Principal Asset Management℠

Manual de Compliance

Principal Claritas

Janeiro 2024

Sumário

1. Introdução.....3

2. Responsabilidades e Atribuições.....3

3. Código de Ética e Conduta Corporativa.....7

4. Política de Brindes, Presentes, Premiações e Entretenimento.....19

5. Política de Segurança e Sigilo das Informações.....21

6. Manual de Gerenciamento de Risco.....40

7. *Know Your Partner (KYP)*.....40

8. *Know Your Client (KYC)*.....42

9. *Know Your Employee (KYE)*.....46

10. *Anti Money Laundering (AML)*.....48

11. *Best Execution*.....50

12. Plano de Recuperação de Desastre e Contingência.....53

13. Alegações que devem ser reportadas.....54

14. Canal de Comunicação.....55

15. Retaliação.....56

16. Responsabilidade.....56

Anexo A.....57

Anexo B.....58

1. Introdução

A Claritas Administração de Recursos Ltda. ("Principal Claritas") adota políticas e processos de *compliance* de acordo com as exigências reguladoras e com o Código ANBIMA de Administração e Gestão de Recursos. Todos os empregados, diretores e estagiários da Principal Claritas ("colaboradores") devem estar familiarizados e cumprir com as políticas e processos da empresa. As informações fornecidas nesta Política representam diretrizes a serem seguidas pelos colaboradores, além das demais políticas, códigos fornecidos e disposições legais, regulamentares e administrativas vigentes que regem as atividades da Principal Claritas e de seus colaboradores.

Como uma prática recomendada, a Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (ANBIMA) e a Comissão de Valores Mobiliários (CVM) requerem que a Principal Claritas desenvolva um programa interno de *compliance* e mantenha um conjunto escrito de políticas e processos destinados a prevenir violações de exigências regulamentares, compilados nesse manual.

Todos os Colaboradores são obrigados a ler, entender e concordar em cumprir com as políticas e processos de compliance contidos neste manual e declarar que o fizeram. Todos devem assinar a declaração de recebimento incluída neste manual ao ingressarem na companhia ou sempre que houver uma atualização do documento. Vide Anexo A.

2. Responsabilidades e Atribuições

A área de Compliance é responsável pela continuidade das questões de compliance da empresa, assim como por supervisionar e garantir que a empresa esteja atuando em compliance com todas as normas e dispositivos regulamentares.

Dentre as atribuições e responsabilidades da área de Compliance, estão:

- Promover o valor fundamental de integridade da companhia através do

desenvolvimento e da manutenção de uma cultura organizacional;

- Armazenar e controlar as políticas da companhia;
- Supervisionar o cumprimento dos procedimentos estabelecidos;
- Observar os padrões éticos na condução dos negócios;
- Atualizar as informações contidas nas políticas, com fundamento na legislação e normas aplicáveis;
- Revisar as políticas e estabelecer controles;
- Monitorar os procedimentos e estabelecer melhorias;
- Disponibilizar as políticas a todos os Colaboradores;
- Realizar os testes necessários para verificar o cumprimento das políticas;
- Efetuar as comunicações necessárias ao COAF;
- Coordenar o Comitê de Risco e Compliance;
- Organizar treinamentos relacionados às políticas de forma a aprimorar o programa de compliance;
- Desenvolver e implementar práticas de compliance que contribuam para práticas responsáveis de negócios e a integridade dos produtos e serviços;
- Entre outras

Qualquer dúvida sobre as políticas e processos contidos neste manual ou sobre qualquer regulamento ou questões de compliance deve ser direcionada ao *Chief Compliance Officer*.

A área de Compliance fornecerá este manual a todos os colaboradores, inclusive na contratação dos novos. Além disso, conduzirá treinamentos periódicos sobre diversos aspectos do manual e armazenará a documentação escrita para fornecer evidências do treinamento.

A área de Compliance informará e comunicará de maneira proativa a Diretoria e a área de Compliance da PFG sobre os assuntos relevantes de compliance, incluindo, mas não se limitando a:

- Questões novas ou alterações significativas em regras, regulação ou boas práticas de negócio;
- Questões internas que possam impactar o negócio; e
- Resultados gerais de processos de gerenciamento de risco de compliance e atividades de monitoramento de compliance nas operações.

2.1 Responsabilidade da Diretoria e do Conselho de Administração

A Diretoria e o Conselho de Administração são conjuntamente responsáveis por desenvolver e estabelecer um programa de compliance efetivo. Isto inclui garantir que a área de Compliance tenha:

- Recursos adequados e apropriados para o nível e complexidade de suas operações;
- Esteja devidamente equipada para desenvolver seu papel e tenha pessoal suficientemente qualificado e com as competências necessárias; e
- Tenha uma pessoa responsável pela área com autoridade e independência suficiente para exercer suas funções.

2.2 Reporte da Área de Compliance

A área de Compliance tem duplo reporte, garantindo a independência e autoridade da área. O Diretor de Compliance indicado na CVM para as atividades de controles internos e compliance se reporta ao Comitê Executivo e ao *Chief Compliance Officer* da *Principal Global Investors.*

2.3 Coordenação com a Área de Risco

Além da interação contínua com a área de Riscos, do Comitê de Riscos e Compliance, e a utilização de diretórios internos em comum para aprimorar os processos e o monitoramento das áreas, a Principal Claritas conta com um sistema terceirizado de Compliance (*Compli.ly*), onde as áreas de risco e compliance possuem acesso e podem interagir e incluir evidências da verificação das atividades em geral da companhia.

2.4 Reporte da Área de Risco

A área de Riscos tem duplo reporte, garantindo a independência e autoridade da área. O Diretor de Riscos e Compliance da Principal Claritas se reporta ao Comitê Executivo e ao *Chief Risk Officer* da *Principal Global Investors*, sendo totalmente independente das áreas de gestão de recursos. É responsável por implementar políticas e estratégias para o gerenciamento de riscos da instituição, além de ser responsável por identificar, medir, monitorar e controlar a exposição aos riscos de mercado, liquidez, crédito, contraparte e operacional.

2.5 Segregação das Atividades

As áreas de administração de carteiras da Principal Claritas estão localizadas em uma área distinta das demais áreas da empresa: operacional, cadastro de clientes, TI, *facilities*, etc.

Os arquivos digitais da Principal Claritas são restritos a cada área, de forma que quando um colaborador é admitido ou transferido para uma área na qual não possui acesso aos arquivos, o gestor responsável e a área de Compliance precisam validar a liberação para o colaborador.

Todos os arquivos digitais que possuem algum tipo de cunho confidencial possuem acesso restrito, de forma que o colaborador permitido ao acesso precisa de um login e senha para visualizar o arquivo.

Além disso, os arquivos físicos das áreas de administração de carteiras ficam em local distinto dos outros arquivos e é necessária autorização da área para ter acesso ao arquivo.

2.6 Comitê de Risco e Compliance

Em regra, o Comitê de Riscos e Compliance é realizado semestralmente, e tem como seus objetivos definir e acompanhar as diretrizes da Política de Gerenciamento de

Riscos da companhia, verificar o cumprimento às regras e disposições que norteiam as atividades da Principal Claritas, além de apurar qualquer irregularidade ou descumprimento, bem como tratar de possíveis falhas e/ou demais assuntos que as áreas de risco e compliance possam considerar relevantes.

2.7 Teste Periódico

A área de Compliance, os membros designados e a equipe de Auditoria Interna da PFG testarão periodicamente a efetividade das políticas escritas e processos de compliance. As revisões podem incluir, em parte, considerações específicas aos seguintes aspectos:

1. Alguma questão de compliance que tenha surgido durante o período;
2. Alguma alteração relevante nas atividades empresariais; e
3. Algum novo risco ou conflito de interesse que a Principal Claritas possa estar sujeita.

3. Código de Ética e Conduta Corporativa

Em conformidade com o Código, a Principal Claritas espera que todos os seus Colaboradores:

1. Atuem com integridade, competência, dignidade e de uma maneira ética quando negociem com o público, clientes, possíveis clientes e outros Colaboradores;
2. Adotem os mais altos padrões de respeito para qualquer possível conflito de interesses com os clientes. Ou seja, nenhum Colaborador deve desfrutar de um benefício em detrimento de outro cliente.
3. Preservem o sigilo de informações que possam ter sido obtidas no curso do negócio e usem tal informação adequadamente e não de uma forma adversa aos interesses dos nossos clientes, a menos que seja obrigado a agir de forma diferente de acordo com a lei aplicável;
4. Conduzam suas finanças pessoais de forma prudente, evitando qualquer ação que possa comprometer sua habilidade de lidar objetivamente com os clientes;

e

5. Cumpram fielmente o regulamento do fundo ou o contrato previamente firmado por escrito com o cliente.

Todos os colaboradores deverão pautar suas condutas em conformidade com os valores da boa-fé, lealdade, transparência, diligência e veracidade, evitando quaisquer práticas que possam ferir a relação fiduciária mantida com os investidores.

3.1 Código de Conduta Global da PFG

Os Colaboradores da Principal Claritas estão sujeitos também ao Código de Conduta Global da *Principal Financial Group* ("PFG"), o qual deve ser lido e obedecido na sua íntegra e cada Colaborador é obrigado a assinar uma declaração de recebimento, confirmando sua adesão às exigências.

3.2 Política de Conflitos de Interesses da PFG

Os Colaboradores da Principal Claritas estão sujeitos à Política de Conflito de Interesses da PFG. Os Colaboradores devem agir de acordo com os melhores interesses da Principal Claritas e da PFG e abster-se de estar em qualquer posição que possa resultar em um conflito ou em uma aparência de um conflito entre seus interesses pessoais e os interesses das empresas da PFG e da Principal Claritas. Os Colaboradores devem administrar seus interesses pessoais e profissionais a fim de evitar que qualquer favor ou presente possa desencadear em um conflito de interesses ou que o julgamento dos negócios possa ser afetado.

Para identificar um possível conflito de interesse, é interessante se perguntar algumas simples questões:

1. É possível que meu interesse pessoal possa influenciar a maneira como eu exerço as minhas atividades? Até mesmo quando nenhum erro ou engano foi cometido?
2. Em virtude da minha relação com a empresa, é possível que eu, um parente ou

um amigo obtenha alguma vantagem pessoal ou financeira?

3. As minhas atividades fora da empresa podem ser interpretadas, de maneira errônea, como atividades da empresa?
4. Os parceiros de negócio, fornecedores, clientes ou acionistas poderiam questionar se as minhas decisões de negócio foram tomadas de maneira objetiva e para o melhor interesse da empresa?

Se a resposta para qualquer dessas perguntas for sim ou caso você não tenha certeza da resposta, você deve conversar com seu gestor e/ou com a área de Compliance.

Os Colaboradores devem obter a aprovação prévia de seu gestor e do Diretor de Compliance se uma atividade ou relacionamento possa apresentar ou possa ser entendida como um conflito de interesses. Mesmo se a atividade ou relacionamento for aprovado de acordo com esta política, ela não deve interferir nas responsabilidades de sua posição atual ou utilizar recursos da empresa. A aprovação para representar qualquer outro Conselho de Administração ou outra entidade não significa que o Colaborador esteja sob a orientação ou a pedido da direção ou de algum membro da PFG e será aprovada pelo Comitê de Risco e Compliance.

Declaração Anual

Colaboradores com posições específicas devem completar um formulário de declaração anual. Estes Colaboradores devem declarar qualquer interesse ou afiliações que possam conflitar com suas atividades como Colaboradores da empresa.

3.3 Normas para concorrência livre

O CADE (Conselho Administrativo de Defesa Econômica) tem como objetivo zelar pela livre concorrência no mercado, sendo o responsável por investigar e decidir sobre matéria concorrencial, além de recomendar a boa prática na condução de condutas anticompetitivas.

Algumas das práticas que não devem ser adotadas são: cartel (acordo no qual é fixado

com a concorrência: preços, clientes, mercados de atuação ou cotas de produção com o intuito de restringir a oferta no mercado e tornar os produtos mais caros), trustes (fusão de várias empresas com o objetivo de formar um monopólio e dominar determinada oferta de produtos ou serviços), dentre outras que não permitem a concorrência leal no mercado.

No caso de alguma dessas condutas serem praticadas, o CADE pode aplicar uma multa que varia entre 0,1% e 20% do valor do faturamento bruto da empresa.

Os Colaboradores não devem participar de condutas que demonstrem caráter anticoncorrencial e, ao ter conhecimento de uma possível violação da política, o Colaborador deve notificar imediatamente a área de Compliance.

3.4 Política Antiboicote da PFG

Os Colaboradores da Principal Claritas estão sujeitos à Política Antiboicote da PFG. A Principal Claritas se compromete a cumprir as leis aplicáveis de boicote e a não participar de boicotes proibidos. O governo americano monitora, e em certos casos, penaliza companhias americanas por estarem ligadas à certas atividades internacionais de boicotes. As atividades internacionais de boicotes geralmente surgem quando uma pessoa estrangeira exige, como condição para fazer negócios, que uma empresa dos EUA (ou a sua filial estrangeira, como definido pelo *Internal Revenue Code*) se abstenha de fazer negócios com os cidadãos, empresas ou governos de outros países estrangeiros.

As leis norte-americanas, em relação às atividades internacionais de boicote, geralmente exigem que cidadãos americanos relatem as operações de boicotes proibidos para o governo dos EUA.

A área de Compliance deve relatar as operações de pedidos de boicote no momento do pedido e no relatório de compliance trimestralmente para a CCO da PFG.

Os Colaboradores da Principal Claritas estão expressamente proibidos de participar de

atividades de boicote, a não ser que o boicote venha de um pedido expresso da PFG. Atualmente, os países proibidos de fazer negócios com os EUA e com empresas estrangeiras ligadas a empresas americanas: Arábia Saudita, Emirados Árabes Unidos (composto pelos seguintes estados: Abu Dhabi, Dubai, Sharjah, Umm All Quwain, Fujairah, Ajman and Ras Al Khaimah), República do Yemen, Qatar, Kuwait, Líbano, Líbia, Iraque e Síria.

3.5 Doações a Partidos Políticos

É vedado aos Colaboradores da Principal Claritas, enquanto representantes da empresa, doar ou contribuir financeiramente de alguma forma a partidos políticos ou candidatos a cargos públicos.

As doações privadas de empresas, conforme posição do Supremo Tribunal Federal, são inconstitucionais. A Principal Claritas tem o compromisso de conduzir seus negócios de forma lícita e de acordo com as normas vigentes.

Os Colaboradores são incentivados a contatar a área de Compliance e/ou seu gestor se eles tiverem dúvidas ou suspeitas em relação ao conteúdo deste capítulo.

3.6 Direitos de Propriedade e Política de Propriedade Intelectual

Os Colaboradores da Principal Claritas devem proteger os direitos de propriedade da Principal Claritas, PFG e de suas empresas associadas. Uma violação nos direitos de propriedade e leis de propriedade intelectual cria uma possível responsabilidade e pode resultar em repercussões legais significativas. Se um Colaborador tiver ciência ou suspeitar de violações relacionadas a esta política, ele deve reportar à área de *Compliance*.

Propriedade Intelectual e Produto do Trabalho

Premissa

Os Colaboradores da Principal Claritas estão sujeitos à Política de Propriedade e

Política de Propriedade Intelectual da PFG. Os Colaboradores devem fazer o seu melhor para proteger os direitos de propriedade intelectual, incluindo, mas não se limitando, às marcas, patentes e direitos autorais. Os Colaboradores e Diretores não devem violar os direitos de propriedade intelectual de terceiros, sob nenhuma circunstância.

Conceito

Propriedade intelectual é uma ideia, processo, invenção, melhoria, projeto, trabalho original, fórmulas, softwares e base de dados, segredos comerciais que são concebidos por um Colaborador ou adquiridos pela Principal Claritas. Este conceito inclui, mas não se limita à informação de mercado, modelos de negócios, algoritmos, propostas, e conceitos, estratégias de investimento, marcas, domínio de internet e direitos autorais que:

- Surgem como um resultado de um trabalho conduzido por um Colaborador, sob o curso normal de negócios ou durante seu período de trabalho.
- São relacionados a negócios, serviços, produtos, pesquisas ou desenvolvimento atual ou previsto na Principal Claritas.

Segredos comerciais são quaisquer informações que têm valor econômico para uma empresa em razão da sua privacidade, dando à empresa uma vantagem em comparação com seus competidores.

A propriedade intelectual não tem necessariamente de ser registrada nas autoridades competentes para ser respeitada pelos Colaboradores.

3.7 Política de Investimentos

Todos os colaboradores da Principal Claritas deverão obedecer às regras previstas na Política de Investimentos para a negociação de valores mobiliários. A Política de Investimentos encontra-se disponível para acesso dos colaboradores no diretório interno da Principal Claritas, bem como disponível ao público em geral no seu website.

3.8 Relações com a Mídia

Como uma empresa global, é fundamental que a informação divulgada à imprensa seja consistente. Para salvaguardar a Principal Claritas e a PFG, todas as perguntas da mídia devem ser analisadas pelo Departamento de Marketing da Principal Claritas.

Membros da mídia podem pedir para falar com os Colaboradores fora da gravação ou no "background". Todas as perguntas da mídia, não importando como são feitas, têm a possibilidade de serem publicadas. Qualquer interação com a mídia ou qualquer tipo de veículo que possa divulgar alguma informação referente à Principal Claritas deve envolver o Departamento de Marketing. Portanto, toda a comunicação com jornalistas e/ou assessorias de imprensa referente à representação de outras empresas, envio de materiais para divulgação, logo, fotos ou vídeos da empresa e/ou colaboradores ou depoimentos a serem publicados em nome da Principal Claritas ou PFG, são expressamente proibidos de serem realizados sem a prévia e expressa ciência da área de Marketing. Se você for contatado pela mídia, notifique o Departamento de Marketing imediatamente.

3.9 Política contra o Suborno e Anticorrupção

A Principal Claritas e seus Colaboradores não podem influenciar terceiros, seja direta ou indiretamente, por meio de pagamento ou recebimento de suborno ou propinas, por outro meio antiético ou que possa prejudicar a reputação da Principal Claritas, por falta de honestidade e integridade. Tal comportamento é inaceitável, quer estejamos lidando com funcionários públicos, com outras corporações ou com outros indivíduos.

A Principal Claritas não irá tolerar Colaboradores que alcancem resultados por meio de violação da lei ou de ato desonesto. Os Colaboradores da Principal Claritas devem recusar qualquer oportunidade que possa colocar os princípios éticos e a reputação da empresa em risco. Suborno e corrupção não são somente contra os nossos valores, mas são ilegais e podem expor tanto o Colaborador quanto a empresa a multas e outras penalidades, inclusive a prisão.

Todos os Colaboradores da Principal Claritas estão sujeitos à Política de Brindes e Entretenimento da Principal Claritas, que limita os valores permitidos para dar e receber brindes e presentes, custear eventos ou acomodações. Esses limites são impostos para que uma eventual atitude não resulte em uma conduta ilícita.

Fazer pagamentos a funcionários públicos ou outros para ganhar ou influenciar decisões de negócios é ilegal em muitos países, inclusive no Brasil. O número de países com leis anticorrupção e contra o suborno tem aumentado, em parte devido aos acordos internacionais para combater o suborno e corrupção. Acordos entre entidades tais como a *Organization for Economic Cooperation and Development (OECD)* e a *United Nations Convention Against Corruption (UNCAC)* desenvolvem a cooperação internacional ao estabelecer leis contra o suborno e ao investigar e processar infrações.

3.10 Lei Anticorrupção do Brasil

A Lei Anticorrupção do Brasil se aplica à Principal Claritas e às empresas a ela afiliadas, sendo estas estrangeiras ou domiciliadas no Brasil e seja o ato ilícito praticado dento ou fora do território nacional. A responsabilidade civil estende-se a todos os Colaboradores da Principal Claritas que cometerem, participarem, ou ajudarem no cometimento do ato ilícito.

A lei considera como infração o ato ilícito, praticado por qualquer pessoa ou entidade, contrário à administração pública do governo nacional ou estrangeiro, ou contrário a pactos que o Brasil seja signatário. Esta política proíbe os Colaboradores da Principal Claritas de:

1. Prometer, oferecer ou dar uma vantagem indevida, direta ou indiretamente, a um funcionário público ou um terceiro relacionado.
2. Financiar, subsidiar, ou patrocinar ato ilegal;
3. Utilizar uma pessoa ou entidade como intermediário para dissimular seus reais interesses ou a identidade dos beneficiários do ato; e
4. Obstruir ou interferir na investigação ou repressão de entidades ou funcionários

públicos.

No que se refere a contratos públicos, esta política proíbe os Colaboradores da Principal Claritas de manipular ou fraudar o processo de licitação ou o balanço econômico e financeiro dos contratos públicos firmados com o governo.

Violar a lei brasileira de anticorrupção pode resultar em penalidades civis e judiciais, além de desligamento da empresa. A responsabilidade por qualquer penalidade civil ou judicial pode estender-se à Principal Claritas, à PFG e suas companhias afiliadas.

Para cumprir com a lei anticorrupção do Brasil, a Principal Claritas:

1. Reforça sua política e seu manual de *compliance* contra o suborno para enfatizar a necessidade dos Colaboradores respeitarem o Manual de *Compliance* da Principal Claritas e o Código Global de Conduta da PFG. Estas regras refletem o compromisso da Principal Claritas com a cultura de integridade onde suborno e corrupção são estritamente proibidos e penalizados;
2. Incentiva os Colaboradores a reportarem condutas ilícitas e atos ilegais, por todos os canais possíveis, inclusive proibindo retaliação contra os Colaboradores que reportarem tais atos;
3. Requer que os gestores sejam cuidadosos ao revisarem e aprovarem despesas que possam ser consideradas suspeitas de acordo com todas as leis anticorrupção;
4. Treina todos de acordo com a cultura ética da empresa e as exigências legais das leis anticorrupção; e
5. Auxilia a Auditoria Interna da PFG em suas revisões periódicas e em *compliance* com a lei anticorrupção brasileira.

3.11 *Foreign Corrupt Practices Act (FCPA) e Bribery ACT (UK)*

A *Foreign Corrupt Practices Act* (FCPA) é uma lei dos Estados Unidos que regula a conduta das empresas norte-americanas, os cidadãos, nacionais e residentes fora dos EUA. O

Bribery Act é uma lei do Reino Unido que se aplica a uma parte dos crimes que ocorrem neste território, e também ao ato ou a omissão se ocorrido no Reino Unido, e quando o infrator tem uma ligação estreita com este (por exemplo, um cidadão britânico, ou um órgão submetido ao Reino Unido). Estamos em conformidade com as duas regras, assim como com as leis anti-suborno de outros países.

Em *compliance* com esta política, a Principal Claritas proíbe qualquer Colaborador de se envolver em corrupção ou suborno de funcionários públicos no Brasil ou no exterior em relação às licitações públicas ou de qualquer outra forma.

3.12 *Office of Foreign Assets Control* (OFAC)

A *Office of Foreign Assets Control* ("OFAC") do Departamento de Tesouraria dos EUA administra e faz cumprir sanções baseadas na política americana estrangeira e metas nacionais de segurança contra países estrangeiros direcionados a regimes terroristas, traficantes de drogas internacionais, aqueles comprometidos com atividades relacionadas à proliferação de armas de destruição em massa, e outras ameaças à segurança nacional, política estrangeira, ou economia dos EUA.

A OFAC mantém e publica uma lista de países, indivíduos, e organizações que são ameaças à segurança nacional ou estão comprometidos com o tráfico de drogas, incluindo uma lista de indivíduos e entidades que são chamados de *Specially Designated Nationals* ou "SDNs" (SDNs, países sancionados e outras listas similares mantidas pela OFAC ou alguma outra autoridade regulamentada que a Principal Claritas pode estar sujeita são referidas em conjunto como "*Sanctioned Targets*").

Todos os cidadãos americanos devem cumprir com a regulamentação da OFAC, independentemente de onde estão localizadas. Além destes, todas as pessoas ou entidades dentro dos EUA e todas as entidades incorporadas aos EUA e suas filiais estrangeiras que sejam integralmente de outra companhia americana devem cumprir com as disposições desta norma.

A Principal Claritas adotou políticas designadas a cumprir o alcance exigido pela

regulamentação aplicada da OFAC para evitar fazer negócio com a *Sanctioned Targets* (a "Verificação OFAC").

Para garantir compliance com as exigências desta política de OFAC, alguns prestadores de serviço terceirizados, dependendo da relevância do serviço prestado, são obrigados a implementar procedimentos para verificar um eventual *matching* dos nomes dos clientes da Principal Claritas com a *Sanctioned Targets*. Quaisquer correspondências com a lista da OFAC *Sanctioned Targets* são avaliadas pelo prestador de serviço terceirizado e, se necessário, reportados à área de *Compliance*. Os prestadores de serviço terceirizados são responsáveis por reportar qualquer confirmação de correspondência com a lista de OFAC e tomar as devidas providências em conjunto com a área *de Compliance* da Principal Claritas. Para garantir *compliance* com esta política, a Principal Claritas deve realizar periodicamente revisões de *due dilligence* de tais prestadores.

Além disso, a Principal Claritas checa periodicamente sua lista de empregados em relação à lista de OFAC para verificar qualquer inconsistência.

Qualquer verificação positiva na lista de OFAC deve ser reportada à área *de Compliance*, que reportará ao CCO da PFG, em relatórios trimestrais.

3.13 Autoridade Reguladora e Judicial

Qualquer pedido, solicitação ou no caso de alguma investigação por um órgão regulador relacionado aos negócios da Principal Claritas deve ser reportado à área de *Compliance* imediatamente, antes de enviar alguma resposta a este. A área de *Compliance* consultará a pessoa apropriada para rever a resposta antes de direcionar a um regulador.

A área de Compliance deve ser também notificada imediatamente sobre qualquer litígio, intimação, ou pedido similar para informação envolvendo a Principal Claritas. A área de Compliance poderá contatar advogados externos e/ou departamento jurídico da PFG com a intimação legal e trabalhará com eles quando necessário e determinará

se quaisquer medidas regulamentares adicionais serão necessárias. Quando a arbitragem ou litígio é estabelecido ou resolvido de alguma maneira, a área de Compliance irá igualmente determinar se medidas regulamentares adicionais serão necessárias.

3.14 Publicidade

Todos os materiais de publicidade, regulamentos e toda a correspondência de cliente devem seguir as mesmas regras gerais quanto ao teor.

Entre as diretrizes gerais, as comunicações:

- Devem estar em *compliance* com a legislação local e com o Código ANBIMA de Regulação e Melhores Práticas.
- Devem ser baseadas nos princípios da negociação justa e de boa fé.
- Devem fornecer uma base sólida para avaliar os fatos e nenhuma informação material pode ser omitida.
- Não podem conter declarações ou reclamações exageradas, enganosas ou injustificadas.
- Devem ter clareza geral e fatos ou *hedges* importantes, que são destinados a melhorar a compreensão, não podem ser relegados a notas de rodapé ou legendas.
- Não devem conter promessas de resultados específicos, reclamações ou opiniões exageradas ou injustificadas, ou garantir a inexistência de riscos.
- Comparações devem ser completas, justas e devem conter sua finalidade.

Os Colaboradores são responsáveis por assegurar que todos os materiais de marketing sejam submetidos à área de Compliance para revisão e aprovação. A área de Compliance pode conceder a aprovação final, negar o uso, ou indicar mudanças exigidas a serem feitas. A Principal Claritas deve reter cópias de todos os materiais de marketing utilizados pelos Colaboradores de acordo com as exigências de armazenamento de registro.

3.15 Reclamações de Cliente/Investidor

De tempos em tempos, e apesar de seus melhores esforços, a Principal Claritas pode receber reclamações de clientes/ investidores sobre serviços ou questões relacionadas. A Principal Claritas responderá todas as reclamações de uma maneira hábil e apropriada a fim de promover excelentes relações com o cliente/investidor, ir de encontro às exigências de compliance e normativos e manter sua reputação de integridade.

Ao desenvolver esta política e procedimentos, a Principal Claritas considerou riscos materiais associados com resolução de reclamações do cliente/investidor. Essas análises incluem riscos como:

- Reclamações não resolvidas em tempo hábil ou ignoradas.
- A reclamação do cliente/ investidor não documentada adequadamente.

A Principal Claritas investigará e responderá todas as reclamações de clientes/investidores em tempo hábil. Os Colaboradores estão proibidos de responder às reclamações do Cliente/ Investidor sem a aprovação da área de Compliance ou do seu gestor.

4. Política de Brindes, Presentes, Premiações e Entretenimento

Todos os Colaboradores da Principal Claritas estão sujeitos à Política de Brindes, Presentes, Premiações e Entretenimento da Principal Claritas e devem observar a Política de Brindes, Presentes, Premiações e Entretenimento da PFG.

Brindes e Presentes, Premiações e Entretenimentos não devem ser dados ou aceitos caso tenham a pretensão de recompensar qualquer pessoa em relação a algum negócio ou transação que envolva a Principal Claritas ou as empresas da PFG ou para permitir que alguém lucre com a posição da Principal Claritas e das empresas da PFG e possam influenciar na reputação das empresas. Sob suas atividades normais, os Colaboradores podem dar ou receber presentes modestos.

Brindes, Presentes e Premiações incluem qualquer coisa de valor, dada ou recebida que não seja entretenimento, incluindo, mas não limitando, a bens, serviços, ingressos de eventos, uso de casa de veraneio ou outras acomodações, etc. A entrada para qualquer evento social, de hospitalidade, caridade, esportivo, ou outra atividade cultural/ de lazer terá sua natureza tratada como Brinde, Presente ou Premiação, caso o Colaborador mantenha parceria com quem deu a entrada. Se quem deu a entrada não possui nenhum negócio com você, o evento terá fim de entretenimento.

1. Brindes recebidos de um parceiro de negócios no valor excedente a R$100,00 devem ser reportados à área de *Compliance*. Quando houver intenção de dar um brinde no valor superior a R$ 300,00, o mesmo deverá ser pré-aprovado pela área de *Compliance*.
2. Qualquer Entretenimento que for recebido e o valor for além de R$500,00 por pessoa deve ser reportado à área de *Compliance*.
3. Qualquer valor de almoço por pessoa está pré-aprovado em R$250,00. Valores acima disso deverão ser aprovados pela área de *Compliance* e pelo gestor responsável.

Itens com valor abaixo de R$ 100,00, como copos, bonés, camisetas e canetas, placas ou anúncios sobre eventos particulares de comemoração são itens de valor simbólico, que são normalmente isentos desta política. Brindes, Presentes e Premiações que incluam logotipos permanentes fixados são geralmente considerados itens com valores simbólicos e são geralmente aceitáveis e não reportados desde que sejam gratuitos. Entretanto, se o item tiver um valor substancial intrínseco, como um *tablet*, um logotipo fixado não faz o item ter valor simbólico e limites de Brindes, Presentes e Premiações são aplicáveis. **Geralmente, vale presente, dinheiro, equivalentes de dinheiro, ou outro instrumento financeiro não devem ser oferecidos ou aceitos, independentemente do valor**. Vale presente pode ser permitido sob certas circunstâncias, como as apresentadas nesta política.

O oferecimento de brindes e entretenimento deve obedecer aos seguintes princípios:

1. O oferecimento de brindes, presentes e entretenimento tem que estar diretamente relacionado ao negócio da empresa. As situações devem ser razoáveis e proporcionais aos fins legítimos que a empresa pretende alcançar com esse tipo de oferta.
2. O oferecimento de brindes, presentes e entretenimento não pode estar atrelado à intenção de influenciar um terceiro para obter ganhos indevidos para a empresa, de recompensar alguém por um negócio obtido em decorrência de determinada ação, decisão ou mesmo omissão dessa pessoa ou caracterizar troca de favores ou benefícios, seja de forma implícita ou explicita.
3. Nenhum tipo de entretenimento, brinde ou presente deve ser provido com uma frequência desarrazoada ou para o mesmo destinatário, de forma que possa aparentar alguma suspeição ou impropriedade.
4. A área de *Compliance* irá analisar e verificar as despesas relacionadas aos brindes para verificar quaisquer atividades irregulares nesse sentido.

5. Política de Segurança e Sigilo das Informações

A Política de Segurança e Sigilo das Informações da Principal Claritas é aplicada a todos os empregados, estagiários e diretores (“Colaboradores”) da Principal Claritas. O objetivo é formalizar os processos e procedimentos adotados pela companhia com relação ao controle de informações confidenciais, reservadas ou privilegiadas a que tenham acesso seus Colaboradores.

Todos os Colaboradores devem assinar documento de confidencialidade sobre as informações confidenciais, reservadas ou privilegiadas que lhes tenham sido confiadas em virtude do exercício de suas atividades profissionais, excetuadas as hipóteses permitidas em lei, conforme Anexo. Vide Anexo B

5.1 Informações Confidenciais

Por Informações Confidenciais entendem-se quaisquer dados, conhecimentos e/ou informações incluindo informação relativa a números financeiros e/ou contábeis, estratégias, planos de ação, planos de negócios, know-how, desenhos, folhas de dados, relatórios e materiais que sejam revelados, fornecidos ou comunicados (seja verbalmente ou por escrito, em forma eletrônica, textos, desenhos, gráficos, projetos ou qualquer outra forma) pela Principal Claritas. Todas as anotações, análises, compilações, estudos e demais documentos elaborados com base em Informações Confidenciais serão também considerados “Informações Confidenciais”.

Desta forma, manter o sigilo das informações da Empresa é essencial para a competitividade, segurança e outras razões comerciais. Fazer isso também minimiza o risco de informações relevantes ilegais e “tipping”.

Todos os Colaboradores da empresa, portanto, devem procurar assegurar o sigilo das informações a que têm acesso. Isto significa que, a menos que a informação esteja disponível publicamente, você deve limitar o acesso a informações para Colaboradores da companhia que tem uma razoável "necessidade de saber" a informação com a finalidade de concretizar o acordo para a qual a informação é fornecida. Assegurar o sigilo de informações não públicas pode exigir a decisão de tais medidas como a adoção de nomes de código, usando senhas para obter informações informatizadas, destruindo documentos confidenciais, bloqueando arquivos e gavetas contendo informações confidenciais, registrando o rótulo "Confidencial", limitando a cópia de documentos sensíveis e mantendo um registro de Empregados que solicitam acesso a documentos ou arquivos.

5.2 Informação Privilegiada

Em complemento a esta Política, todos os Colaboradores da Principal Claritas estão

sujeitos às “Políticas e Processos Designados a Detectar e Prevenir o Uso Indevido de Informações Privilegiadas” da PFG.

Todo gestor de recursos deve estabelecer, manter, e fazer cumprir as políticas e processos designados a fim de prevenir o uso indevido da Informação Material Não Pública (MNPI) em violação das leis e regulamentação de valores mobiliários. O termo Informação Privilegiada é geralmente utilizado para se referir às negociações de valores mobiliários enquanto em posse de MNPI ou comunicar a MNPI a outros.

Qualquer negociação que utilize MNPI está em violação das leis de informações privilegiadas. A violação destas leis pode resultar na imposição de penalidades, não só a quem violou, mas ao empregador também. É importante que todos os Colaboradores estejam familiarizados com os assuntos para estarem capacitados a identificar possíveis problemas com informações privilegiadas.

O que é Informação Relevante?

“Informação Relevante” é geralmente definida como uma informação para a qual existe uma probabilidade substancial de um investidor considerar importante ao tomar decisões de seus investimentos. Informações que os colaboradores devem considerar relevantes incluem, mas não se limitam, à mudança de dividendos, ganhos estimados, alterações nos ganhos estimados previstos, propostas ou acordos significativos de fusão ou aquisição, litígios importantes, problemas de liquidez, novas emissões de títulos e notáveis desenvolvimentos de gestão.

O que é Informação Não Pública?

A informação é considerada não pública até que seja efetivamente comunicada ao mercado.

Insider Trading

Insider Trading (ou uso de informações privilegiadas) é a negociação de valores

mobiliários baseada em MNPI a fim de auferir lucro ou vantagem no mercado. Está ligado a duas proibições: (i) realizar negociações de posse de informação material que não é pública, e (ii) revelar essa informação a terceiros (*Tipping*).

Dentre outras, a Lei 6.385/76 prevê no artigo 27-D o crime de "Utilizar informação relevante ainda não divulgada ao mercado, de que tenha conhecimento e da qual deva manter sigilo, capaz de propiciar, para si ou para outrem, vantagem indevida, mediante negociação, em nome próprio ou de terceiro, com de valores mobiliários".

Qualquer negociação que utilize MNPI está em violação das leis de informações privilegiadas. A violação destas leis pode resultar na imposição de penalidades, não só a quem violou, mas ao empregador também. É importante que todos os Colaboradores estejam familiarizados com os assuntos para estarem capacitados a identificar possíveis problemas com informações privilegiadas.

O que não é *Insider Trading?*

Quando há uma negociação com base em pesquisas elaboradas a partir de dados públicos, no qual o analista utilizou, para tanto, informações públicas, sem que a vantagem na negociação fosse resultado do uso de informações privilegiadas, tal negociação não pode ser considerada *insider trading*.

O *insider trading* é caracterizado se houver vantagem na negociação oriunda da utilização de informação não pública e isso gerar uma clara vantagem em relação aos demais participantes do mercado que não tiveram acesso à informação privilegiada.

Chinese Wall

Para evitar qualquer tipo de conflito de interesse, a Principal Claritas estabelece procedimentos de *chinese wall*. Caso algum Colaborador da Principal Claritas vier a ter conhecimento de MNPI por fazer parte de algum comitê ou cargos em esferas de governança ou ainda, ocupar outro cargo que lhe dê acesso às informações privilegiadas, o mesmo deverá informar à área de Compliance.

A área de *Compliance* garantirá a barreira, assegurando que tais informações serão mantidas em confidencialidade e não circularão entre setores de negociação e que a pessoa com acesso à informação privilegiada não participará das decisões de investimentos da Principal Claritas.

Os procedimentos a seguir serão adotados para garantir o *chinese wall*, caso o Colaborador venha a ter acesso a MNPI:

1. Afastamento dos Comitês onde são discutidas tomadas de decisões de investimentos durante o período de restrição de negociação com os emissores detentores da MNPI;
2. Afastamento de reuniões com os gestores e/ou equipes de gestão destinadas à definição de estratégias e ativos para negociação, durante o período de restrição de negociação com os emissores detentores da MNPI; e
3. Caso o Colaborador pertença à área de Gestão, não só as hipóteses acima deverão ser observadas, como o período de restrição se estenderá aos fundos geridos pela empresa.

Caso o Colaborador e/ou diretor tenha alguma dúvida quanto ao conteúdo das reuniões que possa participar e se tal conteúdo pode ser considerado informação privilegiada, a pauta da reunião deverá ser encaminhada à área de *Compliance* para que esta possa garantir que não se trata de MNPI.

Caso o Colaborador e/ou diretor venha a ter acesso às informações não relevantes, ainda que não públicas, isto é, que não haja possibilidade de ganho/vantagem conforme estabelecido na ICVM 44/2021, a área de *Compliance* será responsável por avaliar tais informações.

Procedimentos

Todos os Colaboradores devem utilizar todas as medidas necessárias para assegurar o controle de informações confidenciais, reservadas ou privilegiadas a que tenham acesso, o que inclui, mas não se limita, aos seguintes procedimentos:

- Proteger todos os meios e documentos que contêm informações confidenciais, discos e papel, como não deixar o computador desbloqueado, especialmente por períodos longos de tempo, como em horário de almoço ou depois do horário de trabalho;
- Remover *flip charts*, apagar informações em *blackboards* e não deixar materiais em salas de reunião;
- Classificar documentos confidenciais ou documentos que contêm segredos comerciais com a marca "Confidencial" sempre que aplicável, a fim de esclarecer aos beneficiários a natureza da informação confidencial;
- Destruir todos os documentos e suas cópias sempre que eles não forem mais necessários;
- Limitar acesso da informação às pessoas que devem ter conhecimento desta em razão de sua atividade ou função;
- Limitar acesso de informação a terceiros que tenham autorização escrita;
- Evitar usar e-mail ou *voice mail* para enviar informação confidencial; e
- Usar senhas para computadores e manter elas em segredo.

Penalidades para Informações Privilegiadas

As penalidades por comunicar ou negociar usando MNPI são severas, tanto para os indivíduos envolvidos na conduta ilegal, quanto para seus empregadores. Uma pessoa pode estar sujeita a algumas ou todas as penalidades descritas abaixo, mesmo que não tenha se beneficiado pessoalmente da violação. As penalidades incluem:

- Sanções Civis
- Indenização triplicada
- Restituição de lucros
- Sentenças de prisão
- Ser impedido de trabalhar no mercado

Além disso, qualquer violação desta política pode resultar em sansões graves pela Principal Claritas, inclusive demissão.

5.3 Política de Privacidade

A privacidade e proteção de todas as informações sensíveis e confidenciais são extremamente importantes para a Principal Claritas e para a *Principal Financial Group*. Durante o curso do negócio, os Colaboradores podem ter acesso a informações confidenciais, reservadas ou privilegiadas. A Principal Claritas gere seriamente essas informações e busca fornecer tratamento justo, seguro e apropriado de toda a informação. O acesso à informação é restrito a estes Colaboradores e a outros que têm a necessidade de acessar a informação para realizar seu trabalho.

O compliance com os processos de privacidade e confidencialidade deverá ser observado por todos os Colaboradores. A área de Compliance é responsável pelo desenvolvimento, armazenamento, implementação, operação e cumprimento desta política.

Todos os Colaboradores, inclusive os que trabalham de casa ou outro tipo de locação remota, são obrigados a cumprir as políticas e padrões de proteção e uso de informação sensível da Principal Claritas. Qualquer violação deve ser reportada à área de Compliance e o descumprimento da política e padrões pode resultar em ação disciplinar e, inclusive, em demissão ou término do vínculo com a empresa.

5.4 Confidencialidade e Segurança

Todos os Colaboradores devem cumprir com as garantias em relação aos dispositivos móveis de segurança, tais como laptop/notebook, tablets, celulares, smartphones e outros dispositivos móveis capazes de acessar ou armazenar dados corporativos em conexão com uma rede comum estão sujeitos a estes padrões, que são:

1. Controles de Acesso – Todos os dispositivos de computação e armazenamento móveis ou processamento de informações da empresa ou de clientes devem

implementar controles de acesso, incluindo um processo de login, fator múltiplo de autenticação e/ou senha *power-on*. As senhas devem respeitar os padrões de segurança e são necessárias antes de acessar as redes, serviços corporativos online e computadores da Principal Claritas. Todos os dispositivos móveis devem incorporar o tempo limite de inatividade.

2. Criptografia – Todos os laptops fornecidos pela Principal Claritas aos seus Colaboradores são protegidos por criptografia completa de disco. Todos os outros dispositivos de armazenamento, computação móvel e comunicação devem usar uma solução de criptografia eficaz para criptografar as informações não-públicas de empresas.
3. Exclusão de Informações – Qualquer dispositivo de computação ou armazenamento usado para fins comerciais deve ter a informação removida de forma segura quando não for mais necessário. Quando o Colaborador deixar a Principal Claritas, os dados devem ser eliminados em todos os sistemas em que se encontram respeitando o prazo de retenção.
4. Sincronicidade e Configuração do Dispositivo – Somente dispositivos de computação aprovados podem ser usados para conectar-se a sistemas da Principal Claritas. Para sincronizar dispositivos de computação móvel com recursos da Principal Claritas, a Segurança da Informação deve aprovar um produto específico a ser utilizado. Todos os dispositivos de computação móveis usados para fins comerciais devem ser configurados seguindo os requisitos aprovados pela Segurança da Informação.
5. Acesso Remoto – Dispositivos de computação móvel só podem se conectar aos computadores e rede da Principal Claritas de locais remotos usando dispositivos corporativos e soluções seguras apropriadas.
6. Dispositivos Wireless – Somente dispositivos wireless aprovados podem ser usados para conectar com os sistemas da empresa.
7. Proteção contra Vírus e Malware – Os dispositivos móveis de computação da empresa devem cumprir com as políticas de proteção contra vírus e devem usar

frequentemente versões aprovadas de solução antivírus da Principal Claritas. Não será permitido que qualquer dispositivo determinado a expor a Principal Claritas a um nível inapropriado de risco se integre ao sistema da empresa. Onde a tecnologia antivírus é capaz de ser implementada, é exigido e esperado que seja mantida em progresso.

8. Técnicas de Segurança Administrativa – Medidas de segurança técnicas e administrativas abrangem informação eletrônica e quem tem acesso permitido. Senhas e dispositivos de criptografia são considerados técnicas de segurança. Todos os servidores, serviços em nuvem, laptops e dispositivos móveis devem ter medidas de segurança.
9. Segurança Física – Segurança física envolve trancar a informação do cliente em gavetas ou armários de arquivo no final do dia. Os Colaboradores não devem deixar a informação do cliente onde alguém possa facilmente acessar. A segurança física também exige que o Colaborador tranque o escritório quando ele ou ela o deixe à noite. Dispositivos móveis, incluindo laptops, tablets e smartphones, devem ser mantidos em posse do Colaborador todo o tempo, a menos que eles tenham depositado em um local seguro como um armário trancado. Um laptop deve ser guardado com um cabo de bloqueio ou cadeado se o Colaborador for deixar o laptop em uma sala de hotel quando estiver viajando.
10. Phishing – de tempos em tempos, a Principal realiza testes de Phishing com todos os Colaboradores da Principal Claritas. O resultado dos testes é encaminhado à área de Compliance da Principal Claritas, que, por sua vez, conscientiza o Colaborador da importância de tomar certos cuidados para manter a ciber segurança na Companhia. Adicionalmente, vide a "**Política de Simulação e Phishing**", que é integrante da Política de Segurança e Sigilo das Informações.
11. Escaneamento da rede - De tempos em tempos, a Principal realiza *scan* com uma ferramenta que também é atualizada frequentemente, com todas as

vulnerabilidades conhecidas e exploradas no mercado. O *scan* é realizado em todos os equipamentos conectados à rede em busca de vulnerabilidade, e desta forma, é possível garantir e prevenir a segurança do nosso parque. O resultado dos *scans* é encaminhado ao gestor da Principal Claritas com cópia para equipe de TI, que, por sua vez, trabalha manter os hardwares, softwares atualizados e *ciber* segurança na Companhia. Mensalmente é realizado o escaneamento de vulnerabilidades e avaliação dos riscos. Se aplicáveis, são feitas as correções e o "reescaneamento".

12. Pentest – Anualmente é realizado, por empresas especializadas, o *Pentest* a fim de garantir a segurança e prevenir que brechas e vulnerabilidades sejam utilizadas por pessoas mal-intencionadas. O *pentest* ajuda a encontrar falhas, brechas e vulnerabilidades dos sistemas voltados à internet e sistemas internos. Os testes são feitos por empresa terceira e apontam os riscos para que sejam realizadas eventuais correções.

5.5 Política de Software

A área de TI é responsável por assegurar que somente sejam instalados softwares que estejam de acordo com os padrões da empresa em seu computador (de propriedade da empresa). O licenciamento para todos os softwares será revisado no local antes da instalação, para assegurar compliance com os termos e condições do acordo. A instalação deve ser completada através da metodologia de aprovação da Principal Claritas. Softwares adquiridos devem ser avaliados segundo os padrões de tecnologia local para garantir a adesão, conforme apropriado. A aprovação prévia da autoridade adequada talvez seja necessária antes de baixar o software da Internet.

O software licenciado para a Principal Claritas não será distribuído a terceiros sem antes passar por uma avaliação de licença pela autoridade local competente.

5.6 Política de Gestão de Acesso

A Política de Gestão de Acesso é aplicada a todos os colaboradores da Principal Claritas. O objetivo da Política é formalizar os processos e procedimentos adotados pela companhia com relação ao acesso físico e digital da Principal Claritas, com o fim de estabelecer diretrizes para proteção de dados, equipamentos, e reduzir, desta forma, os riscos e potenciais acessos a informações e objetos não públicos.

Acesso Físico

A Principal Claritas possui diversos procedimentos para garantir o acesso físico adequado às instalações da companhia, aos seus departamentos ou às informações por ela manuseadas:

1. Sistema QR code ao prédio em que a Principal Claritas está instalada;
2. Biometria e dispositivos móveis cadastrados para acesso às instalações da companhia;
3. Chave para acesso ao CPD;
4. Controle ao Data Center, que somente o *Head* de TI tem acesso;
5. Acionamento diário do alarme nas instalações da companhia, de forma que somente as pessoas autorizadas consigam desativar o alarme;
6. Salas de reunião a fim de que qualquer informação confidencial, assuntos relacionados aos clientes da Principal Claritas ou matérias de cunho sensível sejam tratados em local apartado do restante da companhia;
7. Arquivo de documentos físicos mantidos no escritório da companhia por 5 anos;
8. Os arquivos considerados sensíveis ou detentores de informações relevantes da companhia e/ou de seus Colaboradores são armazenados em locais seguros (armários com trancas) e com acesso exclusivo ao departamento de *Compliance*.
9. Controle de abertura do claviculário (somente a Equipe de TI tem a chave).

Acesso Digital

Para proteger os dados digitais da Principal Claritas, são adotados os seguintes controles:

1. Login e senha no computador de todos os Colaboradores e com duplo fator de autenticação, sendo que a senha é trocada periodicamente;
2. Criptografia nos notebooks dos Colaboradores;
3. Controle de dispositivos *wireless*;
4. Testes de *phishing*;
5. Sincronicidade e configuração do dispositivo, de forma que somente dispositivos aprovados pelos departamentos de TI e *Compliance* têm permissão para se conectar aos sistemas da Principal Claritas;
6. Dispositivos de computação corporativo móvel só podem se conectar aos dispositivos e rede da Principal Claritas usando soluções seguras apropriadas;
7. Procedimentos para garantir proteção contra vírus e *malware*;
8. Exclusão e retenção de informações comerciais quando um Colaborador é desligado da companhia;
9. Bloqueio nos computadores dos Colaboradores a sites e acessos em geral que o departamento de TI considere vulneráveis ou perigosos para a companhia, como acessos a mídias sociais e e-mails pessoais;
10. Sistema de telefonia digital com gravação de todos os ramais (arquivos mantidos por 7 anos);
11. As pastas e arquivos digitais da rede de sistemas da Principal Claritas só são acessados pelos Colaboradores que possuem permissão pelos departamentos de TI e Compliance. Sempre que um Colaborador precisa de acesso a alguma pasta ou arquivo que não está liberado, este deve solicitar aos responsáveis pelos departamentos de TI e Compliance para que estes façam a liberação formal, caso entendam que tal concessão é relevante. Da mesma forma, quando um Colaborador é transferido da área em que estava, a área de TI se encarrega de revisar seus acessos de maneira que ele não tenha acessos indevidos. Os acessos são revisados a cada três meses.

12. Os procedimentos de ingresso e desligamento do Colaborador são conduzidos pelos departamentos de TI, RH e *Compliance* para garantir o acesso ou bloqueio/segurança das informações, conforme explicado abaixo.

Acesso/Segurança das Informações

Quando o Colaborador é aprovado no processo de seleção da Principal Claritas, o departamento de RH envia ao novo Colaborador o Manual de Compliance, o Código de Ética e Conduta Corporativa e as políticas da companhia antes de seu ingresso na companhia para que o mesmo possa ler todos os documentos e contatar a Principal Claritas caso tenha alguma dúvida.

Ao ingressar na Principal Claritas, os departamentos de TI, RH e Compliance da Principal Claritas realizam as seguintes providências: (i) o departamento de RH envia um e-mail de "Boas Vindas", onde constam todas as informações e procedimentos utilizados na companhia referente às regras e diretrizes da Política de Gestão de Acesso; (ii) pessoalmente, um dos integrantes do departamento de TI registra o login e senha de acesso aos computadores e instalações da Principal Claritas; (iii) um dos integrantes do departamento de TI cadastra a biometria e dispositivos móvel para acesso ao escritório e cadastra no sistema de QR code para acesso ao prédio e explica todos os processos informados por e-mail; (iv) a área de Compliance exige que seja preenchida a declaração de recebimento e adesão ao Manual, de maneira que o Colaborador ateste o conhecimento às políticas da Principal Claritas, dentre elas às relativas à segurança de informação.

Quando um Colaborador é desligado ou se desliga da companhia, os departamentos de Compliance, RH e TI da Principal Claritas realizam os seguintes procedimentos a fim de garantir a segurança das informações da companhia: (i) o *Head* de TI bloqueia o acesso aos dados digitais até então permitidos ao colaborador e efetua o bloquei no sistema de acesso ao prédio em que a Principal Claritas está instalada; (ii) ele remove o cadastro da biometria do Colaborador para que este não tenha acesso às instalações

da companhia; (iii) caso o Colaborador tenha em sua posse algum dispositivo móvel da companhia, como notebook, o departamento de RH solicita a devolução; (iv) o departamento de RH solicita ao colaborador que todos os documentos necessários sejam assinados para o seu efetivo desligamento; (v) o responsável de algum desses departamentos e/ou o gestor da área acompanham o Colaborador até a sua efetiva saída do prédio da companhia.

Procedimentos Internos para Tratar Eventual Vazamento de Informações Confidenciais, Reservadas ou Privilegiadas

Não obstante todos os procedimentos e aparato tecnológico robustos adotados pela Principal Claritas para preservar o sigilo das informações confidenciais, reservadas ou privilegiadas, na eventualidade de ocorrer o vazamento de quaisquer Informações, ainda que de forma involuntária, o Diretor de Compliance deverá tomar ciência do fato tão logo seja possível.

A Principal Claritas acredita que a melhor forma de se solucionar uma invasão onde foram obtidas informações confidenciais ou dados sensíveis é ser transparente com a parte prejudicada. Isto é: comunicar imediatamente o cliente, o colaborador ou o prestador de serviço que teve sua informação obtida. Esta comunicação poderá ser realizada por e-mail, telefone, ou, dependendo do caso, pessoalmente. No caso de vazamento de Informações relativas aos fundos de investimento geridos: imediatamente, seguirá com o rito para publicação de fato relevante, nos termos da regulamentação vigente, a fim de garantir a ampla disseminação e tratamento equânime da Informação. Esse procedimento visa assegurar que nenhuma pessoa seja beneficiada pela detenção ou uso da informação confidencial, reservada ou privilegiada atinente ao fundo de investimento.

No caso de vazamentos por razões de ataques cibernéticos, a Principal Claritas adotará as medidas descritas em sua Política de Segurança Cibernética.

Monitoramento

Para garantir que as regras e diretrizes da Política de Gestão de Acesso são obedecidas por todos os colaboradores da Principal Claritas, os Departamentos de C*ompliance,* TI e Risco realizam periodicamente diversos procedimentos:

Departamento de Risco

O Departamento de Risco é responsável por:

1. Auxiliar o departamento de Compliance no processo de *due diligence* com os prestadores de serviços da Principal Claritas.

Departamento de TI

O *Head* de TI realiza periodicamente:

1. Testes de *Business Continuity, Disaster Recovery Plans e Call Tree* a fim de garantir a eficiência dos Planos elaborados para comunicação, contingência e recuperação de desastres da Principal Claritas;
2. Testes de *phishing*.
3. Execução da concessão de acesso físico e digital aos Colaboradores, assim como a sua revisão;
4. Processo de entrada e saída dos Colaboradores com as respectivas necessidades de programas, arquivos e dispositivos;
5. Revisão diária dos relatórios dos firewalls de atividades via Internet e de segurança (falha de autenticação, tentativa e/ou acesso indevido);
6. Revisão periódica no painel e acompanhamento do relatório dos números de alterações de dados dos diretórios compartilhados. Os logs de alterações são

gravados para auditorias futuras;
7. Revisão do painel da ferramenta de antivírus a cada duas horas (oriundos de ataques e vírus para usar as credenciais dos colaboradores indevidamente e/ou acessar, criptografar e compartilhar informação confidencial);
8. Atualizações mensais e/ou eventuais para garantir correções contra vulnerabilidade e elevação de privilégios;
9. *Check list* diário dos servidores para garantir a disponibilidade dos serviços e corrigir falhas eventuais;
10. Verificação mensal dos servidores em busca de eventuais brechas de segurança.

Departamento de *Compliance*

A área de Compliance é responsável por:

1. Enviar, anualmente, o questionário de *due diligence* e cibersegurança para os prestadores de serviços relevantes da Principal Claritas a fim de verificar se estes possuem sistemas e infraestrutura compatíveis com o nível de segurança exigido pela Principal Claritas;
2. Realizar treinamento periódico a respeito das questões de acesso a todos os Colaboradores;
3. Solicitar aos colaboradores o envio da declaração de recebimento e adesão ao Manual e às políticas da Principal Claritas;
4. Analisar e conceder os acessos digitais aos Colaboradores de acordo com as necessidades de trabalho específicas, respeitando a segurança das informações;
5. Esclarecer qualquer dúvida oriunda desta Política.

Gestores

1. Esclarecer as dúvidas de seus colaboradores a respeito desta política;
2. Responsabilizar-se por comunicar a área de TI sobre as eventuais necessidades de novos colaboradores e sobre o desligamento de colaboradores.

5.7 Política de Uso de Mensagem Eletrônica

O objetivo dessa política é garantir o uso correto das mensagens eletrônicas de comunicação por todos os Colaboradores da Principal Claritas. O escopo desta política é aplicável a todos os Colaboradores da Principal Claritas e abrange todas as ferramentas de mensagens eletrônicas de comunicação disponibilizadas pela Principal Claritas. No momento da elaboração desta política as ferramentas de mensagem eletrônica corporativa incluem os e-mails corporativos e Microsoft Teams; Reuters Messenger e Bloomberg Messenger também podem ser disponibilizados dependendo da função do Colaborador, mas estas ferramentas podem mudar ao longo do tempo; caso isto ocorra os colaboradores serão devidamente informados a respeito.

A Principal Claritas oferece os instrumentos de mensagem eletrônica como meios para facilitar o trabalho realizado pelos seus Colaboradores. Desta forma, estes instrumentos devem ser usados primordialmente para que as atividades da empresa sejam realizadas de forma efetiva. As mensagens eletrônicas enviadas ou recebidas pelos meios disponibilizados pela Empresa são de uso corporativo, sendo retido por cinco anos e poderão ser acessadas por outro colaborador da mesma área quando houver desligamento e for necessária a utilização da informação para prosseguir com algum assunto pendente ou para fins de auditoria.

A responsabilidade por esta política é compartilhada entre:

- Área *de* Compliance*;* e
- Área de Tecnologia da Informação.

Além disso, cada Colaborador é responsável pelo uso correto das mensagens eletrônicas corporativas.

Ferramentas

Serão concedidas a todos os Colaboradores, como instrumentos para facilitar as atividades necessárias a cada umas das posições ocupadas pelos por eles, dispositivos de mensagens eletrônicas, como e-mail, *Microsoft Teams, Reuters Messenger* e *Bloomberg Messenger*, estas últimas a depender da função do Colaborador.

Por questões de *compliance* com a regulação vigente e para garantir que a política é cumprida, o uso dessas ferramentas é monitorado. É importante ressaltar que não existe privacidade ou propriedade dos Colaboradores em relação ao uso das mesmas ou seu conteúdo. Da mesma forma, as mensagens e seu conteúdo poderão ser revelados a terceiros em caso de necessidade legal.

As informações dos bancos de dados das mensagens eletrônicas são salvas em fitas, e assim, até mesmo quando são apagadas, elas podem ser recuperadas, dependendo da disponibilidade das mesmas.

O uso pessoal e ocasional é permitido desde que:

- Este uso não interfira direta ou indiretamente com a segurança de e-mail da empresa e/ou de seus Servidores;
- Não interfira com os serviços do Colaborador ou suas obrigações junto à Principal Claritas e;
- Não viole esta política ou qualquer outra lei nacional.

É estritamente proibido:

- Enviar ou encaminhar mensagens contendo comentários ou conteúdo ilegal, difamatórios, ofensivos, racistas ou obscenos;
- Enviar ou encaminhar mensagens com conteúdo que possa denegrir o caráter ou a imagem de qualquer pessoa da empresa;
- Enviar ou encaminhar arquivos de conteúdo confidencial;
- Forjar ou tentar forjar mensagens.

Os Colaboradores não deverão abrir mensagens eletrônicas de destinatários

desconhecidos ou de conteúdo estranho. Em caso de dúvidas, a equipe de Tecnologia da Informação deverá ser contatada.

Monitoramento

De acordo com a regulação e para garantir compliance com a política, o monitoramento das mensagens eletrônicas será feito pela área de Compliance, em conjunto com a área de Tecnologia da Informação.

Normalmente, o monitoramento é feito de forma aleatória a cada trimestre pela área de Compliance por meio de sorteio eletrônico, acompanhado pelo *Head* de Tecnologia da Informação. Entretanto, em caso de suspeita de qualquer atividade irregular ou violação a esta política, o monitoramento poderá ser feito a qualquer tempo.

Esses procedimentos serão documentados e poderão ser auditados a qualquer tempo. No caso de violação a esta política, diferentes medidas poderão ser tomadas de acordo com a gravidade da violação.

Treinamento

A área de Compliance e/ou Tecnologia da Informação fornecerá esta Política de Segurança da Informação a todos os Colaboradores, inclusive na contratação de novos Colaboradores. Além disso, a área de Compliance conduzirá treinamentos periódicos sobre diversos aspectos, dentre eles, a Política de Segurança e Sigilo das informações.

Responsabilidade

Esta Política foi elaborada pelos departamentos de Risco, Compliance e TI. A área de Compliance é responsável pelo armazenamento e revisão desta Política, a cada dois anos ou sempre que houver necessidade ou alteração regulatória.

Qualquer dúvida com relação ao conteúdo desta Política, os colaboradores são incentivados a contatar seu gestor e/ou a área de Compliance.

6. Manual de Gerenciamento de Risco

Com o objetivo de apresentar o modelo de gerenciamento de risco adotado pela área de risco da Principal Claritas, a Principal Claritas possui um Manual de Gerenciamento de Risco específico.

Baseando-se nas estratégias definidas pela equipe de gestão de recursos e aprovados pelo Comitê de Investimentos semanal, o Departamento de Risco realiza a análise dos riscos de mercado, liquidez e de crédito. O monitoramento é efetuado diariamente e tem como função apontar e controlar as posições de risco de mercado, além dos riscos de crédito, liquidez e operacional, de forma contínua e efetiva.

Além do Manual de Gerenciamento de Risco, a Principal Claritas desenvolveu o Manual de Gerenciamento de Liquidez, onde desenvolveu um método em que é avaliada a capacidade de um fundo de honrar os eventuais resgates que possa a vir receber (risco de liquidez de passivo). Neste método, realiza uma análise do histórico de resgate dos fundos, e então, são avaliados quais foram os maiores resgates realizados em diversos períodos para cada fundo de investimento. Também é monitorada a concentração do passivo de cada fundo.

Diariamente a área envia o Relatório de Risco de Liquidez (Ativo e Passivo).

Para mais detalhes, vide o Manual de Gerenciamento de Risco da Principal Claritas disponível no website.

7. *Know Your Partner (KYP)*

O objetivo é mitigar e administrar o risco de prestadores de serviço/fornecedores para a Principal Claritas, garantindo que a empresa realize todas as atividades necessárias

de *due diligence* para a seleção, administração contínua e término na relação com prestadores de serviço/fornecedores.

Todos os colaboradores são responsáveis pelo cumprimento dessa política. Qualquer violação a esta política deve ser reportada de acordo com as regras de conduta e ética estabelecidas neste manual.

A Principal Claritas contrata prestadores de serviço/fornecedores para suportar a realização de suas atividades. Para tanto, é importante que:

- Conduza seus processos com objetivos claros e justos;
- Realize processos de *due diligence*, sempre que possível, ao selecionar seus prestadores de serviço/fornecedores;
- Mitigue riscos relacionados à negociação desses contratos;
- Monitore de forma ativa e administre o risco de gestão de fornecedores e sua performance durante o período de vigência do contrato.

A área responsável pelo contrato e/ou o jurídico vão liderar o processo de negociação contratual. A não ser que os prestadores de serviço/fornecedores tenham seu próprio modelo de contrato, o modelo da Principal Claritas deverá ser utilizado. As cláusulas de mitigação de risco, anticorrupção, de proteção de dados e privacidade (conforme o caso) devem ser incluídas no contrato.

Todos os contratos devem ser encaminhados para o Jurídico, que fará a revisão final e se encarregará de obter as assinaturas necessárias. Uma vez que as assinaturas sejam obtidas, o Jurídico encaminhará a via do prestador de serviço/fornecedor à área responsável que deverá efetuar o envio para o prestador de serviço/fornecedor.

Due Diligence

Periodicamente, as áreas de Risco e *Compliance* efetuam um processo de *due diligence* nos prestadores de serviço/fornecedores relevantes para a atividade da Principal

Claritas.

Os Colaboradores que negociam diretamente com os prestadores de serviços estão geralmente numa melhor posição para avaliar os serviços recebidos. Os Colaboradores em diversos níveis (funcionários, supervisores, gestores) devem fornecer *feedback* relacionado a seus contatos com os prestadores de serviços e qualquer preocupação que possa resultar.

O nível de performance da prestação de serviço ou fornecimento da mercadoria deve ser avaliado pela área responsável e encaminhado às áreas de risco e jurídico/compliance.

Quando necessário, o Colaborador responsável por gerenciar o relacionamento deve acompanhar quaisquer questões relacionadas com o prestador de serviço. Se um Colaborador tiver alguma razão para acreditar que o prestador de serviço não está cumprindo os termos do acordo, o Colaborador deve reportar o assunto à área de Compliance e/ou seu gestor, que, por sua vez, deve determinar se o problema é material e se deve ser encaminhado à Diretoria.

A Principal Claritas realiza um processo de *Due Diligence* com as prestadoras de serviços relevantes para avaliar a reputação, as qualificações da empresa e se está em cumprimento com a Lei Anticorrupção. Além disso, são enviados diferentes tipos de questionário, considerando o tipo de serviço/produto prestado ou fornecido e o tipo de informação mantida pelo prestador de serviço/fornecedor.

8. *Know Your Client (KYC)*

Os formulários de abertura de contas da Principal Claritas e aqueles dos Administradores e as regras "*Know Your Client*" (KYC) são aspectos importantes dos procedimentos contra a lavagem de dinheiro e medidas de prevenção de fraude em geral. Os Colaboradores devem cumprir com estas responsabilidades e auxiliar a Principal Claritas em prevenir e detectar envolvimento com lavagem de dinheiro ou

outra atividade ilegal por clientes potenciais ou existentes e outras pessoas que se beneficiam dos nossos produtos e serviços.

Para evitar envolvimento com a lavagem de dinheiro e/ou outra atividade ilegal, os Colaboradores devem fazer esforços consideráveis para obter informações precisas sobre seus clientes. Os Colaboradores devem utilizar todas as medidas possíveis para identificar a origem dos recursos utilizados para os pagamentos e a natureza das atividades dos negócios dos clientes para avaliar transações ou relações que podem provir de atividade ilegal. Os Colaboradores devem procurar e verificar alertas que possam caracterizar uma transação como suspeita. Transações suspeitas são geralmente definidas como aquelas onde existem circunstâncias indicando que a conduta da(s) pessoa(s) que realiza(m) a operação seja potencialmente improvável, ilegal ou imprópria e que exige dos Colaboradores uma diligência e/ou investigação adicional(is) antes de seguir adiante com a operação.

Além disso, informações suficientes devem ser obtidas para determinar se um indivíduo é ou não uma "pessoa exposta politicamente". O termo "pessoa exposta politicamente" (PEP) geralmente inclui uma atual ou ex-figura politicamente exposta sênior, sua família imediata, e seus associados próximos.

Para efeitos do disposto nesta Política, considera-se PEP:

1. Aquela que desempenha ou tenha desempenhado, nos últimos 5 (cinco) anos, cargos, empregos ou funções públicas relevantes, no Brasil ou em outros países, territórios e dependências estrangeiros, assim como seus representantes, familiares e outras pessoas de seu relacionamento próximo;
2. Cargo, emprego ou função pública relevante exercido por chefes de estado e de governo, políticos de alto nível, altos servidores dos poderes públicos, magistrados ou militares de alto nível, dirigentes de empresas públicas ou dirigentes de partidos políticos; e
3. Familiares de PPE, seus parentes, na linha direta, até o primeiro grau, assim como o cônjuge, companheiro e enteado e outras pessoas de relacionamento

próximo.

O prazo de 5 (cinco) anos referido no inciso (i) acima, deve ser contado, retroativamente, a partir da data de início da relação de negócio ou da data em que o investidor passou a se enquadrar como pessoa politicamente exposta.

São consideradas, no Brasil, PEPs:

1. Os detentores de mandatos eletivos dos Poderes Executivo e Legislativo da União;
2. Os ocupantes de cargo, no Poder Executivo da União:
   a) de Ministro de Estado ou equiparado;
   b) de natureza especial ou equivalente;
   c) de Presidente, Vice-Presidente e Diretor, ou equivalentes, de entidades da administração pública indireta; e
   d) do grupo direção e assessoramento superiores - DAS, nível 6, e equivalentes;
3. Os membros do Conselho Nacional de Justiça, do Supremo Tribunal Federal, dos Tribunais Superiores, dos Tribunais Regionais Federais, dos Tribunais Regionais do Trabalho, dos Tribunais Regionais Eleitorais, do Conselho Superior da Justiça do Trabalho e do Conselho da Justiça Federal;;
4. Os membros do Conselho Nacional do Ministério Público, o Procurador-Geral da República, o Vice-Procurador-Geral da República, o Procurador-Geral do Trabalho, o Procurador-Geral da Justiça Militar, os Subprocuradores-Gerais da República e os Procuradores-Gerais de Justiça dos Estados e do Distrito Federal;
5. Os membros do Tribunal de Contas da União, o Procurador-Geral e os Subprocuradores-Gerais do Ministério Público junto ao Tribunal de Contas da União;
6. Os Presidentes e Tesoureiros nacionais, ou equivalentes, de partidos políticos;
7. Os Governadores e Secretários de Estado e do Distrito Federal, os Deputados Estaduais e Distritais, os Presidentes, ou equivalentes, de entidades da administração pública indireta estadual e distrital e os Presidentes de Tribunais de Justiça, Militares, de Contas ou equivalentes de Estado e do Distrito Federal;

e

8. Os Prefeitos, os Vereadores, os Secretários Municipais, os Presidentes, ou equivalentes, de entidades da administração pública indireta municipal e os Presidentes de Tribunais de Contas de Municípios ou equivalentes.

Também são consideradas pessoas expostas politicamente aquelas que, no exterior, sejam:

1. Chefes de estado ou de governo;
2. Políticos de escalões superiores;
3. Ocupantes de cargos governamentais de escalões superiores;
4. Oficiais generais e membros de escalões superiores do poder judiciário;
5. Executivos de escalões superiores de empresas públicas;
6. Dirigentes de partidos políticos.

A identificação do status de um cliente como PEP não deve resultar automaticamente em uma determinação de maior risco; é um fator que a Principal Claritas deve considerar ao avaliar o risco de uma relação. Os Colaboradores devem procurar e verificar outros alertas. Transações suspeitas são geralmente definidas como circunstâncias que poderiam colocar uma pessoa razoável sob a observação que a conduta ilegal ou imprópria venha ou pode vir a ocorrer. Os aspectos seguintes são exemplos de situações suspeitas que exigem *due diligence* adicional e investigação antes de seguir adiante:

1. Fazer negócios em países de alto risco.
2. Relutância em participar de *due diligence*.
3. Alguma sugestão que leis, regulamentação ou políticas de *compliance* da empresa não precisam ser seguidas.
4. Uso de empresas de fachada.
5. Propriedade ou relação próxima com funcionários públicos.
6. Insistência no pagamento em um terceiro país ou para uma terceira parte não relacionada.

7. Nomeado como uma Parte Designada, SDN, ou alguma lista similar.
8. Conexões com países identificados como não-cooperativos com as medidas internacionais contra lavagem de dinheiro.
9. Falso fornecimento ou informação ilusória.
10. Recusa de divulgar a natureza e origem dos ativos.
11. Recusa a identificar o beneficiário.
12. Endereço da empresa não é o endereço físico, mas uma caixa postal.
13. Falta de preocupação com riscos ou riscos de transações.
14. Estruturar transações para evitar prestar informações obrigatórias.

Os Colaboradores devem reportar transações suspeitas à área de *Compliance* e/ou seus gestores conforme apropriado.

9. *Know Your Employee (KYE)*

Quando um candidato é analisado para trabalhar na Principal Claritas, a área de Compliance e/ou a área de RH, dentre outras checagens, pesquisa se o candidato possui algum relacionamento com uma pessoa exposta politicamente (PEP) ou com algum funcionário/servidor público relevante, dentro ou fora dos EUA.

Além da pesquisa, a área de Compliance e/ou o departamento de RH solicita ao candidato, no momento da sua contratação, que declare e assine que não possui nenhum relacionamento com PEP, seja no Brasil, seja dentro ou fora dos EUA. Caso ele possua algum tipo de relacionamento e se recuse a assinar o termo, a área de Compliance deve:

1. Verificar com o gestor se o cargo a ser ocupado pelo candidato poderia caracterizar algum tipo de favorecimento para a empresa.
2. Garantir com o gestor da área onde o candidato estará alocado que as qualificações profissionais e acadêmicas do indivíduo são adequadas para a posição a ser preenchida. A prova de que um parente de funcionário/servidor

público relevante foi contratado para uma posição na qual não é qualificado poderá resultar em evidências de que o candidato foi contratado para fins impróprios.

3. Garantir que o salário e o tratamento dado ao candidato relacionado com funcionário/servidor público relevante são adequados à posição e consistentes com outros indivíduos em posição similar. A prova de que o parente do funcionário/servidor público relevante está recebendo um salário significativamente mais alto que os outros indivíduos em posições similares sugere que recursos adicionais podem ser fornecidos para influenciar o funcionário/servidor público.
4. Confirmar que a posição não foi criada especificamente para o parente do funcionário/servidor público relevante. Evidências de que a posição foi criada para uma determinada pessoa poderá sugerir que o propósito da Companhia em contratar o indivíduo foi obter influência com o funcionário/servidor público.
5. Certificar-se que, na medida do possível, as responsabilidades do parente do funcionário/servidor público relevante não se enquadram na esfera de conduta sobre o qual o funcionário/servidor público detém tomada de decisão de autoridade reguladora ou similar. Por exemplo, um parente de um funcionário/servidor público responsável pela supervisão bancária não deve ser contratado como *head* para um assunto de banco sujeito aquela autoridade. Da mesma forma, o tomador de decisão de contratação deve ser independente da unidade de negócio que pode interagir com o funcionário/servidor público.
6. Uma vez que o indivíduo seja contratado, garantir que ele ou ela submeta-se a este Manual e aos respectivos treinamentos e que as políticas e procedimentos anticorrupção estão claras ao novo colaborador.
7. A Companhia deve assegurar que suas políticas de armazenamento de registros permitam que os departamentos relevantes mantenham a documentação necessária para refutar qualquer alegação de irregularidade.

10. *Anti Money Laundering (AML)*

Lavagem de dinheiro é o processo pelo qual recursos originados de atividades ilegais são transformados em ativos ou bens de origem aparentemente legal. Assim, a origem ilícita desses ativos ou bens patrimoniais fica dissimulada ou escondida de tal forma que sua origem aparenta estar lícita ou que sua origem seja muito difícil de provar ou demonstrar.

Os responsáveis por estas operações fazem com que os valores obtidos por meio das atividades ilícitas e criminosas (tráfico de drogas, corrupção, comércio de armas, prostituição, crimes de colarinho branco, terrorismo, extorsão, fraude fiscal, entre outros) sejam dissimulados ou escondidos, aparecendo como resultado de operações comerciais legais e que possam ser absorvidas pelo sistema financeiro, de forma natural.

Para isso, a lavagem de dinheiro realiza-se por meio de um processo dinâmico que requer as seguintes fases:

1. Colocação: esta primeira etapa consiste na colocação do dinheiro no sistema econômico. Objetivando ocultar sua origem, o criminoso procura movimentar o dinheiro em países com regras mais permissivas e naqueles que possuem um sistema financeiro mais liberal. 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.
2. Ocultação: a segunda fase do processo tem como objetivo dificultar o rastreamento contábil dos recursos ilícitos. O objetivo é quebrar a cadeia de evidências ante a possibilidade da realização de investigações sobre a origem do dinheiro. A movimentação costuma ser eletrônica, para contas anônimas ou “fantasmas”.
3. Integração: nesta última etapa, os ativos são formalmente incorporados ao

sistema econômico. O investimento é feito em mercado de capitais, imobiliário, obras de arte, etc. Uma vez que esta cadeia esteja formada, fica cada vez mais fácil legitimar o dinheiro ilegal.

Financiamento ao Terrorismo pode ser definido como a reunião de fundos ou de capital para a realização de atividades terroristas. Esses fundos podem ter origem legal – doações, ganho de atividades econômicas lícitas diversas – ou ilegal: as procedentes de atividades criminais (crime organizado, fraudes, contrabando, extorsões, sequestros, etc).

A Principal Claritas e seus colaboradores devem observar atentamente a Política de PLD, divulgada aos colaboradores e disponível em diretório interno, que foi construída em consonância com a regulamentação local e internacional. Dentre estas normas, vale mencionar:

a) Lei 9.613/98 – Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os respectivos ilícitos e cria o COAF, com suas alterações – Lei nº 10.701, de 9 de julho de 2003, Lei nº 12.683, de 09 de julho de 2012 e a Lei nº 13.901, de 11 de Novembro de 2019;

b) Resolução 50/21 da CVM – Dispõe sobre a prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa - PLD/FTP no âmbito do mercado de valores mobiliários;

c) Normas emitidas pelo COAF (especialmente, mas não se limitando as Resoluções COAF n.º 7,15 e 16);

d) ICVM 558 – Dispõe sobre o exercício profissional de administração de carteira de valores mobiliários, mencionando a necessidade de regras sobre controles internos relacionados à PLD;

e) IN RFB 1.037 de 2010 que lista os países considerados como paraísos fiscais;

f) Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro

(ENCCLA), criada em 2003.

O conhecimento de qualquer indício de lavagem de dinheiro deverá ser imediatamente comunicado à área de *Compliance,* sendo esta responsável por averiguar as informações reportadas. A comunicação aos órgãos competentes será efetuada de acordo com as disposições da Política. A área de *Compliance* será igualmente responsável por esclarecer qualquer dúvida que os Colaboradores tenham em relação à Política, treinando-os e conscientizando-os sobre os crimes relacionados à lavagem de dinheiro.

11. *Best Execution*

A Principal Claritas gere fundos privados e carteiras de investimento para seus clientes. A Principal Claritas adotou um processo de gestão de carteira e práticas de negociação que reflete suas obrigações para com os seus clientes e incorpora procedimentos necessários para garantir que os investimentos e as carteiras dos clientes sejam geridos com o máximo de zelo e diligência.

Cada *portfolio manager* ou equipe de gestão é o principal responsável por assegurar que as carteiras de clientes e/ou fundos são administrados de uma maneira coerente com seus objetivos de investimento, políticas, restrições e estratégias. Os processos e ferramentas utilizados para cumprir esta responsabilidade variam, até certo ponto, pelo tipo de carteira. Cada *portfolio manager* ou equipe de gestão de carteira se reporta ao *Chief Investment Officer* (CIO). O CIO supervisiona a gestão de todas as carteiras, preside os Comitês de Investimento da Principal Claritas, e fornece a supervisão para a gestão de carteiras na adesão dos objetivos do investimento, diretrizes e estratégias. Os Comitês de Investimento se reúnem para avaliar performance de investimento, compatibilidade, processos de investimento, e adesão às diretrizes de investimento.

Ao gerenciar as carteiras no dia-a-dia, o *portfolio manager* ou a equipe de gestão,

normalmente compra e vende valores mobiliários em todas as carteiras semelhantes. O *portfolio manager* ou a equipe de gestão administra tais valores mobiliários de maneira compatível com a metodologia de investimento de tomada de decisão aplicável. Entretanto, alocações similares de carteiras podem diferir por razões legítimas. Decisões relacionadas à alocação podem ser feitas com referência a inúmeros fatores, incluindo, se necessário e sem limitação, a:

- Horizonte de investimento da carteira;
- Objetivos de investimento, diretrizes, e restrições;
- Diferentes níveis de investimento para diferentes estratégias (por exemplo, diferentes objetivos na classe de ativos);
- Disponibilidade de caixa para investimentos e fluxo de caixa em diversas carteiras;
- Tamanhos relativos e tamanhos futuros esperados de carteira aplicáveis; e
- Disponibilidade de outras oportunidades de investimentos adequadas.

Considerações de Perfil do Investidor podem incluir, sem limitação:

- Atratividade relativa a títulos de valores mobiliários de diferentes carteiras;
- Concentração de posições em uma carteira;
- Adequação de um valor mobiliário para o *benchmark* de uma carteira e a sensibilidade de um benchmark de uma carteira;
- A tolerância de risco de uma carteira a parâmetro de riscos e estratégias de alocação;
- Uso da oportunidade como uma substituição de valor mobiliário que a Principal Claritas acredita ser atrativa por uma conta; e/ou
- Considerações relacionadas à exposição de uma carteira a uma indústria.

Os gestores de recursos têm a obrigação de buscar a melhor execução para todas as transações de valores mobiliários executadas em nome dos clientes. É política da Principal Claritas buscar a melhor execução para as carteiras e fundos geridos. É importante notar que a melhor execução não significa pagamento de comissão mais baixa. O custo de negociação inclui mais do que só o custo de comissões na negociação executada. Também inclui o custo de impacto ou quanto o preço das ações muda por causa da presença de uma nova ordem.

A Principal Claritas considera uma série de fatores qualitativos e quantitativos na colocação de ordens de compra e venda de valores mobiliários e na seleção de corretoras adequadas, o que inclui, mas não limita a: capacidade de execução, razoabilidade na taxa de *trading errors*, especialização em valores mobiliários específicos, qualidade de crédito, o valor da equipe de *research* e serviços fornecidos, suporte de *Back Office* e capacidade de resposta. A Principal Claritas avalia a qualidade e o custo de serviços recebidos das corretoras/terceiros tanto numa base não oficial quanto numa base periódica e sistêmica. Isso pode incluir:

1. Informal: revisões do período pelos gestores
2. Avaliações periódicas do corretor/contraparte
3. Reuniões periódicas da avaliação da corretagem

De acordo com a Instrução Normativa CVM n° 08/79 e em linha com as melhores práticas adotadas no processo de gestão, são vedadas práticas não equitativas de negociação, como *front running, insider trading, spoofing* e *layering*.

Entende-se como:

• condições artificiais de demanda, oferta ou preço de valores mobiliários aquelas criadas em decorrência de negociações pelas quais seus participantes ou intermediários, por ação ou omissão dolosa provocarem, direta ou indiretamente, alterações no fluxo de ordens de compra ou venda de valores mobiliários;

• manipulação de preços no mercado de valores mobiliários, a utilização de qualquer processo ou artifício destinado, direta ou indiretamente, a elevar, manter ou baixar a cotação de um valor mobiliário, induzindo, terceiros à sua negociação;

• operação fraudulenta no mercado de valores mobiliários, aquela em que se utilize ardil ou artifício destinado a induzir ou manter terceiros em erro, com a finalidade de se obter vantagem ilícita de natureza patrimonial para as partes na operação, para o intermediário ou para terceiros;

• prática não equitativa no mercado de valores mobiliários, aquela de que resulte, direta ou indiretamente, efetiva ou potencialmente, um tratamento para qualquer das partes, em negociações com valores mobiliários, que a coloque em uma indevida posição de desequilíbrio ou desigualdade em face dos demais participantes da operação.

12. Plano de Recuperação de Desastre e Contingência

A Principal Claritas possui um plano de Recuperação de Desastres, Continuidade de Negócios e *Call tree* (“Planos”), que permite que qualquer Colaborador possa comunicar um incidente para o líder da área, e, este por sua vez, fará uma análise da situação utilizando o fluxograma, onde o principal objetivo é manter a integridade e minimizar o tempo de recuperação.

Sempre que houver algum incidente, seja este de menor ou maior impacto, deve-se reportar para o líder da área para que este contate a equipe de TI a fim de iniciar os procedimentos de recuperação e continuidade dos negócios. Caso o incidente seja detectado diretamente pela equipe de TI, o reporte será feito imediatamente à Diretoria para que sejam tomadas as medidas necessárias.

A cobertura dos Planos abrange desde desastres de pequeno impacto até grandes

desastres, o que possibilita responder com rapidez e integridade aos incidentes. Os Planos visam "prever" as possíveis interrupções que possam ocorrer por conta de algum incidente e preparar a Companhia para ter uma resposta rápida, a fim de reduzir os custos e potenciais conseqüências que possam ser gerados por tais interrupções.

As políticas e processos referentes aos Planos são revisados ao menos uma vez por ano e atualizados sempre que necessário. Os Colaboradores da Principal Claritas têm periodicamente treinamento sobre os Planos e suas eventuais atualizações. Para abranger o plano de contingência da Principal Claritas, os usuários utilizam um notebook criptografado para exercer as funções do dia a dia de forma remota, caso seja necessário. Assim, é possível dar continuidade ao negócio durante um incidente que impossibilite a vinda dos Colaboradores ao escritório.

O Administrador de TI é responsável por responder questões sobre o BC Plan e o DR Plan. A equipe da PFG *Business Continuity Planning* e *Disaster Recovery* tem supervisão corporativa e coordena o programa de Continuidade de Negócios e de Recuperação de Desastres.

Para maiores detalhes, vide a Política de Recuperação de Desastres e Continuidade de Negócios.

13. Alegações que devem ser reportadas

Todos os Colaboradores devem reportar suspeita de atividade antiética ou fraudulenta. Os aspectos a seguir são exemplos de alegações que devem ser reportadas sob esta política:

1. Suspeita de furto, peculato ou atividade criminosa.
2. Descumprimento das políticas e processos de *compliance* da empresa.
3. Práticas administrativas em conflito com as obrigações contratuais ou princípios éticos.
4. Compartilhar informação confidencial de propriedade da empresa ou do cliente

com alguém que não tenha interesse legítimos para saber tal informação.

5. Falsificar entradas em registros contábeis da empresa.
6. Violação deste Código, incluindo os seguintes itens:
    - Brindes, Presentes, Premiações e Entretenimento;
    - Conflitos de Interesse;
    - Desonestidade;
    - Aceitar pagamentos não autorizados; e
    - Informação privilegiada.

A Principal Claritas leva a sério sua obrigação com seus Colaboradores e clientes/investidores de conduzir negócios de uma maneira ética e legal. Esta política estabelece diretrizes e procedimentos para lidar com relatos de suspeita de atividade antiética ou fraudulenta. Todos os problemas relatados são devidamente investigados pela área de *Compliance* e o relatório é feito ao *Senior Management* e/ou o Conselho de Administração, conforme apropriado. Todas as questões são mantidas em sigilo, e o acesso à informação relacionada é restrito e seguro.

14. Canal de Comunicação

Em caso de dúvidas, suspeitas ou alegações, a Principal Claritas possui um canal de comunicação confidencial e anônimo, onde qualquer pessoa está autorizada a entrar em contato para submeter questões referentes a esses assuntos, que pode ser acessado pelo link: http://www.claritas.com.br/canal-de-denuncias/. Você ainda pode utilizar o canal de denúncias disponível no link: https://app.compliasset.com/claritasinvestimentos

Existe também o canal de denúncia da Principal onde é possível comunicar qualquer fato que possa vir estar em desacordo com o manual sem se identificar. Tal canal pode ser acessado através do link: https://pfgethicshelpline.tnwreports.com/?lang=en-US

15. Retaliação

Existem proteções legais contra retaliação. A Principal Claritas confirma sua política de longa data contra retaliação para reporte de qualquer tipo de suspeita de conduta infratora ou antiética quando feita de boa-fé. Nenhum acordo de confidencialidade assinado com a empresa deverá proibir qualquer divulgação de informação confidencial ou interna para um regulador conforme exigido ou permitido pela lei.

16. Responsabilidade

A área de Compliance é responsável pelo armazenamento, revisão e atualização deste manual, bem como de sua divulgação aos Colaboradores da empresa.

A atualização do manual poderá ser feita sempre que necessário ou quando houver alteração regulatória, não podendo ultrapassar o prazo de dois anos.

Todos os Colaboradores têm a responsabilidade final de aderir a estas políticas. Os Colaboradores são incentivados a contatar a área de Compliance e/ou seu gestor se eles tiverem dúvidas ou suspeitas em relação ao conteúdo do manual.

Anexo A

Termo de Recebimento e Adesão ao Manual de Compliance

Eu, _____, inscrito(a) no CPF/MF sob o nº _____, na qualidade de _____ (cargo) da Principal Claritas, pelo presente instrumento, atesto que recebi, li e entendi o Manual de *Compliance* da Principal Claritas ("Manual") e confirmo que tenho conhecimento integral de todas as Políticas e procedimentos aqui constantes.

Comprometo-me a cumpri-lo integralmente, confirmando minha ciência acerca das sanções aplicáveis a cada um dos casos de violação das Políticas constantes deste Manual.

Estou ciente do meu compromisso de comunicar a Área de *Compliance* e Risco da Principal Claritas qualquer situação que chegue ao meu conhecimento que esteja em desacordo com as regras definidas neste Manual.

Data:

Assinatura:

Anexo B

Termo de Confidencialidade

Eu, nome, portadora da cédula de RG n° xxx, inscrito no CPF n° xxx, assumo o compromisso de manter a confidencialidade e sigilo sobre todas as informações relacionadas ao cargo, função ou atividade que exercer na Claritas Administração de Recursos Ltda. ("Principal Claritas").

Por este termo de confidencialidade e sigilo comprometo-me:

1. A não utilizar as informações confidenciais a que tiver acesso, para gerar benefício próprio exclusivo e/ou unilateral, presente ou futuro, ou para o uso de terceiros;
2. A não efetuar nenhuma gravação ou cópia da documentação confidencial a que tiver acesso;
3. A não apropriar-se para si ou para outrem de material confidencial e/ou sigiloso da tecnologia que venha a ser disponível;
4. A não repassar o conhecimento das informações confidenciais, responsabilizando-se por todas as pessoas que vierem a ter acesso às informações.

Por Informações Confidenciais entende-se quaisquer dados, conhecimentos e/ou informações obtidos em razão das atividades exercidas, incluindo, mas sem limitação a qualquer documento, informações relativa a números financeiros e/ou contábeis, estratégias, planos de ação, planos de negócios, know-how, desenhos, folhas de dados, relatórios, exemplos, materiais, componentes e/ou métodos, que sejam revelados, fornecidos ou comunicados (seja verbalmente ou por escrito, em forma eletrônica, textos, rascunhos, desenhos, gráficos, projetos ou por qualquer outra forma) pela Principal Claritas ao colaborador. Todas as anotações, análises, compilações, estudos e demais documentos elaborados pelo colaborador com base em Informações Confidenciais serão também considerados "Informações Confidenciais".

A vigência da obrigação de confidencialidade e sigilo, assumida pela minha pessoa por meio deste termo, terá a validade enquanto a informação não for tornada de conhecimento público por qualquer outra pessoa, ou mediante autorização escrita, concedida à minha pessoa pelas partes interessadas neste termo.

Data:
Assinatura: