POLÍTICA DE CONTROLES INTERNOS E COMPLIANCE

URBANO ADMINISTRAÇÃO DE RECURSOS LTDA.

SUMÁRIO

1. OBJETIVO

A política de Controles Internos **("Política")** tem por objetivo descrever a estrutura e metodologia utilizada pela **URBANO ADMINISTRAÇÃO DE RECURSOS LTDA.**, **("Gestora"),** referente a gestão de controles internos e riscos, com o objetivo de entender seu perfil, suas características, e a classificação de riscos inerentes aos principais processos da Gestora, além de estabelecer regras, procedimentos e descrição dos controles a serem observados como parâmetros para o funcionamento dos sistemas de Controles Internos e Compliance da Gestora.

As orientações contidas nesta Política devem ser seguidas por todos os colaboradores da Gestora, independentemente do nível hierárquico.

Seu conteúdo visa garantir o permanente atendimento às normas, políticas e regulamentações vigentes, bem como disseminar a cultura de controles para garantir o cumprimento das normas estabelecidas pelos órgãos reguladores e autorreguladores, e não tem como objetivo o tratamento exaustivo de toda a regulação aplicável às suas atividades.

Qualquer solicitação que envolva orientação ou esclarecimento de temas relacionados a controles internos, ou Compliance deve ser enviada para o e-mail: compliance@urbano.com

A Missão da Gestora preza em atender as demandas de seus clientes de forma segura, transparente e eficiente, por meio de equipe qualificada e experiente, tendo como principais diferenciais os processos e controles exclusivos, desenvolvidos internamente, a partir do conhecimento adquirido ao longo de sua atuação no setor.

O Valor da Gestora preza pela ética em todas as situações, respeitando sempre o ordenamento jurídico nacional e os interesses dos clientes acima dos pessoais. Além de empenho e desenvolvimento técnico da sua equipe interna como o instrumento habilmente aplicado para a obtenção dos melhores resultados, e o relacionamento interno e externo baseado na transparência, confiança e seriedade.

2. ABRANGÊNCIA

De modo a assegurar que todos os colaboradores, independentemente de nível hierárquico e prestadores de serviços, parceiros e fornecedores diretos obtenham conhecimento sobre as políticas, os manuais e os procedimentos adotados pela Gestora, no ato da contratação se faz obrigatória a disponibilização uma cópia do Código de Conduta e Ética Profissional, sendo solicitada, ainda sua adesão e concordância formal.

Adicionalmente, o colaborador, prestador de serviços, parceiros e fornecedores diretos são instruídos a ler as políticas e os manuais disponíveis no website da Gestora.

3. DIRETRIZES

A presente Política deve assegurar o cumprimento das normas, regulamentos e aderência às políticas, os manuais e os procedimentos internos, além de disseminar a cultura sobre a importância dos controles internos.

A Gestora através desse material deve envidar esforços para alinhar a estrutura dos controles internos aos riscos e objetivos do negócio, sendo revisado e atualizado periodicamente de forma a garantir sua efetividade.

Definir e controlar a Governança Corporativa, atribuindo responsabilidades e delegação da autoridade à estrutura hierárquica da Gestora.

Esta política deverá ainda, apresentar as definições necessárias à implantação das funções de Compliance, estabelecendo suas políticas, indicadores de gestão de Controles Internos e os procedimentos/processos de cada área da Gestora para monitorar, de forma pró-ativa e periódica, as funções e áreas da organização, visando a detecção de problemas em potencial e riscos não identificados anteriormente.

Os principais indicadores utilizados pela Gestora, mas não se limitando a eles, serão:

- Avaliações do negócio principal da Gestora (Recursos de Terceiros);
- Avaliação dos negócios secundários (Carteira de Clientes)
- Avaliação de riscos operacionais (riscos por processos)
- Principais indicadores de eficácia dos controles (testes de controles)

Os departamentos internos da Gestora serão responsáveis por desenvolver processos para identificar, medir, monitorar e controlar riscos inerentes a cada um de seus macro processos, com o apoio do departamento de controles Internos e Compliance. Os Controles Internos necessitam de permanente revisão para abranger situações não previstas inicialmente, e os riscos devem ser avaliados segundo sua natureza.

O monitoramento dos riscos e testes de controles serão os instrumento de aferição da qualidade dos processos e das atividades de controle implementadas, permitindo a elaboração e implantação de um plano de melhoria contínua sempre que necessário. Resuntando em melhor desempenho funcional e organizacional, mitigaão de riscos legal, operacional e reputacional, melhoria contínua e qualidade de produtos e serviços.

A implantação de Controles Internos na Gestora deverá atender necessariamente a dois requisitos de forma simultânea, sendo:

1) Identificação dos riscos, área, processo, probabilidade e impacto para a empresa e negócio;
2) Redução dos custos para evitar incorrer em tais riscos.

Após aplicar os dois pontos acima descritos a área de controles internor, deverá analisar os seguintes itens:

a) Identificar a área ou fator de risco mais relevante da Gestora;
b) Determinar valores qualitativos e quantitativos sobre o risco identificado;
c) Avaliar quais são os responsáveis pelo processo e risco em análise;
d) Definir os mecanismos que serão utilizados para tratar as regras, planos de ações, pontos de controle e critérios de monitoramento e regras;

Ao executar essas atividades consideramos que a área de controles internos possui a estrutura da Matriz de Riscos da Empresa. Assim deve ser aplicado o conceito de classificaão desse risco, considerando critérios de classificação de dois itens:.

Probabilidade de ocorrência, e impacto do negócio, que podem ser classificados em cinco níveis:

	Muito Baixo
	Baixo
	Médio
	Alto
	Muito Alto

Tendo o resultado visual dessa matriz de riscos, a Diretoria de Compliance terá condições de aplicar testes e plano de ações corretivos ou mitigadores de riscos com base na criticidade de acada risco evidenciado.

3.1. CONTROLES INTERNOS E GOVERNANÇA CORPORATIVA

Os conceitos de Controles Internos e Governança Corporativa estão fundamentados na segregação de funções/atividades/responsabilidades, de forma a atender as estruturas do negócio e de suporte, permitindo a estruturação de fluxos operacionais dos processos (macros e fluxos detalhados).

Os processos do negócio são aqueles que estão alinhados com as necessidades dos clientes, e cujos resultados podem afetar a imagem da instituição e a fidelização/satisfação dos clientes. Os processos operacionais, que são aqueles que dão embasamento aos processos do negócio.

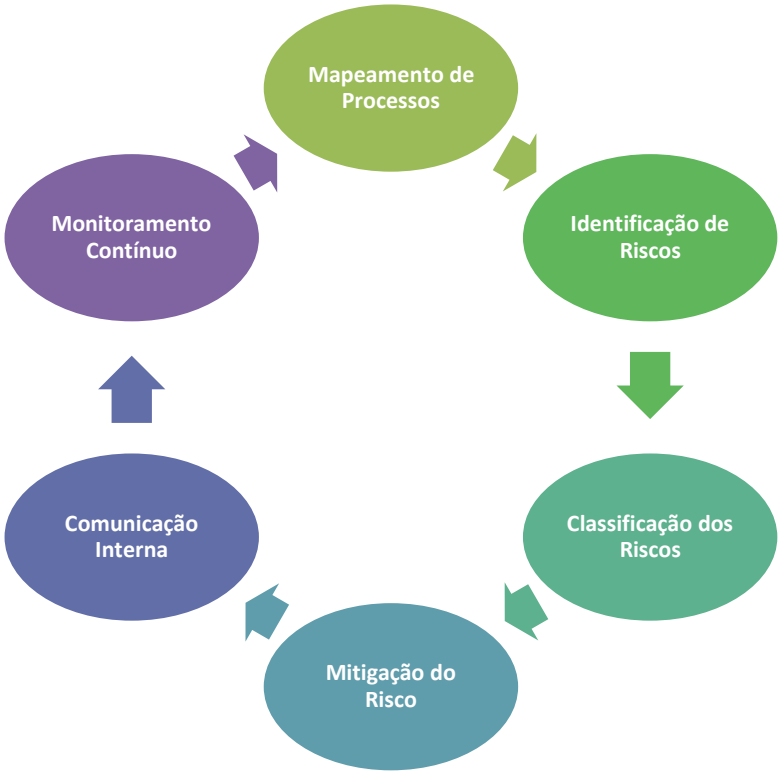
A estrutura de Controles Internos e Governança Corporativa deve possuir robustez suficiente de forma que possa indicar que os processos do negócio e de suporte possuam segurança suficiente para serem executados, de forma a entregar os melhores produtos e serviços aos clientes, prover mecanismos adequados de gerenciamento e controle para os níveis de gestão definidos, informar as pessoas envolvidas sobre a expectativa da sua contribuição para a cadeia de relacionamentos, e assegurar aderência aos comandos regulatórios.

A apuração dos Controles Internos envolvidos a seguinte descrição:

DIRETRIZ	OBJETIVOS	MATERIAL/DOCUMENTOS
Negócio	• Produtos • Serviços	• Planejamento Estratégico • Plano de Negócios – Business Plan
Econômico	• Metas • Resultado	• Mapa de Metas • Orçamento Anual / Budget • Gestão de Riscos • Políticа de Investimentos
Produto	• Tipificação • Compliance • Controles Internos	• Mapa de produto • Topologia do produto • Critérios do regulador • Gestão de Riscos
Imagem	• Percepção e aceitação da gestora pelo mercado • Reconhecimento / Reputação	• Política de Conduta e Ética • Aderências as diretrizes regulatórias
Informação	• Integridade de dados • Confidencialidade • Continuidade	• PCN • Política de SI e Backups íntegros • Gestão de Acesso
Governança	• Responsabilidades definidas • Alçadas delimitadas	• Política de Governança • Organogramas atualizados • Manuais Operacionais Gestão de Acesso

3.2. Metodologia

A Diretoria de Compliance deve atuar de forma ativa para avaliar os riscos operacionais, os instrumentos de controle e minimização dos riscos identificados e desenvolver ações para monitorar os riscos identicados e aceitos pela diretoria executiva e acionistas. Tal qual a metedologia COSO – ERMII define em seu FRAMEWORK.



3.2.1. Atividades de Compliance

A Diretoraia de Compliance e respectiva equipe deve estabelecer as rotinas de fiscalização e de monitoramento sob a responsabilidade do Diretor de Risco, Compliance e PLD de cumprimento das definições impostas pelas políticas internas da empresa, assim como pelas diretrizes dos reguladores e autoreguladores;

Considerando ainda as atividades impostas para a área de Compliance esses deverá estabelecer a segregação das atividades das Gestora visando manter o sigilo e a segregação de informações a que os Colaboradores e Diretores tenham acesso no exercício das suas funções, bem como evitar a existência e disciplinar as situações que impliquem em conflitos de interesses entre as atividades desempenhadas pelas Gestora; e

A atuação com imparcialidade com os Colaboradores, Diretores, prestadores de serviços e demais parceiros da Gestora se faz indispensável.

3.2.2. Regras e Procedimentos Relativos à Segregação de Atividade

A Gestora reconhece a existência do risco de potencial conflito de interesse, para tais situações adotará a política de "Chinese Wall" entre as suas Áreas de Atuação com a finalidade de prevenir o uso impróprio de Informações Confidenciais, relevantes e/ou não públicas e que possam ter impacto no preço de um ativo a ser adquirido pelos fundos de investimento sob sua administração fiduciária e/ou gestão.

A gestão adequada destas informações é particularmente importante para a Gestora, uma vez que o uso indevido de tais informações expõe a Gestora a sérios riscos legais, de imagem e financeiros.

Em face às atividades que compõem o objeto social da Gestora, nos termos dos seus documentos societários, as atividades e áreas da Gestora ("Áreas de Atuação") e empresas do grupo que geralmente são ou podem estar expostas aos conflitos de interesse acima mencionados, refere-se ao exercício de atividades de gestão de recursos de terceiros, bem como a atuação nos mercados financeiro e de capitais como gestor de carteiras administradas e de fundos de investimento em geral, nos termos da regulamentação aplicável ("Gestão de Recursos de Terceiros"), cuja responsabilidade estará aos encargos do "Diretor de Gestão"; e

Considerando que dificilmente uma política consegue prever todas as situações possíveis, é necessário o uso do bom senso e discernimento ao encontrar situações não previstas nesta política. Quando houver dúvidas referente a alguma questão, os Diretores e os Colaboradores da Gestora deverão buscar orientação do Diretor de Risco, Compliance e PLD ou sua equipe, sempre que necessário.

3.2.3. Processos, Controles internos e Auditoria

Preventivamente a Gestora conta com um plano anual de mapeamento e revisão de processos que contempla o monitoramente dos controles aplicáveis à política de "Chinese Wall", como por exemplo a segregação de atividades operacionais e de aprovação na esteira de produtos.

Como uma linha de defesa adicional, a Gestora possui um cronograma de auditoria que também revisa os potenciais conflitos de interesse na empresa.

3.2.4. Espaço Físico

As atividades de Gestão de Recursos de Terceiros é desenvolvida, em espaços totalmente segregados das demais atividades desenvolvidas pela Gestora. O acesso, bem como a permanência em espaço segregado e destinada às atividades do Departamento de Administração de Fundos é restrito a pessoas autorizadas, notadamente, Colaboradores atuantes na referida área. O acesso aos referidos espaços será possível somente por essas pessoas previamente autorizadas, sendo certo que a circulação será restrita e controlada.

A eventual autorização de entrada de pessoa não registrada no sistema eletrônico deve ser solicitada previamente via e-mail e informada ao Diretor de Risco, Compliance e PLD.

3.2.5. Controle de Arquivos Físicos e Eletrônicos

Os arquivos eletrônicos de cada uma das Áreas de Atuação e empresas do grupo serão mantidos segregados entre si. Para tanto, cada uma das Áreas de Atuação e respectivas empresas

contarão com drives que somente poderão ser acessados por seus respectivos Colaboradores e Diretores que estejam na condição de "**above the wall**".

Sem prejuízo da restrição de acesso decorrente da estrutura da rede de informática, **é expressamente vedado aos Diretores e Colaboradores de todas as Áreas de Atuação e empresas do grupo o acesso e/ou gravação de arquivos em drives que não aqueles exclusivos de sua respectiva área, não devendo ser acessados, ainda que caso por qualquer falha do sistema fiquem momentaneamente disponíveis**, os drives das demais Áreas de Atuação e respectivas empresas do grupo.

Ademais, toda a documentação gerada pelas rotinas das Áreas de Atuação e respectivas empresas do grupo deve ser arquivada em locais segregados do servidor, cujo acesso é limitado ao login e senha de pessoas previamente autorizadas.

Adicionalmente aos controles acima descritos, a gestora manterá plano de auditoria interna periódica, sob responsabilidade da área de Compliance, realizando testes qualitativos e quantitativos, acerca do modelo, gestão e governança de concessão de acessos a pastas e documentos restritos e confidecnias da empresa e colaboradores, além de parametrização sisstemica, que evidencie e bloqueie recebimento ou envido de informações indevidas, considerando critérios de parametrizações através de palabras ou termos chaves (sistema de "firewall").

Ao ser identificado acessos indevidos ou transmissões de dados e informações consideradas sencíveis ou confidenciais, o relatório será enviado para o Diretor de Compliance que tomará as povidências e sanções cabíveis.

A gestora ainda adotará controles de Segurança da Informação pertinentes a dados sencíeis de pessoas naturais, conforme definido em legislação própria, atuando com programa de controle de intrusão, sendo contratada empresa especializada para a realização dessa atividade, bem como todos os sistemas e soluções sistêmicas contratadas de tercerios, terão claúsula específica de contorle de acesso e dados, além de segregação de perfil de acesso.

3.2.6. Segurança da informação

A GESTORA envidará os melhores esforçosno sentido de assegurar os pilares da segurança da informação:

- Confidencialidade: Processo pelo qual a informação é disponível de forma controlada com
- base em nível de permissão de acesso.
- Integridade: Processo pelo qual garanta a veracidade da informação, e que esta não seja afetada por alterações indevidas ou imprevistas.
- Disponibilidade: Processo pelo qual a informação está disponível para pessoas autorizadas,
- quando necessário.
- Avaliação dos riscos: A GESTORA poderá estar sujeita a riscos cibernéticos que ameacem a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados. Entre os riscos mais comuns estão:
  - Malwares: softwares desenvolvidos para corromper computadores e redes:
  - Vírus: software que causa danos à máquina, rede, à outros softwares e bancos de dados.
  - Spyware: software malicioso para coletar e monitorar o uso de informações.
  - Ransomware: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.
  - Engenharia social: métodos de manipulação para obter informações confidenciais, como
  - senhas, dados pessoais e número de cartão de crédito:
  - Pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento.

- Phishing: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
- Ataques de DDoS (distributed denial of service) e botnets: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos botnets, o ataque vem de um grande número de computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.
- Invasões (advanced persistent threats): ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

3.2.7. Proteção da informação e segurança cibernética

Os sistemas de informação da GESTORA contam com proteção de ativos de informação contra ameaças internas e externas, intencionais ou acidentais, com os objetivos de assegurar a continuidade do negócio e de minimizar o impacto de violações de segurança. A estrutura de informática e de comunicação é constituída essencialmente pelos recursos especificados a seguir:

- Firewall de Rede. Trata da segurança e proteção da rede;
- Antivírus. Prevenção, contenção e mitigação do impacto de software malicioso na rede, em aplicações e em outros sistemas que poderiam impactar a confidencialidade, a integridade ou a disponibilidade da informação;
- Monitoramento e Registro de proteção da informação. Controles para registro e monitoramento de eventos e de circunstâncias relativos à segurança para fins de atividades investigativas e de auditoria;
- Computação em nuvem. Requisitos de computação em "nuvem" para atender às políticas, normas e aos procedimentos de proteção da informação, além da implementação da infraestrutura, da plataforma e dos serviços criados para dar suporte à estrutura, aos sistemas e aos dispositivos de computação distribuídos em tais ambientes;
- Sistemas de backup. Os meios de armazenamento são servidores locais com o espelhamento das informações na nuvem configurados para recuperação e disponibilização nas condições originalmente padronizadas de armazenamento e consumo das informações;

3.2.8. Influência indevida sobre colaboradores de outras Áreas de Atuação e empresas do grupo

É vedado a todos os Colaboradores das empresas do grupo, sob pena de aplicação das penalidades estabelecidas nesta Política:

a) Tentar persuadir os Colaboradores das demais Áreas de Atuação e respectivas empresas do grupo a alterar opiniões relacionadas ao conteúdo de seus relatórios, análises ou planos de execução de quaisquer de suas tarefas; e

b) Utilizar nos relatórios elaborados Informações Confidenciais, relevantes e/ou não públicas recebidas indevida ou propositadamente por outros Colaboradores. O Colaborador que tomar conhecimento da existência de informações sensíveis vindas de algum Colaborador de outra Área de Atuação ou empresa do grupo deverá informar o Diretor de Risco, Compliance e PLD imediatamente.

3.2.9. Revisão de relatórios de pesquisa elaborados pelas demais Áreas de Atuação e empresas do grupo

Os Colaboradores do Departamento de Administração de Fundos em conjunto com a área de Compliance devem revisar quaisquer relatórios, análises, opiniões ou planos de execução de tarefas preparados por qualquer colaborador das demais Áreas da Gstora, antes de tais documentos serem divulgados publicamente.

3.2.10. Acesso a relatórios, análises e opiniões

Os Colaboradores fornecem importantes serviços para clientes por meio da assistência indireta à área de Administração de Fundos na execução de algumas funções que não envolvem participação em esforços de obtenção de negócios. Entre outras funções, citamos:

a) **Notificação de Potenciais Clientes de Gestão de Recursos de Terceiros:** Esta assistência é permitida, desde que não haja indícios de conflitos de interesse e os Colaboradores exerçam suas respectivas tarefas com independência entre si. Nestes casos, o Diretor de Risco, Compliance e PLD e o Diretor de Gestão devem ser comunicados e envolvidos nesse process; e
b) B**anco de Dados de Relatórios e Análises:** Os Colaboradores que necessitarem de informações, opiniões ou relatórios elaborados por Colaboradores de outras Áreas de Atuação ou empresas do grupo podem acessar a data-base de dados de relatórios desde que estes tenham sido divulgados a clientes e ao público em geral. Os Colaboradores do Departamento de Administração de Recursos não devem contatar diretamente outros Colaboradores para solicitação de relatórios ou informações não divulgadas.

3.2.11. Colaboradores do Departamento de Administração de Fundos e demais Colaboradores

Os Colaboradores de outras Áreas de Atuação e empresas do grupo podem manter relação de trabalho com os colaboradores do Departamento de Administração de Fundos a fim de adquirir uma visão mais aprofundada dos mercados com referência aos instrumentos cobertos pelos analistas e para aconselhá-los no tocante aos valores relativos aos emissores cobertos. No entanto, é importante que o Analista seja independente da mesa na elaboração de seus pareceres.

3.2.12. Posição Privilegiada (“Above the Wall”)

Os Diretores que, por natureza de suas funções, possuem acesso a informações que podem caracterizar conflito de interesse em relação às atividades realizadas pela Gestora que apresentam interesses opostos são considerados above the wall.

Por se encontrarem em posição privilegiada, os Diretores devem atuar com cautela e evitar qualquer uso impróprio ou disseminação de Informações Confidenciais, principalmente às Áreas de Atuação que possuem interesses conflitantes. Além disso, qualquer outra pessoa, em posição considerada above the wall, incluindo Diretores, não devem utilizar o conhecimento privilegiado adquirido no exercício de suas funções para atuar em benefício próprio, da Gestora ou de qualquer outra pessoa a qual tenha poder discricionário. Os Diretores deverão assinar um documento indicando que estão cientes das particularidades de suas funções, o qual será arquivado pelo Diretor de Risco, Compliance e PLD na sede da Gestora.

Como regra geral, a divulgação ou uso inadequado de Informações Confidenciais, relevantes e/ou não-públicas ficam estritamente proibidos. As situações excepcionais relacionadas ao cumprimento de responsabilidades e execução das atividades de administração e gestão que não estiverem previstas nesse Manual devem ser lidadas com bom senso, e em caso de dúvida sobre o procedimento adequado a ser tomado o Diretor ou o Colaborador deverá consultar o Diretor de Risco, Compliance e PLD.

Ao imprimir informações o Colaborador deve ter especial cuidado em não deixar qualquer documento, ou parte de documento na impressora por ele utilizada. É expressamente vedado o acúmulo ou abandono de documentos impressos nas impressoras.

Caso existam arquivos físicos de documentos que contenham Informações Confidenciais, estes deverão ser mantidos em segurança, devendo permanecer em ambiente trancado da respectiva Área de Atuação sempre que não estiverem sendo utilizados. Durante o período em que um Diretor ou um Colaborador mantiver um documento que contenha Informações Confidenciais em seu poder, tal Diretor ou Colaborador deverá tomar todos os cuidados necessários para que referido documento não possa ser acessado ou visualizado por Diretores ou Colaboradores de outras Áreas de Atuação ou empresa do grupo, devendo guardá-lo em segurança sempre que não estiver presente.

Toda comunicação emitida e/ou recebida via e-mail pode, a qualquer tempo, porém somente mediante solicitação formal do Diretor de Risco, Compliance e PLD, ser resgatada pelo administrador da área de tecnologia da informação.

Os Colaboradores e os Diretores deverão notificar imediatamente o Diretor de Risco, Compliance e PLD sempre que tomarem conhecimento de que algum Colaborador ou Diretor está usando inadequadamente Informações Confidenciais, privilegiadas, relevantes e/ou não públicas.

4. REGRAS DE SIGILO E CONDUTAS ADOTADAS

A Gestora obtém rotineiramente Informações Confidenciais e/ou não públicas no contexto de suas atividades. Para funcionar de modo eficaz, as "Chinese Walls" a serem praticadas entre as diferentes Áreas de Atuação da Gestora assim como entre as empresas do grupo deverão incluir políticas e procedimentos destinados a monitorar e restringir o fluxo dessas informações aos Diretores e aos Colaboradores que têm "necessidade de saber" a fim de:

I. Evitar o uso inadequado e/ou fraudulento das referidas informações e a aparência de impropriedade;
II. Cuidar de possíveis conflitos de interesse; e
III. Assegurar o cumprimento das leis e regulamentos aplicáveis.

Cada um dos Diretores e Colaboradores da Gestora receberá um login de identificação pessoal e uma senha para que possam acessar os sistemas de informação da Gestora, sendo que o acesso às informações mantidas em arquivos físicos será restrito e somente permitido mediante a autorização por escrito do Diretor de Risco, Compliance e PLD e identificação pessoal do Diretor ou Colaborador que pretende acessá-lo.

Adicionalmente, sob pena de aplicação das penalidades estabelecidas nesta política, os Diretores e Colaboradores deverão destruir imediatamente, após a sua utilização, os arquivos existentes nos sistemas de informação da Gestora.

Os Diretores e Colaboradores que tiverem acesso aos sistemas de informação da Gestora serão responsáveis pelo uso pessoal e intransferível do seu login e senha, bem como por tomar todas as medidas necessárias de forma a impedir o acesso não autorizado a estes sistemas, devendo manter suas senhas e outros meios de acesso aos sistemas de forma responsável e segura. Os Diretores e Colaboradores da Gestora deverão, ainda, sob pena de se submeter às penalidades estabelecidas no item 5 abaixo, observar estritamente as seguintes regras:

Utilização de e-mail: Todos os Diretores e Colaboradores devem utilizar o e-mail disponibilizado pela Gestora para fins profissionais, sendo proibido o uso para fins particulares. Não é permitida a utilização do e-mail para envio de piadas, correntes, cartões virtuais, promoções pessoais e outros assuntos não relacionados às atividades profissionais do colaborador da Gestora. Vale ainda ressaltar que os Diretores e Colaboradores estão proibidos de enviar, receber e/ou encaminhar mensagens com teor ofensivo, conteúdo pornográfico, racial ou similares. A Gestora reserva-se o direito de remover de sua rede qualquer material considerado ofensivo ou potencialmente ilegal.

Informações eletrônicas ou por telefonia: Os sistemas de comunicação disponibilizados, tais como e-mail, fax e telefones somente deverão ser utilizados para os negócios da Gestora, alertando que as informações de cunho pessoal, trafegadas por meio desses sistemas, não serão consideradas como Informações Confidenciais. Destacamos que é proibido o uso de notebooks ou outros meios de comunicação, para fins pessoais em quaisquer locais internos da Gestora. Caso seja necessário o portador deverá encaminhar para área de Gestão de Pessoas os dados do aparelho para que seja registrado e identificado no prontuário do próprio Diretor ou Colaborador para controle e liberação da área de tecnologia da informação.

4.1. Posições da Carteira

É vedado o acesso dos Colaboradores das demais Áreas de Atuação e empresas do grupo a informações sobre a composição de carteira da Gestão de Recursos de Terceiros e da Administração de Bens Próprios. Na eventualidade do Analista de Pesquisa ter acesso a tais informações esse conhecimento não deve influenciar análises, comentários, opiniões e/ou recomendações, sob pena de responsabilização e aplicação de penalidades civis ou criminais e/ou outras medidas disciplinares aos Colaboradores envolvidos.

4.2. Opiniões sobre operações e negócios dos quais a Gestora não esteja participando

O Colaborador de uma determinada área pode expressar aos Colaboradores das demais Áreas de Atuação ou empresas do grupo sua opinião sobre negócios, sociedades ou emissões de valores mobiliários, desde que o Colaborador em questão não esteja em posse de Informações Confidenciais, relevantes e/ou não públicas.

5. PROGRAMA DE TREINAMENTO

O COMPLIANCE realizará anualmente um programa de treinamentos para os colaboradores da GESTORA, de forma que estes estejam atualizados quanto aos seguintes temas:

- Compliance, Controles Internos e Código de Conduta e Ética;
- Política de Prevenção à Lavagem de Dinheiro.
- Segurança da Informação;
- Investimentos Pessoais;

Os novos Colaboradores e prestadores de serviços diretamente ligados a GESTORA, deverão receber orientações sobre os respectivos manuais, politicas e procediemntos da empresa, bem como assinarem ciência sobre o Codigo de Conduta e Ética da GESTORA. E no prazo máximo de até 30 dias receber os treinamentos de Compliance e Prevenção a Lavagem de Dinheiro.

5.1. Certificações

Atendendo às disposições do Código de Certificação Continuada da ANBIMA, o COMPLIANCE manterá o controle e a supervisão sobre a aplicabilidade e validade de certificações exigidas dos seus Colaboradores no exercício de suas funções.

Para assegurar o cumprimento do disposto nesta Política, o Compliance adota as seguintes diretrizes:

- Manter, em documento escrito, regras, procedimentos e controles internos que contenham:
  - Procedimentos para identificação dos Profissionais Certificados na admissão e no desligamento, bem como para atualização das informações desses profissionais, de modo a manter atualizado o Banco de Dados da ANBIMA;
  - Critérios para determinação das Atividades Elegíveis para cada uma das certificações;
  - Critérios de identificação de elegibilidade de profissionais transferidos;
  - Procedimento adotado para a atualização da certificação dos profissionais que atuam em Atividades Elegíveis quando de seu vencimento.
- Afastamento imediato dos profissionais que desempenhem Atividades Elegíveis sem a devida certificação, ou com a certificação vencida, bem como documentação formal que evidencie esse afastamento, observadas as exceções expressas neste Código.
- Aperfeiçoamento de seus profissionais, capacitando-os e fornecendo constante atualização sobre as certificações, quando aplicável, regras e normas pertinentes às suas atividades.
- Observar as regras de vencimento e atualização das certificações.

6. SANÇÕES ADMINISTRATIVAS

O descumprimento das disposições legais ou regulamentares internas pode acarretar sanções disciplinares e administrativas aos Diretores, Colaboradores ou Estagiários.

Quando a área de Compliance, diretoria ou departamento de recursos humanos (responsável pelo cumprimento e fiscalização das diretrizes da presente política), tiver conhecimento de situações em que o colaborador infringiu qualquer uma das regras ou definições aqui impostas, deverá analisar o caso e tomar as medidas disciplinares cabíveis, conforme abaixo descritas.

O Diretor, colaborador ou estagiário será notificado formalmente para apresentar defesa em até 10 (dez) dias úteis contados do recebimento da notificação, sob pena de serem considerados verdadeiros os fatos imputados e aplicadas as penalidades especificadas adiante. Em todos os casos, as notificações serão tratadas com o maior sigilo possível.

Os procedimentos adotados serão conduzidos pelo gestor ou Diretor da área, a quem cabe também a recomendação final das respectivas penalidades para aprovação pela Diretoria.

As penalidades aplicáveis resumem-se em advertência, suspensão temporária e afastamento definitivo.

A omissão diante da violação conhecida da lei, de qualquer disposição desta política e demais normas internas, não é uma atitude correta e constitui, em si mesma, uma violação das normas internas, passível de aplicação de:

- **Falta Leve:** será considerada "Falta" a violação de qualquer item desta política e das demais normas internas que regem a GESTORA e demais empresas do grupo que, a critério do departamento de Risco, Compliance e PLD, embora tenha ocorrido, não trouxe qualquer prejuízo financeiro, operacional ou à imagem das empresas do grupo.

Penalidade: advertência verbal e anotação no prontuário do Colaborador, mantido para os devidos efeitos de arquivamento ("Prontuário").

- **Falta Grave:** será considerada "Falta Grave" a violação de qualquer item desta política e das demais normas internas, que tenha trazido pequenos prejuízos financeiros, operacionais ou à imagem das empresas do grupo, à critério do departamento de Risco, Compliance e PLD, ou ainda, se houver reincidência de alguma Falta Leve cometida anteriormente, **por no mínimo 3 (três) vezes em um intervalo de 2 (dois) anos**.

  Penalidade: advertência formal, anotação no Prontuário do Colaborador e aplicação de suspensão das atividades pelo período de até 3 (três) dias úteis, formalizada pelo Departamento de Recursos Humanos.

- **Falta Gravíssima:** será considerada "Falta Gravíssima" a violação de qualquer artigo desta política e das demais normas internas, que apresente prejuízos financeiros, operacionais ou à imagem das empresas do grupo, à critério do departamento de Risco, Compliance e PLD, ou ainda, se houver reincidência de alguma Falta Grave cometida anteriormente, **por no mínimo 3 (três) vezes em um intervalo de 2 (dois) anos.**

  Penalidade: afastamento definitivo das atividades exercidas perante a empresa (Desligamento).

A aplicação das penalidades acima não isentam, dispensam ou atenuam a responsabilidade civil, administrativa e criminal, pelos prejuízos resultantes de seus atos dolosos ou culposos resultantes da infração da legislação em vigor e das políticas e procedimentos estabelecidos neste documento.

7. REFERÊNCIAS

TIPO DE DOCUMENTO	NOME DO DOCUMENTO
Lei	LEI Nº 12.683 DE 09 DE JULHO DE 2012
Norma / Regulamento	RESOLUÇÃO CVM Nº 21, DE 25 DE FEVEREIRO DE 2021. RESOLUÇÃO CVM Nº 35, DE 26 DE MAIO DE 2021.

8. HISTÓRICO

VERSÃO	DESCRIÇÃO DA ATUALIZAÇÃO	APROVADOR	DATA DA VERSÃO
1.0	Primeira publicação.	ANTONIO CARBONARI FILHO	03/03/2022