HORIZONTES ASSET LTDA.

POLÍTICA DE SEGREGAÇÃO, CONFIDENCIALIDADE E BARREIRAS DE INFORMAÇÃO

Versão	2.0
Data-base	Maio/2026
Elaboração	Projeto de estruturação jurídico-regulatória e de governança
Classificação	Documento interno / base institucional para uso regulatório, autorregulatório e de diligência.
Objetivo	Disciplinar a circulação de informações, a segregação entre áreas e os controles de acesso da gestora.
Abrangência	Sócios, diretores, equipe interna, participantes de comitês, terceiros alocados e prestadores que recebam documentos ou dados da gestora.
Responsável	Diretoria de Compliance, Risco e PLD/FTP, com apoio do middle office e da diretoria executiva.
Aprovador	Diretoria estatutária e Comitê de Compliance, PLD/FTP e Controles Internos.
Base normativa principal	Resolução CVM 21, arts. 24, 27 e 28; Regras e Procedimentos ANBIMA de Deveres Básicos; governança interna da gestora.

1. Finalidade e desenho das barreiras de informação

Esta política estabelece como a HORIZONTES ASSET LTDA. organizará a circulação de informações, a segregação de funções, os controles de acesso e a prevenção de uso indevido de informação privilegiada, informação sensível ou informação proprietária. O objetivo é assegurar que cada pessoa acesse apenas o que precisa para desempenhar sua função, que conflitos sejam identificados antes de contaminarem a decisão e que a independência das funções de compliance, risco e PLD/FTP seja material e demonstrável.

A política foi desenhada para uma estrutura enxuta, porém institucional, e para um estágio em que a gestora passará a operar nos próximos 60 dias com FIDC consignado público

e privado, fundo imobiliário e fundo multimercado. A combinação dessas estratégias exige cuidado reforçado porque reúne, em uma mesma casa, análise de crédito, relacionamento com cedentes e estruturadores, diligência de ativos reais, eventual interação com securitizadoras, negociação em mercados líquidos e produção de material para investidores e prestadores.

2. Segregação funcional por núcleo

A área de gestão é responsável por análise econômica, seleção de ativos, construção de tese, acompanhamento de portfólio, interação técnica com comitês de investimento e preparação de ordens. A área de modelagem apoia o núcleo de gestão, assim como a área da vertical imobiliária, que somente participa de decisões relacionadas a FII, ativos reais, créditos imobiliários, CRI e temas correlatos. O acesso desses profissionais deve refletir sua necessidade técnica, sem abertura indiscriminada a documentos de compliance, arquivos de denúncias, relatórios de monitoramento sensível ou bases de natureza administrativa que não guardem relação com sua atuação.

A Diretoria de compliance responde por compliance, risco e PLD/FTP de forma independente. Sua função não se confunde com a tomada de decisão de investimento nem com a execução operacional. Isso significa, na prática, que ela deve ter livre acesso à informação necessária para testar, monitorar e questionar a atividade da gestora, sem depender de autorização da área de gestão; ao mesmo tempo, não pode ser capturada pelo racional comercial ou econômico das áreas monitoradas. O middle office deve apoiar reconciliação, arquivo, registros, execução operacional e interface com prestadores, sem substituir o juízo independente de risco ou compliance. Por fim, há apoio administrativo e documental da área administrativa, com acesso apenas aos repositórios necessários à formalização, agenda regulatória e arquivo.

3. Fluxos sensíveis e trilhas reforçadas

Serão considerados fluxos sensíveis, entre outros, os dossiês de crédito, os arquivos de cessão e elegibilidade de FIDC, as bases de inadimplência, os materiais de comitê, as listas restritas de negociação pessoal, os registros de incidentes, os relatórios de PLD/FTP, os mapas de conflito, os materiais públicos ainda não aprovados, os documentos de originação e estruturação, os arquivos de diligência imobiliária, os pareceres jurídicos, os dados pessoais e os registros operacionais cuja divulgação indevida possa afetar o mercado, o investidor ou a própria gestora.

Documentos relacionados a CRI, FII, ativos reais e estruturação imobiliária receberão marcação de sensibilidade reforçada quando houver atuação prévia ou paralela do time em estruturação, originação, consultoria ou negociação do ativo fora do veículo gerido. Nesses casos, o acesso técnico será restrito aos profissionais necessários para a análise, e o processo deverá ser acompanhado pela Diretoria de Compliance desde o início, com formação de trilha documental específica para conflito e independência.

4. Controles de acesso, repositórios, terceiros e ambiente digital

Os repositórios eletrônicos da gestora deverão ser organizados por pastas de governança, gestão, risco, PLD/FTP, middle office, societário, terceiros, recursos humanos, produtos em implantação e veículos ativos. O acesso será concedido por perfil e revisto periodicamente. Não se admite compartilhamento informal de credenciais, uso de contas genéricas, envio indiscriminado de documentos sensíveis por aplicativos não controlados nem armazenamento disperso de versões críticas.

Os repositórios eletrônicos da Gestora são hospedados em ambiente corporativo de nuvem (Amazon Web Services - AWS), com autenticação centralizada via Active Directory corporativo e acesso remoto exclusivo por VPN com autenticação multifator (MFA via TOTP). A segregação lógica é materializada pelas seguintes camadas técnicas: (i) Unidades Organizacionais (OUs) e grupos do Active Directory, definidos por núcleo funcional (gestão, compliance/risco/PLD-FTP, middle office, administrativo, vertical imobiliária); (ii) permissões NTFS no file server corporativo, atreladas aos grupos do AD; (iii) Group Policies (GPOs) que aplicam regras de segurança e mapeamento de drives por perfil; e (iv) Security Groups específicos por componente da infraestrutura. A revisão semestral dos privilégios é conduzida pela Diretora de Compliance, Risco e PLD/FTP em conjunto com o prestador de TI contratado, com revogação imediata de acessos de pessoas desligadas. Os prestadores críticos de tecnologia da informação atualmente contratados (BAlves Gestão em TI, Manucom Tecnologia Ltda. e Nullpointer) estão sujeitos aos critérios estabelecidos no item 5 da Política de Segurança Cibernética.

Prestadores de nuvem, sistemas, administrador fiduciário, custodiante, controladoria, plataformas de assinatura, data rooms e quaisquer terceiros que recebam ou processem documentos da gestora deverão estar cobertos por contrato com cláusulas de confidencialidade, segurança, cooperação regulatória, devolução ou destruição de dados e comunicação de incidentes. O Middle office e área administrativa apoiarão o controle operacional desses acessos; A Diretoria de Compliance supervisionará sua aderência; A Diretoria Executiva aprovará contratações críticas.

5. Treinamento, monitoramento e resposta a desvios

Todos os profissionais e terceiros abrangidos deverão receber treinamento inicial e reciclagens periódicas sobre confidencialidade, informação privilegiada, uso de listas, tráfego de documentos, arquivos sensíveis e barreiras de informação. O treinamento deve ser específico o suficiente para refletir a realidade da gestora: um profissional que atue com FIDC precisa compreender riscos de dados de devedores e de cessão; quem atue com FII e CRI precisa compreender riscos de originação, estruturação e diligência imobiliária; quem atue com multimercado precisa compreender riscos de ordens em preparação e alinhamento entre gestão e execução.

O treinamento contempla também conteúdo sobre uso da infraestrutura tecnológica da Gestora, manejo seguro de credenciais, vedação ao compartilhamento de senhas e procedimentos de reporte de incidentes de segurança da informação ou de dados pessoais.

Qualquer violação, suspeita de violação ou fragilidade relevante identificada em acesso, compartilhamento, armazenamento, transporte ou uso de informação deverá ser tratada como incidente de governança. O fato será registrado, apurado e submetido à resposta proporcional, que poderá incluir reforço de controle, mudança de acesso, treinamento adicional, apuração disciplinar, reporte aos sócios e, quando cabível, medidas externas.

Em caso de violação ou suspeita de violação envolvendo dados pessoais, o tratamento observará adicionalmente o disposto na Política de Segurança Cibernética, com acionamento da Encarregada pelo Tratamento de Dados Pessoais (DPO), Diretora de Compliance, Risco e PLD/FTP, Natália Uchôa Brandão, para fins de avaliação de impacto, comunicação à ANPD e comunicação aos titulares afetados, quando aplicável.

Histórico de revisões

Versão	Data-base	Aprovação	Principais alterações
1.1	14/04/2026	Diretoria Executiva	Versão anterior em vigor.
2.0	**Maio/2026**	**Diretoria Executiva**	**Inclusão, no item 4, de parágrafo detalhando a segregação lógica via Active Directory, Group Policies (GPOs), permissões NTFS e Security Groups, com infraestrutura hospedada em AWS, e citação nominal dos prestadores críticos de TI (BAlves, Manucom,**

Versão	Data-base	Aprovação	Principais alterações
			Nullpointer). Inclusão, no item 5, de parágrafo sobre treinamento em segurança da informação e manejo seguro de credenciais. Inclusão, no item 5, de parágrafo sobre tratamento de incidente envolvendo dados pessoais com acionamento da Encarregada pelo Tratamento de Dados Pessoais (DPO/LGPD) — Natália Uchôa Brandão.

Aprovação

São Paulo, 19 de maio de 2026.

IRAPUA DE CARVALHO DANTAS:00800251458

Assinado de forma digital por IRAPUA DE CARVALHO DANTAS:00800251458

Irapuã de Carvalho Dantas
Diretor Executivo
Horizontes Asset Ltda.