Confidenciais sejam acessíveis exclusivamente por Colaboradores previamente autorizados pelo Diretor de Compliance, Riscos e PLD/FT.

Este controle visa a preservação do sigilo das informações de clientes e a prevenção de potenciais conflitos de interesse ou do uso indevido de Informações Confidenciais.

Adicionalmente, o controle do tráfego de dados entre os Colaboradores é realizado por meio de sistemas de firewall e mecanismos de controle de acesso à rede, que são responsáveis pela proteção das Informações Confidenciais e pela efetiva segregação das informações entre os grupos de Colaboradores que detêm o direito de acesso. Tais controles são parametrizados nas autorizações de perfis de acesso e nas restrições de usuários da rede, permitindo o rastreamento (log) de quem acessou dados ou sistemas específicos e impedindo acessos não autorizados.

Neste sentido, foram definidos níveis de acesso distintos para os membros da área de Compliance e Riscos e do Departamento Técnico, em observância ao princípio do need-to-know.

2. Gerenciamento de Riscos de Segurança da Informação

O Gestor adota uma postura proativa no gerenciamento de riscos de segurança da informação. Para tanto, atuará por meio de rotinas e procedimentos elaborados e executados por prestadores de serviço especializados em TI, visando assegurar um ambiente operacional resguardado contra qualquer tipo de risco que possa comprometer a integridade das informações e da rede interna de computadores, mitigando contingências que possam afetar a qualidade da gestão.

3. Estrutura de Tecnologia da Informação e Hardware

Em complemento às diretrizes de segurança, o Gestor manterá uma rede integrada de computadores, submetida a revisões periódicas quanto à capacidade, segurança e nível de atualização de seus componentes, com o suporte técnico de empresa terceirizada contratada.

Serão implementadas rotinas de backup nos seguintes termos:

- Mensal: Cópia de segurança de arquivos em Hard Disk (HD) externo.

- Semanal e Diário: Cópia de segurança em servidores próprios, incluindo o backup de e-mails.

Adicionalmente, serão adotados procedimentos contínuos relacionados aos softwares de antivírus, responsáveis por proteger, ininterruptamente (24 horas por dia), a rede interna e os dispositivos individuais de cada Colaborador.

Com relação ao sistema de correio eletrônico (e-mail), o Gestor utilizará equipamentos atualizados e seu servidor será hospedado em ambiente de alta disponibilidade e segurança, como o Exchange Online da Microsoft. Essa escolha garante a alta disponibilidade do serviço, viabiliza o trabalho remoto e a utilização de computadores reserva, quando necessário, e assegura a manutenção de registros que suportarão auditorias e inspeções, em conformidade com as políticas internas e regulamentares.

A administração dos identificadores de Colaboradores (IDs) e dos computadores ocorrerá de forma centralizada por meio de um servidor, o que permite:

- O monitoramento das atividades dos usuários.
- O particionamento seguro de diretórios (pastas).
- A configuração dos perfis de acesso em estrita observância às prerrogativas e necessidades inerentes aos cargos dos Colaboradores.

4. Estrutura de Comunicação e Suporte

No que concerne à estrutura de telefonia, o Gestor disporá de um sistema PABX com canais dedicados na sala de gestão, uma linha exclusiva para a utilização de fax e linhas móveis corporativas para uso dos Colaboradores, conforme a necessidade de comunicação.

Por fim, será garantido a todos os Colaboradores acesso a suporte técnico relacionado aos sistemas de tecnologia da informação por meio de múltiplos canais, incluindo telefone central, contato direto com o celular dos técnicos e, ainda, por meio de visitas técnicas periódicas e/ou emergenciais.