
# *COMPLIANCE* E CONTROLES INTERNOS

# CERTIFICAÇÃO

# SEGURANÇA DA INFORMAÇÃO

# CYBERSEGURANÇA

**POLÍTICA DE *COMPLIANCE* E CONTROLES INTERNOS**

**Versão Atualizada: JUNHO/2022**

## Objetivo

Formalizar os procedimentos para gerenciamento dos riscos de *compliance* e controles internos na BARI GESTÃO DE RECURSOS LTDA. ("BARI").

## A quem se aplica?

Sócios, diretores e funcionários que participem, de forma direta, das atividades diárias e negócios, representando a BARI (doravante, "Colaboradores").

Os Colaboradores devem atender às diretrizes e procedimentos estabelecidos nesta Política, informando qualquer irregularidade ao Diretor de Risco, *Compliance* e PLD.

## Estrutura e Responsabilidades

Cabe à BARI garantir, por meio de regras, procedimentos e controles internos adequados, o permanente atendimento à legislação, regulação, autorregulação e políticas internas vigentes.

Todos devem adotar e cumprir as diretrizes e controles aplicáveis à BARI contidas nesta Política, zelando para que todas as normas éticas, legais, regulatórias e autorregulatórias sejam cumpridas por todos aqueles com quem são mantidas relações de cunho profissional, comunicando imediatamente qualquer violação ou indício de violação ao Diretor de Risco, *Compliance* e PLD.

Cabe à alta administração da BARI:

1-) A responsabilidade pelos controles internos e o gerenciamento dos riscos de *compliance*;

2-) Indicar um diretor estatutário responsável por *compliance* e controles internos,[1] devendo tal profissional ter acesso a todas as informações e pessoas na BARI quando do exercício de suas atribuições;

3-) Aprovar, estabelecer e divulgar esta Política; e

4-) Garantir a efetividade do gerenciamento do risco de *compliance*.

O Diretor de Risco, *Compliance* e PLD deve:

[1] Com capacidade técnica e função independente das relacionadas à administração de carteiras de valores mobiliários, ou em qualquer atividade que limite a sua independência, na instituição ou fora dela.

1-) Auxiliar a alta administração a assegurar a efetividade do Sistema de Controles Internos e *Compliance* da BARI, atuando no gerenciamento efetivo de tais atividades no seu dia a dia;

2-) Gerenciar o Conselho de Ética, garantindo seu adequado funcionamento;

3-) Designar os secretários das reuniões do Conselho de Ética;

4-) Monitorar e exercer os controles e procedimentos necessários ao cumprimento das normas.

É responsabilidade de todos os Colaboradores o cumprimento das normas legais, regulatórias e autorregulatórias aplicáveis às suas atividades, bem como de todas as normas internas da BARI.

Qualquer suspeita, indício e/ou evidência de desconformidade por eles verificada deve ser imediatamente comunicada ao Diretor de Risco, *Compliance* e PLD.

O Diretor de Risco, *Compliance* e PLD se reporta apenas à alta administração da BARI, com autonomia e independência para indagar a respeito de práticas e procedimentos adotados nas suas operações/atividades, devendo adotar medidas que coíbam ou mitiguem as eventuais inadequações, incorreções e/ou inaplicabilidades.

Os controles e monitoramentos determinados nesta Política são prerrogativa exclusiva dos integrantes da Área de *Compliance* da BARI, sendo exercidos de forma autônoma e independente, com ampla liberdade de discussão e análise dos temas sob sua responsabilidade: o Diretor de Risco, *Compliance* e PLD tem poder de **veto** – mas não *de voto* – nos Comitês de negócios da BARI.

A Área de *Compliance* é formada pelo diretor estatutário responsável e por mais um profissional, e se dedicam ao exercício das atividades de cumprimento de regras, políticas, procedimentos e controles internos, incluindo o cumprimento das normas relativas ao combate e prevenção à lavagem de dinheiro, ao financiamento do terrorismo e à corrupção (além de também acumular a função de controle de risco).

## Revisão e Atualização

Esta Política deverá ser revisada e atualizada a cada 2 (dois) anos, ou em prazo inferior, se assim necessário por mudanças legais/regulatórias/autorregulatórias.

## Escopo e Atribuições do *Compliance*

A atuação do Diretor de Risco, *Compliance* e PLD tem por escopo:

**Temas Normativos**

- ✓ Controlar a aderência a novas leis, regulação e normas de autorregulação aplicáveis à BARI e às suas atividades;
- ✓ Controlar e monitorar as licenças legais e certificações necessárias, e a sua obtenção, renovação e/ou manutenção junto às autoridades reguladoras/autorreguladoras competentes;
- ✓ Auxiliar a alta administração da BARI no relacionamento com órgãos reguladores, e assegurar que as informações requeridas sejam fornecidas no prazo e qualidade requeridos;
- ✓ Realizar testes internos, revisões e relatórios obrigatórios nas frequências definidas nas políticas e manuais internos, bem como na legislação, regulação e autorregulação em vigor.

**Boas Práticas**

- ✓ Disseminar e promover as informações necessárias para o cumprimento das políticas internas e das normas legais, regulatórias e de autorregulação aplicáveis;
- ✓ Exercer seu controle, garantindo que as políticas e manuais pertinentes estejam atualizados e mantidos em diretório acessível a todos que delas devam ter conhecimento;
- ✓ Disponibilizar aos novos Colaboradores as políticas internas aplicáveis, e coletar os termos de ciência e aderência por eles assinados;
- ✓ Estabelecer controles para que todos os Colaboradores da BARI que desempenhem funções ligadas à gestão de fundos de investimento ou de carteiras administradas atuem com independência;[2]
- ✓ Garantir que os controles internos sejam compatíveis com os riscos da BARI em suas atividades;[3]
- ✓ Analisar informações, indícios ou identificar, administrar e, se necessário, levar temas para análise e deliberação no Conselho de Ética;
- ✓ Orientar previamente e/ou acompanhar o responsável pela comunicação à imprensa em contatos telefônicos, entrevistas, publicação de artigos ou qualquer outra forma de manifestação de opinião através de veículo público (inclusive na internet).

**Governança**

- ✓ Aprovar a oferta de novos produtos e prestação de novos serviços pela BARI, a partir de *inputs* técnicos do Comitê de Investimento;
- ✓ Atuar para que haja efetividade na segregação física de atividades conflitantes;
- ✓ Monitorar e buscar a efetiva aplicação dos documentos de *compliance* e controles internos abaixo listados;

---

[2] E atentem ao seu dever fiduciário para com os clientes, e que os interesses comerciais - ou aqueles de seus clientes - não desviem o foco de seu trabalho.

[3] Bem como efetivos e consistentes com a natureza, complexidade e risco das operações realizadas para o exercício profissional de administração de carteiras de valores mobiliários.

- ✓ Servir como canal para comunicações de desconformidades regulatórias e/ou de temas relacionados ao Código de Ética e Conduta Profissional da BARI e às suas demais políticas;
- ✓ Implementação de Regras e Guarda de Evidências – monitoramento da implementação de procedimentos, de cumprimento das normas e políticas internas, bem como de mecanismos de guarda de evidências;
- ✓ Salvaguarda de Informações - devem ser mantidos, pelo prazo mínimo de 5 (cinco) anos,[4] os documentos e informações exigidos pela regulação aplicável.[5]

## Análise e Comunicação aos Órgãos Competentes

Toda desconformidade em temas de conduta pessoal e profissional - e a sua respectiva análise efetuada pelo *Compliance* - deve ser submetida ao Conselho de Ética da BARI para conclusão e deliberação dos passos a serem dados a tal respeito.

Nos casos aplicáveis de desvio da norma específica das atividades reguladas, o Diretor de Risco, *Compliance* e PLD deve comunicar os respectivos órgãos competentes, nos prazos regulatórios, como seguem:

- ✓ A CVM deve ser comunicada no prazo máximo de 10 (dez) dias da verificação da respectiva ocorrência ou sua identificação, ou em prazo menor, se assim exigido pela regulação aplicável;

- ✓ O COAF deve ser comunicado no prazo de 24 (vinte e quatro) horas da verificação da respectiva ocorrência ou sua identificação.

Os demais prazos aplicáveis à BARI encontram-se previstos no Anexo I a esta Política, bem como na planilha de controle interno detalhada, intitulada "Quadro de Rotinas".

## Documentos de *Compliance* e Controles Internos

O Sistema de *Compliance* e Controles Internos da BARI está previsto em seus documentos internos, que englobam todas as suas políticas, manuais e Código de Ética e Conduta Profissional, além de procedimentos e organismos internos.

## Documentos Específicos Disponibilizados no *Website* da BARI

Cabe ao Diretor de Risco, *Compliance* e PLD preencher os respectivos Formulários de Referência da BARI e mantê-los em seu *website*. Tais formulários devem ser atualizados obrigatoriamente até o dia **31 de março** de cada ano.

[4] Ou prazo superior por determinação expressa da CVM.

[5] Bem como correspondências, internas e externas, papéis de trabalho, relatórios e pareceres relacionados com o exercício de suas funções. Os documentos e informações podem ser guardados em meio físico ou eletrônico, admitindo-se a substituição de documentos originais por imagens digitalizadas.

Adicionalmente, cabe ao Diretor de Risco, *Compliance* e PLD manter no *website* da BARI, em suas versões atualizadas, ao menos os documentos abaixo assinalados com asteriscos (obrigatórios pela regulamentação em vigor). Os demais documentos, poderão ser disponibilizados, a critério da gestora:

- ✓ **Código de Ética e Conduta Profissional;***
- ✓ **Formulário de Referência da BARI;***
- ✓ **Política de *Compliance* e Controles Internos;***
- ✓ **Política de Gestão de Riscos;***
- ✓ **Política de Investimentos Pessoais e da Empresa;***
- ✓ **Política de Rateio de Ordens de Investimento;***
- ✓ **Política de Exercício do Direito de Voto em Assembleias Gerais;***
- ✓ **Política de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Corrupção;**
- ✓ **Plano de Contingência e Continuidade de Negócios; e**
- ✓ **Política de Investimento e Crédito.**

**(*) Deverão ser obrigatoriamente colocadas no site da BARI**

## Testes e Relatórios Anuais

Para verificação dos controles internos, sua efetividade e consistência com a natureza, complexidade e riscos das operações realizadas pela BARI, é realizado um teste anual de aderência, o qual deve ser formalizado em relatório.[6]

Os relatórios relativos aos controles internos e à prevenção à lavagem de dinheiro são de responsabilidade do Diretor de Risco, *Compliance* e PLD – o relatório relativo a questões de *suitability* é de obrigação da Diretor de *Suitability*: os relatórios, são encaminhados à alta administração da BARI anualmente, até o último dia útil de **ABRIL** de cada ano.[7]

Os Relatórios Anuais em questão ficam disponíveis para consulta da CVM, na sede da BARI.

## Segregação de Atividades e Conflitos de Interesse

Cabe ao Diretor de Risco, *Compliance* e PLD assegurar e verificar que sejam devidamente segregadas das atividades de gestão de quaisquer outras atividades eventualmente desempenhadas pela BARI (ou empresas na qual a BARI, seus sócios, diretores ou colaboradores possuam participação acionária ou interesses econômicos), que com aquelas guardem qualquer tipo de conflito, real ou potencial, em qualquer grau, aspecto, medida, tempo e/ou forma: a segregação em questão deverá se dar tanto física quanto logicamente, com restrição de acesso a dependências, sistemas, diretórios e arquivos

[6] V. modelo no Anexo II, e orientação sobre o respectivo conteúdo no Anexo III – tal relatório diz respeito exclusivamente à atividade de administração de carteiras de valores mobiliários.

[7] Com conteúdo relativo ao ano civil imediatamente anterior.

apenas aos Colaboradores autorizados de cada área pertinente da BARI - e, se for o caso, entre estes e colaboradores de empresas de seu grupo econômico -, nos termos de suas Políticas.

Todas e quaisquer atribuições de controle na BARI – notadamente, mas sem limitação, o próprio *compliance* e o gerenciamento de riscos – não dependem nem estão sujeitas às suas áreas de negócios, de forma a assegurar a total autonomia de tais controles frente a cogitações de ordem comercial, ou de gestão de fundos ou carteiras de valores mobiliários.

O bom uso de instalações, equipamentos e informações comuns é obrigatório para todos os funcionários. As estações de trabalho, incluindo as autônomas e os equipamentos portáteis, devem ter, sem exceção, senha de inicialização tendo seu acesso bloqueado após minutos de inatividade, liberado apenas com senha do usuário da própria estação.

As áreas de negócios possuem acesso restrito a seus profissionais, para garantir segurança e segregação física da área da área responsável pela administração de carteiras de valores mobiliários e de eventuais demais atividades conflitantes (a título de exemplo, caso sejam futuramente desenvolvidos negócios relacionados à intermediação, estruturação, distribuição de valores mobiliários ou outra atividade qualquer de cunho conflitante).

A segregação física é monitorada pela área de *Compliance* mediante a governança e monitoramento de pessoas com acesso (físico e lógico) a suas áreas de competência.

Com relação à segregação de informações, há procedimentos internos relacionados à confidencialidade de informações devidamente classificadas, conforme detalhado nos termos da Política de Segurança de Informação.

Como regra geral, os Colaboradores detentores de Informações Confidenciais, em função de seu cargo ou função, devem estabelecer barreiras de acesso a dados e informações aos demais Colaboradores, cujo acesso seja dispensável e/ou não autorizado/essencial.

Essas barreiras servem para atender a diversos propósitos, incluindo a conformidade com leis e regulamentos que governam o tratamento e a utilização de certos tipos de informações, evitar situações que possam suscitar um potencial conflito de interesses e coibir a má utilização de dados e/ou informações.

A análise de produtos ou serviços oferecidos pela BARI deve sempre privilegiar o melhor interesse do investidor, e, caso envolva a oferta de produtos ou serviços da BARI deve se dar por atributos técnicos e de melhor benefício ao investidor.

Deve se mitigar, especialmente potenciais conflitos de interesse, sempre na busca das melhores alternativas ao investidor, de forma transparente, quando envolver:

- ✓ a atividade de gestão que eventualmente envolva a alocação em fundos geridos pela própria BARI; e
- ✓ a atividade de gestão e outras atividades quaisquer que venham a ser desenvolvidas pela BARI, e que envolva o investimento por parte dos veículos sob gestão da BARI ou de clientes.

Tais hipóteses devem considerar não apenas produtos e serviços ofertados pela BARI, mas também empresas do grupo, ou nas quais a BARI, sócios, diretores ou Colaboradores tenham participação acionária ou interesses econômicos ou pessoais, parcerias estratégicas etc.

## Contratações Externas

Em sua atividade de gestão de carteiras, a BARI não realiza quaisquer contratações de prestadores de serviço em nome dos fundos sob sua gestão,[8] seja de atividades reguladas pela CVM ou autorreguladas pela ANBIMA, cabendo tais contratações aos respectivos administradores dos referidos fundos.

Assim, esta Política se aplica somente às contratações feitas pela própria BARI, em seu próprio nome e benefício.

A contratação de serviços de terceiros deve ser precedida das seguintes providências:[9]

- ✓ Exigência de documentos e das certidões reputadas convenientes, seguindo, quando aplicável, procedimentos semelhantes aos descritos na Política de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Corrupção;
- ✓ De acordo com a avaliação de conveniência dos profissionais envolvidos, solicitar a assinatura, pelos terceiros a serem contratados, de "Acordo de Não Divulgação" (*Non-Disclosure Agreement* ou "NDA"); e
- ✓ Nos processos de negociação de qualquer contrato a ser celebrado pela BARI, o Colaborador envolvido na negociação deverá informar aos Diretores qualquer relacionamento familiar ou pessoal, sejam laços de amizade ou negociais, que tenha com membros do potencial contratado.

Após a contratação dos respectivos serviços, a Área de *Compliance* poderá, a seu critério, supervisionar os contratados.[10]

O processo para contratação de terceiros poderá vir acompanhado ou não de concorrência prévia, visando a obter o melhor "custo-benefício" dos melhores prestadores de serviço do mercado. Cabe à área responsável pela contratação definir ou não se será adotado este procedimento, sendo responsável inclusive por dar as devidas justificativas pelo "não uso", na hipótese de questionamento.

---

[8] Portanto, não são previstas neste documento regras de Supervisão Baseada em Risco, conforme previstas na autorregulação da ANBIMA.

[9] O *Compliance* poderá demandar medidas adicionais pré-contratação, tais como visita às dependências do prestador de serviço, *clippings* de mídia impressa/internet, além de outras medidas reputadas cabíveis/convenientes à contratação.

[10] A supervisão poderá ser realizada mediante procedimentos diversos a critério do *Compliance*, tais como visitas *in loco*, *clippings* de mídia impressa/internet, requisição periódica de certidões administrativas/judiciais, além de outras medidas reputadas cabíveis/convenientes à contratação.

A contratação de terceiros deverá ser orientada pelas seguintes diretrizes:

- ✓ O critério principal para escolha e contratação de terceiros será a modalidade menor preço, mediante a obtenção de orçamentos em número determinado pelo Diretor de Risco, *Compliance* e PLD para escolha do fornecedor ou prestador de serviços;
- ✓ Em casos excepcionais em que um fornecedor mais caro seja escolhido, a contratação deverá ser justificada com os outros critérios (por exemplo: prazo, qualidade, *expertise*, menor impacto ambiental etc.);
- ✓ Não haverá exigência de concorrência:
    - Nas compras e contratações para valores inferiores a R$ 5.000,00 (cinco mil reais), desde que os pagamentos não se refiram a parcelas de um mesmo serviço;
    - Quando já houver um contrato com prestadores de serviços recorrentes, não sendo, neste caso, necessário realizar concorrência a cada contratação ou compra;
    - Em compras e contratações em casos de especialidade do fornecedor/prestador;
    - Em compras e contratações em casos emergenciais, caracterizados pela urgência de atendimento de situação que possa ocasionar prejuízo ou comprometer as atividades da BARI, e que não pôde ser previsto antecipadamente.

## Contratação de Corretoras

Quando e se houver tal contratação, o processo deverá ser respaldado por análise criteriosa e objetiva de aspectos qualitativos da corretora de valores mobiliários. Dentre os aspectos qualitativos analisados, devem ser avaliados principalmente a reputação, o porte, a posição no ranking da B3, os selos de certificação que a corretora possui por meio do programa de qualificação da B3 e os custos.

O Diretor responsável pela gestão das carteiras dos fundos de investimentos ou o membro da equipe de gestão por ele autorizado, indicará ao Diretor de *Compliance* o nome da corretora que pretende recomendar para contração.

A Área de *Compliance* da BARI realizará um processo de *due diligence* da corretora indicada, por meio do Questionário ANBIMA de *Due Diligence* para Contratação de Corretoras, disponível através do link:

(http://www.anbima.com.br/data/files/66/46/EF/AD/CB1F561086B1AE5678A80AC2/QDD_servicos_qualificados_e_corretoras.pdf).

A Área de *Compliance* manterá uma lista de corretoras aprovadas no processo de *due diligence* e os membros da equipe de gestão executarão ordens exclusivamente através

das corretoras constantes dessa lista. O Diretor de *Compliance* atualizará a lista de corretoras aprovadas conforme as novas relações forem estabelecidas ou relações existentes forem terminadas ou modificadas.

No que diz respeito a contratações em nome dos fundos de investimentos sob sua gestão, a BARI se limita à contratação apenas de corretoras - sempre que possível - pertencentes a uma lista previamente apontada pelo administrador dos fundos sob sua gestão (caso a contratação não seja realmente feita pelo próprio administrador fiduciário).

Requisitos ligados à reputação no mercado das corretoras são avaliados, com o objetivo de identificação de eventuais atividades ilícitas ou de lavagem de dinheiro, corrupção e financiamento do terrorismo, bem como se a corretora também tem práticas de prevenção à lavagem de dinheiro e anticorrupção: para tal, estes são analisados em sistemas de clipping, verificação de Pessoas Expostas Politicamente (PEPs), listas restritivas e outras investigações internas da BARI, tais como serviços equivalentes às consultas Serasa, SPC e processos judiciais (cíveis e/ou criminais, inclusive ambientais), com vistas a atestar a sua idoneidade e reputação.

## Requisitos Contratuais

Os contratos estabelecidos com as corretoras devem estabelecer:

- ✓ As obrigações e deveres das partes envolvidas;
- ✓ A relação e as características dos serviços que serão contratados e exercidos por cada uma das partes;
- ✓ A obrigação de cumprir suas atividades em conformidade com as disposições previstas nas normas aplicáveis da ANBIMA e da CVM, especificamente, no que aplicável, para cada tipo de fundo de investimento; e
- ✓ Que os terceiros contratados devem, no limite de suas atividades, deixar à disposição do administrador fiduciário todos os documentos e informações exigidos pela regulação em vigor que sejam necessários para a elaboração de documentos e informes periódicos obrigatórios, salvo aqueles considerados confidenciais, nos termos da regulação vigente.

As contratações de corretoras necessariamente devem ser aprovadas pelos Diretores, em processo de análise prévia coordenado pelo Diretor responsável por *Compliance* e PLD. A avaliação deve considerar, ao menos:

- ✓ Tempo de existência da corretora e composição acionária;
- ✓ Políticas internas e governança;
- ✓ Preço e qualidade dos serviços;
- ✓ Estrutura tecnológica, operacional, sistemas, controles etc.;
- ✓ Atendimento aos programas de capacitação e excelência da B3;
- ✓ Processos eventualmente existentes (CVM, B3, BACEN, ANBIMA etc.);
- ✓ Solidez patrimonial, estrutura operacional, corpo de funcionários e capacitação técnica;

- ✓ Aspectos reputacionais e experiência anterior de profissionais da BARI com a corretora;
- ✓ Qualificação das áreas de execução, *research*, prêmios recebidos etc.

## Classificação e Supervisão por Nível de Risco

A partir dos atributos acima, as corretoras serão classificadas em 3 níveis de risco, a saber: (i) baixo; (ii) médio e (iii) alto.

As corretoras classificadas como de baixo risco, passam por processo de revisão/atualização a cada 24 (vinte e quatro) meses; as de médio risco, a cada 18 (dezoito) meses; e, as de alto risco, a cada 12 (doze) meses.

A metodologia da BARI para aferição do nível de risco segue os seguintes critérios:

**Alto Risco** - são consideradas de "alto risco" as corretoras que, individual ou cumulativamente:

- ✓ Tenham quaisquer apontamentos verificados no processo de pré-contratação da BARI, sem oferecer, ou tendo se recusado a dar, justificativa para as ocorrências constatadas;
- ✓ Não estejam em dia com as suas eventuais obrigações regulatórias junto aos órgãos competentes, e/ou com suas obrigações autorregulatórias, quando aplicáveis;
- ✓ Tenham apontamentos judiciais ou administrativos em seus nomes, ou de qualquer de seus sócios, administradores ou colaboradores, sem oferecer, ou tendo se recusado a dar, as devidas explicações para tanto;
- ✓ Tenham apontamentos verificados no processo de *screening* da BARI, via mídia impressa ou na internet, sem justificativa plausível para tal;
- ✓ Se recusem a permitir o acesso de Colaboradores do *Compliance* da BARI às suas dependências, quando do procedimento de pós-contratação;
- ✓ Tenham em seus quadros PEPs, conforme definidas na respectiva Política da BARI;
- ✓ Falhem em atender, sem justificativa, outros critérios reputados convenientes pela BARI na verificação de suas atividades/idoneidade.

**Médio Risco** - são consideradas de "médio risco" as corretoras que, individual ou cumulativamente:

- ✓ Tenham apontamentos verificados no processo de pré-contratação da BARI, oferecendo, porém, justificativa plausível para tanto;
- ✓ Estejam em processo de regularização de suas eventuais obrigações regulatórias junto aos órgãos competentes, e/ou de suas obrigações autorregulatórias, quando aplicáveis;

- ✓ Tenham apontamentos judiciais ou administrativos em seus nomes, ou de qualquer de seus sócios, administradores ou colaboradores, oferecendo, porém, as devidas explicações para tanto;
- ✓ Tenham apontamentos verificados no processo de *screening* da BARI, via mídia impressa ou na internet, justificando a contento da BARI a ocorrência verificada;
- ✓ Falhem em atender, mas remediando posteriormente, outros critérios reputados convenientes pela BARI na verificação de suas atividades/idoneidade.

**Baixo Risco** - são consideradas de "baixo risco" as corretoras que:

- ✓ Não tenham quaisquer apontamentos verificados no processo de pré-contratação da BARI;
- ✓ Estejam em dia com as suas eventuais obrigações regulatórias junto aos órgãos competentes, e/ou com suas obrigações autorregulatórias, quando aplicáveis;
- ✓ Não tenham apontamentos judiciais ou administrativos em seus nomes, ou de qualquer de seus sócios, administradores ou colaboradores;
- ✓ Não tenham apontamentos verificados no processo de *screening* da BARI, via mídia impressa ou na internet, sem justificativa plausível para tal;
- ✓ Atendam, com sucesso, outros critérios reputados convenientes pela BARI na verificação de suas atividades/idoneidade.

A contagem de prazo é válida a partir do efetivo uso das Corretoras em operações, e, para aquelas em que houver uso frequente de operações (ao menos 4 – quatro – vezes ao mês). A mera aprovação da Corretora, sem seu uso efetivo, não dá início à contagem de prazo.

No caso de eventos extraordinários, como falhas na execução de ordens, aquisições ou alterações societárias e notícias ou fatos relevantes divulgados à público e ao mercado, que justifiquem fiscalização em prazo menor, tal procedimento deve ser realizado e documentado com a urgência necessária.

## *Soft Dollar*

A prática de *soft dollar* é vedada na BARI, salvo exceções expressas e circunstanciadas pelo Diretor de Risco, *Compliance* e PLD, e apenas se comprovada a conveniência da ferramenta permutada na eficiência da gestão de fundos e carteiras a cargo da BARI.

## POLÍTICA DE CERTIFICAÇÃO

## Versão Atualizada: JUNHO/2022

### A quem se aplica?

Sócios, diretores e funcionários da BARI GESTÃO DE RECURSOS LTDA. ("BARI"), que desempenhem atividades diretas de gestão profissional de carteiras de títulos e valores

mobiliários, com alçada de decisão sobre o investimento, desinvestimento e manutenção dos recursos dos veículos a cargo da BARI ("Colaboradores").

Assim sendo, a BARI requer dos profissionais acima as Certificações da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais - ANBIMA para gestão de recursos de terceiros, sempre que aplicável às suas atividades, sendo:

- **Certificação de Gestores ANBIMA (CGA)** - destinada àqueles que desempenham o exercício profissional de gestão de recursos de terceiros em fundos regulados pela Instrução CVM n. 555 classificados como renda fixa, ações, multimercados, cambiais, e em carteiras administradas;

- **Certificação de Gestores ANBIMA para Fundos Estruturados (CGE)** - destinada àqueles que desempenham o exercício profissional de gestão de recursos de terceiros em Fundos de Índice[11] (ETFs), FIIs e FIDCs.

Os Colaboradores devem atender às diretrizes e procedimentos estabelecidos nesta Política, informando qualquer irregularidade aos respectivos Diretores de Risco, *Compliance* e PLD.

## Responsabilidades

O Diretor de Risco, *Compliance* e PLD é responsável pelos controles que garantem o atendimento às demandas relativas à necessidade ou não de certificação dos profissionais da BARI.

## Revisão e Atualização

Esta política deverá ser revisada a atualizada a cada 2 (dois) anos, ou em prazo inferior, caso assim necessário por mudanças legais/regulatórias/autorregulatórias.

## Controles

O Diretor de Risco, *Compliance* e PLD mantém controle dos Colaboradores da BARI com as seguintes informações:

- ✓ dados profissionais;
- ✓ data de admissão;
- ✓ data de desligamento, quando aplicável;
- ✓ atividade exercida;
- ✓ área de atuação;

[11] No caso de profissionais que atuem na gestão de Fundos de Índice (ETFs), também é aceita a CGA como certificação adequada.

- ✓ cargo;
- ✓ tipo de gestor, quando aplicável;
- ✓ endereço eletrônico individual;
- ✓ se dispõe de certificação ANBIMA e a sua validade.

O Diretor de Risco, *Compliance* e PLD é responsável por verificar que todos os Colaboradores elegíveis à CGA sejam certificados e que as respectivas certificações estejam válidas.

Compete ao Diretor de Risco, *Compliance* e PLD garantir que um Colaborador não certificado não exerça função que pressuponha certificação ou que a obtenha nos termos ditados pela ANBIMA.

Caso o Colaborador não disponha da certificação aplicável, o Diretor de Risco, *Compliance* e PLD é responsável por manter a documentação formal que evidencie o afastamento do Colaborador das atividades elegíveis à certificação.

Cabe ao Diretor de Risco, *Compliance* e PLD monitorar o cumprimento das demais diretrizes estabelecidas no Código de Certificação da ANBIMA.

As certificações pendentes e o afastamento das funções elegíveis devem ser reportadas ao Diretor de *Compliance*, que deve monitorar a sua devida regularização.

## Admissões de Colaboradores

O Diretor de Risco, *Compliance* e PLD deve acompanhar as informações sobre novas admissões e transferências internas, e se os novos Colaboradores possuem a respectiva certificação ANBIMA eventualmente aplicável.

Os candidatos a cargos que pressupõem a CGA ou CGE devem ser contratados com certificações válidas. Eventuais exceções deverão ser avaliadas pelo Diretor de Risco, *Compliance* e PLD e reportadas aos Diretores para controle das respectivas atividades e possível afastamento das funções até a efetiva obtenção da certificação aplicável.

Compete à Área de *Compliance* cadastrar, no site da ANBIMA, o novo funcionário e/ou colaborador transferido internamente, o que deve ocorrer no mesmo mês da contratação/transferência. Além disso, deve manter sempre atualizados os seus controles internos.

## Treinamentos e Reciclagens

A Área de *Compliance*, será responsável por difundir as melhores práticas dentro da BARI, por meio de treinamentos, sempre que houver uma atualização nas diretrizes de segurança ou demais políticas internas.

A frequência e renovação destes treinamentos presenciais dependerá da velocidade de crescimento e novas contratações da gestora, e será considerado pela diretoria.

Independentemente de novos treinamentos, cada novo colaborador tem acesso a todas as políticas e manuais internos para aculturamento das regras definidas pela gestora.

Sempre que houver mudanças significativas nas políticas (motivadas por decisão interna, ou adaptação a novos normativos), ou tópicos de segurança, serão promovidos treinamentos de reciclagem, mesmo se não houver novos Colaboradores contratados.

A BARI pode fazer uso de suas consultorias externas para apoio profissional em treinamentos e reciclagens. Os treinamentos contam com lista de presença. Os treinamentos têm periodicidade anual, caso haja mudança nos quadros de colaboradores, ou, atualizações significativas de políticas e procedimentos.

O programa de treinamento deve incluir em sua agenda anual os temas relacionados a PLDFT, e ser obrigatório a todos os Colaboradores com linguagem clara e que aborde as especificidades de cada função desempenhada.

Os treinamentos ministrados para os Colaboradores internos devem atender aos seguintes critérios:

- ✓ Ser aplicado no ingresso de todo novo Colaborador;
- ✓ Ser ministrado anualmente a todos os Colaboradores;
- ✓ Prover insumos para reciclagem das áreas e pessoas com deficiência de aprendizado.

O Programa de Treinamentos de PLDFT da BARI deve considerar os Terceiros Relevantes. Nesse sentido, conforme acordo entre as partes, o Diretor de Risco, *Compliance* e PLD poderá considerar a apresentação, pelo Terceiro Relevante, de evidência de realização de treinamento de PLDFT, âmbito interno do referido Terceiro Relevante, de forma satisfatória a critério da Diretoria. Sendo, portanto, dispensado da participação nos treinamentos oferecidos pela Gestora.

O programa de treinamentos é aplicável a administradores, empregados e Colaboradores que possuam acesso a informações confidenciais, participem do processo de decisão de investimento ou participem da prospecção de novos negócios. O treinamento deve abranger as políticas e procedimentos adotados pela BARI e será sempre compatível com a atividade desempenhada pelo administrador, sócio ou funcionário.

A BARI promoverá a conscientização e difusão de melhores práticas sobre proteção dos dados na empresa, através de ações educativas e treinamentos periódicos.

## Licenças e Desligamentos

No caso de licenças e desligamentos, o Diretor de Risco, *Compliance* e PLD deve verificar se o Colaborador está vinculado à BARI no site da ANBIMA, e, nesse caso, desvincular o profissional, o que deve ocorrer impreterivelmente no mesmo mês de licença e/ou desligamento.

Os profissionais em licença não devem continuar vinculados no período em que estiverem de licença. Quando retornarem, deverá ser efetuado o vínculo novamente.

## Banco de Dados da ANBIMA

O Diretor de Risco, *Compliance* e PLD é responsável pela veracidade e manutenção do banco de dados da ANBIMA atualizado.

## Código de Ética e Conduta Profissional

Cabe ao Diretor de Risco, *Compliance* e PLD requerer dos novos Colaboradores a assinatura formal do Termo de Conhecimento e Adesão ao Código de Ética e Conduta Profissional e das demais políticas da BARI, até o último dia do mês subsequente à sua contratação.

# POLÍTICA DE CONFIDENCIALIDADE, SEGURANÇA DA INFORMAÇÃO E CYBERSEGURANÇA

**Versão Atualizada: JUNHO/2022**

## Objetivo

Estabelecer princípios e diretrizes de proteção das informações no âmbito da BARI GESTÃO DE RECURSOS LTDA. ("BARI").

## A quem se aplica?

Sócios, diretores, funcionários, prestadores de serviço, terceirizados, consultores e demais pessoas físicas ou jurídicas contratadas ou outras entidades, que participem, de forma direta, das atividades diárias e negócios, representando a BARI (doravante, "Colaboradores").

## Contexto Operacional e de Negócios

Esta Política foi elaborada considerando as seguintes premissas e particularidades do modelo operacional e de negócio da BARI:

- ✓ A BARI não possui sistemas desenvolvidos internamente, executando suas atividades utilizando sistemas de terceiros, todos apenas acessíveis via *web*, não possuindo nenhum sistema que necessite de instalações locais para ser executado;
- ✓ Os fornecedores dos sistemas utilizados pela BARI se comprometem com disponibilidade, segurança e planos de contingência compatíveis com as necessidades da BARI;
- ✓ Os Colaboradores da BARI estabelecem tratativas e formalizam seus

entendimentos com clientes por meio de ferramentas e aplicativos de mensagens e/ou e-mail corporativo;

- ✓ A BARI aloca recursos sob gestão mediante a utilização de corretoras/plataformas de investimento acessíveis pela *web* e disponíveis para qualquer dispositivo eletrônico (*laptops*, *smartphones*, *tablets* ou computadores de mesa);
- ✓ Os dispositivos eletrônicos (*laptops*, *smartphones*, *tablets*) utilizados no exercício das atividades da BARI possuem senha de acesso e criptografia;
- ✓ A BARI utiliza redes sem fio para fornecer acesso à *web* para seus Colaboradores, prestadores de serviço ou visitantes, todas devidamente protegidas por senhas. Em caso de indisponibilidade temporária para acesso à *web*, os Colaboradores utilizam redes/roteadores de redundância. Neste caso, e em caso de trabalho remoto, os Colaboradores da BARI comprometem-se a utilizar redes sem fio seguras para desempenhar suas atividades;
- ✓ O espaço físico/escritório da BARI deve ser o local preferencialmente utilizado para as suas atividades, reuniões com clientes, Comitês e reuniões comerciais com Colaboradores ou terceiros. Porém, as atividades, rotinas e sistemas da BARI estão parametrizados para serem passíveis de desempenhado remoto.

## Responsabilidades

Os Colaboradores devem atender aos procedimentos estabelecidos nesta Política, informando quaisquer irregularidades ao Diretor de Risco, *Compliance* e PLD, que deverá avaliá-las e submetê-las ao Conselho de Ética, conforme o caso.

O Diretor de Risco, *Compliance* e PLD deve garantir o atendimento a esta Política, sendo o responsável na BARI por temas de segurança da informação/cibernética.

## Revisão e Atualização

Esta Política deverá ser revisada e atualizada a cada 2 (dois) anos, ou em prazo inferior, caso necessário em virtude de mudanças legais/regulatórias/autorregulatórias.

## Informações Confidenciais

São consideradas "Informações Confidenciais" aquelas não disponíveis ao público, que:

- ✓ Identifiquem dados pessoais ou patrimoniais (da BARI ou de clientes);
- ✓ Sejam objeto de acordo de confidencialidade celebrado com terceiros;
- ✓ Identifiquem ações estratégicas – dos negócios da BARI, seus clientes ou dos portfólios sob gestão;[12]
- ✓ Todas as informações técnicas, jurídicas e financeiras, escritas ou arquivadas eletronicamente, que digam respeito às atividades da BARI, e que sejam

[12] Cuja divulgação possa prejudicar a gestão dos negócios, clientes e portfólios a cargo da BARI, ou reduzir sua vantagem competitiva.

devidamente identificadas como sendo confidenciais, ou que constituam sua propriedade intelectual ou industrial, e não estejam disponíveis, de qualquer outra forma, ao público em geral;

- ✓ As que sejam assim consideradas em razão de determinação legal, regulamentar e/ou autorregulatória; e que
- ✓ O Colaborador utiliza para autenticação de sua identidade (senhas de acesso ou crachás), que são de uso pessoal e intransferível.

Não caracteriza descumprimento desta Política a divulgação de Informações Confidenciais: (i) mediante prévia autorização do Diretor de Risco, *Compliance* e PLD, (ii) em atendimento a ordens do Poder Judiciário ou autoridade regulatória, administrativa ou legislativa competente, bem como (iii) quando a divulgação se justificar, por força da natureza do contexto da revelação da informação, a advogados, auditores e contrapartes.

Em caso de dúvida, o Colaborador deverá consultar previamente o Diretor de Risco, *Compliance* e PLD acerca da possibilidade de compartilhamento da Informação Confidencial.

## Disposições Gerais

Os seguintes princípios norteiam a segurança da informação na BARI:

**Confidencialidade**: o acesso à informação deve ser obtido somente por pessoas autorizadas, e quando for de fato necessário;

**Disponibilidade**: as pessoas autorizadas devem ter acesso à informação sempre que necessário;

**Integridade**: a informação deve ser mantida em seu estado original, visando a protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

As seguintes diretrizes devem ser seguidas por todos os Colaboradores da BARI:

- ✓ As informações confidenciais devem ser tratadas de forma ética e sigilosa, e de acordo com as leis e normas internas vigentes, evitando-se mau uso e exposição indevida;
- ✓ A informação deve ser utilizada apenas para os fins sob os quais foi coletada;
- ✓ A concessão de acessos às informações confidenciais deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades;
- ✓ A identificação de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas;
- ✓ Segregação de instalações, equipamentos e informações comuns, quando aplicável;
- ✓ A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento.

Qualquer risco ou ocorrência de falha na confidencialidade e na segurança da informação deve ser reportado ao Diretor de Risco, *Compliance* e PLD.

## Identificação, Classificação e Controle da Informação

O Colaborador que recebe ou prepara uma informação pode, se eventualmente necessário, classificá-la como "Confidencial". Para tal conclusão, devem ser considerados as questões de natureza legal e regulatória, de estratégia negocial, os riscos do compartilhamento, as necessidades de restrição de acesso e os impactos no caso de utilização indevida das informações.

Caso haja informação de natureza "Confidencial", o acesso a mesma deve ser restrito e controlado.

Sempre que necessário, contratos de confidencialidade da informação devem ser assinados com terceiros, sob supervisão do Diretor de Risco, *Compliance* e PLD, e, se reputado necessário, da assessoria jurídica da BARI.

A informação deve receber proteção adequada. Em caso de dúvida, o Colaborador deverá consultar o Diretor de Risco, *Compliance* e PLD.

O descarte de Informação Confidencial armazenada em meio físico deve ser efetuado utilizando preferencialmente máquina fragmentadora/trituradora de papéis ou incineradora.

## Mesa Limpa

Nenhuma Informação Confidencial deve ser deixada à vista nos locais de trabalho dos Colaboradores, mesmo quando trabalhando remotamente. Ademais, ao usar uma impressora coletiva, o documento impresso deve ser imediatamente recolhido.

## Gestão de Acessos

Os serviços de rede, internet e correio eletrônico disponíveis na BARI são de sua propriedade exclusiva, sendo permitido o uso moderado para fins particulares.

A BARI poderá, a qualquer momento, mediante prévia aprovação do Diretor de Risco, *Compliance* e PLD, e sem obrigação de cientificação prévia:

- ✓ inspecionar conteúdo e registrar o tipo de uso dos *e-mails* feitos pelos usuários;
- ✓ disponibilizar esses recursos a terceiros, caso entenda necessário;
- ✓ solicitar aos usuários justificativas pelo uso efetuado;
- ✓ monitorar acesso a sites, aplicativos etc.;
- ✓ bloquear acesso a sites.

No caso de mudança de área ou desligamento do Colaborador, a respectiva senha de acesso é cancelada, visando ao impedimento de acesso não autorizado pelo ex-Colaborador.

Os equipamentos, ferramentas e sistemas concedidos aos Colaboradores devem ser configurados com os controles necessários para cumprir os requerimentos de segurança aplicáveis à BARI.

Apenas os Colaboradores devidamente autorizados terão acesso[13] às dependências e sistemas a que estiverem liberados, bem como aos arquivos, diretórios e/ou pastas na rede da BARI, mediante segregação física e lógica.

## Gestão de Riscos, Tratamento de Incidentes de Segurança da Informação, Continuidade de Negócio e *Backups*

Os riscos e incidentes de segurança da informação devem ser reportados ao Diretor de Risco, *Compliance* e PLD, que adotará as medidas cabíveis.

No caso de vazamento de informação, ou acesso indevido a informação, o Diretor de Risco, *Compliance* e PLD deverá ser imediatamente comunicado, para a tomada das medidas cabíveis.[14]

## Testes de Controles

A efetividade desta Política é verificada por meio de testes periódicos dos controles existentes, com intervalos não superiores a 1 (um) ano, sob responsabilidade do Diretor de Risco, *Compliance* e PLD, e reportados aos demais Diretores.

Os testes[15] devem verificar se:

- ✓ Os recursos humanos e computacionais são adequados ao porte e às áreas de atuação;
- ✓ Há adequado nível de confidencialidade e acessos às informações confidenciais, com identificação de pessoas que tem acesso a estas informações;
- ✓ Há segregação física e lógica;
- ✓ Os recursos computacionais, de controle de acesso físico e lógico, estão protegidos;
- ✓ A manutenção de registros permite a realização de auditorias e inspeções.

[13] Quaisquer exceções deverão ser previamente solicitadas ao Diretor de Risco, *Compliance* e PLD.

[14] Podendo variar de simples repreensão pelo acesso, ou mensagem ao destinatário errôneo da mensagem enviada (para que apague em definitivo o seu conteúdo), até o estudo e implementação efetiva de providências judiciais, quando e se for o caso, sem prejuízo da investigação e eventual punição dos Colaboradores envolvidos.

[15] Que podem ser realizados por terceiros, ou objeto de obrigação contratual, passível de reporte por prestadores de serviço, provedores de dados, aplicativos e ferramentas/*softwares*. Tais conteúdos podem ser passíveis de compor o relatório anual de *Compliance* exigido pela regulação aplicável da CVM.

## Riscos de Cybersegurança

As principais ameaças e riscos aos ativos cibernéticos da BARI são:

- *Malwares* – *softwares* desenvolvidos para corromper os computadores e redes, como:
  - ✓ vírus: *software* que causa danos às máquinas, redes, *softwares* e bancos de dados;
  - ✓ cavalos de troia: aparecem dentro de outro *software*, criando uma entrada para invasão da máquina;
  - ✓ *spywares*: *software* maliciosos que coletam e monitoram as atividades das máquinas invadidas;
  - ✓ *ransomware*: *softwares* maliciosos que bloqueiam o acesso a sistemas e bases de dados, solicitando resgates para restabelecimento do uso/acesso.
- Engenharia social – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito, como, por exemplo:
  - ✓ *pharming*: direciona o usuário para um site fraudulento, sem o seu conhecimento;
  - ✓ *phishing*: *links* veiculados por e-mails simulando pessoas ou empresas confiáveis que enviam comunicação eletrônica aparentemente oficial para obter informações confidenciais;
  - ✓ *vishing*: simulação de pessoas ou empresas confiáveis para, por meio de ligações telefônicas, obtenção de informações confidenciais;
  - ✓ *smishing*: simulação de pessoas ou empresas confiáveis para, por meio de mensagens de texto, obtenção de informações confidenciais;
  - ✓ ataques de DDOS (*distributed denial of services*) e *botnets* – ataques visando a negar ou atrasar o acesso aos serviços ou sistemas da instituição;
  - ✓ invasões (*advanced persistent threats*) – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

## Obrigações de Cybersegurança

Na prestação de seus serviços, a BARI obtém e lida com informações sensíveis, não disponíveis ao público em geral, e que podem ocasionar perdas irreparáveis em casos de malversação, negligência ou vazamentos.[16]

O responsável por tais questões na BARI é o Diretor de Risco, *Compliance* e PLD.

São itens obrigatórios de cybersegurança (empresa):

[16] Os riscos potenciais relativos a tais dados envolvem invasões, disseminação errônea ou dolosa, acesso indevido e/ou seu roubo/desvio.

- A adequada proteção dos ativos cibernéticos da BARI, aí incluídos sua rede, sistemas, *softwares*, websites, equipamentos e arquivos eletrônicos.
- Restrição e controle do acesso e privilégios de usuários não pertencentes ao quadro de colaboradores da BARI;
- Invalidar contas de Colaboradores e prestadores de serviço em seu desligamento;
- Quando necessário, bloquear chaves de acesso de usuários, e, quando necessário, realizar auditoria para verificação de acessos indevidos;
- Excluir ou desabilitar contas inativas;
- Fornecer senhas de contas privilegiadas somente a Colaboradores que necessitem efetivamente de tais privilégios, mantendo-se o devido registro e controle;
- Garantir o cumprimento do procedimento de *backup* para os servidores e ativos cibernéticos, eletrônicos e computacionais da BARI;
- Detectar, identificar, registrar e comunicar ao Diretor de Risco, *Compliance* e PLD as violações ou tentativas de acesso não autorizadas;
- Organizar treinamentos relacionados à segurança dos ativos de informação sempre que necessário;
- Nos casos em que tais serviços e controles acima sejam terceirizados, é necessário que as condições contratuais garantam que o prestador de serviço atesta esta proteção;
- Caso necessário, a partir de resultados apresentados nos testes de aderência, revisar tais práticas;
- A BARI dispõe de segurança nos servidores para acesso à sua rede, visando a manter o ambiente de trabalho disponível e livre de vírus e acessos indesejados. O sistema de prevenção a ataques de vírus é regularmente atualizado;
- É realizado *backup* de arquivos de forma sistemática. Os dados de *backup* atualizados são armazenados em local seguro, com monitoramento.

São itens **OBRIGATÓRIOS** de cybersegurança (Colaboradores):

- Somente enviar mensagens para as pessoas envolvidas no assunto tratado, certificando-se dos endereços de destino escolhidos;
- Somente imprimir as mensagens quando realmente necessário;
- Ao identificar mensagem com título ou anexo suspeito, certificar-se sobre a segurança em abrí-la, para evitar vírus ou códigos maliciosos;
- No caso de recebimento de mensagens que contrariem as regras estabelecidas pela BARI, **NUNCA** as repassar, alertando o responsável da sua área e o Diretor de Risco, *Compliance* e PLD, se for o caso;
- Ao se ausentar do seu local de trabalho, mesmo quando estiver trabalhando remotamente e mesmo que temporariamente, bloquear a estação de trabalho;

- Quando sair de férias ou se ausentar por períodos prolongados, o Colaborador deve utilizar o recurso de ausência temporária de e-mail;
- Utilizar equipamentos, aplicativos, impressoras, acesso a sites, e e-mail (e demais ferramentas tecnológicas) com a finalidade primordial de atender aos interesses da BARI;[17]
- Tecnologias, marcas, metodologias e quaisquer informações que pertençam à BARI não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas ou desenvolvidas pelo próprio Colaborador em seu ambiente de trabalho;
- Cada Colaborador terá acesso somente a pastas eletrônicas relacionadas à sua área e às pastas comuns a todos os Colaboradores.

São itens **VEDADOS** de cybersegurança (Colaboradores):

- Enviar e-mail ou acessar sites que promovam a veiculação de mensagens, produtos, imagens ou informações que interfiram na execução das atividades profissionais;[18]
- Trocar informações que causem quebra de sigilo bancário e/ou possuam caráter confidencial ou estratégico;[19]
- Prejudicar intencionalmente usuários da internet, mediante desenvolvimento de programas, acessos não autorizados a computadores e alteração de arquivos, programas e dados na rede da BARI;
- Divulgar propaganda ou anunciar produtos ou serviços particulares pelo correio eletrônico da BARI;
- Alterar qualquer configuração técnica dos *softwares* que comprometam o grau de segurança, ou impeçam/dificultem seu monitoramento pelo Diretor de Risco, *Compliance* e PLD;
- Contratar provedores de acesso sem autorização prévia ou ciência do Diretor de Risco, *Compliance* e PLD;
- Uso de compartilhadores de informações, tais como redes *Peer-toPeer* (P2P – p. ex., Kazaa, eDonkey, eMule, BitTorrent e semelhantes) nas dependências da BARI.

**Exceções** a esta Política de Cybersegurança (Colaboradores):

- Caso haja uso de equipamentos ou dispositivos eletrônicos de propriedade dos Colaboradores para desempenhar suas atividades na BARI, estes se comprometem a adotar as medidas de segurança anteriormente citadas a fim de preservar seus equipamentos e minimizar o risco de comprometimento de segurança às informações sensíveis da BARI, seus clientes e parceiros de negócio,

[17] Os computadores, arquivos, e, arquivos de e-mails corporativos poderão ser inspecionados, **independentemente de prévia notificação ao Colaborador**, a fim de disseminação errônea ou dolosa, acesso indevido e/ou roubo/desvio de informações.

[18] Sendo proibido, sobretudo, conteúdo pornográfico, racista ou ofensivo à moral e aos princípios éticos.

[19] Exceção, é claro, a fluxos de informações necessários para a gestão de fundos e carteiras com instituições envolvidas nas operações dos clientes.

podendo utilizar tais equipamentos para os diversos fins que considerar pertinentes;

- É facultado ao Diretor de Risco, *Compliance* e PLD autorizar exceções a esta Política, devendo estar formalizadas por e-mail.

**ANEXO I**

## Quadro de Obrigações Periódicas

### I.) Informações Periódicas

| Norma | Artigo | Tema | Obrigação | Período |
|---|---|---|---|---|
| RCVM 21 | 25, *caput* e I a III | Relatório Anual | Entrega do relatório à administração | Último dia útil de abril a cada ano<br>(data base 31/12) |
| RCVM 21 | 17, *caput* e II | Formulário de Referência | Envio do FR pelo CVMWeb | Anualmente, até 31/03<br>(data base 31/12) |
| RCVM 51 | 1.º, II | Declaração Eletrônica de Conformidade | Envio pelo CVMWeb | Anualmente, até 31/03<br>(data base 31/12) |
| RCVM 50 | 4.º, III | Política de PLD | Atualização dos dados cadastrais dos clientes/investidores e/ou verificação da efetiva atualização dos citados dados pelo administrador/distribuidor | No máximo a cada 5 (cinco) anos |
| RCVM 50 | 6.º, I a VII, e §§ | Relatório Anual de PLD | Entrega do relatório à administração da JOURNEY<br>(obs: pode estar compreendido no Relatório Anual de *Compliance*, em vez de ser apresentado em separado) | Anualmente, até o último dia útil do mês de abril |

| | | | | |
|---|---|---|---|---|
| RCVM 50 | 23, *caput* e Parágrafo Único | Política de PLD | Declaração Negativa de PLD à CVM | Anualmente, até o último dia útil do mês de abril |
| Código Certificação ANBIMA | 23, § 2.º | Base de Dados ANBIMA | Inclusão e atualização no banco de dados administrado pela ANBIMA das informações relativas aos colaboradores certificados, em processo de certificação, com a certificação vencida, e/ou em processo de atualização da certificação | Mensalmente, até o último dia do mês subsequente à data do evento |

## II.) Informações Eventuais

| Norma | Artigo | Tema | Obrigação | Período |
|---|---|---|---|---|
| RCVM 51 | 1.º, I | Atualização de dados cadastrais | Atualização via CVMWeb | 7 (sete) dias úteis contados do evento que deu causa à alteração |
| RCVM 50 | 22 e §§ | Política de PLD | Comunicar ao COAF todas as situações e operações detectadas, ou propostas de operações que possam constituir-se em sérios indícios de LDFT | 24 (vinte e quatro) horas a contar da conclusão da análise que caracterizou a atipicidade da operação, respectiva proposta, ou mesmo da situação atípica detectada |
| RCVM 21 | 18, VIII | Violação à regulação | Informar à CVM a ocorrência ou indícios de violação da sua regulação | 10 (dez) dias úteis da ocorrência ou sua identificação |

| | | | | |
|---|---|---|---|---|
| Ofício Circular CVM/SIN 10/15 | Item 37 | Atualização cadastral | Envio à CVM do contrato social atualizado, no caso de mudança de denominação social ou de substituição de diretor responsável pela gestão | 7 (sete) dias úteis do fato que deu causa à alteração |

**ANEXO II**

**Modelo de Relatório de Aderência[20]**

Ilmos. Srs.

Sócios e Diretores da

BARI GESTÃO DE RECURSOS LTDA.

Ref.: Relatório Anual – Resolução CVM nº 21, de 25 de fevereiro de 2021 ("RCVM 21")

Ano Base: [•]

Prezados Senhores,

Em cumprimento ao disposto no art. 25 da RCVM 21, vimos apresentar a V.Sas. o relatório pertinente às atividades da BARI GESTÃO DE RECURSOS LTDA. ("BARI"), no ano de [•] ("Relatório").

De acordo com a RCVM 21, o mencionado Relatório contém:

- ✓ As conclusões dos exames efetuados;
- ✓ As recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e
- ✓ A manifestação do diretor responsável pela administração de carteiras de valores mobiliários, ou, quando for o caso, pelo diretor responsável pela gestão de risco, a respeito das eventuais deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las (cf. art. 25, I, II e III, da RCVM 21).

Este relatório ficará à disposição da Comissão de Valores Mobiliários ("CVM") na sede da BARI, para eventuais posteriores checagens, verificações e/ou fiscalizações por parte da CVM.

Além dos aspectos acima, V.Sas. encontrarão também, no corpo do presente Relatório, os resultados do Teste de Aderência determinado na Política de *Compliance* e

[20] O **relatório da RCVM 30** deverá ter conteúdo similar, **porém sobre o tema de *suitability***. Além disso, conforme o art. 6.º, §2º, da RCVM 50, de 2021, deverá haver também o envio de um relatório sobre o tema de **prevenção à lavagem de dinheiro**, que pode ser enviado no corpo deste relatório ou em documento apartado (o modelo pertinente encontra-se na Política de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo a à Corrupção) - Consultar também os itens **mínimos** constantes do Ofício Circular CVM/SIN n.º 2, de 23 de fevereiro de 2021.

Controles Internos da BARI, e o correspondente parecer final do Diretor de Risco *Compliance* e PLD, que assina o presente documento.

Assim sendo, passamos abaixo à exposição dos elementos pertinentes do presente Relatório.

I. Conclusão dos Exames Efetuados (RCVM 21, art. 25, I)

*(enumerar detalhadamente por área/ocorrência, com todas as informações pertinentes, incluindo datas da verificação da ocorrência e sua natureza)*

II. Recomendações sobre as Deficiências Encontradas e Cronogramas de Saneamento (RCVM 21, art. 25, II)

*(enumerar detalhadamente por área/ocorrência, com todas as informações pertinentes, incluindo estimativas de datas de acompanhamento e conclusão das soluções)*

III. Manifestações dos Diretores Correspondentes de Gestão e de Risco sobre as Verificações Anteriores e Respectivas Medidas Planejadas (RCVM 21, art. 25, III)

*(enumerar detalhadamente por área/ocorrência, com todas as informações pertinentes, incluindo os resultados esperados e os efetivamente alcançados)*

IV. Parecer Final do Diretor de Risco, *Compliance* e PLD

*(enumerar detalhadamente)*

Sendo então o que nos cumpria para o momento, aproveitamos o ensejo desta correspondência para nos colocarmos à disposição de V.Sas. para os eventuais esclarecimentos porventura reputados necessários.

Atenciosamente,

[•]
BARI GESTÃO DE RECURSOS LTDA.
Diretor de Risco, *Compliance* e PLD

**ANEXO III**

**Orientações Gerais sobre o Conteúdo Técnico do Teste de Aderência[21]**

A Diretoria de Risco, *Compliance* e PLD deve estruturar registro e controle ativo, ao longo do ano, para composição do Relatório Anual (descrito no Anexo I), ao menos sobre as seguintes matérias relacionadas abaixo.

Tais temas devem – ao longo do ano – quando necessário, ser objeto de acompanhamento próximo da alta gestão (sócios e diretores) da BARI.

Tal controle deve ser feito em planilhas específicas, servindo como ferramenta de *compliance* e controle de risco operacional.

O controle ao longo do ano dos eventos abaixo, e seu registro é uma das obrigações centrais do Diretor de *Compliance*.

I. Conclusão dos Exames Efetuados (RCVM 21, art. 25, I)

*(enumerar detalhadamente por área/ocorrência, com todas as informações pertinentes, incluindo datas da verificação da ocorrência e sua natureza)*

→ Deve constar em planilha de controle o registro dos seguintes eventos (ao menos) ocorridos ao longo do ano, suas consequências / perdas e as atitudes corretivas adotadas:

- ✓ erros operacionais atinentes a operações dos fundos;
- ✓ erros relativos à movimentação financeira de clientes;
- ✓ falhas em pagamentos de remuneração de distribuidores ou corretagem de fundos pagas a corretoras ou quaisquer prestadores de serviço;
- ✓ desenquadramentos de carteiras, comunicação com administrador e reenquadramento;
- ✓ qualquer outro descumprimento de norma legal constatado;
- ✓ eventos de liquidez dos fundos;
- ✓ falhas operacionais relativas à infraestrutura tecnológica e plano de correção implementado;
- ✓ acionamentos do plano de contingência e continuidade de negócios;
- ✓ falhas de fornecedores;
- ✓ falhas relativas a quaisquer políticas internas ou normas legais e plano de correção implementado;
- ✓ mudanças expressivas em parâmetros de liquidez dos fundos;

[21] Consultar também os itens mínimos constantes do Ofício Circular CVM/SIN n.º 2, de 23 de fevereiro de 2021, dispostos no Anexo IV a seguir.

- ✓ eventos relacionados ao gerenciamento de risco, com especial atenção a risco de crédito e liquidez;
- ✓ ofícios ou qualquer outro alerta e comunicação recebidos de reguladores, ou processos administrativos junto à CVM, ANBIMA e demais reguladores aplicáveis, ou em alçadas do poder judiciário;
- ✓ descumprimento de obrigações relativas à certificação;
- ✓ descumprimento de contratos quaisquer;
- ✓ quebra de dever de sigilo contratual;
- ✓ quaisquer eventos adicionais considerados relevantes pelo *compliance* e que tenham colocado em risco a empresa, seus colaboradores, clientes, carteiras sob gestão ou as boas práticas de mercado.

**ANEXO IV**

**Conteúdo Mínimo do Relatório Anual**

| Temas | Aspectos mínimos |
|---|---|
| Requisitos legais para o exercício da atividade | - se as exigências para manutenção do registro tanto do diretor responsável pela atividade, quanto da pessoa jurídica – estão sendo cumpridos, e, em especial, a manutenção de recursos humanos e computacionais adequados ao porte e à área de atuação da pessoa jurídica.<br>- Verificar os requisitos de reputação ilibada dos diretores e dos controladores da BARI. |
| Envio de informes | - se os informes periódicos e eventuais devidos têm sido enviados no prazo estabelecido nas normas da CVM. Isso inclui verificar se o Formulário de Referência enviado pelo Sistema CVMWeb e disponível no site da BARI está sendo atualizado quando cabível. |
| Atualização de dados cadastrais | - Atestar que os dados cadastrais da BARI no cadastro da CVM estão atualizados e se as atualizações têm sido feitas de maneira tempestiva. |
| Políticas | - Se os documentos e manuais exigidos constam no website da BARI em sua versão atualizada;<br>- apontar se eventuais ajustes em políticas e documentos foram consequência de mudanças regulatórias, ou exigências do regulador, ou se consequência de mudanças internas, decisões gerenciais, ou mesmo se foram motivadas por apontamentos recebidos em processos de *due diligence*. |
| Colaboradores | - apontar se houve o descumprimento do respectivo Código de Ética e demais políticas internas pelos administradores, empregados e colaboradores, e relatar como se deu o equacionamento caso tenha havido desvios profissionais mais graves, se estes resultaram em sanções e/ou consequências (financeiras, comerciais, de imagem etc.) à BARI e ao colaborador em questão, com destaque para as medidas tomadas para sua prevenção futura.<br>- relatar também os procedimentos de verificação do atendimento ao cumprimento da Política de Investimentos Pessoais e da Empresa, e, ainda, se houve eventual ocorrência de eventos a ela relativos, práticas abusivas de mercado por funcionários (*insider trading*, *front running*, *spoofing* etc.) ou práticas que possam ter |

| | |
|---|---|
| | colocado em risco o adequado funcionamento dos fundos de investimento e da BARI.<br><br>- se o programa de treinamento de administradores, empregados e Colaboradores foi cumprido, e a eventual necessidade de ajustes e aprimoramentos no programa, de forma a levar em conta, inclusive, achados passados da própria Área de *Compliance*. |
| Conflitos de interesse | - se as políticas de prevenção aos possíveis conflitos de interesse foram cumpridas de forma eficaz, inclusive quanto ao exercício de atividades externas por administradores, Colaboradores e empregados, tais como a participação em conselhos de administração, fiscal, consultivos, ou comitês de companhias investidas ou potencialmente investidas pelos veículos de investimento geridos ou administrados, bem como a correta divulgação no Formulário de Referência dos potenciais conflitos de interesses com outras atividades da instituição, e suas empresas ligadas. |
| Segurança da Informação e Plano de Continuidade de Negócios | - se o controle de informações confidenciais é eficaz, e ainda a existência de testes periódicos de segurança dos sistemas. Caso tenham ocorrido incidentes, relatar as providências tomadas e seus status atualizado.<br><br>- se os recursos computacionais e demais registros mantidos das operações e negócios estão protegidos contra adulterações e também permitem auditoria com relato dos testes efetuados.<br><br>- se a guarda e a manutenção dos arquivos da empresa pelo prazo estabelecido nas normas preserva sua integridade e disponibilidade;<br><br>- se os planos de contingência, continuidade de negócios e recuperação de desastres previstos são factíveis e têm condições de ser implantados de imediato conforme testes realizados. Relatar se houve acionamento do plano, se houve reavaliações, revisões, e se o mesmo se encontra adequado às condições correntes. |

| | |
|---|---|
| Segregação de atividades | - Avaliação, por meio de testes, sobre a segregação física, de sistemas e de pessoal entre as diversas áreas da empresa, inclusive quanto ao acesso a instalações e sistemas, atestando se está operacional e atendendo seus objetivos, evitando o vazamento indevido de dados e informações entre diferentes áreas da BARI. |
| Gestão de Riscos e Rateio de Ordens | - se os manuais internos estão aderentes ao que é exigido pela CVM e verificar seu cumprimento. Caso existam evidências de não conformidade, deverá ser feito relato detalhado das falhas encontradas e das medidas adotadas para regularização.<br><br>- se a política de gestão de riscos (mercado, crédito, liquidez, contraparte, operacionais) foi cumprida e se está adequada às normas e regulamentos;<br><br>- relatar desvios e desenquadramentos ocorridos no cumprimento dos mandatos pelos gestores e quais medidas foram adotadas.<br><br>- apurar se a política de gestão de risco de mercado foi adequada para apurar eventos de maior volatilidade ocorridos durante o ano.<br><br>- se as ferramentas técnicas utilizadas passaram por alterações ou revisões (seja pela gestora, ou por seu fornecedor), se há novas funcionalidades, controles ou relatórios que foram implementados, ou se há a expectativa para o exercício futuro.<br><br>- sobre risco operacional, são recomendadas as apresentações de estatísticas dos eventos ocorridos ao longo do ano, seu diagnóstico e aprimoramentos motivados.<br><br>- sobre risco de crédito, apurar se a área de gestão está dando o tratamento estabelecido nas políticas em situações especiais, tais como eventos de default, atrasos de pagamentos, revisões de cláusulas de títulos, reavaliação ou mudanças de garantias. |

| | |
|---|---|
| Ambiente Regulatório | - analisar a efetividade do mapeamento e controle de mudanças regulatórias que afetaram a instituição, e em que medidas os devidos ajustes feitos (políticas, procedimentos, profissionais, controles etc.) já se encontram encerrados, implementados, em fase de análise, bem como quais foram os ajustes feitos em decorrência disso.<br><br>- verificar se os ofícios recebidos de reguladores, autorreguladores e demais autoridades foram tratados de forma adequada e se levaram a melhorias operacionais. |