# POLÍTICA DE CONTROLE DE INFORMAÇÕES CONFIDENCIAIS

ALFA

novembro/2022

## Índice

## 1. OBJETIVO

A presente Política objetiva estabelecer as regras para minimizar eventuais riscos decorrentes do acesso a informações confidenciais por parte dos envolvidos direta e/ou indiretamente nas atividades de administração de carteiras de valores mobiliários. Juntamente com o monitoramento da área de controles internos, objetivam controlar as práticas de negócio abrangendo os recursos humanos e tecnológicos.

## 2. ABRANGÊNCIA

A presente Política deve ser rigorosamente observada pelas seguintes áreas:

- ✓ Diretoria de *Asset Management*;
- ✓ Diretoria de Administração Fiduciária.

## 3. CONTROLES FÍSICOS E LÓGICOS

As Diretorias de *Asset Management* e de Administração Fiduciária possuem acesso restrito, apenas seus funcionários as acessam por meio de controle de acesso biométrico e sistema de cadastro e monitoramento dos usuários.

É expressamente proibida a presença ou circulação de pessoas estranhas ao ambiente das áreas abrangidas sem a prévia autorização e/ou acompanhamento de um Gerente. O acesso deve ser restrito aos integrantes da área e aos respectivos Diretores.

Os sistemas utilizados possuem controle de acesso com permissões concedidas pelos administradores dos sistemas, mediante solicitação do gestor do usuário e com controle e revisão da Área de TI - Administração da Rede. O usuário necessariamente deve ser habilitado na Rede Corporativa da instituição e as permissões de acesso aos sistemas são controladas por perfis previamente definidos.

As informações geradas dos sistemas de gestão e controle de ordens OMNIS - Nexxus, OMNIS Atribuição de Performance, OMNIS Enquadramento, Sistema Carteira e do sistema de passivo (CRK Cotista) são registradas em áreas pré-definidas e sem a possibilidade de edição. Da mesma forma, as informações encaminhadas pelos custodiantes, que serão importadas para os sistemas citados, possuem a mesma restrição.

As informações são classificadas conforme sua criticidade e sensibilidade possibilitando um nível adequado de proteção para a informação.

As áreas abrangidas possuem acessos restritos na Rede Corporativa que são acessados somente pelos funcionários previamente definidos pelos seus gestores e passam por revisão semestral.

Os acessos concedidos passam por revisões periódicas. Eventuais distorções são submetidas ao gestor do usuário e os acessos são bloqueados até que se esclareçam as eventuais divergências.

Os funcionários desligados são informados pelo Departamento de Cultura, Gente & Gestão à Área de TI - Administração da Rede que efetua a inativação de acesso à Rede Corporativa e os gestores dos sistemas conduzem a inativação em seus respectivos sistemas. No caso de transferências internas, os acessos são revogados, cabendo ao novo gestor do usuário solicitar os acessos necessários à nova função.

Adicionalmente aos controles descritos acima, todos os funcionários, sem exceção, devem seguir as diretrizes da Política de Segurança da Informação e Cibernética.

## 4. SIGILO BANCÁRIO

As informações privilegiadas de clientes e/ou das operações com ativos dos fundos de investimento e carteiras administradas, sejam elas cadastrais, econômico-financeiras ou de valores, devem ser tratadas com absoluto sigilo e discrição, sendo terminantemente proibida qualquer divulgação fora dos ambientes das áreas abrangidas e estritamente necessárias às atividades.

No que se refere à remessa de posições de investimentos, contratos e outros documentos, devem ser tomadas as devidas precauções no que concerne ao correto endereçamento e adequado fechamento dos envelopes, inclusive colocando-os em envelope plástico de segurança.

É terminantemente proibido o envio de extratos e posições de clientes, por e-mail, sem o travamento por senha previamente pactuada.

As ligações telefônicas para a troca de informações sobre a negociação de ativos poderão ser gravadas.

O envio e o recebimento de informações de ativos dos fundos e carteiras administradas devem ser realizados exclusivamente por meio dos sistemas disponibilizados pelos custodiantes contratados.

As áreas de homologação de sistemas devem conter a base de dados com os dados de clientes de forma mascarada, de modo que os prestadores de serviços de TI não tenham acesso a esses dados.

## 5. PADRÃO DE CONDUTA

Todos os integrantes das áreas abrangidas devem observar fielmente o **Código de Ética e Conduta do Conglomerado Alfa.** Este documento é entregue a cada funcionário quando da sua contratação ou quando da atualização do Código, sob protocolo. Está também disponível no Portal Corporativo, no menu "Livro Azul".

### a. SIGILO

As informações sobre as atividades das áreas abrangidas devem ser mantidas sob absoluto sigilo e confidencialidade, inclusive em relação às outras áreas do Conglomerado Alfa. Os funcionários das áreas abrangidas devem ter plena e total

consciência desta política, que deve ser reforçada pelos Gestores das áreas durante as reuniões periódicas. Os novos contratados devem ser orientados pessoalmente pelas suas Chefias sobre esta política.

### b. TERMOS

Os funcionários das áreas abrangidas devem assinar os termos de confidencialidade, além do já citado Código de Ética e Conduta do Conglomerado Alfa. Cabe ao Gerente providenciar as assinaturas no primeiro dia de trabalho do funcionário na Gerência.

## 6. INFORMAÇÕES PRIVILEGIADAS

Não é permitida em hipótese alguma, a troca de informações com áreas igualmente detentoras de informações privilegiadas.

Os gestores das áreas abrangidas devem estar sempre atentos às conversas e atitudes da sua equipe e levar ao conhecimento do seu respectivo Diretor ou da Auditoria Interna, qualquer desvio de conduta que venha a ser detectado.

## 7. CONTROLES INTERNOS

A Gerência Geral de *Compliance* é a responsável por implantar controles internos voltados às atividades por ela desenvolvidas, incluindo os sistemas de informações, e realizar o monitoramento adequado.

A presente política deverá ser revisada com periodicidade mínima anual.