Política de *Compliance* e Controles Internos

Versão Atualizada: Agosto de 2021

Esta Política trata de:

1-) *Compliance* e controles internos;

2-) Certificação;

3-) Confidencialidade, Segurança da Informação e Cybersegurança

ANEXO I - Quadro de Obrigações Periódicas da JOURNEY

ANEXO II - Modelo de Relatório de Aderência

ANEXO III - Orientações Gerais sobre o Conteúdo Técnico do Teste de Aderência

ANEXO IV – Conteúdo Mínimo do Relatório Anual de *Compliance*

Objetivo

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

A quem se aplica?

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

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

Estrutura e Responsabilidades

Cabe à JOURNEY 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 JOURNEY 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 *Compliance*.**

Cabe à alta administração da JOURNEY:

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 JOURNEY 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 *Compliance* deve:

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

2-) Gerenciar o Comitê de *Compliance* e Risco Operacional (*"*Comitê de *Compliance"*) e o Conselho de Ética, garantindo seu adequado funcionamento e o registro em ata das decisões tomadas;

3-) Designar os secretários das reuniões do Comitê de *Compliance* e 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 JOURNEY.

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

O Diretor de *Compliance* se reporta **apenas** à alta administração da JOURNEY, 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 JOURNEY, sendo exercidos de forma **autônoma e independente**, com ampla liberdade de discussão e de análise dos temas sob sua responsabilidade, sendo que o Diretor de *Compliance* detém o poder de veto em assuntos de natureza regulatória e de conformidade de políticas (ver documento "Comitês – Termos de Referência").

A Área de *Compliance* se dedica 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.

[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.

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.

Escopo e Atribuições do *Compliance*

A atuação do Diretor de *Compliance* tem por escopo:

Temas Normativos

- ✓ Controlar a aderência a novas leis, regulação e normas de autorregulação aplicáveis à JOURNEY e às suas atividades, e apresentar o resultado de suas verificações no Comitê de *Compliance*;
- ✓ Controlar e monitorar as licenças legais e certificações necessárias, e a sua obtenção/renovação/manutenção junto às autoridades reguladoras/autorreguladoras competentes;
- ✓ Auxiliar a alta administração da JOURNEY 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 JOURNEY que desempenhem funções ligadas à consultoria ou gestão de fundos de investimento ou de carteiras administradas atuem com independência[2];
- ✓ Garantir que os controles internos sejam compatíveis com os riscos da JOURNEY em suas atividades[3];
- ✓ Analisar informações, indícios ou identificar, administrar e, se necessário, levar temas para análise e deliberação no Comitê de *Compliance* e/ou 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).

[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.

Governança

- ✓ Aprovar novas políticas internas no Comitê de *Compliance*, ou a sua revisão, por força de mudanças na legislação, regulação ou autorregulação aplicáveis, ou ainda, de decisões internas da JOURNEY;
- ✓ Aprovar a oferta de novos produtos e prestação de novos serviços pela JOURNEY, a partir de *inputs* técnicos do Comitê de Investimento;
- ✓ Atuar para que haja efetividade na segregação física de atividades conflitantes;
- ✓ Apresentar o resultado de seus controles e verificações no Comitê de *Compliance*;
- ✓ Monitorar e buscar a efetiva aplicação dos documentos de *Compliance* e controles internos abaixo listados;
- ✓ Servir como canal para comunicações de desconformidades regulatórias e/ou de temas relacionados ao Código de Ética e Conduta Profissional da JOURNEY e às demais políticas da JOURNEY;
- ✓ Convocar, gerenciar, organizar e secretariar o Comitê de *Compliance*, registrando suas decisões em atas;
- ✓ **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 JOURNEY 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 *Compliance* 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 JOURNEY encontram-se previstos no **Anexo I** a esta Política, bem como na Planilha de controle interno detalhada, intitulada "**Quadro de Rotinas"**.

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

[5] Bem como correspondência, interna e externa, 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.

Documentos de *Compliance* e Controles Internos

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

Documentos Específicos Disponibilizados no Website da JOURNEY

Cabe ao Diretor de *Compliance* preencher o respectivo Formulário de Referência da JOURNEY e mantê-lo em seu *website*. **Tal formulário deve ser atualizado obrigatoriamente até o dia 31 de março de cada ano.**

Adicionalmente, cabe ao Diretor de *Compliance* e PLD manter no *website* da JOURNEY, em suas versões atualizadas, os seguintes documentos:

- ✓ **Código de Ética;**
- ✓ **Política de *Compliance*, Certificação, Segurança da Informação e Cybersegurança;**
- ✓ **Política de Investimentos Pessoais e da Empresa;**
- ✓ **Política de Rateio de Ordens de Investimento;**
- ✓ **Política de Investimentos e Crédito;**
- ✓ **Política de Gestão de Riscos (inclui Gerenciamento do Risco de Liquidez);**
- ✓ **Política de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Corrupção;**
- ✓ **Política de Exercício de Direito de Voto em Assembleias Gerais;**

Teste e Relatório Anual

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

O relatório é de responsabilidade do Diretor de *Compliance*, e, após ratificação pelo Comitê de *Compliance*, é encaminhado à alta administração da JOURNEY anualmente, até o último dia útil de **ABRIL** de cada ano[7].

O Relatório Anual fica disponível para consulta da CVM, na sede da JOURNEY. Tal relatório contém:

- ✓ **As conclusões dos exames efetuados relativos aos controles internos e *Compliance*, inclusive o Teste Anual dos Sistemas de Informações - os testes periódicos dos sistemas de informações, em**

[6] V. modelo no Anexo II e orientação sobre o respectivo conteúdo no Anexo III.

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

especial para os mantidos em meio eletrônico, efetuados pela Diretoria de *Compliance*[8];

- ✓ **As recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e**
- ✓ **A manifestação do Diretor de Gestão, ou, quando for o caso, dos Diretores de Risco e de *Compliance* a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las.**

Organismos Relacionados a *Compliance* e Controles Internos

Comitês

Os comitês da Journey são divididos em:

- Comitê de Crédito;
- Comitê de Investimentos e de Riscos ("Comitê de Gestão") e
- Comitê de Compliance e Risco Operacional ("Comitê de Compliance")

As características e o ordenamento destes comitês estão descritos no documento "Comitês – Termos de Referência".

Conselho de Ética

O Conselho de Ética tem suas atribuições descritas na forma definida no Código de Ética e Conduta Profissional da JOURNEY.

Segregação de Atividades

Cabe ao **Diretor de *Compliance*** assegurar e verificar que sejam devidamente segregadas da atividade de gestão todas e quaisquer atividades eventualmente desempenhadas pela da JOURNEY que com aquela guarde qualquer tipo de conflito, real ou potencial, em qualquer grau, aspecto, medida, tempo e/ou forma.

Ademais disso, a JOURNEY dispõe de instalações que garantem a segregação entre as suas atividades de administração de carteiras de valores mobiliários e as demais atividades desempenhadas pela JOUNEY e/ou por outras empresas de seu grupo, que possam ter eventual conflito de interesse com as suas atividades de gestão de carteiras.

[8] Devem: (i) assegurar que os recursos humanos e computacionais estão adequados ao porte e à área de atuação da JOURNEY, (ii) garantir o adequado nível de confidencialidade e acessos às informações confidenciais, (iii) assegurar que os recursos computacionais estão protegidos contra adulterações e (iv) assegurar que a manutenção de registros permite a realização de auditorias e inspeções.

Contratações Externas

A JOURNEY não realiza quaisquer contratações de prestadores de serviço em nome dos fundos sob sua gestão[9], seja de atividades reguladas pela CVM ou autorreguladas pela ANBIMA, cabendo tais contratações aos respectivos administradores dos referidos fundos.

Esta Política se aplica somente às contratações feitas pela própria JOURNEY em seu próprio nome e benefício.

A contratação de serviços de terceiros deve ser precedida das seguintes providências[10]:

- ✓ **Exigência de documentos e das certidões reputadas convenientes, seguindo, quando aplicável, procedimentos semelhantes aos descritos na Política de Prevenção à Lavagem de Dinheiro;**
- ✓ **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 JOURNEY, o Colaborador envolvido na negociação deverá informar ao Comitê de *Compliance* sobre qualquer relacionamento familiar ou pessoal, sejam laços de amizade ou negocial, que tenha com membros do potencial contratado.**

Após a contratação dos respectivos serviços, a área de *Compliance* da JOURNEY poderá, a seu critério, supervisionar os contratados[11].

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.

Qualquer eventual exceção às normas acima deverá ser reportada no Comitê de *Compliance*.

A contratação de terceiros deverá ser orientada pelas seguintes diretrizes:

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

[10] 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.

[11] 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.

- ✓ 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 *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 nos seguintes casos:
    - Compras e contratações para valores inferiores a R$ 10.000,00 (dez 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 necessário realizar concorrência a cada contratação ou compra;
    - Compras e contratações em casos de fornecedor/prestador especializado;
    - Compras e contratações em casos emergenciais, que serão caracterizados pela urgência de atendimento de situação que possa ocasionar prejuízo ou comprometer o trabalho, e que não pôde ser previsto antecipadamente.

Soft Dollar

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

Proteção de Dados

A JOURNEY recebe informações pessoais de clientes apenas para fins cadastrais, não havendo possibilidade nem intenção de lhes destinar finalidade ou tratamento diversos de tais objetivos.

Sem prejuízo do teor acima, o(a) cliente tem sempre assegurado seu direito a:

- ✓ acesso a seus dados em poder da JOURNEY, a qualquer tempo;
- ✓ correção de dados incompletos, inexatos ou desatualizados;
- ✓ anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei n.º 13.709, de 14 de agosto de 2018 ("LGPD");
- ✓ portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa;

- ✓ eliminação dos dados pessoais tratados com o consentimento do titular, exceto no caso de dever de sua conservação para cumprimento de obrigações regulatórias e das hipóteses do art. 16 da LGPD;

- ✓ informação das entidades públicas e privadas com as quais a JOURNEY porventura tenha realizado o uso compartilhado de dados;

- ✓ recusa de seu consentimento ao tratamento dos dados pessoais em poder da JOURNEY, com informação das consequências de sua negativa; e

- ✓ revogação de seu consentimento, mediante manifestação expressa.

Política de Certificação

A quem se aplica?

Sócios, diretores e funcionários da JOURNEY CAPITAL ("JOURNEY"), 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 JOURNEY ("Colaboradores").

Assim sendo, a JOURNEY requer dos profissionais elencados acima, relativamente à atividade de gestão de carteiras, a "Certificação de Gestores ANBIMA" (CGA), sempre que aplicável às suas atividades.

Responsabilidades

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

Revisão e Atualização

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

Controles

O Diretor de *Compliance* mantém controle dos Colaboradores da JOURNEY com as seguintes informações:

- ✓ **dados profissionais;**
- ✓ **data de admissão;**

- ✓ **data de desligamento, quando aplicável;**
- ✓ **atividade exercida;**
- ✓ **área de atuação;**
- ✓ **cargo;**
- ✓ **tipo de gestor, quando aplicável;**
- ✓ **endereço eletrônico individual;**
- ✓ **se dispõe de certificação ANBIMA e a sua validade.**

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

A CGA é válida por prazo indeterminado, *desde que* o profissional esteja exercendo atividades que dela sejam objeto.

Compete ao Diretor de *Compliance* 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, a Diretoria de *Compliance* é responsável por manter a documentação formal que evidencie o afastamento do Colaborador das atividades elegíveis à certificação.

Cabe ao Diretor de *Compliance* 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 Comitê de *Compliance,* que deve monitorar a sua devida regularização.

Quaisquer outras situações identificadas aplicáveis à matéria devem ser objeto de análise, aprovação, formalização ou eventual assunção de risco no âmbito do Comitê de *Compliance*.

Admissões de Colaboradores

O **Diretor de *Compliance*** 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 certificação CGA devem ser contratados com certificações válidas. Eventuais exceções deverão ser avaliadas pelo Diretor de *Compliance* e reportadas ao Comitê de *Compliance* 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.

Licenças e Desligamentos

No caso de licenças e desligamentos, o **Diretor de *Compliance*** deve verificar se o Colaborador está vinculado à JOURNEY 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 *Compliance*** é responsável pela veracidade e manutenção do banco de dados da ANBIMA atualizado **(aplicável para atividades relacionadas à gestão de recursos de terceiros)**.

O controle de admissão, licença e demissão consta na agenda regulatória do Comitê de *Compliance*, onde são formalizados tais registros, devendo as **eventuais atualizações junto à entidade ocorrer até o último dia do mês subsequente ao evento.**

Código de Ética e Conduta Profissional

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

Política de Confidencialidade, Segurança da Informação e Cybersegurança

Objetivo

Estabelecer princípios e diretrizes de proteção das informações no âmbito da JOURNEY CAPITAL ("JOURNEY").

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 JOURNEY (doravante, "Colaboradores").

Responsabilidades

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

O **Diretor de *Compliance*** deve garantir o atendimento a esta Política, sendo o responsável na JOURNEY 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 JOURNEY ou de clientes);**
- ✓ **Sejam objeto de acordo de confidencialidade celebrado com terceiros;**
- ✓ **Identifiquem ações estratégicas – dos negócios da JOURNEY, seus clientes ou dos portfólios sob gestão ou consultoria[12];**
- ✓ **Todas as informações técnicas, jurídicas e financeiras, escritas ou arquivadas eletronicamente, que digam respeito às atividades da JOURNEY, e que sejam 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;**
- ✓ **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 *Compliance***, (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 *Compliance*** acerca da possibilidade de compartilhamento da Informação Confidencial.

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

Disposições Gerais

Os seguintes princípios norteiam a segurança da informação na JOURNEY:

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 JOURNEY:

- ✓ 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 *Compliance*.

Identificação, Classificação e Controle da Informação

O Colaborador que recebe ou prepara uma informação deve identificar a sua natureza. Algumas informações podem ser classificadas como “Confidenciais”.

Para tal, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

O acesso às Informações Confidenciais **deve ser restrito e controlado**.

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

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

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. 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 JOURNEY **são de sua propriedade exclusiva**, sendo permitido o uso moderado para fins particulares, mediante autorização prévia do **Diretor de *Compliance***.

A JOURNEY poderá, a qualquer momento, mediante prévia aprovação do Diretor de *Compliance,* 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.**

No caso de mudança de área ou desligamento do Colaborador, a respectiva senha de acesso é imediatamente adaptada para compatibilizar/adequar o acesso, ou cancelada em definitivo, visando ao impedimento de acesso não autorizado pelo ex-Colaborador.

O **Diretor de *Compliance*** pode definir bloqueio a sites caso necessário. O monitoramento pode ser feito sem necessidade de prévia ciência dos Colaboradores.

O acesso a sites de armazenamento de arquivos em "nuvem" é permitido.

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

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 JOURNEY, 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 *Compliance***, que adotará as medidas cabíveis.

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

O plano de contingência e de continuidade dos principais sistemas e serviços deve ser objeto de testes, visando a reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

No caso de vazamento de informação, ou acesso indevido a informação, o Diretor de *Compliance* 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 *Compliance*** e reportados ao Comitê de *Compliance*.

Os testes 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.**

Riscos de Cybersegurança

As principais ameaças e riscos aos ativos cibernéticos da JOURNEY 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;

[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.

- ✓ *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 JOURNEY 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[15].

O responsável por tais questões na JOURNEY é o **Diretor de *Compliance***.

São itens obrigatórios de Cybersergurança (empresa):

- A adequada proteção dos ativos cibernéticos da JOURNEY, aí incluídos sua rede, sistemas, *softwares*, websites, equipamentos e arquivos eletrônicos.
- Restrição e controle do acesso e privilégios de usuários remotos e externos;
- 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 JOURNEY;
- Detectar, identificar, registrar e comunicar ao Diretor de *Compliance* e PLD as violações ou tentativas de acesso não autorizadas;

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

- 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 JOURNEY dispõe de *firewall* 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 Cybersergurança (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 JOURNEY, NUNCA as repassar, alertando o responsável da sua área e o Diretor de *Compliance*, se for o caso;
- Ao se ausentar do seu local de trabalho, 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 JOURNEY [16];
- É permitido o uso pessoal (de forma moderada) dos equipamentos de informática e de comunicação de propriedade da JOURNEY, sempre lembrando que pertencem à JOURNEY e são rastreáveis e sujeitos a monitoramento;[17]

[16] 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;

[17] Sem a necessidade de ciência prévia do Colaborador, bem como podem se tornar públicos em caso de auditoria, exigência judicial ou regulatória.

- Tecnologias, marcas, metodologias e quaisquer informações que pertençam à JOURNEY 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;
- A gravação de cópias de arquivos e instalação de programas em computadores deverá ser previamente autorizada pelo responsável pelo departamento da JOURNEY;
- Em regra, os acessos a dispositivos móveis, como pen drives, HDs externos, cartões de memória, estão bloqueados na JOURNEY, devendo as eventuais exceções devem ser previamente aprovadas pelo responsável pelo *Compliance*;
- Cada Colaborador terá acesso somente a pastas eletrônicas relacionadas à sua área e às pastas comuns a todos os Colaboradores.

São itens VEDADOS de Cybersergurança (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];
- Divulgar informações ou trocar arquivos com configurações dos equipamentos e de negócios da JOURNEY, ou qualquer outra informação sobre a JOURNEY, seus negócios, clientes, produtos, equipamentos ou Colaboradores, sem prévia aprovação[19];
- Trocar informações que causem quebra de sigilo bancário e/ou possuam caráter confidencial ou estratégico;
- Prejudicar intencionalmente usuários da internet, mediante desenvolvimento de programas, acessos não autorizados a computadores e alteração de arquivos, programas e dados na rede da JOURNEY;
- Divulgar propaganda ou anunciar produtos ou serviços particulares pelo correio eletrônico da JOURNEY;
- Alterar qualquer configuração técnica dos *softwares* que comprometam o grau de segurança, ou impeçam/dificultem seu monitoramento pelo **Diretor de *Compliance***;
- Contratar provedores de acesso sem autorização prévia do **Diretor de *Compliance***;
- Redirecionar caixa postal pessoal (e-mail de outros provedores) para a sua caixa postal de correio eletrônico na JOURNEY e vice-versa.
- Uso de compartilhadores de informações, tais como redes *Peer-toPeer* (P2P – p. ex., Kazaa, eDonkey, eMule, BitTorrent e semelhantes) nas dependências da JOURNEY;
- *Download* de músicas, vídeos ou quaisquer outros arquivos que possam comprometer o bom funcionamento da infraestrutura da JOURNEY ou que violem direitos autorais.

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

[19] Em caso de exigência de alguma autoridade ou entidade autorreguladora, o Colaborador deverá solicitar orientação ao Diretor de *Compliance* e PLD.

ANEXO I

Quadro de Obrigações Periódicas da JOURNEY

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 (data base 31/12)
RCVM 21	17, *caput* e II	Formulário de Referência	Envio do FR pelo CVMWeb	Anualmente, até 31/03 (data base 31/12)
ICVM 510	1.º, II	Declaração Eletrônica de Conformidade	Envio pelo CVMWeb	Anualmente, até 31/03 (data base 31/12)
ICVM 617	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
ICVM 617	6.º, I a VII, e §§	Relatório Anual de PLD	Entrega do relatório à administração da JOURNEY (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
ICVM 617	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	Mensalmente, até o último dia do mês

			ANBIMA das informações relativas aos colaboradores certificados, em processo de certificação, com a certificação vencida, e/ou em processo de atualização da certificação	subsequente à data do evento

II.) Informações Eventuais

Norma	Artigo	Tema	Obrigação	Período
ICVM 510	1.º, I	Atualização de dados cadastrais	Atualização via CVMWeb	7 (sete) dias úteis contados do evento que deu causa à alteração
ICVM 617	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

JOURNEY CAPITAL ADMINISTRAÇÃO DE RECURSOS LTDA.

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

Prezados Senhores,

Em cumprimento ao disposto no art. 25 da RCVM 21, vimos apresentar a V.Sas. o relatório pertinente às atividades da **JOURNEY CAPITAL ADMINISTRAÇÃO DE RECURSOS LTDA.** ("JOURNEY") 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 JOURNEY, 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 Controles Internos da JOURNEY, e o correspondente parecer final do Diretor *Compliance* e Controles Internos, 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)

[20] O relatório da ICVM 539 deverá ter conteúdo similar, porém sobre o tema de *suitability*.

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 *Compliance* e PLD

(inserir com detalhes)

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,

[•]

JOURNEY CAPITAL ADMINISTRAÇÃO DE RECURSOS LTDA.

Diretor de *Compliance* e PLD

ANEXO III

Orientações Gerais sobre o Conteúdo Técnico do Teste de Aderência

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

Tais temas devem – ao longo do ano – ser endereçados e monitorados no Comitê de *Compliance*, Controles Internos e Ética, e, quando necessário, ser objeto de acompanhamento próximo da alta gestão (sócios e diretores) da JOURNEY.

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 Comitê de *Compliance*, Controles Internos e Ética.

I. **Conclusão dos Exames Efetuados**

(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 a 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;**
- ✓ **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 de *Compliance*

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. - verificar os requisitos de reputação ilibada dos diretores e dos controladores da JOURNEY.
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 JOURNEY está sendo atualizado quando cabível.
Atualização de dados cadastrais	- atestar que os dados cadastrais da JOURNEY 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 JOURNEY em sua versão atualizada; - 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 JOURNEY e ao colaborador em questão, com destaque para as medidas tomadas para sua prevenção futura. - 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 JOURNEY. - 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. - 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. - se a guarda e a manutenção dos arquivos da empresa pelo prazo estabelecido nas normas preserva sua integridade e disponibilidade; - 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 JOURNEY.

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. - se a política de gestão de riscos (mercado, crédito, liquidez, contraparte, operacionais) foi cumprida e se está adequada às normas e regulamentos; - relatar desvios e desenquadramentos ocorridos no cumprimento dos mandatos pelos gestores e quais medidas foram adotadas. - apurar se a política de gestão de risco de mercado foi adequada para apurar eventos de maior volatilidade ocorridos durante o ano. - 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. - sobre risco operacional, são recomendadas as apresentações de estatísticas dos eventos ocorridos ao longo do ano, seu diagnóstico e aprimoramentos motivados. - 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. - verificar se os ofícios recebidos de reguladores, autorreguladores e demais autoridades foram tratados de forma adequada e se levaram a melhorias operacionais.