

Política de PLD-FT

Versão Maio.2025

INTRODUÇÃO

Esta Política tem por **objetivo: Definir e estabelecer as diretrizes para a prevenção, detecção, reporte e encaminhamento dos crimes de lavagem de dinheiro, financiamento ao terrorismo e à proliferação de armas de destruição em massa, bem como corrupção (“PLD/FTPC”).**

RESPONSÁVEIS PELA Política de Prevenção aos Crimes de Lavagem de Dinheiro, Financiamento ao Terrorismo

Diretoria Jurídica e de Compliance

ABRANGÊNCIA

Fairfax Brasil Seguros Corporativos S/A

Fairfax Brasil Participações Ltda, coligadas e controladas

APLICAÇÃO

Imediata

NORMATIVOS VINCULADOS

Política de Governança Corporativa, Código de Ética e Manual de Boas Práticas; Manual de Due Diligence na Plataforma Neoway; Política de Compliance (Conformidade); Política Canal de Denúncias; Política de Adequação de Produtos e Desenvolvimento de Novos Produtos; Política de Contratos e Homologação de Fornecedores; Política de Novos Projetos; Política de Alçadas.

Histórico de revisões:

Histórico de revisões:

Versão	Data	Comentários
08	25/05/2025	Ajustes no texto do item 1. e sobre procedimento de comunicação ao COAF.
07	28/02/2025	Adequações na redação do documento para atendimento do Relatório da Auditoria/2025
06	24/09/2024	Adequações decorrentes do Relatório de Efetividade – data-base 12.2023
05	07/12/2023	Adequações pontuais na redação do documento
04	11/07/2023	Adequações pontuais na redação do documento
03	30/06/2022	Adequações pontuais na redação do documento
02	30/08/2021	Adequações pontuais na redação do documento
01	30/04/2021	Publicação

1. INTRODUÇÃO



O objetivo desta Política é promover a disseminação da cultura, procedimentos e controles internos destinados à prevenção e combate aos crimes de lavagem de dinheiro, financiamento ao terrorismo e à proliferação de armas de destruição em massa, bem como corrupção (“PLD/FTPC”).

Esta Política é aplicável a todos os colaboradores, corretores de seguros, parceiros de negócios e prestadores de serviços terceirizados, da Fairfax Brasil Seguros Corporativos SA e Fairfax Brasil Participações Ltda, coligadas e controladas, independentemente do nível hierárquico, nos termos da Lei nº 9.613/1998, lei nº 12.846/2013, lei 13.260/2016 e da Circular Susep nº 612/2020 e demais regulamentos referentes à prevenção à lavagem de dinheiro e ao financiamento do terrorismo bem como, cumprir e seguir os procedimentos previstos nesta Política.

A Fairfax Brasil Seguros Corporativos S/A e empresas da holding Fairfax, através de seus administradores e colaboradores, estão comprometidas nas medidas de prevenção aos crimes de lavagem de dinheiro, terrorismo e corrupção, bem como, com a efetividade e melhoria contínua de suas políticas, processos, procedimentos e controles internos.

Esta Política está assim dividida:

- i. Principais aspectos da Lei nº 9.613/1998 e alterações, que dispõem sobre os crimes de lavagem ou ocultação de bens, direitos e valores a prevenção da utilização do sistema financeiro para os ilícitos previstos na Lei e que cria o Conselho de Controle de Atividades Financeiras – COAF);
- ii. Principais aspectos da Lei de combate ao terrorismo nºs 13.260/2016;
- iii. Principais aspectos da Lei nº 13.810/2019, que dispõe sobre o cumprimento de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas, incluída a indisponibilidade de ativos de pessoas naturais e jurídicas e de entidades, e a designação nacional de pessoas investigadas ou acusadas de terrorismo, de seu financiamento ou de atos a ele correlacionados;

- iv. Principais aspectos da Circular Susep nº 612/2020 - que dispõe sobre as políticas, os procedimentos e os controles internos destinados especificamente à prevenção e combate aos crimes de “lavagem” ou ocultação de bens, direitos e valores, ou aos crimes que com eles possam relacionar-se, bem como, à prevenção e coibição do financiamento ao terrorismo e à proliferação de armas de destruição em massa, bem como corrupção (“PLD/FTPC”).

Destaca-se, por oportuno, que esta Política não elimina a necessidade da atenta leitura dos textos das leis e circulares vigentes.



Considerando que as Seguradoras também podem servir de canal para o crime de lavagem de dinheiro e financiamento do terrorismo, a Susep – Superintendência de Seguros Privados, publicou normativos infralegais para coibir a prática deste crime através do mercado segurador brasileiro.

As regras da Susep, bem como a legislação em vigor sobre a prevenção à lavagem de dinheiro e financiamento ao terrorismo devem ser cumpridas, caso contrário, a seguradora e seus gestores poderão sofrer severas penalidades.



Portanto, todos devem tomar conhecimento com muita atenção do conteúdo desta Política.

2. GOVERNANÇA CORPORATIVA DA FAIRFAX

De acordo com a definição do Banco Mundial, Governança Corporativa é “a maneira pela qual o poder é exercido no gerenciamento dos recursos econômicos e sociais para o desenvolvimento”.

O Departamento de Compliance, Sistema de Controles Internos (SCI), Estrutura de Gestão de Riscos (EGR) e Auditoria Interna, são áreas complementares, independentes, com reporte direto para a alta direção, e que trabalham em conjunto para garantir a boa Governança Corporativa na Fairfax Brasil.



Sistema de Controles Internos - SCI



Jurídico

Consultoria e assessoria jurídica na prevenção de riscos legais e regulatórios e contencioso.



Compliance

Risco reputacional; conformidade com políticas e normativos legais e infralegais; prevenção aos crimes de lavagem de dinheiro, financiamento ao terrorismo, corrupção, atuação em situações de conflito de interesses e canal de denúncia.



Gestão de Riscos; Privacidade; Fraudes

Mapeamento de riscos operacionais; mensuração de riscos; planos de ações.



Segurança da Informação e Privacidade

Prevenção e coibição aos riscos de segurança da informação; riscos cibernéticos; riscos de privacidade (vazamento de dados pessoais); riscos de fraude.



Auditoria

Checagem e supervisão

2.1. Papéis e Responsabilidades

É muito importante entender o escopo de atuação de cada um desses departamentos, para o cumprimento da Circular Susep nº 612/2020.

Presidência

Alta administração da Fairfax Brasil, responsável pelos planos e decisões estratégicas da companhia.

Diretoria Estatutária

Alta administração da Fairfax Brasil, composta por seis diretores estatutários, inclusive nomeados perante a Susep para cargos específicos definidos por normativos infralegais, responsável por auxiliar a presidência nos planos e decisões estratégicas da companhia.

Compliance

Zelar pelo risco reputacional; implementar as políticas e procedimentos de prevenção aos crimes de lavagem de dinheiro, terrorismo e corrupção. Através da Unidade de Conformidade, garantir que as operações da companhia estejam aderentes com as leis e regulamentações aplicáveis, boas práticas e suas próprias políticas e normativos internos. Responsável pelo canal de denúncias e análise de situações de conflito de interesses.

2.1. Papéis e Responsabilidades

Diretor estatutário de prevenção aos crimes de lavagem de dinheiro	Diretor estatutário nomeado para as funções de diretor responsável pelo cumprimento do disposto na Lei nº 9.613/98, nos termos da Circular Susep nº 612/2021.
Sistema de Controles Internos - SCI	Responsável por medir e acompanhar a eficácia de todos os processos e procedimentos da companhia. Conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, implementação, operacionalização, monitoramento, análise crítica e melhoria contínua dos controles internos através de toda a organização. Faz parte do Sistema de Controles Internos as seguintes áreas de controles: Jurídico, Compliance, Riscos, Segurança da Informação e Auditoria.
Gestão de Riscos	Responsável pelo mapeamento de riscos da companhia, decorrentes de falhas operacionais, mensuração de riscos e implementação de planos de ações. Processos e procedimentos empregados de forma coordenada para identificar, avaliar, mensurar, tratar, monitorar e reportar os riscos da organização, tendo por base a adequada compreensão dos tipos de risco, de suas características e interdependências, das fontes de riscos e de seu potencial impacto sobre o negócio.
Auditoria	Responsável por efetuar a checagem e supervisão.
Tecnologia	Responsável por implementar os desenvolvimentos sistêmicos necessários aos controles internos de prevenção aos crimes de lavagem de dinheiro, terrorismo e corrupção.
Comissão de Compliance	A Comissão de Compliance tem por objetivo decidir, de forma colegiada, os casos envolvendo suspeita de lavagem de dinheiro, para efeitos de deliberação e implementação de planos de ações. As decisões serão coletivas, por maioria de votos. Em caso de empate, o voto soberano será do diretor responsável por lavagem de dinheiro. Os membros votantes da Comissão de Compliance são: 1) diretor de controles internos e responsável perante à Susep pela prevenção aos crimes de lavagem de dinheiro e terrorismo (também será desempatador); 2) diretor estatutário convidados, responsável pela área demandante; 3) diretora jurídica e de compliance; 4) gestor de auditoria.
Recursos Humanos	Responsável por auxiliar o Departamento de Compliance nos treinamentos obrigatórios, bem como, implementar a Política de Compliance junto a todos os colaboradores.
Área de Sinistros	Responsável por auxiliar o Departamento de Compliance em inibir pagamentos de sinistros em que a seguradora possa ser usada como veículo para lavar dinheiro, auxiliando também na checagem de informações cadastrais de segurados e beneficiários de seguros.

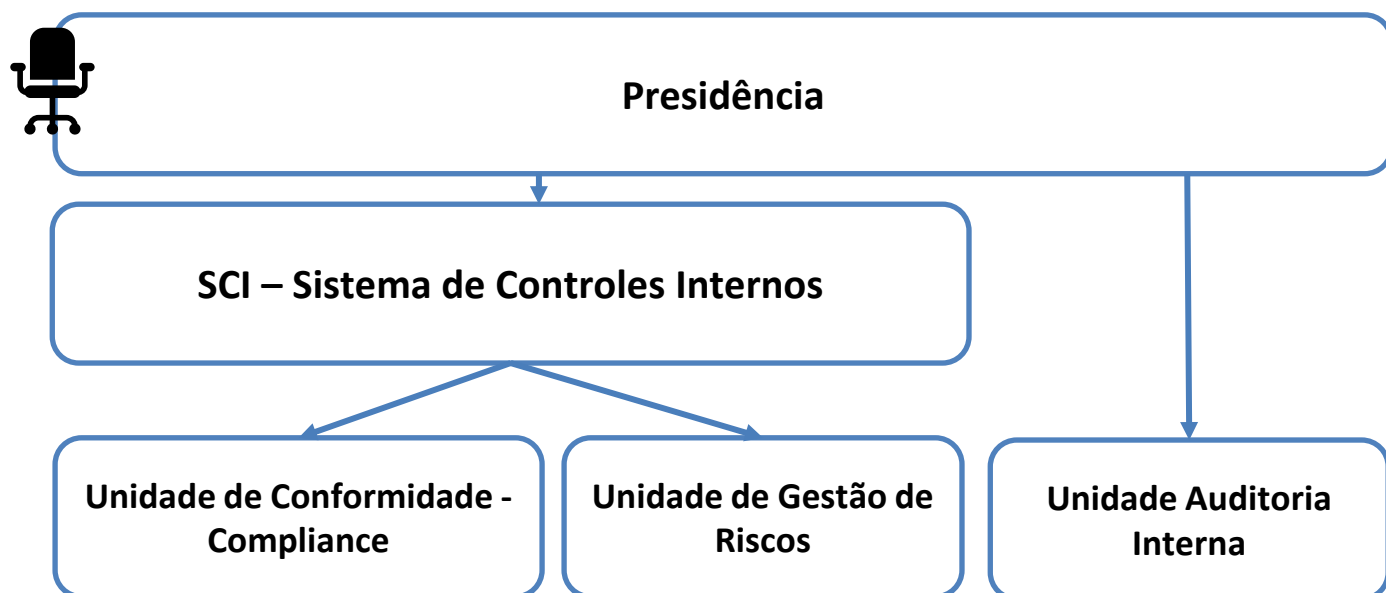
2.1. Papéis e Responsabilidades

Heads das áreas de negócios e de back-office	São responsáveis por implementar, em suas respectivas áreas de atuações, as medidas divulgadas pela área de Compliance, na prevenção dos crimes de lavagem de dinheiro, financiamento do terrorismo e corrupção.
Área de cadastro	Responsável pelo cadastro de parceiros de negócios, trabalhando em conjunto com o Departamento de Compliance, na análise de compliance desses parceiros.
Colaboradores	Os colaboradores são treinados e nas atividades rotineiras devem sempre estar atentos e auxiliar na detecção de operações suspeitas.

2.2. Estrutura Organizacional e de Compliance

A Fairfax, com o apoio de sua diretoria e todos os colaboradores, está comprometida com os padrões éticos e de conduta; treinamentos eficazes e periódicos; a análise de prevenção e mitigação de riscos; a manutenção de um canal de denúncias eficaz e confidencial; controles internos eficazes.

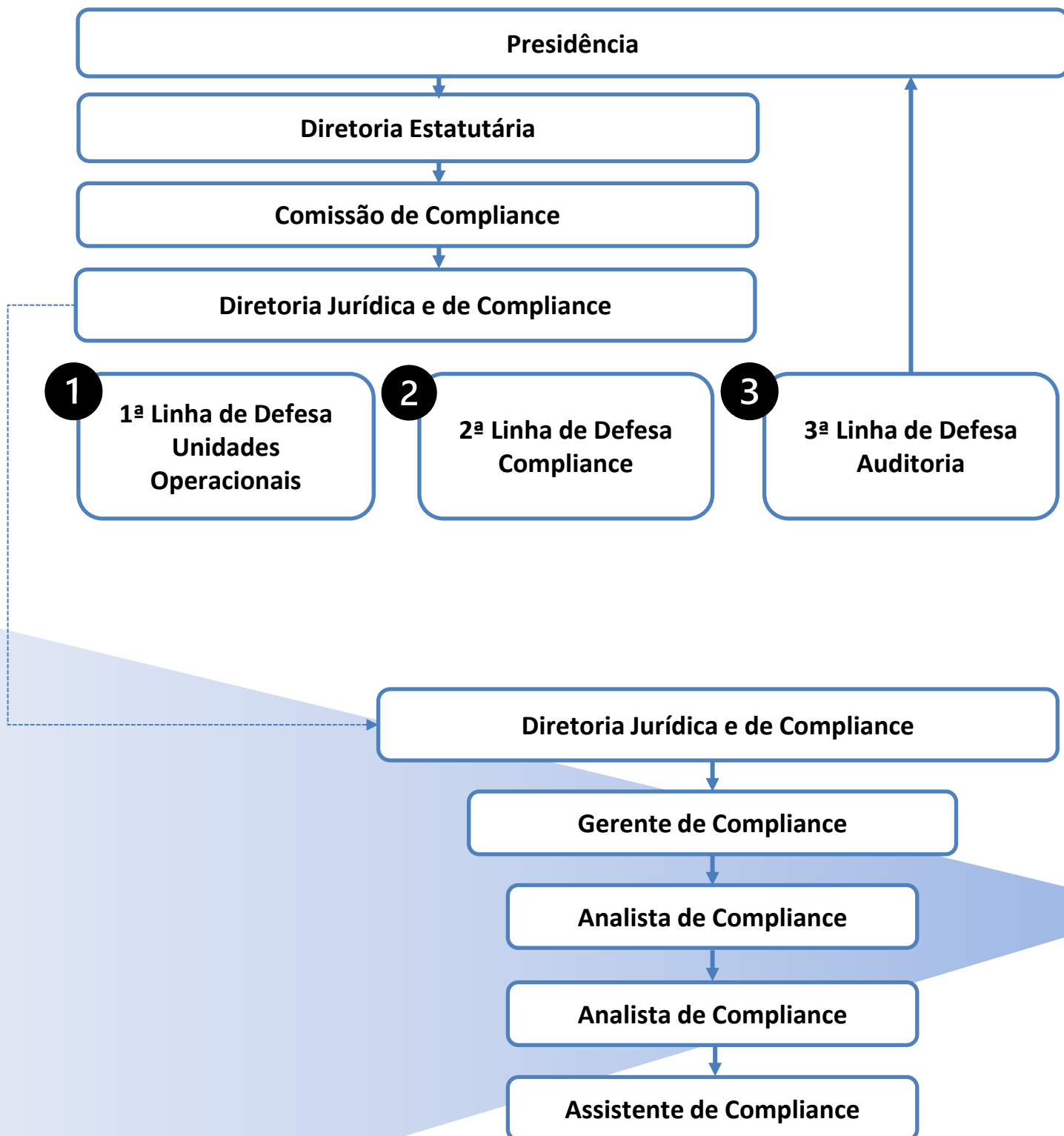
A área de Compliance, que também engloba a Unidade de Conformidade, é uma das áreas independentes e autônomas, com reporte direto à alta direção e que faz parte do Sistema de Controles Internos.



Estrutura Organizacional e de Compliance



No que se refere à estrutura do Departamento de Compliance, que faz parte da Diretoria Jurídica & Compliance, e subordinada a Diretoria Estatutária de Controles Internos, é composta da seguinte maneira:



3. Lei nº 12.683 de 09 de julho de 2012 e Circular Susep nº 612/2020 – Sistema Brasileiro de Prevenção à Lavagem de Dinheiro e ao Financiamento ao Terrorismo:

3.1. Conceito:

Em 03 de Março de 1998, o Brasil, dando continuidade aos compromissos internacionais assumidos a partir da assinatura da Convenção de Viena de 1988, aprovou, com base na respectiva Exposição de Motivos, a chamada Lei de Lavagem de Dinheiro (Lei nº 9.613), atualmente alterada pela Lei nº 12.683, de 09.07.2012.

Com a alteração trazida pela Lei nº 12.683/2012, **qualquer infração penal relacionada com as situações previstas no artigo 1º desta Lei, caracteriza o crime de lavagem de dinheiro.**

Também está **sujeito à mesma pena, quem se utiliza de atividade econômica ou financeira, de bens, de diretos ou de valores decorrentes de crimes.**

De acordo com esta Lei, considera-se crime de lavagem de dinheiro:



“Art. 1º Ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal. Pena: reclusão, de 03 (três) a 10 (dez) anos e multa.

§ 1º Incorre na mesma pena quem, para ocultar ou dissimular a utilização de bens, direitos ou valores provenientes de infração penal:

os converte em ativos lícitos;

os adquire, recebe, troca, negocia, dá ou recebe em garantia, guarda, tem em depósito, movimenta ou transfere;

importa ou exporta bens com valores não correspondentes aos verdadeiros.

§ 2º Incorre, ainda, na mesma pena quem:

I - utiliza, na atividade econômica ou financeira, bens, direitos ou valores que sabe serem provenientes de qualquer dos crimes antecedentes referidos neste artigo;

utiliza, na atividade econômica ou financeira, bens, direitos ou valores provenientes de infração penal; (Redação dada pela Lei nº 12.683, de 2012);

participa de grupo, associação ou escritório tendo conhecimento de que sua atividade principal ou secundária é dirigida à prática de crimes previstos nesta Lei”.

Fases do Crime de Lavagem de Dinheiro

Assim, o crime de lavagem de dinheiro caracteriza-se por um conjunto de operações comerciais ou financeiras que buscam a incorporação na economia de cada país, de modo transitório ou permanente, de recursos, bens ou valores de origem ilícita e que se desenvolvem por meio de um processo dinâmico que envolve, teoricamente, três fases independentes que, com frequência, ocorrem simultaneamente: Colocação, Ocultação e Integração.

COLOCAÇÃO

A colocação caracteriza-se pela colocação do dinheiro no sistema econômico, objetivando ocultar sua origem e tem as seguintes características:

- Criminoso costuma movimentar o dinheiro em países com regras mais permissivas e naqueles que possuem um sistema financeiro liberal.
- A colocação se efetua por meio de depósitos, compra de instrumentos negociáveis ou compra de bens.
- Para dificultar a identificação da procedência do dinheiro, os criminosos aplicam técnicas sofisticadas e cada vez mais dinâmicas, tais como o fracionamento dos valores que transitam pelo sistema financeiro e a utilização de estabelecimentos comerciais que usualmente trabalham com dinheiro em espécie.

OCULTAÇÃO

A ocultação consiste em dificultar o rastreamento contábil dos recursos ilícitos e tem as seguintes características:

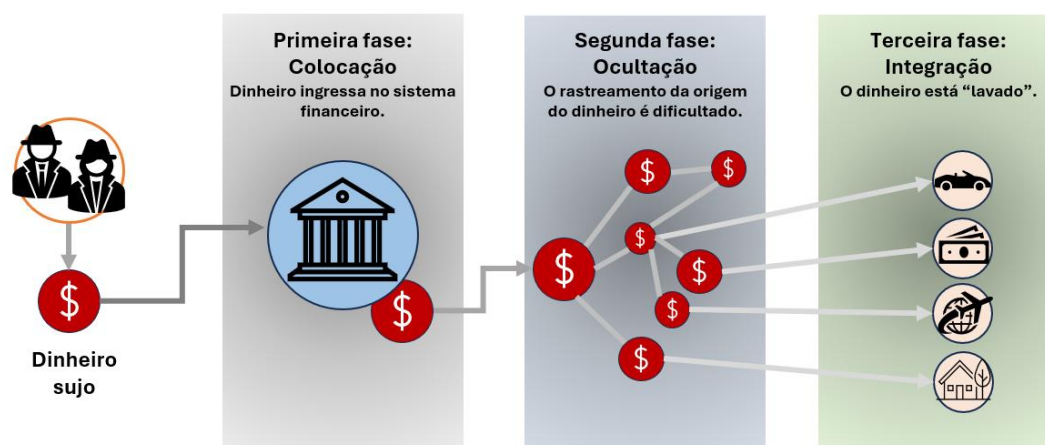
- objetivo é quebrar a cadeia de evidências ante a possibilidade da realização de investigações sobre a origem do dinheiro.
- os criminosos buscam movimentar o dinheiro de forma eletrônica, transferindo os ativos para contas anônimas – preferencialmente, em países amparados por lei de sigilo bancário – ou realizando depósitos em contas "fantasmas".

INTEGRAÇÃO

A integração consiste em incorporar os ativos provenientes do crime no sistema econômico e tem as seguintes características:

- As organizações criminosas buscam investir em empreendimentos que facilitem suas atividades podendo tais sociedades prestarem serviços entre si.
- Uma vez formada a cadeia, torna-se cada vez mais fácil legitimar o dinheiro ilegal.

Fases do Crime de Lavagem de Dinheiro



Assim, torna-se necessário identificar toda e qualquer operação suspeita, principalmente na colocação do dinheiro proveniente do crime no sistema financeiro, e comunicar o fato às autoridades. Se isso não ocorrer, o dinheiro do crime será integrado às operações legais corriqueiras e não será mais possível pegar os criminosos.

3.2. Atribuições legais na prevenção e coibição dos crimes de lavagem de dinheiro e financiamento ao terrorismo

O arcabouço legal brasileiro para lidar com o problema da lavagem de dinheiro foi definido pela Lei nº 12.683, de 09 de julho de 2012, que alterou a Lei nº 9.613, de 3 de março de 1998, a qual dispõe sobre as medidas legais necessárias, a definição do crime de lavagem de dinheiro, as medidas preventivas, o sistema de comunicação de operação suspeita, a criação do COAF – Conselho de Controle de Atividades Financeiras e os vários mecanismos de cooperação internacional.

Referida Lei, combinada com a Circular Susep nº 612/2020, obriga **as sociedades seguradoras** e de capitalização; os resseguradores locais e admitidos; as entidades abertas de previdência complementar; as sociedades cooperativas autorizadas a funcionar pela Susep; as sociedades corretoras de resseguro; as sociedades corretoras de seguros, de capitalização e de previdência complementar aberta, **a adotarem políticas, procedimentos e os controles internos destinados à prevenção e ao combate aos crimes de lavagem de dinheiro e financiamento ao terrorismo.**

Assim, os procedimentos e controles internos devem ser efetivos e consistentes com a natureza, complexidade e riscos das operações realizadas, baseados nas seguintes premissas:

- i. Identificação;
- ii. Avaliação;
- iii. Controle e monitoramento dos riscos.

A Lei nº 12.683, de 09 de julho de 2012, que alterou a Lei nº 9.613, de 3 de março de 1998, atribuiu às pessoas jurídicas de diversos setores econômico-financeiros maior responsabilidade na identificação de seus respectivos clientes e manutenção de registros de todas as operações e na comunicação de operações suspeitas aos órgãos responsáveis, incluindo o COAF, sujeitando-as ainda às penalidades administrativas pelo descumprimento das obrigações.

3.3. Identificação, avaliação, controle e monitoramento dos riscos:

Uma das práticas fundamentais na prevenção aos crimes de lavagem de dinheiro e financiamento ao terrorismo é a identificação da partes com as quais a empresa mantém relacionamento. Tais práticas, dentro de Compliance, são conhecidas como:



Conheça o seu Colaborador (KYE – Know Your Employee);



Conheça o seu Cliente (KYC – Know Your Client);



Conheça o seu Parceiro//Prestador de Serviço (KYP – Know Your Partner – KYS – Know Your Supplier).

Sendo assim, para cumprimento das práticas acima, os procedimentos devem incluir a obtenção, a verificação e a validação da autenticidade de informações de identificação.

Para tanto, utilizamos ferramentas que nos disponibilizam a consulta através da confrontação dessas informações com as disponíveis em bancos de dados de caráter público e privado.

Dessa forma, para identificação de nossos clientes, colaboradores, parceiros e prestadores de serviços, poderemos solicitar, minimamente, as seguintes informações:



I- Quando **pessoa natural**:

- a) nome completo;
- b) número de inscrição no Cadastro de Pessoas Físicas (CPF); e
- c) endereço residencial.



II- Quando **pessoa jurídica**:

- a) a denominação ou razão social;
- b) o número de identificação no Cadastro Nacional de Pessoa Jurídica (CNPJ), ou registro equivalente para as empresas isentas do CNPJ;
- c) endereço da sede;
- d) as informações do subitem I para controladores até o nível de pessoa natural, principais administradores e procuradores; e
- e) as informações do subitem I para beneficiários finais.

No processo de identificação, além das informações acima, também levamos em consideração se se trata de uma Pessoa Politicamente Exposta (PEP), bem como informações que avaliam a capacidade financeira da pessoa física (renda) ou jurídica (faturamento) e tais condições são avaliadas em nosso processo de due diligence, de acordo com os critérios de riscos estabelecidos pela Companhia.

Com todas as informações que possibilitam a identificação dos nossos colaboradores, clientes, parceiros e prestadores de serviços, a Companhia adota critérios de avaliação e mensuração de riscos, para determinar em qual momento do relacionamento tais informações serão validadas, o que poderá variar, desde o momento da proposta de seguro, até o sinistro, o que é determinado de acordo com o perfil de risco mapeado para a pessoa e/ou produto contratado.

Identificação, avaliação, controle e monitoramento dos riscos:



3.3.1. Conheça seus Colaboradores (KYE – Know Your Employee)

Cabe ao Departamento de Pessoas e Sustentabilidade (Recursos Humanos) da Fairfax, obter as informações necessárias para a identificação do colaborador, solicitando, ao menos, aquelas relacionadas no subitem I, do item 3.3. O departamento de Compliance será o responsável por fazer a confrontação das informações obtidas pelo Departamento de Pessoas e Sustentabilidade (Recursos Humanos), através de ferramenta de consulta de dados públicos e privados, a qual terá por base os critérios estabelecidos no perfil de riscos aprovado pela Companhia.

A cada nova contratação, o Departamento de Pessoas e Sustentabilidade (Recursos Humanos) deverá enviar as informações mínimas necessárias do colaborador, para que o Departamento de Compliance possa fazer a análise de due diligence e, anualmente, a base de colaboradores deverá passar por nova consulta, para fins de monitoramentos do perfil de riscos de todos.

É de responsabilidade do Departamento de Pessoas e Sustentabilidade (Recursos Humanos) incluir e manter atualizado nos sistemas de controles da Fairfax, as informações cadastrais dos colaboradores, garantindo que tais informações sejam transmitidas de forma transparente ao Departamento de Compliance.

3.3.2. Conheça seus prestadores de serviços, corretores de seguros, resseguradores, brokers de resseguro e demais parceiros de negócios (KYP – Know Your Partner – KYS – Know Your Supplier)



Sempre que parceiros, prestadores de serviços terceirizados, fornecedores, corretores, brokers de resseguro e demais parceiros de negócio desejarem ter relacionamento comercial com a Fairfax, deverão disponibilizar as informações e documentos necessários para a sua devida identificação, sendo tais documentos, minimamente, os seguintes:

- Estatuto/Contrato Social atualizado;
- Eleição da diretoria/procurações, conforme o caso;
- Comprovante de endereço;
- Cópia do CNPJ;
- Cópia do CNPJ dos sócios PJ. Se houver sócio PF, cópia do RG e CPF do sócio relevante (acima de 5% de participação).
- Formulário de Compliance de homologação, preenchido e assinado.

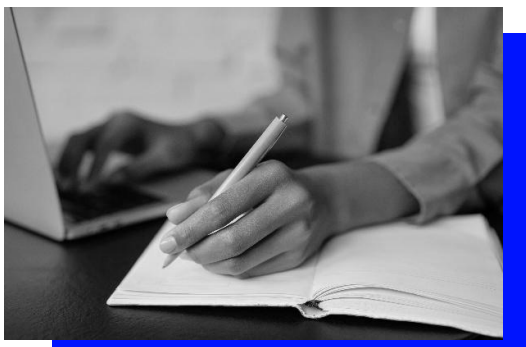


Identificação, avaliação, controle e monitoramento dos riscos:

Com as informações e documentos cadastrais disponibilizados, a Companhia realizará o procedimento de homologação, para avaliar a viabilidade do relacionamento comercial, de acordo com os critérios de avaliação de riscos definidos.



Anualmente, as informações cadastrais serão confrontadas em ferramenta de consulta de banco de dados públicos e privados, para verificar se o perfil de risco avaliado no início da contratação ainda é o mesmo e o Departamento de Compliance será acionado, em caso de alteração.



3.3.3. Conheça seu cliente: (KYC – Know Your Client)

Para fins da presente Política, entenda-se “cliente”, o segurado, o tomador, o beneficiário e qualquer outra identificação que possa ter, para se referir ao destinatário final da indenização do seguro.

As informações cadastrais do cliente, englobam aquelas estipuladas nos subitens I, II do item 3.3., serão obtidas no momento da contratação do seguro.

Em caso de seguro coletivo, os documentos e informações cadastrais dos segurados serão mantidos no Estipulante e compartilhados com a companhia, sempre que solicitado.

Cabe à área de sinistros, no momento da liquidação do sinistro, fazer a verificação, validação e/ou atualização de informações cadastrais do cliente, através da obtenção dos documentos cadastrais mínimos exigidos no artigo 20 da Circular Susep nº 612/2020, que são os mesmos estipulados nos subitens I, II do item 3.3., acima.

A validação da autenticidade das informações cadastrais ocorre por meio de ferramenta, que toma por base a consulta à bases de dados de caráter públicos e privados que, em conjunto com os critérios de riscos estabelecidos pela Companhia, define o perfil de risco do cliente e avalia se o mesmo atende ao apetite de risco da Fairfax.

Dentro dos parâmetros de apetite de riscos da Companhia, as informações cadastrais do cliente serão confrontadas na ferramenta de consulta de banco de dados públicos e privados em uma periodicidade que poderá variar de acordo com o perfil de risco de cada cliente, podendo ser anual, semestral ou sempre que houver uma alteração no status da apólice (cancelamento ou renovação).

De acordo com os critérios e parâmetros estabelecidos pela Fairfax, em sua avaliação interna de riscos, o Diretor responsável pelo cumprimento da Lei nº 9.613, de 1998 (Lei de Prevenção e Combate ao Crime de Lavagem de Dinheiro e Financiamento ao Terrorismo) e Circular Susep nº 612/2020, poderá, exceto para os casos classificados como de maior risco, dispensar procedimentos de due diligence destinados ao fim de conhecer os clientes.

3.4. COAF - Conselho de Controle de Atividades Financeiras



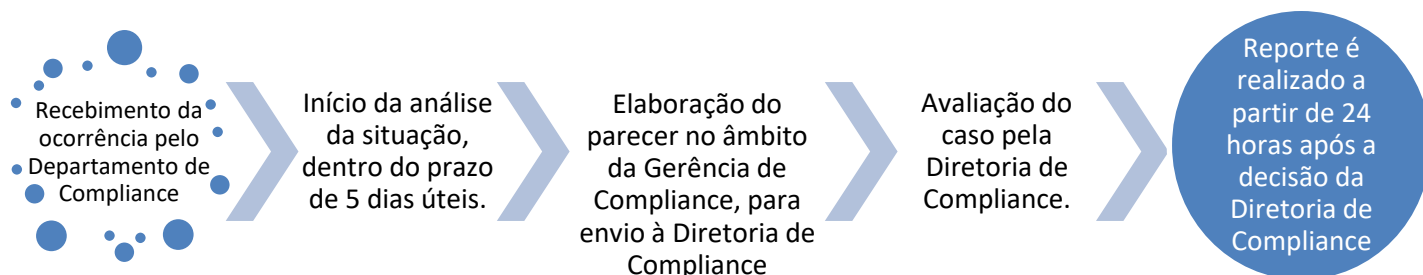
A Lei nº 9.613/98, alterada pela Lei nº 12.683/2012, criou o COAF – Conselho de Controle de Atividades Financeiras, órgão vinculado ao Ministério da Fazenda para cuidar dos assuntos ligados a lavagem de dinheiro e financiamento ao terrorismo.

Dentro do que é estabelecido em nossas diretrizes de prevenção e combate ao crime de lavagem de dinheiro, financiamento do terrorismo, proliferação de armas de destruição em massa, todos são responsáveis por prevenir e coibir a prática de tais crimes.

Dentro dessa obrigação, a Circular Susep n.612/2020, estabeleceu a identificação de situações ou operações suspeitas, as quais, quando presentes no âmbito do seguro, devem ser comunicadas ao COAF.

Sempre que identificada uma operação ou situação suspeita, deve ser enviado um e-mail para o **compliance@fairfax.com.br** com a descrição e evidências da ocorrência.

As situações ou operações suspeitas reportadas, terão o seguinte ciclo de análise dentro da companhia:



Além do procedimento acima, a comunicação é realizada de forma automática, não dependendo de qualquer análise ou juízo de valor, dentro do prazo de 24 (vinte e quatro) horas, a partir da confirmação das seguintes situações:



- i. Operações realizadas com pagamento de prêmio, contribuição, aporte e aquisição de título de capitalização em espécie, em valor igual ou superior a R\$ 10.000,00 (dez mil reais); ou
- ii. pagamentos de resgates, indenizações ou sorteios, realizados em conta no exterior, mediante geração do código Swift da operação, em valor igual ou superior a R\$ 100.000,00 (cem mil reais).

Além disso, como forma de mapeamento, monitoramento e controle dos casos que devem ser comunicados ao Coaf, também realizamos a captura das situações e operações suspeitas, descritas no artigo 36 da Circular Susep nº 612/2020, em dois momentos:

- a) **No momento do pagamento do sinistro**, onde o regulador, poderá identificar o motivo da operação suspeita, se for o caso, desde que tenhamos evidências suficientes para tanto;
- b) **Mensalmente, através de contato direto com os departamentos da Companhia**, para saber se no mês foram identificadas situações ou operações suspeitas.

3.4. COAF - Conselho de Controle de Atividades Financeiras

Nesta hipótese de caracterização de operação suspeita, o Departamento de Compliance e Jurídico serão acionados. O Departamento de Compliance fará a análise para reporte ao Coaf e o Departamento Jurídico dará recomendações jurídicas para proteger a companhia no caso de pagamento da indenização.

Para o disposto neste item, entende-se como situações ou operações suspeitas, as descritas no artigo 36 da Circular Susep nº 612/2020:



- i. **Contratação, por estrangeiro não residente no Brasil**, de apólice de seguro na Fairfax Brasil;
- ii. **Propostas ou operações incompatíveis com o perfil socioeconômico**, capacidade financeira ou ocupação profissional do cliente, beneficiário, terceiros, e outras partes relacionadas;
- iii. Propostas ou operações **discrepantes das condições normais** de mercado;
- iv. Pagamento **a beneficiário sem aparente relação** com o contratante de seguros;
- v. **Mudança de titular** do negócio ou bem imediatamente anterior ao sinistro;
- vi. Pagamento de prêmio **fora da rede bancária**;
- vii. Pagamento de prêmio por **pessoa estranha à operação** ou desobrigada a esse pagamento;
- viii. **Transações cujas características peculiares**, principalmente no que se refere às partes envolvidas, valores, forma de realização, instrumentos utilizados, ou pela falta de fundamento econômico ou legal, mesmo que tragam vantagem à Fairfax, ao ressegurador ou ao corretor, **possam caracterizar indício de lavagem de dinheiro**, financiamento do terrorismo, ou de qualquer outro ilícito;
- ix. **Utilização desnecessária de uma rede complexa** de corretoras de resseguro para a contratação de resseguro ou retrocessão;
- x. **Avisos de sinistros** aparentemente legítimos, mas **com frequência anormal**;
- xi. **Variações relevantes de importância segura** sem causa aparente;
- xii. Pagamentos de indenizações realizadas **no exterior acima de R\$100.000,00**;
- xiii. Propostas ou operações em que **não seja possível identificar o beneficiário final**, no processo de identificação.

3.4.1. Situações de dispensa de aviso ao COAF

Nas situações em que o Departamento de Compliance entender que não se trata de uma operação suspeita para efeitos de reporte ao Coaf, a Diretora de Compliance providenciará o devido parecer no prazo de 05 dias a contar da análise efetuada pelo analista de Compliance, e enviará o pedido de dispensa de reporte ao Coaf ao Diretor de Controles Internos, acompanhado de informações e documentos que embasam a dispensa.

3.5. Leis nºs 13.260/2016 e Lei nº 13.810/2019 de combate ao terrorismo e indisponibilidade de ativos de quaisquer valores e cumprimento de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas - CSNU, incluída a indisponibilidade de ativos de pessoas naturais e jurídicas e de entidades, e a designação nacional de pessoas investigadas ou acusadas de terrorismo, de seu financiamento ou de atos a ele correlacionados:

Nos termos da Lei nº 13.260/2016, **são atos terroristas:**



- I. Usar ou ameaçar usar, transportar, guardar, portar ou trazer consigo explosivos, gases tóxicos, venenos, conteúdos biológicos, químicos, nucleares ou outros meios capazes de causar danos ou promover destruição em massa, sabotar o funcionamento ou apoderar-se, com violência, grave ameaça a pessoa ou servindo-se de mecanismos cibernéticos, do controle total ou parcial, ainda que de modo temporário, de meio de comunicação ou de transporte, de portos, aeroportos, estações ferroviárias ou rodoviárias, hospitais, casas de saúde, escolas, estádios esportivos, instalações públicas ou locais onde funcionem serviços públicos essenciais, instalações de geração ou transmissão de energia, instalações militares, instalações de exploração, refino e processamento de petróleo e gás e instituições bancárias e sua rede de atendimento;
- II. atentar contra a vida ou a integridade física de pessoa.



A pena é a reclusão, de doze a trinta anos, além das sanções correspondentes à ameaça ou à violência.

Por sua vez, a Lei nº 13.810/2019, que tem por objetivo combater o crime de terrorismo, prevê que **pessoas investigadas ou acusadas de terrorismo, de seu financiamento ou de atos a ele correlacionados, podem sofrer sanções impostas por resoluções do Conselho de Segurança das Nações Unidas - CSNU**, incluída a indisponibilidade de ativos de pessoas naturais e jurídicas e de entidades. Assim, em razão da executoriedade imediata na República Federativa do Brasil das resoluções sancionatórias do CSNU e as designações de seus comitês de sanções, **ficam as instituições financeiras brasileiras obrigadas a cumprir os embargos e sanções internacionais.**

Sendo assim, todos os ofícios do Poder Judiciário e/ou Órgãos Governamentais, incluindo a Susep, relacionados a bloqueios/indisponibilidade de bens e/ou inclusão de pessoas em restritivos nacionais e/ou internacionais, relacionados à lavagem de dinheiro e financiamento do terrorismo, são recebidos pelo Departamento de Compliance, que aciona a área de TI, para a realização do rastreamento sistêmico, para verificação de relacionamento com tais pessoas, para que eventuais medidas de devida diligência sejam adotadas.

O Departamento de Compliance é o responsável pelo controle dos ofícios e cartas circulares da Susep, principalmente pela divulgação à Companhia, das restrições impostas a pessoas e/ou países com embargos e sanções pelo CSNU.



Além disso, através da ferramenta de consulta de banco de dados de caráter público e privado utilizada pela Companhia, o Departamento de Compliance também realiza consulta de segurados em listas internacionais de embargos e sanções e garante que a ferramenta esteja sempre atualizada, quando do recebimento de Ofícios pela Susep que enquadrem pessoas com embargos e sanções.

Assim, no que se refere ao **cumprimento da Lei nº 13.810/2019, no momento da subscrição do risco e do pagamento de um sinistro**, conforme critérios definidos na Avaliação Interna de Riscos, se o CNPJ e CPF do segurado e/ou beneficiário tiver alguma sanção imposta por resoluções do CSNU, o **Departamento de Compliance será envolvido para análise da sanção e/ou restrição imposta**. A análise ocorrerá em até 05 dias úteis, com parecer de compliance sobre as medidas a serem tomadas, como reporte ao COAF, no prazo de 24 horas a contar da conclusão da análise.

3.6. Treinamentos



Os novos colaboradores recebem os seguintes treinamentos no momento do onboarding, ou seja, no primeiro dia de trabalho :

- i.Prevenção aos crimes de lavagem de dinheiro, terrorismo e corrupção;
- ii.Código de Ética e de Conduta;
- iii.Compliance.

Ao longo da jornada do colaborador dentro da Companhia, adotamos como medidas de desenvolvimento da cultura organizacional voltadas à prevenção à lavagem de dinheiro e ao financiamento do terrorismo, o **envio de comunicados periódicos sobre os temas**, bem como realização de **cursos de reciclagem que ocorrem a cada dois anos**.

O Departamento de Pessoas e Sustentabilidade (Recursos Humanos-RH) é o responsável pela convocação dos colaboradores e controle de presença, tanto no curso de onboarding, quanto no curso de reciclagem.

Na contratação de serviços externos, credenciamento de corretores de seguros e demais parceiros de negócio, por ocasião da formalização do contrato, o Departamento de Compliance informa o caminho no site da Fairfax para acesso ao treinamento de prevenção aos crimes de lavagem de dinheiro, financiamento ao terrorismo e corrupção, bem como, o Código de Ética e de Conduta.

No caso de parceiros de negócios, como corretores de seguros, broker de resseguros e resseguradores, por também estarem sujeitos à fiscalização da Superintendência de Seguros Privados – Susep e cumprimento da Circular Susep nº 612/2020, não receberão o treinamento de prevenção aos crimes de lavagem de dinheiro, financiamento do terrorismo e corrupção, mas serão instruídos a consultarem o site da Fairfax para leitura e compreensão do Código de Ética e Conduta, do Manual de Boas Práticas e da presente Política.

3.7. Comissão de Compliance e Departamento de Compliance



O objetivo da Comissão de Compliance é analisar e decidir em conjunto com o diretor estatutário de controles internos, também responsável perante à Susep pela prevenção e combate aos crimes de lavagem de dinheiro, e financiamento ao terrorismo ou corrupção.

As decisões serão coletivas, por maioria de votos. Em caso de empate, o voto soberano será do diretor responsável perante à Susep pela prevenção e combate aos crimes de lavagem de dinheiro e financiamento ao terrorismo.

Os membros votantes da Comissão de Compliance são:

Diretor de controles internos, responsável perante à Susep pelo cumprimento das normas de prevenção e coibição aos crimes de lavagem de dinheiro e terrorismo (também será desempataador);

Diretor estatutário convidado, responsável pela área demandante;

Diretora jurídica e de compliance;

Gestor de auditoria.

Os assuntos sob a responsabilidade da Comissão de Compliance são:

- i. Análise de operações suspeitas para efeitos de deliberação quanto à eventual dispensa de reporte ao COAF;
- ii. Análise de operações suspeitas para efeitos de deliberação quanto à emissão ou não de um seguro;
- lii . iii. Análise de operações suspeitas para efeitos de deliberação quanto ao pagamento de um sinistro, com suspeitas de fraude ou mesmo lavagem de dinheiro ou financiamento do terrorismo ou proliferação de armas de destruição em massa;
- iv. Análise de operações suspeitas, envolvendo colaboradores, clientes, prestadores de serviços e parceiros de negócios;
- v. Definição de planos de ações para cumprimento da Circular Susep nº 612/2020.

A Comissão de Compliance se reúne a cada bimestre ou em periodicidade menor, sempre que necessário.

Da reunião será lavrada uma ata, que junto com o relatório do caso e a decisão tomada serão arquivados na rede corporativa, no Departamento de Compliance.

O Departamento de Compliance é a área responsável pela prevenção e coibição ao risco reputacional da empresa; garantir a conformidade com políticas e normas; e garantir as medidas prevenção aos crimes de lavagem de dinheiro, financiamento ao terrorismo e proliferação de armas de destruição em massa.

Com relação à repressão aos crimes de lavagem de dinheiro, financiamento ao terrorismo, proliferação de armas de destruição em massa e corrupção, o Departamento de Compliance, terá como atividades:

- ✓ Implementar sistemas e procedimentos para o monitoramento, a seleção e a análise de operações e situações suspeitas;
- ✓ Efetuar o reporte de operações suspeitas ao COAF;
- ✓ Coordenar a gestão do programa de prevenção aos crimes de lavagem de dinheiro, financiamento ao terrorismo, proliferação de armas de destruição em massa e corrupção;
- ✓ Submeter para análise da Comissão de Compliance, as operações e situações suspeitas envolvendo segurados, colaboradores, prestadores de serviços e parceiros de negócios;
- ✓ Subsidiar o diretor estatutário, responsável pela prevenção aos crimes de lavagem de dinheiro junto à Susep, com relação às ações em andamento de monitoramento, avaliação e análise de operações e situações suspeitas;
- ✓ Realizar treinamento de prevenção aos crimes de lavagem de dinheiro, financiamento do terrorismo, proliferação de armas de destruição em massa e corrupção, Código de Ética e Conformidade e disseminar a cultura de prevenção.



3.8. Due diligence, monitoramento e controle da efetividade dos controles internos de prevenção aos crimes de lavagem de dinheiro, financiamento do terrorismo e proliferação de armas de destruição em massa

Anualmente, até o dia 31 do mês de março do ano subsequente, será realizada a avaliação da efetividade dos controles internos adotados pela companhia como métodos de prevenção aos crimes de lavagem de ,financiamento do terrorismo e proliferação de armas de destruição em massa, com o objetivo de verificar o cumprimento da presente Política e dos procedimentos estabelecidos para sua implementação e monitoramento contínuo, bem como identificar e corrigir eventuais deficiências. Essa avaliação será efetuada através do Departamento de Auditoria, que poderá contratar ou não consultor terceirizado para a realização do trabalho, nos termos do Capítulo XII da Circular Susep n.612/2020.

3.9. Registro das Operações envolvendo pagamentos

Todos os pagamentos efetuados pela Companhia, seja em razão de sinistros liquidados, devolução de prêmio, pagamento de serviços, pagamento às congêneres, deverão ser suportados por documentos que justifiquem tais pagamentos. Os documentos ficarão arquivados nas áreas responsáveis pela solicitação do pagamento.

Nenhum sinistro é pago ou prêmio devolvido sem contabilização nos registros oficiais da Companhia. O sistema ERP (Join) contempla o registro eletrônico de todas as operações financeiras relacionadas a seguro. Além do registro no sistema, na pasta eletrônica de sinistro, que é carregada no sistema, há documentos comprobatórios da operação, bem como, fica registrado no sistema os prêmios recebidos e devolvidos. O mesmo ocorre com pagamentos a prestadores de serviços.

3.13. Avaliação Interna de Risco



Nos termos do artigo 6º e Capítulo VI da Circular Susep nº 612/2020, a Companhia deve fazer uma Avaliação Interna de Risco, que contemplará critérios de riscos para todos os I - clientes; II - beneficiários; III - modelo de negócio e a área geográfica de atuação; IV - operações, transações, produtos e serviços, abrangendo todos os canais de distribuição e a utilização de novas tecnologias; e V - atividades exercidas pelos colaboradores, parceiros e prestadores de serviços terceirizados, com o objetivo de identificar, compreender e mensurar o risco de utilização de seus produtos e serviços na prática da lavagem de dinheiro, financiamento do terrorismo e proliferação de armas de destruição em massa.

A Avaliação Interna de Riscos, será reavaliada a cada dois anos, nos termos do artigo 15, III da Circular Susep nº 612/2020 ou sempre que for necessário.

3.11. Desenvolvimento de novas tecnologias

A avaliação de riscos de lavagem de dinheiro, financiamento do terrorismo e proliferação de armas de destruição em massa, em novas tecnologias, se dará no momento da homologação de Compliance do prestador de serviços de tecnologia, por meio do preenchimento do formulário de Compliance + avaliação do score de riscos, de acordo com a Política de Contratos e Homologação.

Se após análise, o prestador for considerado score de risco alto, a análise passará pelos critérios de aprovação hierárquico, ou seja, em uma primeira instância pela gerência de Compliance, em uma segunda, pela Diretoria Jurídica e de Compliance que, se considerar necessário, poderá acionar a Comissão de Compliance para deliberação colegiada.

3.12. Desenvolvimento de novos produtos e novos canais de venda

A avaliação de riscos de lavagem de dinheiro, financiamento do terrorismo e proliferação de armas de destruição em massa, relacionado ao desenvolvimento de novos produtos e canais de venda, será efetuado pela Unidade de Conformidade, antes da implantação do produto e/ou do novo canal de vendas, nos termos das Políticas de Adequação de Produtos e Desenvolvimento de Novos Produtos e Novos Projetos.

3.13. Correção das Deficiências

Todas as perdas verificadas em razão de eventual crime de lavagem de dinheiro, deverão ser reportadas no BDPO – Banco de Dados de Perdas Operacionais. O responsável por fazer o registro no BDPO é a área originária da perda.

As deficiências detectadas nos relatórios de efetividade ou mesmo no relatório de efetividade da empresa terceira ou mesmo no relatório de auditoria interna, deverão ser reportadas à Comissão de Compliance, diretoria estatutária e ao gestor da área com deficiências, para posterior mapeamento de gestão de riscos e implantação de planos de ações de melhorias.

3.14. Penalidades

As pessoas obrigadas que deixarem de cumprir o disposto na Circular Susep nº 612/2020, nos termos da Resolução CNSP nº 393/2020, estarão sujeitas às seguintes sanções administrativas, cumulativamente ou não:



- i. Advertência;
- ii. Multa equivalente ao dobro do valor da operação;
- iii. Multa equivalente ao dobro do lucro obtido ou que presumivelmente seria obtido pela realização da operação; ou
- iv. Multa de até R\$20.000.000,00 (vinte milhões de reais);
- v. Inabilitação pelo prazo de até 10 anos para o exercício do cargo ou função (responsabilização da pessoa física);
- vi. Cassação da autorização para o exercício da atividade.

4. Normas de Conduta Fairfax



- ✓ A Fairfax **não faz nenhuma doação a partidos políticos.**
- ✓ É **vedado o pagamento de comissão de corretagem de seguros em contratos firmados com a administração pública**, que não tenha previsão no edital de licitação.
- ✓ A Fairfax **não efetuará pagamento de indenização**, cujo sinistro esteja relacionado com a prática de crime de lavagem de dinheiro, financiamento do terrorismo, proliferação de armas de destruição em massa ou corrupção.
- ✓ A Fairfax **não subscreverá riscos** relacionados com crimes de lavagem de dinheiro ou corrupção.
- ✓ Segurados e/ou parceiros de negócios classificados com score vermelho (alto risco), **não poderão formalizar negócios com a Fairfax** e a indenização será suspensão para análise jurídica e de compliance.
- ✓ Somente a Comissão de Compliance ou diretoria estatutária poderão autorizar a formalização de negócios com clientes ou parceiros de negócios com score vermelho.
- ✓ A Diretoria Jurídica e de Compliance poderá analisar os casos de score vermelho, e com base no parecer de Compliance, reclassificar o risco para score amarelo (médio).
- ✓ Todo e qualquer prestador de serviços deverá passar pela homologação cadastral de Compliance, antes da formalização do contrato de prestação de serviços.

5. Comprometimento da alta administração com a efetividade e a melhoria contínua da política, dos procedimentos e dos controles internos relacionados com a prevenção à lavagem de dinheiro e ao financiamento do terrorismo:

- ✓ A diretoria da Fairfax Brasil Seguros Corporativos S/A, **está comprometida com a melhoria contínua desta Política de PLD/FT, bem como, com todos os procedimentos e controles internos de prevenção** aos crimes de lavagem de dinheiro, financiamento do terrorismo, proliferação de armas de destruição em massa e corrupção.
- ✓ A **promoção da cultura organizacional de PLD-FT é feita constantemente** pelas diversas áreas que compõem a Governança Corporativa da Fairfax, através de treinamentos corporativos, newsletter, controles internos, auditoria interna e externa, investimentos tecnológicos e em pessoas.
- ✓ As dúvidas a respeito desta Política deverão ser direcionadas para o Departamento de Compliance na seguinte caixa departamental: **compliance@fairfax.com.br**.



DIRETORIA JURÍDICA & COMPLIANCE

compliance@fairfax.com.br