



## MANUAL DE COMPLIANCE

contato@oikoswm.com  
www.oikoswm.com  
+55 11 2507 4756  
Rua Jerônimo da Veiga 45, 6º andar  
São Paulo - SP  
04536-000

# MANUAL DE COMPLIANCE

DATA DA ÚLTIMA REVISÃO	01/04/2021
ÁREA RESPONSÁVEL	COMPLIANCE

# ÍNDICE

<u>1</u>	<u>CONSIDERAÇÕES INICIAIS</u>	<u>4</u>
<u>2</u>	<u>COMPLIANCE E ENFORCEMENT</u>	<u>4</u>
<u>3</u>	<u>PREVENÇÃO E TRATAMENTO DE FRAUDES E LAVAGEM DE DINHEIRO</u>	<u>6</u>
<u>4</u>	<u>LEI ANTICORRUPÇÃO BRASILEIRA E DECRETO REGULAMENTAR</u>	<u>8</u>
<u>5</u>	<u>POLÍTICA DE CONFIDENCIALIDADE: SIGILO E CONDUTA</u>	<u>9</u>
<u>6</u>	<u>POLÍTICA DE SEGREGAÇÃO DE ATIVIDADES: “CHINESE WALL”</u>	<u>10</u>
<u>7</u>	<u>PROGRAMA DE SEGURANÇA CIBERNÉTICA</u>	<u>10</u>
7.1	AVALIAÇÃO DE RISCOS E POLÍTICA DE CLASSIFICAÇÃO DAS INFORMAÇÕES	10
7.1.1	AVALIAÇÃO DE RISCOS	10
7.1.2	POLÍTICA DE CLASSIFICAÇÃO DAS INFORMAÇÕES	11
7.2	AÇÕES DE PROTEÇÃO E POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES	11
7.2.1	AÇÕES DE PROTEÇÃO	12
7.2.2	POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES	12
7.3	ROTINAS DE MONITORAMENTO E TESTES	13
7.4	PLANO DE RESPOSTA A INCIDENTES E CONTINUIDADE DE NEGÓCIOS	13
7.4.1	PLANO DE RESPOSTA A INCIDENTES	13
7.4.2	PLANO DE CONTINUIDADE DE NEGÓCIOS	14
7.5	RESPONSABILIDADE E REVISÃO	14
<u>8</u>	<u>TREINAMENTO E POLÍTICA DE CERTIFICAÇÃO</u>	<u>15</u>
8.1	TREINAMENTO E PROCESSO DE RECICLAGEM	15
8.2	POLÍTICA DE CERTIFICAÇÃO	15
<u>9</u>	<u>DÚVIDAS OU AÇÕES CONTRÁRIAS</u>	<u>15</u>
<u>10</u>	<u>ACOMPANHAMENTO DAS POLÍTICAS DESCRITAS NOS CÓDIGOS</u>	<u>16</u>
<u>11</u>	<u>SANÇÕES</u>	<u>17</u>



## 1 CONSIDERAÇÕES INICIAIS

O Manual de Compliance (“Manual”) da Oikos Gestão de Recursos Ltda. (“Oikos”) dispõe sobre padrões de comportamento, princípios, conceitos e valores, com o objetivo de dirimir conflitos de interesses, garantir a confidencialidade das informações bem como promover práticas de prevenção e combate a atividades ilícitas.

Os parâmetros de conduta previstos neste Manual têm como base as principais normas e regulamentos do mercado financeiro e se norteiam nos princípios da integridade, transparência, igualdade, ética, qualidade e eficiência de seus serviços.

Todas as regras de comportamento definidas neste documento devem ser respeitadas e cumpridas pelos Sócios Diretores, funcionários e estagiários da Oikos (“Equipe” ou “Colaboradores”). A adoção de tais condutas influencia positivamente o ambiente de trabalho e fortalece a relação com clientes da Oikos, bem como contribui para o bom funcionamento do mercado financeiro.

A adesão as Políticas definidas nesse Manual é obrigatória e ocorre no início do vínculo contratual com a Oikos, mediante a assinatura de Termo de Responsabilidade e Termo de Confidencialidade, constantes no Código de Ética da Oikos. Todos que vierem a ingressar a Equipe da Oikos devem se assegurar do perfeito entendimento do completo conteúdo deste Manual, “Código de Ética”, “Manual de Risco”, “Política de Investimentos Pessoais”, “Política de Divisão e Rateio de Ordens entre as Carteiras de Valores Mobiliários” (em conjunto denominados, “Códigos”), bem como das leis e normas aplicáveis à Oikos.

Condutas pautadas no bom senso, transparência, verdade e que afastem conflitos e desvios éticos devem sempre ser incentivadas e adotadas em todas e quaisquer circunstâncias. A Oikos e sua Equipe não admitem e repudiam qualquer manifestação de preconceitos relacionados à origem, raça, religião, classe social, sexo, deficiência física ou qualquer outra forma de preconceito que possa existir.

A eventual aplicação de sanções (advertência, suspensão ou demissão) decorrentes do descumprimento das normas e princípios estabelecidos neste Manual, ou dos demais Códigos, é de responsabilidade exclusiva dos Sócios Diretores da Oikos, exceto do Diretor de Compliance. Em todos os casos, será garantido ao membro da Equipe amplo direito de defesa.

A Oikos não assume a responsabilidade de membros da Equipe que atuem em contrariedade aos dispositivos desse Manual, ou dos demais Códigos, que descumpram a lei ou que cometam qualquer tipo de infração civil, administrativa ou penal, no exercício de suas funções.

Será facultado a Oikos o exercício do direito de regresso em face do responsável pelas práticas descritas acima, caso venha a ser responsabilizada ou sofra prejuízo de qualquer natureza por atos de membros de sua Equipe.

O membro da Equipe que tiver conhecimento ou suspeita de ato não compatível com os dispositivos deste Manual ou dos demais Códigos, deverá reportar tal acontecimento ao Diretor de Compliance. O membro da Equipe que se omitir de tal obrigação poderá sofrer, além de ação disciplinar, demissão ou desligamento por justa causa.

As Políticas estabelecidas nesse Manual serão revisadas anualmente, e alteradas caso constata-se necessidade de atualização de seu conteúdo.

## 2 COMPLIANCE E ENFORCEMENT

O presente ponto dispõe acerca das políticas relativas ao monitoramento, fiscalização, verificação e aplicação das medidas e penalidades (Compliance e Enforcement) relacionadas ao cumprimento do disposto no presente Manual ou nos demais Códigos da Oikos.

O objetivo dos controles e procedimentos internos adotados pela Oikos é o de assegurar, no maior grau possível, o cumprimento das regras previstas neste Manual, bem como dos demais Códigos da Oikos, e dos demais normativos aplicáveis.

A coordenação direta das atividades relacionadas a este Manual será uma atribuição do “Diretor de Compliance” responsável pelo cumprimento das regras, políticas, procedimentos e controles internos da Oikos.

São obrigações do Diretor de Compliance:

- Acompanhar as políticas descritas neste Manual, bem como nos demais Códigos da Oikos;
- Levar quaisquer pedidos de autorização, orientação ou esclarecimento ou casos de ocorrência, suspeita ou indício de prática que não esteja de acordo com as disposições deste Manual, ou dos demais Códigos, e das demais normas aplicáveis à atividade da Oikos para apreciação dos Sócios Diretores da Oikos.
- Atender prontamente todos os Colaboradores da Oikos.
- Identificar possíveis condutas contrárias a este Manual ou aos demais Códigos.

O Compliance tem como principal objetivo monitorar, fiscalizar, verificar e aplicar medidas e penas relacionadas ao cumprimento, ou não, dos Códigos que regem os princípios, conceitos e valores que orientam a conduta de todos aqueles que possuam cargo, função, posição, relação societária, empregatícia, comercial, profissional, contratual ou de confiança com a Oikos.

O Compliance adotará postura ativa e contará com toda a estrutura necessária para exercer suas funções. Entre os pontos que demonstram tal preocupação, estão os seguintes:

- O acesso às informações confidenciais e sigilosas da Oikos está restrito e é diferenciado conforme as funções desempenhadas por cada um dos colaboradores. O controle de acesso a tais informações será realizado por meio de senhas pessoais e intrasferíveis outorgadas, de acordo com a função que será desempenhada por determinado colaborador, impossibilitando, assim, que qualquer tipo de conteúdo seja tangível a todos. O Compliance terá acesso a todas as pastas e arquivos eletrônicos da Oikos, tendo plenos poderes e condições técnicas de monitorar o conteúdo transmitidos e recebidos pelos Colaboradores;
- O acesso às instalações físicas da Oikos é totalmente controlado e acessível somente pelos colaboradores. O Compliance tem acesso ao registro do sistema eletrônico e telefônico, de modo que tem totais condições de verificar, “ao vivo”, a boa normalidade das ações incorridas dentro da Oikos;
- Todo conteúdo que está na rede será acessível pelo Compliance da Oikos;
- A Oikos realizará inspeções com periodicidade mensal, a cargo do Diretor de Compliance, com base em sistemas de monitoramento eletrônico, independentemente da ocorrência de descumprimento ou suspeita ou indício de descumprimento de quaisquer das regras estabelecidas nos Códigos ou aplicáveis às atividades da Oikos.
- Mensagens de correio eletrônico de Colaboradores poderão ser interceptadas e abertas para ter a regularidade de seu conteúdo verificada, computadores poderão ser auditados e conversas telefônicas poderão ser gravadas e escutadas sem que isto represente invasão da privacidade dos Colaboradores já que se trata de ferramentas de trabalho disponibilizadas pela Oikos.
- Adicionalmente, será realizado um monitoramento mensal, a cargo do Diretor de Compliance, sobre uma amostragem significativa dos Colaboradores, escolhida aleatoriamente pelo Diretor de Compliance, para que sejam verificados os arquivos eletrônicos, inclusive e-mails, bem como as ligações telefônicas dos Colaboradores selecionados, com o objetivo de verificar possíveis situações de descumprimento às regras contidas nos Códigos.

Está claro que o Compliance da Oikos adotará uma postura ativa e possui as ferramentas necessárias para exercer suas funções e fazer com que a Oikos e seus colaboradores sigam estritamente as regras aplicáveis à gestora e, em caso de descumprimento, que sejam aplicadas as penalidades necessárias.

Todo e qualquer Colaborador da Oikos que souber de informações ou situações em andamento, que possam afetar os interesses da Oikos, gerar conflitos ou, ainda, se revelarem contrárias aos termos previstos nos Códigos, deverá informar ao Diretor de Compliance ou aos Sócios Diretores, para que sejam tomadas as providências cabíveis.

São atribuições dos Sócios Diretores da Oikos relacionadas a este Manual:

- Definir os princípios éticos a serem observados por todos os Colaboradores da Oikos, constantes dos Códigos ou de outros documentos que vierem a ser produzidos para este fim, elaborando sua revisão periódica.
- Promover a ampla divulgação e aplicação dos preceitos éticos no desenvolvimento das atividades de todos os Colaboradores da Oikos, inclusive por meio dos treinamentos previstos no item 8 deste Manual.
- Apreciar todos os casos que cheguem ao seu conhecimento sobre o descumprimento dos preceitos éticos e de compliance previstos nos Códigos ou nos demais documentos aqui mencionados, e também apreciar e analisar situações não previstas.
- Analisar situações que possam ser caracterizadas como conflito de interesse, pessoal ou profissional, nos termos previstos nos Códigos ou nos demais documentos aqui mencionados.
- Garantir o sigilo de eventuais denunciadores de delitos ou infrações, mesmo quando estes não solicitarem, exceto nos casos de necessidade de testemunho judicial.
- Solicitar sempre que necessário, para a análise de suas questões, o apoio de assessores profissionais.
- Tratar todos os assuntos que cheguem ao seu conhecimento dentro do mais absoluto sigilo e preservando os interesses e a imagem institucional e corporativa da Oikos, como também dos Colaboradores envolvidos.

E, ainda, cabe aos Sócios Diretores da Oikos definir e aplicar eventuais sanções aos Colaboradores, nos termos do estipulado no item 11 deste Manual.



### 3 PREVENÇÃO E TRATAMENTO DE FRAUDES E LAVAGEM DE DINHEIRO

Seguindo o determinado pela Lei 9.613, de 03 de março de 1998 e de acordo com a Circular 3.461, de 24 de agosto de 2009 e Carta-Circular 2.826, de 4 de dezembro de 1998, ambas editadas pelo Banco Central do Brasil, bem como a Instrução CVM 301, de 16 de abril de 1999, a prevenção da utilização dos ativos e sistemas da Oikos para fins ilícitos, tais como crimes de "lavagem de dinheiro", ocultação de bens e valores, é dever de todos os Colaboradores da Oikos.

Qualquer suspeita de operações financeiras e não financeiras que possam envolver atividades relacionadas aos crimes de lavagem de dinheiro, ocultação de bens e valores, bem como incorporar ganhos de maneira ilícita, para a Oikos, clientes ou para o Colaborador, devem ser comunicadas imediatamente aos Sócios Diretores da Oikos.

A análise será feita caso a caso, ficando sujeitos os responsáveis às sanções previstas neste Manual, inclusive desligamento ou exclusão por justa causa, no caso de Colaboradores que sejam sócios da Oikos, ou dispensa por justa causa, no caso de Colaboradores que sejam empregados da Oikos, e ainda às consequências legais cabíveis. Além disso, para clientes, a Oikos, constatada uma situação que se enquadre no descrito acima, comunicará imediatamente às entidades cabíveis, notadamente a CVM e o COAF, e cessará a realização de operações com tal cliente.

A Oikos e os Colaboradores obrigam-se a zelar para que os seguintes procedimentos sejam mantidos, em particular em relação a clientes que não sejam fundos de investimentos administrados por instituição financeira: (i) as informações cadastrais dos clientes deverão ser mantidas atualizadas; (ii) a compatibilidade entre a atividade econômica e capacidade financeira e o perfil de risco deverão ser verificados; (iii) todas e quaisquer operações consideradas anormais deverão ser comunicadas ao Diretor de Compliance, que será responsável por comunicar as referidas operações aos Sócios Diretores da Oikos, conforme o caso, na forma da regulamentação aplicável.

São mantidos controles e registros internos consolidados que permitem verificar, além da adequada identificação do cliente, a compatibilidade entre as correspondentes movimentações de recursos, atividade econômica e capacidade financeira.

ão monitoradas notícias veiculadas na mídia que estejam relacionadas à lavagem de dinheiro e aos clientes da Oikos. O objetivo é identificar possíveis clientes vinculados aos fatos e realizar a respectiva análise.

Movimentações financeiras que possam indicar a existência de crime, em razão de suas características, valores, formas de realização e instrumentos utilizados ou que não apresentem fundamento econômico ou legal, bem como aquelas com indícios de financiamento ao terrorismo devem ser comunicadas ao Diretor de Compliance.

A Oikos deverá dispensar especial atenção na contratação de serviços de administração de carteira por clientes (i) investidores não residentes, especialmente quando constituídos sob a forma de trusts e sociedades com títulos ao portador; (ii) investidores com grandes fortunas geridas por áreas de instituições financeiras; e (iii) pessoas politicamente expostas.

A Oikos compromete-se a comunicar à CVM, em até 24h a contar da ocorrência do fato, todas as transações ou propostas que possam constituir-se em sérios indícios de crimes de "lavagem" ou ocultação de bens, direitos e valores provenientes dos crimes elencados na legislação aplicável, caso se verifique (i) a existência de características excepcionais no que se refere às partes envolvidas, forma de realização ou instrumentos utilizados; ou (ii) a falta objetiva de fundamento econômico ou legal para a operação.

A Oikos deverá comunicar o Conselho de Controle de Atividades Financeiras - COAF, dentro de um prazo máximo de 24 horas da ocorrência de quaisquer transações, ou propostas de transação, que possam constituir indicações de crimes referentes à "lavagem" ou ocultação de ativos, direitos e objetos de valor derivados de infrações penais, nos termos da Lei 9.613/98, incluindo terrorismo ou seu financiamento, ou relacionados a eles.

Adicionalmente, nos termos da Instrução CVM 534, a Oikos deverá fornecer à CVM uma declaração anual negativa atestando que não houve transações ou propostas de transações durante o ano anterior passíveis de comunicação, com base na Lei 9.613/98 e regulamentação aplicável, se este for o caso. O Diretor de Compliance possui soberania e autonomia para comunicação de indícios da ocorrência dos crimes previstos na Lei 9.613 ou a eles relacionados.

O grande objetivo da política em questão é dotar a Oikos de procedimentos eficazes, por meio de uma estrutura permanente de vigilância, visando minimizar o risco de lavagem de dinheiro e financiamento ao terrorismo nas atividades de gestão realizadas pela Oikos.

A Oikos reforça que todos os colaboradores são responsáveis pelo estabelecimento de um ambiente permanente de controle, no qual seja possível monitorar todas as operações de clientes e não clientes, pessoas físicas e jurídicas, com vistas a identificar ações ilícitas relacionadas aos crimes de lavagem de dinheiro ou financiamento ao terrorismo. Ao identificar situações do tipo, devem reportar ao Diretor de Compliance.

A Oikos se ampara nas seguintes Políticas e procedimentos:

- Política Conheça seu Cliente e Suas Atividades:



Objetivo de identificar e conhecer a origem dos recursos financeiros de seus clientes, suas atividades, bem como a potencialidade dos seus negócios. No caso de pessoas jurídicas, a Oikos buscará identificar o beneficiário final. Dessa forma, está protegendo sua reputação e reduzindo os riscos de seus produtos e serviços serem utilizados para legitimar recursos provenientes de atividades ilícitas.

Tal checagem será feita de forma passiva, isto é, mediante recebimento de informações dos clientes, e ativa, mediante consulta de listas restritivas, sites de busca e órgãos reguladores.

O Diretor de Compliance, responsável pela presente política, estabelecerá os critérios para adequação do nível de monitoramento de clientes, como atividade/profissão. Tais critérios poderão ser submetidos e discutidos com os demais sócios-diretores, cabendo ao Diretor de Compliance a decisão final.

As informações dos clientes serão constantemente atualizadas pelo cliente e pela Oikos.

- Política Conheça Seu Colaborador e Parceiro:

A Oikos considera ser de sua responsabilidade o conhecimento sobre seus colaboradores, por meio de acompanhamento acerca dos aspectos comportamentais, padrões de vida e respectivos resultados operacionais, atentando para alterações inusitadas e significativas nestas variáveis.

Tal checagem será feita de forma passiva, isto é, mediante recebimento de informações dos colaboradores e parceiros, e ativa, mediante consulta de listas restritivas, sites de busca e órgãos reguladores.

As informações dos colaboradores e parceiros serão constantemente atualizadas pelo cliente e pela Oikos.

- Procedimentos para Pessoas Expostas Politicamente (PEP):

Pela definição, Pessoas Expostas Politicamente ("PEPs") são os agentes públicos que desempenham ou tenham desempenhado, nos últimos cinco anos, no Brasil ou em países, territórios e dependências estrangeiros, cargos, empregos ou funções públicas relevantes, assim como seus representantes e familiares e outras pessoas de seu relacionamento próximo.

As Circulares 3.461/09 e 3.654/13, do Bacen e a Instrução nº 301 da CVM, dispõem sobre os procedimentos a serem observados pelos agentes financeiros para o estabelecimento de relação de negócios e acompanhamento das movimentações financeiras de PEPs, os quais devem:

- Ser estruturados de forma a possibilitar a identificação de pessoas consideradas politicamente expostas; e
- Identificar a origem dos fundos envolvidos nas transações dos clientes, identificados como PEPs, podendo ser considerada a compatibilidade das operações com o patrimônio constante nos respectivos cadastros.

A Oikos adota medida de vigilância reforçada e contínua da relação de negócio mantida com pessoa politicamente exposta.

A Oikos possui um processo de treinamento inicial de todos os seus colaboradores, conforme melhor detalhado em item abaixo.

Caberá ao Diretor de Compliance o monitoramento e fiscalização do cumprimento, pelos colaboradores, da presente política de combate à "lavagem de dinheiro" da Oikos, sendo certo que contará com o apoio necessário de escritório de advocacia e com assessoria de tecnologia, informação e contábil.

A Oikos realizará revisões e auditorias contínuas de sua política de lavagem de dinheiro, seja pelos sócios-diretores e por colaboradores sorteados para realização de tal auditoria, seja por entidades externas.

- Política de Monitoramento de Ativos e Contrapartes:

A Oikos, como instituição que realiza a gestão de fundos de investimento e de carteiras administradas, é responsável pela análise e verificação na aquisição de ativos e valores mobiliários com a finalidade de prevenção e tratamento de fraudes e lavagem de dinheiro.

Deste modo, a Oikos estabelece procedimentos que visam identificar e controlar operações efetuadas fora dos padrões praticados no mercado, como a análise diária das carteiras sob gestão e a análise dos valores de mercado dos ativos que as compõem.

Por sua vez, as contrapartes de quaisquer operações efetuadas pela Oikos, em razão de suas atividades de gestão de fundos de investimento e carteiras administradas, devem ser entendidas como "clientes", estando assim sujeitas à Política Conheça seu Cliente e Suas Atividades da gestora, a fim de prevenir que se utilizem dos veículos de investimento geridos para atividades ilegais ou impróprias.

Constatada uma situação que se enquadre no descrito acima, a Oikos comunicará imediatamente às entidades cabíveis, notadamente a CVM e o COAF, e cessará a realização de operações com tal cliente, se for o caso.

Ressalta-se, que as operações envolvendo os ativos listados abaixo, em função de sua contraparte e do mercado nos quais são negociados, já terem passado por processo de prevenção à lavagem de dinheiro, eximem a Oikos de diligência adicional em relação ao monitoramento e controle das contrapartes:

- Ofertas públicas iniciais e secundárias de valores mobiliários, registradas de acordo com as normas emitidas pela CVM;
- Ofertas públicas de esforços restritos, dispensadas de registro de acordo com as normas emitidas pela CVM;
- Ativos e valores mobiliários admitidos à negociação em bolsas de valores, de mercadorias e futuros, ou registrados em sistemas de registro, custódia ou de liquidação financeira, devidamente autorizados em seus países de origem e supervisionados por autoridade local reconhecida;
- Ativos e valores mobiliários cuja contraparte seja instituição financeira ou equiparada; e
- Ativos e valores mobiliários de mesma natureza econômica daqueles acima listados, quando negociados no exterior, desde que (i) sejam admitidos à negociação em bolsas de valores, de mercadorias e futuros, ou registrados em sistema de registro, custódia ou de liquidação financeira, devidamente autorizados em seus países de origem e supervisionados por autoridade local reconhecida pela CVM, ou (ii) cuja existência tenha sido assegurada por terceiros devidamente autorizados para o exercício da atividade de custódia em países signatários do Tratado de Assunção ou em outras jurisdições, ou supervisionados por autoridade local reconhecida pela CVM.

## 4 LEI ANTICORRUPÇÃO BRASILEIRA E DECRETO REGULAMENTAR

A Lei Anticorrupção Brasileira (Lei no 12.846, de 1o de agosto de 2013) e respectivo Decreto Regulamentar 8.420, de 18 de março de 2015 (coletivamente “Normas Brasileiras Anticorrupção”), dispõem sobre a responsabilidade civil e administrativa de sociedades brasileiras ou estrangeiras que atuem no Brasil por conta de atos de seus diretores, gerentes, funcionários e outros agentes que atuem em nome da sociedade que envolvam a prática de corrupção contra a administração pública, nacional ou estrangeira, inclusive organizações públicas internacionais, como suborno e fraude em licitações e contratos administrativos da administração pública. Representantes de fundos de pensão públicos também devem ser considerados agentes públicos para os propósitos das Normas Brasileiras Anticorrupção.

Tais Normas Brasileiras Anticorrupção complementam a legislação penal aplicável para pessoas físicas.

Nos termos das Normas Brasileiras Anticorrupção, suborno significa prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público, ou a terceira pessoa a ele relacionada, incluindo os chamados “pagamentos facilitadores”.

Para que uma entidade seja condenada nos termos da Lei Anticorrupção, não é necessário comprovar a intenção ou má-fé do agente, apenas que o pagamento de suborno foi realizado ou oferecido.

Os Colaboradores devem questionar a legitimidade de quaisquer pagamentos requeridos por autoridade ou funcionário público que não contenha claro fundamento legal ou regulamentar.

Nenhum Colaborador poderá ser penalizado devido a atraso ou perda de negócios resultantes de sua recusa em pagar ou oferecer suborno a agentes públicos.

Nos termos das Normas Brasileiras Anticorrupção, dentre outros cabíveis, a Oikos e seus Colaboradores adotam os seguintes procedimentos internos e padrões de conduta a fim de minimizar os riscos de ocorrência de práticas de corrupção envolvendo seus Colaboradores:

- Comprometimento dos Diretores, em especial do Diretor de Compliance, evidenciado pelo apoio expresso e inequívoco às Normas Brasileiras Anticorrupção;
- Padrões de conduta, políticas e procedimentos de integridade aplicáveis a todos os Colaboradores, independentemente de cargo ou função exercidos;
- Treinamentos periódicos sobre as Normas Brasileiras Anticorrupção;
- Análise periódica de riscos para realizar adaptações necessárias às condutas e regras internas;
- Registros contábeis que reflitam de forma completa e precisa as transações;
- Controles internos que assegurem a pronta elaboração e confiabilidade de relatórios e demonstrações financeiras;
- Independência, estrutura e autoridade do Diretor de Compliance para fazer valer, de forma eficaz, as diretrizes e normas previstas neste Manual;
- Procedimentos que assegurem a pronta interrupção de irregularidades ou infrações detectadas e a tempestiva remediação dos danos gerados;
- Diligências apropriadas para contratação e supervisão, de terceiros, tais como, fornecedores, prestadores de serviço, agentes intermediários e associados;
- Verificação, durante processos de fusões, aquisições e reestruturações societárias, do cometimento de irregularidades ou ilícitos ou da existência de vulnerabilidades;



- Monitoramento contínuo do programa de compliance e das normas aqui previstas, visando assegurar que continuem efetivas na prevenção, detecção e combate à ocorrência dos atos lesivos contra a administração pública; e
- Doações para candidatos e partidos políticos somente mediante pré-aprovação do Diretor de Compliance, sendo vedada doações efetuadas diretamente pela Oikos.

Os Colaboradores devem comunicar imediatamente ao Diretor de Compliance caso tenham notícia de violação ou suspeita de violação das Normas Brasileiras Anticorrupção. Se o Diretor de Compliance estiver envolvido em tal prática ou suspeita, as medidas disciplinares serão determinadas pelos demais Sócios Diretores da Oikos.

## 5 POLÍTICA DE CONFIDENCIALIDADE: SIGILO E CONDUTA

Conforme disposto no Termo de Confidencialidade constante no Código de Ética da Oikos, nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada fora da Oikos. Fica vedada qualquer divulgação, no âmbito pessoal ou profissional, que não esteja em acordo com as normas legais e de compliance da Oikos.

Qualquer informação sobre a Oikos, seu know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e dos fundos geridos pela Oikos, operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela Oikos, estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Oikos e a seus sócios e clientes, obtida em decorrência do desempenho das atividades do Colaborador na Oikos, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado pelo Diretor de Compliance, podendo esta delegar tal função.

A informação obtida em decorrência da atividade profissional exercida na Oikos não pode ser divulgada, em hipótese alguma, a terceiros não Colaboradores ou a Colaboradores não autorizados. Enquadram-se neste item, por exemplo, estratégias de investimento ou desinvestimento, relatórios, estudos realizados pelas áreas de análise, opiniões internas sobre ativos financeiros, informações a respeito de resultados financeiros antes da publicação dos balanços e balancetes dos fundos de investimento geridos pela Oikos, transações realizadas e que ainda não tenham sido divulgadas publicamente, além daquelas estabelecidas no Termo de Confidencialidade no Código de Ética da Oikos.

Conforme disposto no Termo de Confidencialidade constante no Código de Ética da Oikos, qualquer invenção, desenvolvimento, conceito, ideia, processo ou trabalho, por escrito ou não, que possa ou não ser patenteado, ou ter seus direitos reservados, que o colaborador desenvolva sozinho, ou com outro integrante da Equipe, durante seu período de contratação pela Oikos, e que esteja direta ou indiretamente relacionado com o negócio da Oikos, ("Propriedade Intelectual") pertencem à Oikos.

Como condição para sua contratação, o funcionário atribui exclusivamente à Oikos todos os seus direitos, títulos ou interesses em quaisquer propriedades da Oikos, inclusive aquelas cuja criação ou desenvolvimento tenha iniciado e/ou de qualquer forma participado, e concorda em entregar qualquer documento que seja necessário para garantir, registrar ou melhorar a atribuição da Propriedade Intelectual da Oikos. Essa obrigação continua válida mesmo após o término da relação de trabalho com a Oikos.

Na questão de confidencialidade e tratamento da informação, o Colaborador deve cumprir o estabelecido nos itens a seguir.

### Informação Privilegiada

Para fins deste Manual, bem como dos demais Códigos, considera-se Informação Privilegiada qualquer informação relevante a respeito de qualquer companhia, que não tenha sido divulgada publicamente e que seja obtida de forma privilegiada (em decorrência da relação profissional ou pessoal mantida com um cliente, com pessoas vinculadas a empresas analisadas ou investidas ou com terceiros).

Exemplos de Informações Privilegiadas: informações verbais ou documentadas a respeito de resultados operacionais de empresas, alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (IPO), e qualquer outro fato que seja objeto de um acordo de confidencialidade firmado por uma empresa com a Oikos ou com terceiros.

As Informações Privilegiadas devem ser mantidas em sigilo por todos que a elas tiverem acesso, seja em decorrência do exercício da atividade profissional ou de relacionamento pessoal.

### Insider Trading e "Dicas"

Insider Trading significa a compra e venda de títulos ou valores mobiliários com base no uso de informação privilegiada, com o objetivo de conseguir benefício próprio ou de terceiros (compreendendo os Colaboradores da Oikos).

"Dica" é a transmissão, a qualquer terceiro, estranho às atividades da Oikos, de informação privilegiada que possa ser usada com benefício na compra e venda de títulos ou valores mobiliários.



O disposto nos itens de “Informação Privilegiada” e “Insider Trading e ‘Dicas’” deve ser analisado não só durante a vigência de seu relacionamento profissional com a Oikos, mas também após o seu término.

É proibida a prática das condutas mencionadas acima por qualquer Colaborador da Oikos, seja agindo em benefício próprio ou de terceiros.

## **6 POLÍTICA DE SEGREGAÇÃO DE ATIVIDADES: “CHINESE WALL”**

A Oikos desempenha exclusivamente atividades voltadas para a administração e gestão de títulos, valores mobiliários e fundos de investimento, exclusivamente de terceiros, diretamente ou por delegação a outros administradores. A Oikos não desempenha a atividade de Distribuição de produtos financeiros.

Todos os Colaboradores da Oikos que tiverem suas atividades profissionais relacionadas com a administração de ativos e carteiras de valores mobiliários, nos termos dos artigos 24 e 25 da Instrução CVM nº 558, de 26 de março de 2015, serão alocados para desempenhar suas funções em estações de trabalho destinadas a cada área, apartadas por estruturas fixas (divisórias) e claramente identificadas para possibilitar uma clara distinção de cada uma das áreas caso a empresa venha a fazer Distribuição de produtos financeiros.

Os Colaboradores que tiverem suas atividades profissionais relacionadas com a administração de ativos e carteiras de valores mobiliários serão disponibilizados linhas telefônicas específicas e diretórios de rede com acesso restrito, promovendo, desta forma, a efetiva segregação das atividades desempenhadas pela Oikos caso a empresa venha a fazer distribuição de produtos financeiros.

Nesse contexto, o Diretor de Compliance terá ampla e total liberdade para execução dos seus serviços.

## **7 PROGRAMA DE SEGURANÇA CIBERNÉTICA**

A Oikos Gestão de Recursos Ltda. (“Oikos”), desde o início de suas operações, adota e constrói soluções digitais apoiada nos avanços tecnológicos mais recentes, o que lhe permite desempenhar suas atividades de forma ágil, dinâmica e eficiente. As facilidades trazidas pelo emprego destes recursos cibernéticos trazem consigo o consequente desafio de proteger de forma eficaz esta infraestrutura muito relevante para a execução dos processos da Oikos. Assim, buscando assegurar a confidencialidade, integridade e disponibilidade de dados e sistemas de informação utilizados, a Oikos desenvolveu seu Programa de Segurança Cibernética.

Compatível com a natureza das atividades desempenhadas pela Oikos, este Programa de Segurança Cibernética procura empregar recursos de segurança de forma inteligente, partindo da diligente Avaliação de Riscos e cenários de ameaças cibernéticas associados a cada processo operacional relevante da empresa. Identificadas e classificadas as necessidades de proteção de acordo com seu nível de criticidade, Ações de Proteção adequadas são definidas com o objetivo de mitigar riscos e impedir a ocorrência de potenciais incidentes de segurança. São estabelecidas Rotinas de Monitoramento e Testes para habilitar a capacidade de detecção de anomalias e incidentes, além de um Plano de Resposta a Incidentes que busca garantir a contenção, tratamento e recuperação em casos de detecção de ocorrências relevantes. Finalmente, a responsabilidade por tratar e responder às questões de segurança é determinada, assim como a frequência de revisão deste Programa de Segurança Cibernética.

### **7.1 AVALIAÇÃO DE RISCOS E POLÍTICA DE CLASSIFICAÇÃO DAS INFORMAÇÕES**

Para garantir que o Programa de Segurança Cibernética seja implementado de maneira adequada às reais necessidades da Oikos, seja compatível com as características e o tamanho da empresa e adote medidas de proteção e resposta compatíveis com os riscos e ameaças reais, a Avaliação de Riscos é o primeiro passo deste programa e leva em consideração a natureza das atividades desempenhadas pela Oikos, a arquitetura de seu ambiente cibernético e as pessoas que fazem uso dos serviços e informações presentes nesse ambiente. Atenção especial se dá à definição da Política de Classificação das Informações, que estabelece regras que buscam permitir o tratamento adequado das informações de acordo com sua natureza em termos de privilégio, relevância e sensibilidade.

#### **7.1.1 AVALIAÇÃO DE RISCOS**

A Oikos atua na administração de carteiras de valores mobiliários, devidamente habilitada pela CVM para o exercício profissional de gestão de recursos. Dessa forma, tem como principal responsabilidade a aplicação de recursos financeiros nos mercados de valores mobiliários por conta dos investidores, com autorização para compra e venda de títulos e valores mobiliários. As atividades desempenhadas compreendem a seleção, avaliação, aquisição, alienação, subscrição, conversão e execução dos demais direitos inerentes aos ativos financeiros e às modalidades operacionais características das carteiras.



Durante a Avaliação de Riscos os processos e ativos relacionados ao desempenho destas atividades são identificados e avaliados considerando diversos cenários de ameaças que possam comprometer sua segurança. Estes cenários de ameaças consideram tanto os vários métodos de ataques cibernéticos conhecidos, como malware, engenharia social, ataques de negação de serviços e invasões, quanto ameaças hipotéticas desconhecidas que, de alguma maneira, venham a comprometer a confidencialidade, integridade ou disponibilidade dos ativos relevantes ao desempenho das atividades da Oikos.

Uma matriz de avaliação de riscos é utilizada para classificar o nível de risco de cada vulnerabilidade identificada. Essa matriz considera os possíveis impactos (financeiros, operacionais e reputacionais) e também o grau de exposição ou probabilidade de ocorrência dos incidentes, considerando que o grau de exposição de cada ameaça é calculado como função do nível de complexidade funcional dos ativos e processos e seu grau de conectividade, encontrando assim um critério objetivo de classificação de exposição.

## 7.1.2 POLÍTICA DE CLASSIFICAÇÃO DAS INFORMAÇÕES

Além da classificação de risco das vulnerabilidades, também são estabelecidas as regras de classificação das informações presentes no ambiente cibernético da Oikos, permitindo que as informações sejam tratadas de forma compatível com sua natureza em termos de sensibilidade, relevância e privilégio. São consideradas quatro classes de confidencialidade: Privada, Confidencial, Interna e Pública, de acordo com os seguintes critérios:

### - Informações Privadas

Informações Privadas são aquelas informações produzidas para consumo exclusivo do próprio produtor. Todas as informações produzidas por usuários da Oikos são automaticamente classificadas como Privadas. Além do próprio produtor da informação, também o Diretor de Compliance tem autorização para consumir informações classificadas como Privadas. Informações que não declarem sua classificação devem ser manuseadas como se estivessem explicitamente classificadas como Privadas. São exemplos de Informações Privadas: anotações pessoais, arquivos temporários, históricos de navegação e relatórios gerados a partir dos sistemas da Oikos.

### - Informações Confidenciais

Informações Confidenciais são aquelas informações produzidas para consumo de uma pessoa ou grupos de pessoas explicitamente designadas. O próprio produtor das informações tem autoridade para classificá-las como Confidenciais e deve fazê-lo declarando explicitamente a lista de consumidores autorizados, considerando a natureza privilegiada das informações, sua relevância e sensibilidade. Consumidores autorizados não se limitam a pessoas internas à Oikos, muitas vezes são clientes, parceiros ou órgãos reguladores. Na falta da declaração explícita de consumidores autorizados, entende-se que a classificação correta da informação é Privada. São exemplos de Informações Confidenciais: correios eletrônicos, chamadas telefônicas e código fonte de aplicações.

### - Informações Internas

Informações Internas são aquelas informações produzidas para livre consumo dentro da Oikos. São necessariamente informações de natureza não privilegiada, alta relevância e baixa sensibilidade. Apenas o Diretor de Compliance tem autoridade para classificar informações como Internas. O produtor de informações que se encaixem nestes critérios deve encaminhar solicitação ao Diretor de Compliance para que estas informações sejam classificadas como Internas. São exemplos de Informações Internas: avisos de manutenção dos sistemas da Oikos.

### - Informações Públicas

Informações Públicas são aquelas informações produzidas para livre consumo dentro e fora da Oikos. São necessariamente de natureza não privilegiada e baixa sensibilidade. Apenas o Diretor de Compliance tem autoridade para classificar informações como Públicas. O produtor de informações que se encaixem nestes critérios deve encaminhar solicitação ao Diretor de Compliance para que estas informações sejam classificadas como Públicas. São exemplos de Informações Públicas: apresentações institucionais, códigos de regras e manuais de procedimentos.

Identificados e classificados os riscos relacionados ao desempenho de atividades da Oikos, são estabelecidas as Ações de Proteção com o objetivo de mitigar estes riscos, impedir a ocorrência de potenciais incidentes de segurança e definir regras para o correto manuseio das informações produzidas na empresa.

## 7.2 AÇÕES DE PROTEÇÃO E POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES

As Ações de Proteção têm como objetivo mitigar os riscos identificados na Avaliação de Riscos e impedir a ocorrência de potenciais incidentes de segurança, sendo priorizadas de acordo com a classificação de risco das vulnerabilidades avaliadas. Na Política de



Segurança das Informações, atenção especial é dada à necessidade de garantir a segurança e sigilo daquelas informações classificadas como Privadas, Confidenciais ou Internas, de acordo com a Política de Classificação das Informações.

### 7.2.1 AÇÕES DE PROTEÇÃO

#### - Autenticação, Autorização e Auditoria

Cada sócio, diretor, administrador, profissional, terceiro contratado ou qualquer pessoa que acesse o ambiente cibernético da Oikos é um usuário de serviços cibernéticos e precisa ser devidamente identificado através de credenciais únicas, pessoais e exclusivas. Estas credenciais devem autenticar e identificar o usuário dentro do ambiente cibernético da Oikos. Senhas são um tipo comum de credencial e, para permitir o efetivo controle dos acessos de forma individualizada, precisam respeitar níveis mínimos de complexidade e periodicidade mínima de atualização de 180 dias. A natureza das atividades desempenhadas por cada usuário deve determinar seu perfil de autorização e limitar seus privilégios de acesso a ativos cibernéticos respeitando a segregação das atividades e estabelecendo barreiras naturais de contenção de ameaças. Todos os eventos de login e alteração de credenciais devem ser registrados de forma a serem rastreáveis e auditáveis.

#### - Provisionamento e Gestão de Mudanças de Privilégios

O provisionamento de novos usuários de serviços cibernéticos deve se dar de acordo com o perfil de acesso inicial de cada novo usuário, determinado pela natureza das atividades que serão desempenhadas. Durante o ciclo de vida dos usuários dentro do ambiente cibernético da Oikos, mudanças de atividades desempenhadas podem ocorrer e devem ser acompanhadas de mudanças no perfil de acesso. Novos privilégios de acesso necessários devem ser autorizados e também os antigos privilégios de acesso desnecessários devem ser revogados, limitando sempre o escopo dos privilégios à natureza mais atual das atividades desempenhadas por cada usuário. Cuidados especiais devem ser adotados quando um usuário é desligado. Todos os privilégios devem ser revogados e todas as credenciais invalidadas, porém os identificadores de usuários devem ser mantidos para que não se comprometa a capacidade de rastreamento e auditoria de eventos passados.

#### - Segregação de Serviços

Os fluxos de dados entre os diferentes dispositivos dentro do ambiente cibernético da Oikos devem ser limitados de forma a permitir apenas a comunicação estritamente necessária para o desempenho das atividades da empresa. Soluções de firewall e filtros de pacotes devem ser configuradas com regras implícitas que neguem toda comunicação que não esteja explicitamente permitida, implementando na camada de rede os mesmos princípios de contenção que regem o limite dos privilégios de acesso nas demais camadas. Em especial, medidas de segurança de borda devem limitar os acessos entre clientes e servidores dos diferentes serviços presentes no ambiente cibernético da Oikos de forma a estabelecer barreiras naturais de contenção de ameaças e respeitar a segregação de atividades.

#### - Proteção de Estações de Trabalho e Dispositivos Móveis

As estações de trabalho utilizadas no ambiente cibernético da Oikos devem ser configuradas de forma a garantir que operem com as atualizações de sistemas operacionais mais recentes, com as aplicações de software estritamente necessárias ao desempenho das atividades do usuário no ambiente cibernético da Oikos e que implementem mecanismos de varredura e proteção contra malware e criptografia de dados em repouso, principalmente no caso de dispositivos móveis.

#### - Proteção de Servidores e Aplicações

Os servidores utilizados no ambiente cibernético da Oikos devem ser dimensionados e distribuídos de forma a garantir os níveis de redundância necessários para que a disponibilidade dos serviços críticos seja preservada mesmo em casos de falhas de aplicações, equipamentos, dispositivos de rede, links de internet ou até data centers inteiros. Os servidores devem sofrer manutenção programada para garantir que apresentem as atualizações de sistemas operacionais mais recentes, as aplicações de software estritamente necessárias ao desempenho da prestação dos serviços no ambiente cibernético da Oikos e a realização de backup diário, garantindo a capacidade de recuperação e restabelecimento de serviços em caso de falhas.

### 7.2.2 POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES

O ambiente cibernético da Oikos trata informações classificadas de acordo com a Política de Classificação das Informações e adota, através desta Política de Segurança das Informações, medidas de proteção que pretendem promover o correto manuseio, armazenamento e descarte de forma a resguardar a sensibilidade das informações adequada a cada classe de confidencialidade.

Cada usuário do ambiente cibernético da Oikos produz informações sempre que registra, modifica, copia, divulga ou distribui dados, seja em meio físico ou digital, no desempenho de suas atividades. É obrigação de cada usuário produtor de informações classificá-las explicitamente de acordo com a Política de Classificação das Informações, considerando a natureza privilegiada das informações, sua relevância e sensibilidade. Também é obrigação de cada usuário produtor limitar a exposição das informações



apenas a consumidores autorizados e deve, para isso, se utilizar dos recursos de proteção disponíveis no ambiente cibernético da Oikos, como controle de acesso a arquivos digitais, criptografia de dados em repouso e armazenamento físico seguro.

Cada usuário do ambiente cibernético da Oikos consome informações sempre que recebe, manuseia ou acessa dados, seja em meio físico ou digital, no desempenho de suas atividades. É obrigação de cada usuário consumidor de informações se certificar de que está autorizado ao consumo antes de fazê-lo, verificando a classificação da informação e a lista de consumidores autorizados. Toda informação que não declare sua classificação ou lista de consumidores autorizados deve ser tratada como se estivesse explicitamente classificada como Privada. É obrigação de cada usuário consumidor alertar o Diretor de Compliance sempre que for exposto indevidamente a informações. Também é obrigação de cada usuário consumidor buscar a orientação do Diretor de Compliance sempre que tiver dúvidas quanto ao manuseio das informações no ambiente cibernético da Oikos ou qualquer outra dúvida relacionada a questões de segurança deste ambiente.

Sempre que um usuário consumidor reproduz, modifica, copia, divulga ou distribui as informações que consome ele assume as responsabilidades de usuário produtor de informações e passa a responder pela classificação e definição de lista de consumidores autorizados, além do vazamento indevido de informações. Os usuários são orientados a limitar o compartilhamento de informações ao grupo original de consumidores autorizados, sabendo que existe grave risco de vazamento indevido de informações sempre que o grupo de consumidores autorizados é alterado.

O Diretor de Compliance tem autoridade para consumir todas as informações tratadas no ambiente cibernético da Oikos e é o único usuário deste ambiente com autoridade para classificar informações como Internas ou Públicas. O Diretor de Compliance é responsável por implantar e manter treinamento de conscientização de segurança das informações oferecido a todos os usuários do ambiente cibernético da Oikos.

Definidas as Ações de Proteção e a Política de Segurança das Informações, são estabelecidas as Rotinas de Monitoramento e Testes para identificar situações de anomalia em que as medidas de proteção não tenham sido suficientes para evitar incidentes.

### 7.3 ROTINAS DE MONITORAMENTO E TESTES

Rotinas de Monitoramento e Testes capazes de detectar anomalias e incidentes são estabelecidas como procedimentos de segurança no ambiente cibernético da Oikos com o objetivo de antecipar o acionamento do Plano de Resposta a Incidentes e Continuidade de Negócios e, assim, permitir a contenção, tratamento e recuperação em caso de incidentes.

Indicadores de saúde dos processos operacionais críticos são criados a partir da observação dos parâmetros de normalidade dentro do ambiente cibernético da Oikos. Estes indicadores são monitorados continuamente e alertas são gerados sempre que os valores apresentados fogem do padrão de normalidade estabelecido.

Todas as rotinas de manutenção e backup são explicitamente monitoradas e todas as falhas nestas rotinas geram alertas. Logs e trilhas de auditoria são analisados rotineiramente de forma a permitir a identificação de tentativas de ataques e demais anomalias. O estado de disponibilidade de servidores e demais ativos críticos do ambiente cibernético da Oikos é monitorado de forma contínua e alertas são gerados sempre que a disponibilidade destes ativos críticos foge dos padrões de normalidade. Todas as aplicações desenvolvidas pela Oikos são instrumentadas com capacidade de registro de eventos com diferentes níveis de criticidade e um mecanismo de tratamento especial para todos os eventos registrados com criticidade relevante produz o envio de notificações automáticas ao Diretor de Compliance.

Definidas as rotinas de supervisão, monitoramento e detecção, é estabelecido um Plano de Resposta a Incidentes para garantir a contenção, tratamento e recuperação em caso de detecção de ocorrências relevantes.

### 7.4 PLANO DE RESPOSTA A INCIDENTES E CONTINUIDADE DE NEGÓCIOS

Considerando os cenários de ameaça identificados na Avaliação de Riscos, este Programa de Segurança Cibernética estabelece o Plano de Resposta a Incidentes visando garantir a contenção, tratamento e recuperação em caso de detecção de incidentes que comprometam a confidencialidade, integridade ou disponibilidade de ativos e processos do ambiente cibernético da Oikos. O Plano de Continuidade de Negócios dá atenção especial à necessidade de garantir a recuperação da execução dos processos identificados como críticos, permitindo a suficiente continuidade do desempenho das atividades de negócios da Oikos.

#### 7.4.1 PLANO DE RESPOSTA A INCIDENTES

Em resposta a alertas quanto a incidentes que afetem a segurança do ambiente cibernético da Oikos, o Diretor de Compliance, que responde pelas questões de segurança da empresa, deve ser primeiramente notificado e decidir sobre a composição imediata do Grupo de Resposta, envolvendo aquelas pessoas capacitadas a responder de maneira adequada ao incidente, dependendo dos ativos afetados.



O Grupo de Resposta deve então avaliar a natureza do incidente buscando identificar sua causa raiz e potencial de impacto. A primeira medida de resposta deve buscar a contenção do incidente e pode, para isso, sacrificar a disponibilidade de sistemas limitando o alcance do evento. Contido o incidente, o Grupo de Resposta deve buscar restabelecer a disponibilidade dos serviços do ambiente cibernético, empregando medidas para evitar reincidência. Finalmente, o Diretor de Compliance deve avaliar a necessidade e realizar a comunicação do incidente às partes apropriadas.

Toda documentação relacionada ao gerenciamento do incidente deve ser arquivada para que os aprendizados acumulados sejam considerados durante o processo de revisão deste Programa de Segurança Cibernética.

## 7.4.2 PLANO DE CONTINUIDADE DE NEGÓCIOS

Com o objetivo de garantir a disponibilidade de todos os ativos e processos identificados como críticos na Avaliação de Riscos, este Programa de Segurança Cibernética estabelece um Plano de Continuidade de Negócios definindo os procedimentos de recuperação adequados para restabelecer a disponibilidade de ativos e processos críticos, bem como responsabilidades pela execução destes procedimentos e ainda a frequência de testes de validação para que a capacidade de desempenhar atividades críticas no ambiente cibernético da Oikos seja efetivamente preservada.

### - Ambiente Servidor

A maior concentração de ativos críticos identificados na Avaliação de Riscos se dá no Ambiente Servidor, localizado em data centers externos ao escritório sede da Oikos que apresentam garantias de disponibilidade mínima de 99,95%. Além das garantias de disponibilidade dos data centers, medidas de Proteção de Servidores e Aplicações estabelecem regras de dimensionamento e distribuição de forma a garantir os níveis de redundância necessários para que a disponibilidade dos serviços críticos seja preservada mesmo em casos de incidentes que comprometam data centers inteiros.

Em casos extremos em que estas medidas de Proteção de Servidores e Aplicações não sejam suficientes para preservar a disponibilidade de serviços críticos, novas instâncias de servidores devem ser ativadas em data centers disponíveis, análogos aos afetados, recuperando cópias de segurança de dados que permitam manter a integridade e consistência dos estados dos serviços originalmente afetados.

É responsabilidade do Diretor de Tecnologia e sua equipe executar estes procedimentos de recuperação se apoiando nas facilidades oferecidas pela arquitetura de nuvem adotada no ambiente cibernético da Oikos para que os tempos de resposta e recuperação sejam mínimos.

### - Ambiente Cliente

O Ambiente Cliente se limita à localidade do escritório sede da Oikos e apresenta os únicos ativos críticos identificados na Avaliação de Riscos externos ao Ambiente Servidor. Os únicos serviços críticos oferecidos no Ambiente Cliente aos usuários do ambiente cibernético da Oikos são os serviços de estações de trabalho e acesso à internet. O escritório sede da Oikos oferece redundâncias nestes serviços, garantindo que falhas isoladas em estações de trabalho ou acesso à internet não comprometam o desempenho das atividades críticas identificadas.

Em casos extremos em que as medidas de proteção não sejam suficientes para preservar a disponibilidade dos serviços críticos, serão oferecidos os serviços de estações de trabalho e acesso à internet aos usuários identificados como participantes de atividades críticas através de ativação de site backup.

É responsabilidade do Diretor de Tecnologia e sua equipe executar estes procedimentos de recuperação, garantindo que os controles de acesso e demais medidas de proteção sejam mantidos durante sua execução, preservando os demais aspectos de segurança do ambiente cibernético da Oikos.

### - Validação e Testes

Testes semestrais de execução dos procedimentos de recuperação devem ser realizados, permitindo avaliar a real eficácia das ações implementadas e assim determinar a manutenção ou indicar a necessidade de revisão dos procedimentos, participando da evolução contínua deste Programa de Segurança Cibernética da Oikos.

## 7.5 RESPONSABILIDADE E REVISÃO

Considerando a natureza dinâmica do ambiente cibernético de que trata este Programa e atendendo às exigências normativas, a Oikos estabelece que seu Programa de Segurança Cibernética será revisado e atualizado anualmente. Estabelece ainda que o Diretor de Compliance é a pessoa com autoridade e responsabilidade para responder às questões de segurança cibernética em nome da Oikos.



## **8 TREINAMENTO E POLÍTICA DE CERTIFICAÇÃO**

### **8.1 TREINAMENTO E PROCESSO DE RECICLAGEM**

A Oikos possui um processo de treinamento inicial de todos os seus Colaboradores, especialmente aqueles que tenham acesso a informações confidenciais ou participem de processos de decisão de investimento. Especificamente no que se refere à prevenção de lavagem de dinheiro, o treinamento é realizado para todos os colaboradores, inclusive terceirizados.

Assim que cada Colaborador é contratado, ele participará de um processo de treinamento em que irá adquirir conhecimento sobre as atividades da Oikos, suas normas internas, especialmente sobre este Manual e demais Códigos, além de informações sobre as principais leis e normas que regem as atividades da Oikos e terá oportunidade de esclarecer dúvidas relacionadas a tais princípios e normas.

Não obstante, a Oikos entende que é fundamental que todos os Colaboradores, especialmente aqueles que tenham acesso a informações confidenciais ou participem de processos de decisão de investimento, tenham sempre conhecimento atualizado dos seus princípios éticos, das leis e normas.

Neste sentido, a Oikos adota um programa de reciclagem dos seus Colaboradores, à medida que as regras e conceitos contidos neste Manual sejam modificados, com o objetivo de fazer com que os mesmos estejam sempre atualizados, estando todos obrigados a participar de tais programas de reciclagem.

A implementação do processo de treinamento inicial e do programa de reciclagem continuada fica sob a responsabilidade do Diretor de Compliance e exige o comprometimento total dos Colaboradores quanto a sua assiduidade e dedicação.

Tanto o processo de treinamento inicial quanto o programa de reciclagem deverão abordar as atividades da Oikos, seus princípios éticos e de conduta, as normas de Compliance, as políticas de segregação, quando for o caso, e as demais políticas descritas nos Códigos (especialmente aquelas relativas à confidencialidade, segurança das informações e negociação pessoal), bem como as penalidades aplicáveis aos Colaboradores decorrentes do descumprimento de tais regras, além das principais leis e normas aplicáveis às referidas atividades.

### **8.2 POLÍTICA DE CERTIFICAÇÃO**

A Oikos adota a Certificação como mecanismo de qualificação de seus Colaboradores, visando elevar a capacitação técnica desses profissionais. A presente Política de Certificação visa atender às exigências regulatórias da CVM e dos Códigos ANBIMA no exercício de atividades passíveis de certificação obrigatória.

Todos os Colaboradores da Oikos que tiverem suas atividades profissionais definidas como Atividades Elegíveis (Distribuição de Produtos de Investimento, Gestão de Recursos de Terceiros ou Gestão de Patrimônio) deverão possuir certificação adequada previamente ao exercício de suas atividades e deverão mantê-la válida e atualizada enquanto desempenharem tais atividades.

A determinação da Certificação necessária para o desempenho das atividades de cada Colaborador, quando essa for Atividade Elegível, é uma atribuição da área de Compliance, em observância aos códigos, normas, políticas e regulamentação vigente, e realizada a cada processo de admissão ou transferência de área de um Colaborador.

Também é atribuição da área de Compliance a validação das certificações e a atualização das informações dos Colaboradores certificados no Banco de Dados da ANBIMA, nos eventos de admissão, demissão ou transferência de área.

Todo Colaborador que exerça Atividade Elegível será notificado por escrito, por meio eletrônico que documente a notificação, da necessidade de atualização da certificação previamente a seu vencimento.

Todo Colaborador que exerça Atividade Elegível será notificado por escrito, por meio eletrônico que documente a notificação, do afastamento imediato de suas atividades quando não possuir certificação válida.

## **9 DÚVIDAS OU AÇÕES CONTRÁRIAS**

Este Manual se propõe a avaliar as mais diversas situações que podem eventualmente ocorrer e é natural, portanto, que surjam dúvidas ao enfrentar situações concretas, que possam contrariar os princípios e normas deste Manual e dos demais Códigos que orientam as ações da Oikos.

Em caso de dúvida em relação a quaisquer das matérias constantes deste Manual, ou dos demais Códigos, também é imprescindível que se busque auxílio imediato junto ao Diretor de Compliance, para obtenção de orientação mais adequada.



Mesmo que haja apenas a suspeita de uma potencial situação de conflito ou ocorrência de uma ação que vá afetar os interesses da Oikos, o Colaborador deverá seguir essa mesma orientação. Esta é a maneira mais transparente e objetiva para consolidar os valores da cultura empresarial da Oikos e reforçar os seus princípios éticos.

Para os fins do presente Manual, bem como dos demais Códigos, portanto, toda e qualquer solicitação que dependa de autorização, orientação ou esclarecimento expresso do Diretor de Compliance, bem como eventual ocorrência, suspeita ou indício de prática por qualquer Colaborador que não esteja de acordo com as disposições dos Códigos e das demais normas aplicáveis às atividades da Oikos, deve ser dirigida pela pessoa que necessite da autorização, orientação ou esclarecimento ou que tome conhecimento da ocorrência ou suspeita ou possua indícios de práticas em desacordo com as regras aplicáveis, ao Diretor de Compliance.

## **10 ACOMPANHAMENTO DAS POLÍTICAS DESCRITAS NOS CÓDIGOS**

Mediante ocorrência de descumprimento, suspeita ou indício de descumprimento de quaisquer das regras estabelecidas nos Códigos ou aplicáveis às atividades da Oikos que cheguem ao conhecimento do Diretor de Compliance, de acordo com os procedimentos estabelecidos neste Manual, o Diretor de Compliance utilizará os registros e sistemas de monitoramento eletrônico e telefônico para verificar a conduta dos Colaboradores envolvidos.

Todo conteúdo que está na rede será acessado pelos Sócios Diretores da Oikos, caso haja necessidade. Arquivos pessoais salvos em cada computador serão acessados caso os Sócios Diretores da Oikos julguem necessário. A confidencialidade dessas informações deve ser respeitada e seu conteúdo será disponibilizado ou divulgado somente nos termos e para os devidos fins legais ou em atendimento a determinações judiciais.

Os Sócios Diretores da Oikos poderão utilizar as informações obtidas em tais sistemas para decidir sobre eventuais sanções a serem aplicadas aos Colaboradores envolvidos, nos termos deste Manual.

A Oikos realizará inspeções com periodicidade mensal, a cargo do Diretor de Compliance, com base em sistemas de monitoramento eletrônico, independentemente da ocorrência de descumprimento ou suspeita ou indício de descumprimento de quaisquer das regras estabelecidas nos Códigos ou aplicáveis às atividades da Oikos.

Mensagens de correio eletrônico de Colaboradores poderão ser interceptadas e abertas para ter a regularidade de seu conteúdo verificada, computadores poderão ser auditados e conversas telefônicas poderão ser gravadas e escutadas sem que isto represente invasão da privacidade dos Colaboradores já que se trata de ferramentas de trabalho disponibilizadas pela Oikos.

Adicionalmente, será realizado um monitoramento mensal, a cargo do Diretor de Compliance, sobre uma amostragem significativa dos Colaboradores, escolhida aleatoriamente pelo Diretor de Compliance, para que sejam verificados os arquivos eletrônicos, inclusive e-mails, bem como as ligações telefônicas dos Colaboradores selecionados, com o objetivo de verificar possíveis situações de descumprimento às regras contidas nos Códigos.

Além dos procedimentos de supervisão periódica realizados pelo Diretor de Compliance, os Sócios Diretores da Oikos poderão, quando julgarem oportuno e necessário, realizar inspeções sobre quaisquer Colaboradores.





## 11 SANÇÕES

A eventual aplicação de sanções decorrentes do descumprimento dos princípios e regras estabelecidos nos Códigos é de responsabilidade dos Sócios Diretores da Oikos, com exceção do Diretor de Compliance, a seus exclusivos critérios, garantido ao Colaborador, contudo, amplo direito de defesa. Poderão ser aplicadas, sem prejuízo das medidas judiciais cabíveis, conforme gravidade do descumprimento verificado, penas de: (i) carta de advertência, (ii) suspensão do Colaborador e (iii) dispensa do Colaborador.

A Oikos não assume a responsabilidade de Colaboradores que transgridam a lei ou cometam infrações no exercício de suas funções. Caso a Oikos venha a ser responsabilizada ou sofra prejuízo de qualquer natureza por atos de seus Colaboradores, poderá exercer o direito de regresso em face dos responsáveis.