POLÍTICA DE REGRAS, PROCEDIMENTOS E CONTROLES INTERNOS

Reliance Serviços Financeiros Ltda. e/ou da **Reliance Serviços Internacionais Ltda.**

Sumário

APRESENTAÇÃO E APLICABILIDADE

A Reliance é uma empresa de consultoria de investimentos que atua nos mercados doméstico e internacional, por intermédio, respectivamente, da **RELIANCE SERVICOS FINANCEIROS LTDA**, inscrita no CNPJ/MF sob o nº 02.647.198/0001.25 e da **RELIANCE SERVIÇOS INTERNACIONAIS LTDA.**, inscrita no CNPJ/MF sob o nº 24.129.548/0001.02 (ambas consideradas, simplesmente, "Reliance"), cuja principal ferramenta é a capacidade de unir conhecimento e experiência no mercado financeiro, com o intuito de compreender as necessidades de seus clientes, o que permite criar sugestões de investimentos compatíveis com as necessidades de cada cliente no curto, médio e longo prazo.

Esta Política de Regras, Procedimentos e Controles Internos ("Política") tem por objetivo estabelecer regras, procedimentos e descrição dos controles a serem observados para o fortalecimento e funcionamento dos sistemas de controles internos das duas empresas de consultoria supracitadas, e servirá de referência para todos aqueles que possuam cargo, função, posição, relação societária, empregatícia, de estágio, comercial, profissional, contratual ou de confiança com a Reliance ("Colaboradores"), tanto na sua atuação interna quanto na sua comunicação com os diversos públicos externos, principalmente aqueles Colaboradores que possam vir a ter acesso a Informações Confidenciais, conforme definição trazida pelo Código de Ética e Conduta da Reliance.

Além disso, esta Política foi elaborada em conformidade com o disposto na Instrução CVM nº 592, de 17 de novembro de 2017 e alterações posteriores ("ICVM 592").

Atuando com transparência, a Reliance manterá versões atualizadas desta Política em seu website (https://www.reliance.com.br/index.html), juntamente com os demais documentos exigidos pela regulamentação vigente.

COMPLIANCE E SISTEMA DE CONTROLES INTERNOS

Na Reliance o controle e monitoramento no que se refere ao cumprimento das regras e procedimentos internos e especificamente da Política de Prevenção e Combate à Lavagem de Dinheiro é de responsabilidade da área de Compliance, que é liderada pela Diretora de Compliance, representada na figura da Sra. Renata Silveira.

A Diretoria de Compliance tem como função assegurar o cumprimento das regras, políticas e procedimentos internos, assim como adequação dos procedimentos internos às leis e regulamentação aplicáveis pela CVM, e demais órgãos ou entidade de autorregulação. A Diretora de Compliance tem a responsabilidade de divulgar e treinar continuamente os Colaboradores para garantir a adequação, fortalecimento e o funcionamento do sistema de controles internos da Reliance e a constante avaliação e revisão dos procedimentos internos a fim de minimizar preventivamente eventuais riscos operacionais, potenciais situação de conflitos de interesse, falhas de segurança, o uso inadequado de autoridade e qualquer outro descumprimento ao Código de Ética e de Conduta e demais políticas internas.

Cabe à Diretora de Compliance a observação de toda regulamentação pertinente aos serviços de consultoria de valores mobiliários, bem como a responsabilidade de atualizações das políticas internas e do Código de Ética e Conduta, nos termos da regulamentação vigente.

Os Colaboradores estão obrigados a comunicar à Diretora de Compliance, mesmo que meramente suspeitas, todas as situações, comportamentos ou operações que possam de alguma forma violar as regras e políticas internas ou o Código de Ética e Conduta da Reliance.

É obrigatória a adesão formal de todos os Colaboradores à presente Política. Para tanto, todos os Colaboradores aderem à esta Política assinando o Termo de Compromisso, Responsabilidade e Confidencialidade constante do Anexo I ao Código de Ética e Conduta da Reliance.

Periodicamente, poderá ser requisitado aos Colaboradores que assinem novos Termos de Compromisso, Responsabilidade e Confidencialidade, reforçando o conhecimento e concordância com os termos desta Política e do Código de Ética e Conduta.

a) Monitoramento

As áreas de serviços, administrativa e de tecnologia realizam rotinas de controle de processos específicos de acordo com as políticas internas, tais como:

- Política de Prevenção e Combate à Lavagem de dinheiro (PLD), Cadastro, KYC (perfil) e Suitability:
    - Controle de Vencimentos para processo de PLD a cada 24 meses:
    - Ficha Cadastral, Suitability, Perfil do Cliente, Cartão de Assinatura e Vencimentos de documentos.
    - Desenquadramentos dos Suitabilitys;
- Formalização de Serviços com clientes:
    - Controle de pendências Contrato de Consultoria de Valores Mobiliários;
    - Controle do envio de Relatórios de Remuneração, quando aplicável;

- Política de Segurança e de Segurança da Informação:
    - Controle de Acessos
    - Monitoramento de Mensagens eletrônicas
    - Teste de Plano de Contingência de Negócios (PCN)

- Código de Ética e Conduta:
    - Controle dos Termos de Adesão do Colaborador

- Política de Investimentos Pessoais
    - Suitability/Formulário de Investimentos Pessoais

- Certificação:
    - Controle sobre Certificação (cadastro, atualização e vencimentos).

1) POLÍTICA DE SEGURANÇA DA INFORMAÇÃO.

A política de segurança tem como objetivo estabelecer regras e procedimentos do uso dos ativos e dos recursos da Reliance visando minimizar os riscos operacionais e estabelecer padrões para a utilização de informações pela Reliance.

A política contém os critérios e procedimentos para a gestão dos bens de informação da Reliance, contemplando:

- Controle dos bens de informação;
- Controle de Acesso;
- Avaliação, homologação e utilização de hardwares e softwares;
- Aspectos de segurança;
- Comunicação

É de suma importância que cada Colaborador observe e siga a política e procedimento e orientações estabelecidas a seguir:

a) Backup

Todos os backups da Reliance devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Os Colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros. As mídias de backup (como DAT, DLT, LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e distantes o máximo possível do datacenter.

As fitas de backup devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, e de preferência com etiquetas não manuscritas.

O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.

É necessária a previsão, em orçamento anual, da renovação das mídias em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial. Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas.

É necessário que seja inserido, periodicamente, o dispositivo de limpeza nas unidades de backup, nos termos da planilha de controle de mídias.

As mídias de backups históricos ou especiais deverão ser armazenadas em instalações seguras, preferencialmente com estrutura de sala-cofre, distante no mínimo 10 quilômetros da Reliance.

Os backups imprescindíveis, críticos, para o bom funcionamento dos negócios da Reliance, exigem uma regra de retenção especial, seguindo assim as determinações fiscais e legais existentes no país.

Na situação de erro de backup e/ou *restore* é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser autorizados apenas mediante justificativa formal da área de TI.

Quaisquer atrasos na execução de backup ou *restore* deverão ser informados e justificados para o gerente responsável pela área de TI.

Testes de restauração (*restore*) de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do backup.

Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

Para formalizar o controle de execução de backups e *restores*, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado pelo gerente de TI da Reliance.

Os colaboradores responsáveis descritos nos devidos procedimentos e na planilha de responsabilidade poderão delegar a um custodiante a tarefa operacional quando, não puderem operacionalizar. Contudo, o custodiante não poderá se eximir da responsabilidade do processo.

b) Correio Eletrônico

O uso do correio eletrônico do Reliance é para fins corporativos e relacionados às atividades do Colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique a Reliance e também não cause impacto no tráfego da rede.

Acrescentamos que é proibido aos Colaboradores o uso do correio eletrônico:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da Reliance;
- Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a Reliance ou suas unidades vulneráveis a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- Apagar mensagens pertinentes de correio eletrônico visando eliminar evidencia de possíveis erros;
- Produzir, transmitir ou divulgar mensagem que: (i) contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Reliance; (ii) contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador; (iii) vise obter acesso não autorizado a outro computador, servidor ou rede; (iv) vise

interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado; (v) vise burlar qualquer sistema de segurança; (vi) vise vigiar secretamente ou assediar outro usuário; (vii) vise acessar informações confidenciais sem explícita autorização do proprietário; (viii) vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa; (ix) tenha conteúdo considerado impróprio, obsceno ou ilegal; (x) seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros; (xi) contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas; (xii) tenha fins políticos locais ou do país (propaganda política); (xiii) inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato: Nome do colaborador; nome da empresa; telefone(s); correio eletrônico; monitoramento do correio eletrônico pela equipe de TI.

c) Computadores e Recursos Tecnológicos

Os equipamentos disponíveis aos Colaboradores são de propriedade da Reliance, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as eventuais recomendações operacionais fornecidas internamente, as quais serão devidamente formalizadas.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico da área de TI da Reliance.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar a área de TI.

Arquivos pessoais e/ou não pertinentes ao negócio da Reliance (fotos, músicas, vídeos, etc..) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos Colaboradores deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os Colaboradores da Reliance detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da área de ti da Reliance.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas:

- Todos os computadores de uso individual deverão ter senha de Bios para restringir o acesso de Colaboradores não autorizados. Tais senhas serão definidas pela Área de TI da Reliance, que terá acesso a elas para manutenção dos equipamentos.
- Colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador.
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico TI da Reliance ou por terceiros devidamente contratados para o serviço.
- O usuário, sempre que se ausentar da estação de trabalho deve bloqueá-la para impedir o acesso não autorizado.

d) Do Monitoramento e da Auditoria do Ambiente

Para garantir a segurança e o bom funcionamento dos sistemas, a área de TI da Reliance poderá:

- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet e outros componentes da rede – a informação

gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

- Tornar acessível as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de solicitação formal por parte da Diretora de Compliance;
- Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

e) Contas de Acesso e Senhas

Criação de Contas de Acesso

A solicitação para criação de uma nova conta de acesso à rede da Reliance deve seguir as seguintes condições:

- Todo cadastramento de conta de acesso à rede da Reliance deve ser efetuado mediante solicitação formal, sob a aprovação da Diretora de Compliance.
- As solicitações relativas à criação de cada conta devem ser mantidas registradas e armazenadas de forma segura pela área de TI;
- Todos os usuários devem assinar um termo de responsabilidade pela utilização da conta de acesso.
- A nomenclatura das contas de acesso de usuários deve seguir padrão definido pela Reliance, nome.sobrenome;

Exclusão e Bloqueio de Contas de Acesso

A solicitação para exclusão / bloqueio de conta de acesso à rede da Reliance deve seguir as seguintes condições:

- Toda exclusão ou bloqueio de conta de acesso à rede da Reliance deve ser efetuado mediante solicitação formal, sob a aprovação da Diretora de Compliance.
- A exclusão da conta de acesso do usuário deve ser solicitada caso haja: falecimento; aposentadoria; outros afastamentos que caracterizem encerramento do vínculo com a instituição. O RH da Reliance deverá informar no prazo máximo de

até três dias úteis, os desligamentos, as aposentadorias, os afastamentos e as movimentações de usuários.

Senha de usuários comuns

Todas as senhas, de usuários comuns, para autenticação na rede da Reliance devem seguir os seguintes critérios mínimos:

- Toda senha deve ser constituída de, no mínimo, 8 caracteres sendo obrigatório o uso de caracteres alfanuméricos (com letras maiúsculas e minúsculas e número);
- A senha não poderá conter parte do nome do usuário, por exemplo: se o usuário chama-se Jose da Silva, sua senha não pode conter partes do nome como "1221jose" ou "1212silv";
- A data de expiração da senha deve ser de no máximo 90 dias, caso não seja alterada, esta será bloqueada;
- É obrigatória a troca de senha ao efetuar o primeiro logon;
- É proibida a repetição das 3 últimas senhas já utilizadas.

Senha de Administradores locais e administradores

Todas as senhas, de administradores locais e administradores de domínio, para autenticação na rede da Reliance devem seguir os seguintes critérios mínimos:

- Toda senha deve ser constituída de, no mínimo, 10 caracteres sendo obrigatório o uso de caracteres alfanuméricos (com letras maiúsculas, minúsculas e números) e caracteres especiais;
- A senha não poderá conter parte do nome do usuário, por exemplo: se o usuário chama-se Jose da Silva, sua senha não pode conter partes do nome como "12$@joseSI" ou "12$@JOsilv";
- A data de expiração da senha deve ser de no máximo 60 dias, caso não seja alterada, esta será bloqueada; É obrigatória a troca de senha ao efetuar o primeiro logon;
- É proibida a repetição das 7 últimas senhas já utilizadas.

Utilização de Contas de Acesso e Senhas

A conta de acesso é o instrumento para identificação do usuário na rede Reliance e caracteriza-se por ser de uso individual e intransferível e sua divulgação é vedada sob qualquer hipótese.

Qualquer utilização, por meio da identificação e da senha de acesso, é de responsabilidade do usuário aos quais as informações estão vinculadas.

As contas de administradores locais das estações de trabalho ou de servidores de rede só devem ser utilizadas quando estritamente necessário.

As contas de serviços utilizadas em servidores de rede, backup, correio eletrônico, banco de dados, aplicações, entre outros, devem ser utilizadas somente para execução de ações ligadas à sua natureza, de forma automática, sem intervenção manual através de logon/acesso.

As contas com privilégio de administração de rede devem ser utilizadas somente para execução das atividades correspondentes à administração do ambiente conforme as responsabilidades atribuídas, em equipamentos previamente definidos. As variáveis necessárias para acesso e administração devem ser de conhecimento restrito aos administradores dos equipamentos de rede e chefia respectiva.

f) Internet

A Reliance, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos à internet.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da Reliance, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

Os colaboradores não poderão em hipótese alguma utilizar os recursos da Reliance para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

Os colaboradores não poderão utilizar os recursos do Reliance para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

g) Testes Periódicos

Periodicamente, a Reliance realiza testes de segurança em todo o seu sistema de informação. Dentre as medidas, incluem-se, mas não se limitam:

(i) Verificação do Login dos Colaboradores;
(ii) Alteração das senha de acesso dos Colaboradores, observadas as diretrizes constantes na seção “Contas de Acesso e Senhas” da presente política;
(iii) Testes no firewall;
(iv) Testes nas restrições impostas aos diretórios;
(v) Manutenção periódica de todo o “hardware” pela equipe de TI da Reliance;
(vi) Testes no “back-up” (salvamento de informações), observadas as diretrizes constantes da seção “Backup” da presente política.

2) PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN)

O Plano de Continuidade de Negócios da Reliance – aplicável para todas as empresas mencionadas no referido documento - tem como objetivo minimizar os danos e as perdas às atividades essenciais da Reliance, desenvolvendo um conjunto de estratégias de forma a garantir que os serviços possam ser executados de forma contínua e ininterrupta durante o processo de contingencia.

A Reliance possui um plano que visa permitir que após um processo de ativação de contingência possa-se reassumir o processamento das operações críticas enquanto o processo de contingência se mantiver, conforme adiante detalhado.

Ademais, o plano prevê também as medidas tomadas em caso de saída de algum dos diretores da Reliance. Caso ocorra a situação, uma reunião extraordinária de sócios deverá ser realizada a fim de se definir o novo diretor.

Todos os procedimentos a serem adotados em caso de ativação de contingência estão descritos no Plano de Contingência da Reliance.

O Plano de Contingência é revisado anualmente pela equipe de Tecnologia da Reliance e então reenviados aos Colaboradores. Cada Colaborador chave do processo assina um termo declarando ter ciência do seu papel durante o processo de ativação de contingência.

De acordo com as definições do Plano de Contingência anualmente são revisados, testados o ambiente de contingência da Reliance pela equipe de Tecnologia da Reliance. A documentação dos testes é então enviada para a Diretoria de Compliance.

3) TREINAMENTO E CERTIFICAÇÃO

3.1 Treinamento

A Reliance incentiva o treinamento para seus Colaboradores, objetivando obter sua capacitação e desenvolvimento para aprimorar a qualidade do recurso humano no atendimento ao negócio.

Estimula-se o auto treinamento com supervisão, participação de reuniões internas, projetos e a liberdade de questionamento e esclarecimento de dúvidas no ambiente interno.

Além disso, os Colaboradores participam e realizam cursos externos de graduação (para os não graduados), pós-graduação e cursos de especialização ou de capacitação em determinados tópicos de interesse do Colaborador e da Reliance. Os superiores hierárquicos podem sugerir cursos aos Colaboradores ou o Colaborador poderá solicitá-los ao superior hierárquico. Cabe ao superior hierárquico a aprovação do curso perante a administração da

Reliance. Os cursos podem ser subsidiados integralmente ou parcialmente pela Reliance de acordo com a aprovação.

Cabe ainda a Reliance disponibilizar e custear aos seus Colaboradores a participação de programas de treinamento determinados e exigidos pela regulamentação, assim como a realização de exames de certificação requeridos para a função, conforme o caso, assim como programas validos para atualização das mesmas.

Sem prejuízo dos treinamentos técnicos supracitados, a Reliance adota uma política de treinamento contínuo dos Colaboradores, cujo objetivo é torná-los aptos a seguir todas as regras dispostas nas políticas internas da Reliance. Todos os Colaboradores receberão o devido treinamento acerca de todas as políticas e procedimentos. Assim, serão proporcionados aos Colaboradores uma visão geral das políticas internas da Reliance, de forma que os mesmos se tornem aptos a exercer suas funções aplicando conjuntamente todas as normas nelas dispostas.

Poderão ser ministradas a todos os Colaboradores da Reliance palestras internas, a fim de dar ciência sobre (i) as políticas adotadas pela Reliance; (ii) a regulamentação vigente e aplicável aos negócios da Reliance e, ainda, (iii) eventuais problemas ocorridos, sobretudo para alertar e evitar práticas que possam ferir a regulamentação vigente no exercício das atividades desenvolvidas pela Reliance. Referidas palestras serão de participação obrigatória, comprovada mediante assinatura do Colaborador em lista de presença. Não sendo possível a participação do Colaborador, sua ausência deverá ser justificada à Diretora de Compliance da Reliance, sendo certo que a ausência deverá ser reposta na data mais próxima possível.

Todo o treinamento interno proposto pela Reliance, além de enfatizar a observância das regras e da relação fiduciária com os clientes, terá como objetivo abordar os procedimentos operacionais da Reliance, especialmente no que diz respeito às informações de natureza confidencial e adoção de posturas éticas e em conformidade com os padrões estabelecidos.

Os treinamentos relacionados ao conteúdo das políticas internas da Reliance serão realizados, com periodicidade mínima anual, pela Diretora de Compliance, sendo obrigatórios a todos os Colaboradores. Quando do ingresso de um novo Colaborador, a Diretora de Compliance aplicará o devido treinamento de forma individual para o novo Colaborador.

A Diretora de Compliance poderá, ainda, conforme achar necessário, promover treinamentos esporádicos visando manter os Colaboradores constantemente atualizados em relação às políticas internas da Reliance.

Treinamentos Específicos exigidos:

- Prevenção e Combate à Lavagem de Dinheiro e Treinamento Contínuo – Todos os Colaboradores da Reliance;
- Treinamento e Certificação (que seja aceita pela ANBIMA e CVM para a atividade de consultoria de valores mobiliários);

3.2 Certificação

Conforme as diretrizes trazidas pela ICVM 592, a Reliance tomará todas as medidas para que a equipe responsável pela atividade de consultoria de valores mobiliários, seja formada por, no mínimo (i) 30% (trinta por cento) de consultores certificados ou registrados, até 31 de dezembro de 2018; (ii) 50% (cinquenta por cento) de consultores certificados ou registrados, até 30 de junho de 2019; e (iii) 80% (oitenta por cento) de consultores certificados ou registrados, até 31 de dezembro de 2019.

A não aderência do profissional aos requisitos mínimos com relação às certificações requeridas implicará no afastamento do mesmo da atividade.

Caberá ao setor de RH a identificação dos profissionais elegíveis a certificações, requerendo do Colaborador e ao seu superior imediato a certificação exigida na admissão ou na transferência a cargos que requerem certificações ou qualquer outro requisito mínimo estabelecido pelas entidades reguladoras do mercado. Deve, ainda, manter relatório de controle mensal sobre cargos, certificações e vencimentos das certificações, assim como a devida atualização e gestão dos cadastros e bancos de dados nas entidades reguladoras.

3.2.1 Procedimentos:

- **Critérios que definem as atividades elegíveis às certificações.**

Os critérios são de acordo com a área de atuação na Reliance e também de acordo com o código de certificação da ANBIMA e a própria ICVM 592. Para a área técnica (consultoria de valores mobiliários) as certificações serão exigidas na forma estabelecida pela ICVM 592, e de

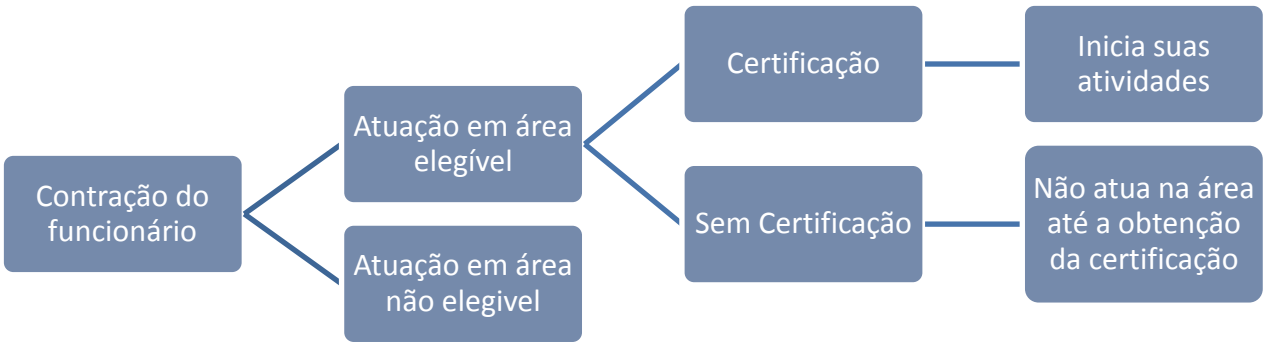
acordo com as Certificações admitidas pela CVM como válidas para o exercício da atividade de consultoria de valores mobiliários.

Independentemente da área de atuação a Reliance incentiva todos a obterem algum tipo de certificação, proporciona cursos e treinamentos e reembolsa o pagamento das despesas para isso.

- **Identificação dos profissionais certificados na admissão e no desligamento:**

A formalização das contratações e dos desligamentos de funcionários está sob responsabilidade da área administrativa, que também cuida dos registros, atualizações e desligamentos no Banco de Dados de certificação ANBIMA, o que facilita a identificação nas movimentações. Para os profissionais que mudam área é requerida a certificação, desde que venha a exercer atividades elegíveis.

Segue o fluxograma do procedimento de identificação dos profissionais na admissão:



- **Afastamento dos profissionais sem devida certificação.**

Caso o profissional elegível não esteja com a certificação vigente, de acordo com o cronograma estabelecido pela CVM para a certificação de toda a área técnica, ele é

descredenciado de suas funções até regularizar sua certificação. No entanto, a Reliance mantém um controle das atualizações das certificações conforme descrito abaixo.

- **Vigências das Certificações**

Os mecanismos utilizados pela Reliance para o controle de vencimento das certificações são:

A. Verificação periódica no site de certificação;
B. Controle em planilha excel (apenas com os funcionários certificados);
C. Agendamento via Microsoft Outlook;

Para o item C, a área administrativa envia para os profissionais o aviso no Outlook para a notificação dos vencimentos da sua Certificação. As atualizações são realizadas via curso, e utilizamos o programa de treinamento da empresa Treina Educação Corporativa.

A área administrativa acompanha se o profissional realizou ou não a atualização da certificação, e garante que este o faça dentro do prazo, através de novos avisos. Após a realização da atualização, o profissional envia o certificado à área administrativa que, por conseguinte, efetua imediatamente a atualização no banco de dados da ANBIMA.

Ademais, a área recebe da empresa Treina um relatório semanal sobre o status de atualizações dos profissionais.

- **Atualização do Banco de Dados de certificação ANBIMA:**

A manutenção do banco de dados da ANBIMA é realizada pela área administrativa e as informações são revisadas bimestralmente pela área de Compliance. Qualquer alteração é feita até o último dia do mês subsequente do acontecimento do evento.

A Reliance não inclui estagiários e prestadores de serviço no banco de dados da ANBIMA.

Procedimentos em relação aos profissionais certificados que estão em licença médica somente serão feitos caso ocorra o vencimento da certificação em seu período de licença.

4) SEGREGAÇÃO DE ATIVIDADES

O presente tópico dispõe acerca da política de segregação física de atividades da Reliance, tendo como objetivo estabelecer as regras que orientam a segregação física das instalações entre áreas responsáveis pelas atividades de consultoria das áreas responsáveis pelas atividades de administração de carteiras e distribuição de títulos e valores mobiliários.

Existe a segregação física das instalações entre as equipes envolvidas no processo de gestão de investimentos realizado pela Reliance Asset Management, para as equipes das áreas de atendimento e consultoria a clientes, bem como também existe a segregação física com relação às equipes operacionais envolvidas no processo de distribuição de fundos e/ou de outros valores mobiliários.

Equipamentos, rede e arquivos utilizados pela Reliance são organizados de modo a garantir atuação independente pelas diferentes áreas e segregação total de suas atividades. Tal organização consiste na utilização de um sistema operacional de tecnologia da informação para o controle e bloqueio de informações, a fim de preservar as informações confidenciais e permitir a identificação de pessoas que tenham acesso.

O acesso aos sistemas voltados para a consultoria de valores mobiliários é restrito, regido por perfis de acesso e controlado por senhas e registros de log.

O acesso físico aos servidores e equipamentos individuais também é controlado e restrito às pessoas autorizadas, de forma a garantir a integridade das informações e impedir o acesso de pessoas não autorizadas.

A Diretoria de Compliance controlará os acessos concedidos aos Colaboradores, e cabe ao superior hierárquico a responsabilidade pela análise da necessidade e verificação da correta utilização dos acessos e ferramentas concedidas.

5) POLÍTICA DE PREVENÇÃO À LAVAGEM OU OCULTAÇÃO DE BENS, DIREITOS E VALORES (PLD).

A “Lavagem de Dinheiro” é o nome dado aos diversos processos através dos quais é possível ocultar ou disfarçar a “identidade”, “propriedade” e “origem” do dinheiro ilegalmente obtido, a fim de que este pareça proveniente de fonte legítima.

O Diretor de Compliance será o responsável pela prevenção à lavagem ou ocultação de bens, direitos e valores (PLD).

Todas as instituições que fazem parte do sistema financeiro podem, inadvertidamente, ser usadas como intermediárias em processos de “Lavagem de Dinheiro”.

A Reliance espera que cada um dos seus Colaboradores, independentemente de sua função e ou cargo hierárquico, tenha conhecimento absoluto das regras fiscais e éticas que norteiam a prevenção à lavagem de dinheiro e, aplique-as com eficiência e eficácia, não permitindo que os negócios realizados em suas atividades estejam correndo tal risco. A Reliance emprega sempre seus maiores esforços em dotar os negócios de controles e regras eficazes para combater estas práticas.

O Colaborador, independentemente de seu cargo ou grau hierárquico, deve manter-se alerta e atento às informações que possam ser consideradas suspeitas de seus clientes e ou outros Colaboradores e sempre que observar uma possibilidade de prática de tal crime, comunicá-la de imediato ao Diretor de Compliance. Não deve revelar ao comitente ou indiciado que sua operação é suspeita de lavagem de dinheiro.

Qualquer indicio de negligência do Colaborador em relação à possibilidade de ocorrer um processo de lavagem de dinheiro nas atividades da Reliance, é considerada falta gravíssima e, portanto, sujeito a penalidades, inclusive de atribuir-lhe a responsabilidade de cometimento de crime de lavagem de dinheiro.

Os Colaboradores estão obrigados a comunicar à administração, mesmo que meramente suspeitadas, as seguintes informações e/ou operações que tomem conhecimento durante a prestação do serviço de consultoria, envolvendo operações financeiras:

- Cujos valores se afigurem incompatíveis com a ocupação profissional, rendimentos e/ou à situação patrimonial / financeira de qualquer das partes envolvidas, tomando-se por base, as informações cadastrais respectivas;
- Realizadas repetidamente entre as mesmas partes, nas quais hajam seguidos ganhos ou perdas no que se refere a algum dos envolvidos;
- Que evidenciem oscilação significativa em relação ao volume e/ou frequência de negócios de qualquer das partes envolvidas;
- Cujos desdobramentos contemplem características que possam constituir artifício para burla da identificação dos efetivos envolvidos e/ou respectivos beneficiários;
- Cujas características e/ou desdobramentos evidenciem atuação, de forma persistente, em nome de terceiros;
- Que evidenciem mudança repentina e objetivamente injustificada, relativamente às modalidades operacionais usualmente utilizadas pelos envolvidos; e
- Desvio de operações / clientes para outras instituições financeiras, de forma a lesar os interesses da Reliance.

a) Conheça seu Cliente / KYC

A Reliance adota um conjunto de regras e procedimentos internos com o objetivo de conhecer seu cliente, buscando identificar e conhecer a origem e a constituição do patrimônio e dos recursos financeiros destes.

Sendo assim, em atendimento com as boas práticas de mercado, e a fim de assegurar a conformidade com a legislação e a regulamentação que disciplinam a prevenção e o combate à lavagem de dinheiro e ao financiamento ao terrorismo, a Reliance realiza o processo de “Conheça seu Cliente”. Este processo está descrito no Manual de KYC (Conheça seu Cliente) e será abordado também adiante, no capítulo que trata de Suitabilty.

Para isso, é imprescindível que os Colaboradores conheçam o cliente e cumpram com todas as etapas previstas no Manual de KYC (Conheça seu Cliente) e de Suitabilty. Antes de iniciar suas operações na Reliance o Cliente deverá fornecer todas as informações cadastrais solicitadas, mediante o preenchimento da ficha cadastral e a entrega de documentos conforme a regulamentação vigente. Os procedimentos de KYC da Reliance exigem a identificação adequada de cada Cliente.

A Reliance também mantem processos diferenciados de análise e monitoramento em relação à manutenção de relacionamento com Politicamente Expostas e clientes de Alto Risco (que estão incluídos em grupos que representam vulnerabilidade à lavagem de dinheiro).

6) POLÍTICA DE ANTICORRUPÇÃO

A Reliance, comprometida com as normas legais, adota medidas anticorrupção, de acordo com o previsto na Lei 12.846.

A Lei 12.846, de 1º de agosto de 2013, que entrou em vigor em 29 de janeiro de 2014, dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências.

De acordo com esta lei, a responsabilidade administrativa e civil das empresas pela prática de atos lesivos à administração pública será objetiva, isto é, independente da apuração de culpa.

É imperativo que cada um dos Colaboradores, independente da sua função e/ou cargo hierárquico, tenha conhecimento absoluto da lei anticorrupção, ainda, todos eles devem aderir e assinar o Termo de Confidencialidade que inclui a cláusula de ciência e procedimentos previstos na lei.

Assim, a Reliance adota medidas a fim de assegurar o cumprimento dos previstos na lei anticorrupção, de modo que não tolera em suas atividades o ato de oferecer, prometer ou autorizar que se dê qualquer bem ou valor a agentes públicos, ou de funcionários de empresas do setor privado, diretamente ou por intermédio de terceiros, a fim de influenciar a ação de tais agentes ou funcionários para obter vantagens impróprias, como também, o descumprimento das normas da legislação anticorrupção, sob pena de rescisão contratual por justa causa, sem prejuízos de eventuais medidas judiciais que sejam cabíveis.

7) SUMÁRIO DE POLÍTICAS E MANUAIS RELIANCE

Este sumário sintetiza todas as políticas e manuais internos adotados pelas empresas integrantes do grupo econômico da Reliance, aplicáveis de acordo com o segmento da empresa

a. Políticas

- Política de Controles Internos – Última revisão: Novembro/2018 (disponível em www.reliance.com.br)
- Política de Investimentos Pessoais – Última revisão: Novembro/2018 (disponível em www.reliance.com.br)
- Plano de Contingência – Última revisão: Novembro/2018 (arquivos internos).
- Código de Ética e Conduta – Última revisão: Novembro/2018 (disponível em www.reliance.com.br)

b. Manuais

- Manual de Suitability – Última revisão: Novembro /2018 (arquivos internos).
- Manual de Cadastramento de Clientes – Última revisão: Maio/2013 (arquivos internos).
- Manual Conheça seu Cliente – KYC – Última revisão: Outubro/2013 (arquivos internos).
- Manual de Procedimentos Administrativos – Última revisão: Novembro/2013 (arquivos internos).

8) DÚVIDAS

As dúvidas sobre os aspectos abordados ou questões não previstas neste documento poderão ser esclarecidas com o uso do discernimento do que é certo, com base nos padrões aqui descritos ou, ainda, junto a seu superior hierárquico ou Diretora de Compliance.

ANEXO I

QUESTIONÁRIO DE SUITABILITY

(“Questionário”)

ANEXO II

TERMO DE CIÊNCIA DE DESENQUADRAMENTO

NOME DO CLIENTE: _____

CPF/MF OU CNPJ/MF: _____

Prezado Cliente,

Ao datar e assinar esta declaração, você terá confirmado ter plena ciência de que as recomendações de investimento que pretende receber da **Reliance Serviços Financeiros Ltda..** e/ou da **Reliance Serviços Internacionais Ltda** podem não ser compatíveis com seu perfil de investidor e, portanto, apresentam maiores riscos do que os investimentos mais conservadores adequados a seu perfil.

[Local], [==] de [==] de 20[==].

_____

Nome:

CPF ou CNPJ: