Manual de Compliance

Outubro de 2020

1. Introdução
2. Função de Compliance
3. Gestão de Riscos
4. Exercício da atividade de administração de carteiras
5. Sigilo das informações
6. Informações privilegiadas
7. Política de Rateio de Ordens
8. Política de compra e venda de valores mobiliários
9. Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo
10. Órgãos reguladores e autorreguladores
11. Treinamento
12. Segurança da Informação
13. Matriz de Segregação
14. Uso de senhas
15. Manutenção de arquivos

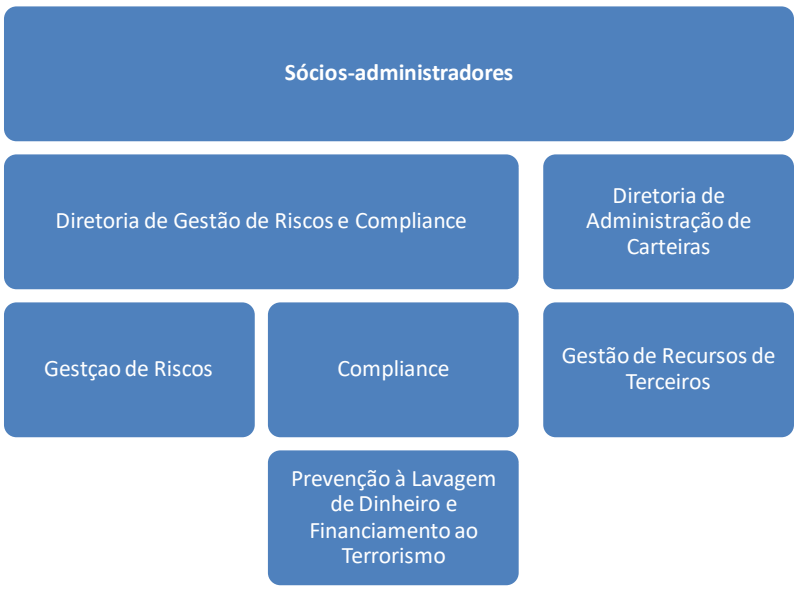
1. Introdução

A Solidus Administração de Patrimônio Ltda, "SAP" é uma gestora de recursos de terceiros, com sede em Porto Alegre, especializada em investimentos em ações, com foco na análise fundamentalista.

Os fundos, clubes de investimentos e carteiras de pessoas físicas ou jurídicas, "Carteiras Administradas" sob gestão da SAP possuem uma gestão ativa, buscando retornos de longo prazo acima do índice de referência (Ibovespa).

Atua também na gestão de fundos de renda fixa e multimercados, buscando investimentos diretos e em fundos de outras gestoras criteriosamente selecionadas, objetivando retorno consistente para seus cotistas.

A estrutura da SAP está assim organizada:



2. Função de Compliance

Estar em Compliance é estar em conformidade com preceitos éticos e legais inerentes a atividade desempenhada, atuando de forma a manter íntegros os bens tangíveis e intangíveis da empresa.

É função da área de Compliance, mas obrigação de todos que se façam cumprir todas as normas cabíveis, com o intuito de mitigar toda exposição aos riscos inerentes à atividade de administração de carteira, principalmente riscos legais e de imagem.

Para garantir o cumprimento de todas as atividades em acordo com o determinado neste Manual e demais políticas aplicáveis à empresa, a área de Compliance executa testes e faz verificações periódicas, atuando fortemente junto aos colaboradores e executando as seguintes atividades:

- Análise dos controles previstos nos manuais, políticas e normas vigentes, propondo a criação de novos controles e melhorias naqueles considerados deficientes e monitorar as correções das eventuais deficiências;
- Acompanhamento do desenvolvimento das atividades voltadas para o estabelecimento de novos normativos, cuidando para que os mesmos definam claramente as responsabilidades de cada área, bem como estabeleçam os pontos de controle dos riscos;
- Intermediação do relacionamento entre as áreas, resultante de pontos divergentes para o estabelecimento de conformidade;
- Determinação da adequada segregação de funções e separação de responsabilidades, orientando o controle das atividades para evitar o conflito de interesses e para evidenciar pontos de controle;
- Monitoramento permanentemente do cumprimento das políticas, regras, normas, procedimentos e legislação que regulam os negócios, auxiliando na implementação dos mesmos, assegurando sempre a preservação da imagem da instituição perante o mercado de modo geral;
- Garantia da existência e divulgação das informações para a gestão dos riscos relacionados aos negócios da empresa;
- Atuação como ponto de contato junto ao BACEN, CVM, ANBIMA, auditorias externas entre outras;
- Reporte à Diretoria, quanto às medidas adotadas ou impasses para a implementação de alterações.
- Implementação e fiscalização do cumprimento pelos colaboradores do Manual de Compliance e outras políticas, especialmente ao que se refere ao sigilo das informações;
- Elaboração semestral de relatório de avaliação das atividades e identificação de inconformidades e reporte à Diretoria da empresa, com a devida disponibilidade do conteúdo à CVM;
- Realização de ações corretivas para descobrir deficiências;
- Avaliação diária dos relatórios emitidos pelos sistemas que monitoram a gestão de risco, prevenção de lavagem de dinheiro, desenquadramentos previstos na legislação entre outros;
- Agendamento e apresentação dos resultados do monitoramento diário dos testes realizados na Reunião Mensal dos Comitês de Gestão de Riscos, Compliance e Prevenção à Lavagem de Dinheiro.

3. Gestão de Riscos

Os riscos inerentes à atividade e também os procedimentos para monitoramento e mitigação, são definidos em manual próprio, com a definição de responsabilidades, conforme organograma.

4. Exercício da atividade de administração de carteiras

A administração de carteiras é assim definida na Instrução CVM nº 558/2015:

"É o exercício profissional de atividades relacionadas, direta ou indiretamente, ao funcionamento, à manutenção e à gestão de uma carteira de valores mobiliários, incluindo a aplicação de recursos financeiros no mercado de valores mobiliários por conta do investidor."

No exercício desta atividade, o administrador de carteira de valores mobiliários deve pautar sua conduta da seguinte forma:

- Agir com boa fé, transparência, diligência e lealdade em relação aos seus clientes;
- Buscar atender os objetivos de investimento de seus clientes;
- Evitar práticas que possam ferir a relação fiduciária mantida com seus clientes;
- Cumprir fielmente e fazer cumprir as políticas, diretrizes e cláusulas previstas nos regulamentos, estatutos e contratos firmados com os clientes;
- Manter em perfeita ordem e de forma atualizada as informações relacionadas às operações realizadas e demais documentos gerados em função do exercício de sua atividade, disponibilizando aos clientes, sempre que solicitado;
- Transferir às carteiras quaisquer benefícios ou vantagens alcançados em razão da sua condição de administração de carteiras de valores mobiliários, observada exceção específica para fundos de investimentos;
- Estabelecer em contrato específico, as suas obrigações e direitos; e
- Informar à CVM, a ocorrência de violações à legislação em até 10 (dez) dias úteis da identificação da ocorrência.

Ao administrador de carteira é vedado:

- Atuar como contraparte, direta ou indiretamente, em negócios com carteira que administre, exceto quando houver autorização prévia, por escrito ou previsão no regulamento dos fundos de investimento e quando não tiver poder discricionário sobre a carteira, mesmo que formalmente contratado.
- Modificar as características dos serviços prestados sem formalização;
- Garantir níveis de rentabilidade ou prometer retorno futuro das carteiras administradas;
- Contrair ou efetuar empréstimos em nome dos seus clientes, exceto nos casos de colocação de ativos em garantia de operações das próprias carteiras e o empréstimo de títulos, usando os sistemas autorizados pelo Banco Central do Brasil e CVM;
- Prestar fiança, aval, aceite ou coobrigar-se de qualquer forma em relação aos ativos administrados;
- Negociar os valores mobiliários das carteiras que administra com a finalidade de gerar receitas de corretagem ou rebates que favoreçam a si ou a terceiros; e
- Negligenciar a defesa dos direitos e interesses dos clientes.

4.1 Comitê de Investimentos

O Comitê de Investimentos, constituído para auxiliar na tomada de decisões relativas à gestão de recursos, deve observar os deveres e vedações previstos no item 3.

4.2. Segregação de Funções (Chinese Wall):

A Solidus Administração de Patrimônio, “SAP” possui controle comum à Solidus S/A CCVM, “Solidus”, sendo estas empresas ligadas, mas que atuam de forma segregada e com atividades bem definidas em seus respectivos manuais e políticas.

A administração de carteira de valores mobiliários, segmento gestão de recursos, está totalmente segregada das demais funções da Solidus.

A gestão dos recursos das Carteiras Administradas Pessoas Físicas e Jurídicas, Clubes e Fundos de Investimentos, designados “Carteiras Administradas” é realizada pela SAP e as atividades de controles, compliance, prevenção à lavagem de dinheiro e gestão de riscos são realizadas e monitoradas em conjunto com a Solidus, administradora fiduciária das Carteiras Administradas, sendo a estrutura e diretoria destas atividades compartilhadas entre si, conforme facultado pela legislação vigente.

As instalações da SAP são segregadas fisicamente das demais áreas da Solidus. Os sistemas utilizados pela área de gestão são acessados através do uso de senhas e o acesso à sede da empresa é controlado, sendo autorizada a entrada apenas a pessoas ligadas à atividade de gestão de recursos, risco e Compliance.

Os relatórios e estudos produzidos são de uso exclusivo das pessoas envolvidas na área de gestão.

5. Sigilo das informações

Os colaboradores devem zelar pela confidencialidade de quaisquer informações a que tiverem acesso, que tenham obtido ou tomado conhecimento em função das atividades que desempenham ou desempenharam para a SAP, por prazo indeterminado.

Não deve ser transmitida nenhuma informação relativa às operações em andamento ou informações recebidas de pessoas que sejam especialistas em mercado financeiro, cuja publicidade possa influenciar o mercado.

Todos os papéis e documentação relacionados à empresa e seus clientes deverão ser mantidos em local seguro, de modo a minimizar o risco de que pessoas não autorizadas venham a ter acesso a informações confidenciais.

Relatórios envolvendo posição das Carteiras Administradas são confidenciais e aqueles que não ficam arquivados são destruídos. Os colaboradores são constantemente alertados quanto à necessidade de sigilo das informações as quais tenham acesso.

Os colaboradores não estão autorizados a discutir informações confidenciais em locais públicos ou através de telefone celular ou viva-voz.

De acordo com a legislação brasileira, a divulgação de informações confidenciais ou privilegiadas causando danos a outrem, constitui crimes tipificados nos artigos 153, 154 do Código Penal e artigo 12 da Lei nº 7.492/86 e na Lei Complementar nº 105.

6. Informações privilegiadas

É vedado aos colaboradores da SAP qualquer tipo de operação no mercado financeiro que seja realizada de posse de informação privilegiada.

Por informação privilegiada, entende-se qualquer informação que não tenha sido divulgada ao público em geral e que tenha caráter relevante (informação material).

Os colaboradores que detiverem qualquer informação privilegiada obtida no exercício de suas atividades estão estritamente proibidos de divulgá-la a pessoas não relacionadas às suas atividades na SAP.

7. Política de Rateio de Ordens

A gestora, por ser titular de Conta Máster, que possibilita a negociação de grandes lotes de ativos nos ambientes de negociação, possui um sistema que possibilita o rateio das quantidades negociadas em benefício das Carteiras Administradas.

Os critérios de divisão foram previamente estabelecidos e são equitativos, impossibilitando o favorecimento de quaisquer carteiras em detrimento às outras.

Para isso é utilizada planilha eletrônica, que contém as informações da carteira de ativos, composição do caixa disponível e seus devidos passivos.

O rateio é feito ao final do pregão, na fase de especificação das operações, através do envio de arquivo com o resultado das divisões para a corretora em que se realizaram as operações.

7.1 Objetivos

A Política de Rateio busca alcançar os seguintes objetivos:

- Efetuar a divisão das operações de valores mobiliários de forma a equilibrar o percentual investido em relação ao patrimônio total das carteiras administradas;
- Alocar os ativos negociados nas carteiras a preços médios iguais;
- Balancear a composição das carteiras segundo a estratégia definida pelo gestor para cada carteira administrada;
- Respeitar as restrições impostas pelo Regulamento, Estatuto e Contrato de cada carteira, especialmente o que se refere a operações com derivativos, Day trades, composição e concentração;
- Ratear os custos com as operações de forma equitativa;

7.2 Diretrizes que norteiam o rateio

As posições por ativo de cada carteira devem ser analisadas previamente, validando as estratégias definidas pelo gestor e as necessidades de rebalanceamento das carteiras em função das estratégias de cada uma.

O sistema que define os rateios deve ser automatizado e utilizar fórmulas previamente parametrizadas.

Se o gestor operar em mais de uma corretora, o rateio deve ser realizado por instituição, considerando o preço médio e as quantidades;

Os totais das operações realizadas no dia devem ser enviadas pelas corretoras e recebidas pelo gestor.

7.3 Procedimentos do rateio

7.3.1 Operações com ativos que já compõem a carteira

O gestor, através do sistema de rateio de ordens, atualiza os dados das carteiras administradas e realiza uma pesquisa naquelas que já têm o ativo a ser negociado.

No sistema, o gestor informa o percentual definido por ação dentro da sua estratégia de gestão, que calcula as quantidades necessárias a serem compradas ou vendidas. Somadas as quantidades de todas as carteiras, fecha-se o lote do ativo, objeto da ordem a ser passada para a mesa de operações da Corretora, em nome da Conta Máster.

O gestor, através do terminal de consulta à sessão de negociação, acompanha a execução da ordem global.

Após a execução da ordem, o gestor encaminha o rateio por e-mail com o código das carteiras e a quantidade definida para cada uma.

Nos casos da ordem não ser executada de forma completa, devido às condições de mercado, a quantidade executada é rateada proporcionalmente entre as carteiras administradas.

Além da definição das quantidades a serem negociadas para cada carteira, o gestor analisa através deste sistema, as liquidações em andamento e o caixa disponível para cada uma, com o intuito de não haver insuficiência de recursos para honrar suas liquidações.

7.3.2 Operações com ativos que não compõem as carteiras

O gestor, através do sistema analisa o patrimônio de cada carteira, o percentual comprado e o caixa disponível, já considerando as liquidações futuras, e registra o percentual a comprar de um novo ativo. O sistema fornece a quantidade por carteira e a soma que resulta no lote a ser negociado através da Conta Máster.

A realização da ordem é acompanhada pelo gestor e se não for executada de forma completa, as quantidades são atribuídas proporcionalmente às carteiras administradas.

Para a negociação de opções, que a liquidação é D+1, as carteiras administradas são analisadas individualmente para verificar o caixa disponível.

Para todos os casos de rateio de ordens, o gestor gera um arquivo que é enviado para a mesa de operações da Corretora, e que realiza as especificações para os devidos comitentes, enviando confirmação da conclusão do rateio para o gestor.

Estes arquivos são armazenados na rede, como forma de comprovação, pelo prazo mínimo de 05 (cinco) anos.

8. Política de Compra e Venda de Valores Mobiliários

A SAP tem como política relacionada à compra e venda de valores mobiliários por parte dos diretores, gestores e colaboradores (pessoas vinculadas):

- Dar prioridade na execução das ordens às Carteiras Administradas, Clubes e Fundos de Investimentos;
- As ordens dos clientes vinculados à Solidus são obrigatoriamente especificadas quando da sua colocação no sistema de negociação;
- Os clientes vinculados não poderão atuar na contraparte de ordens das Carteiras Administradas, Clubes e Fundos de Investimentos.

Os colaboradores são orientados sobre a impossibilidade de operar em outras Corretoras, conforme instrução legislação vigente, que estabelece que pessoas vinculadas somente poderão negociar valores mobiliários por conta própria, direta ou indiretamente, por intermédio da sociedade a que estiverem vinculadas.

9. Prevenção à Lavagem de Dinheiro e ao Financiamento ao Terrorismo

9.1 Definição e características

A Lei nº 9.613, no seu artigo 1º, tipifica o crime de lavagem como: “Ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos e valores provenientes, direta ou indiretamente, de infração penal”

“Lavagem” de Dinheiro é o processo pelo qual o criminoso transforma recursos ganhos em atividades ilícitas em ativos com uma origem aparentemente legal.

Essa prática geralmente envolve múltiplas transações, usadas para ocultar a origem dos ativos financeiros e permitir que eles sejam utilizados sem comprometer os criminosos.

Os mecanismos mais utilizados no processo de "lavagem" envolvem teoricamente três etapas independentes que, com freqüência, ocorrem simultaneamente.

- 1ª Etapa - Colocação – a primeira etapa do processo é a 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 liberal. A colocação se efetua por meio de depósitos, compra de instrumentos negociáveis ou compra de bens. Para dificultar a identificação da procedência do dinheiro, os criminosos aplicam técnicas sofisticadas e cada vez mais dinâmicas, tais como o fracionamento dos valores que transitam pelo sistema financeiro e a utilização de estabelecimentos comerciais que usualmente trabalham com dinheiro em espécie.
- 2ª Etapa - Ocultação – a segunda etapa do processo consiste em 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. Os criminosos buscam movimentá-los de forma eletrônica, transferindo os ativos para contas anônimas – preferencialmente em países amparados por lei de sigilo bancário ou realizando depósitos e operações em contas “fantasmas” e de “laranjas”.
- 3ª Etapa - Integração – nesta última etapa, os ativos são incorporados formalmente ao sistema econômico. As organizações criminosas buscam investir em empreendimentos que facilitem suas atividades – podendo tais sociedades prestar serviços entre si. Uma vez formada a cadeia, torna-se cada vez mais fácil legitimar o dinheiro ilegal.

9.2 Embasamento legal

- Legislação Federal

Lei nº 9.613, de 03.03.1998

Lei Complementar nº 105, de 10.01.2001

- Banco Central Do Brasil - BCB

Carta Circular nº 3.542, de 12/03/2012

Circular nº 3461, de 24/07/2009

- Comissão De Valores Mobiliários - CVM

Instrução nº 301, de 16.04.1999

9.3 Objetivo

Considerando as disposições da Convenção das Nações Unidas contra os Crimes de “Lavagem" e ou Ocultação de Bens, Direitos e Valores, assinada em Viena, Áustria, em 20.12.1988, vigente desde 11.11.1990 e a Convenção Internacional para a Supressão do Financiamento ao Terrorismo adotado pela Assembleia Geral das Nações Unidas em 09/12/1999, a SAP adotará todas as medidas cabíveis, definidas em Lei e pelos órgãos competentes brasileiros, para a prevenção e combate a esses crimes.

O objetivo da política da SAP é direcionar os esforços com vistas à prevenção e ao combate aos crimes de “lavagem” de dinheiro, minimizando, assim, os riscos que tais ilícitos venham a ocorrer na empresa, focando principalmente a conscientização de todos os colaboradores e a identificação de operações e proposição de operações suspeitas a serem realizadas nas Carteiras Administradas que a gestora não tenha total poder decisório.

Esse esforço envolve:

- Conscientização de todos sobre a importância do tema;
- Mitigação os riscos legais, de imagem e operacionais;
- Esclarecimento dos riscos da ocorrência deste crime, como qualquer outro, na instituição;
- Preservação do Sistema Financeiro Nacional; e
- Cumprimento da legislação vigente.

A SAP, por não atuar como distribuidor de suas Carteiras Administradas, atividade que cabe à Solidus, não realiza a captação de clientes e nem realiza seu cadastramento e coleta de informações financeiras e cadastrais.

Entretanto, como forma de mitigar o risco de Lavagem de Dinheiro e Financiamento ao Terrorismo, a área de Compliance, irá:

- Acompanhar e analisar mensalmente todas as movimentações de aplicações e resgates realizadas pelos cotistas, com o objetivo de detectar movimentos atípicos que possam ferir a política de prevenção à lavagem de dinheiro e financiamento ao terrorismo; e
- Analisar a montagem e criação de novos produtos, que serão aprovados em reunião do Comitê de Prevenção à Lavagem de Dinheiro.

A Solidus, como instituição credenciada para a função de Distribuidor é quem cadastra e efetiva os testes e controles voltados à prevenção e combate aos crimes de “lavagem” de dinheiro que possam ocorrer nas operações dos clientes. Suas obrigações são consolidadas em política específica da Instituição que possui alto padrão de monitoramento e forte atuação na Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo.

9.4 Políticas e diretrizes

A SAP atua na prevenção e combate aos Crimes de “Lavagem” por meio dos seguintes instrumentos:

- Normas Legais e Regulamentares;
- Estrutura Organizacional;
- Política de PLD/FT;
- Política “Conheça seu Funcionário”;
- Política de Treinamento;
- Princípios Éticos e Código de Conduta;

A Política de PLD será revisada e aprovada sempre que se façam necessárias atualizações com o objetivo de provar maior controle e segurança aos procedimentos adotados pela corretora na prevenção à lavagem de dinheiro.

Todas as revisões e alterações serão aprovadas em reunião do Comitê de Compliance.

Para garantir que todos os colaboradores tenham ciência e se comprometam com as diretrizes, obrigações e deveres oriundos desta política, será obrigatória a sua leitura e para atestar, a área de Compliance coletará a assinatura de todos no “Termo de Ciência e Compromisso” das políticas e manuais, além de promover treinamento específico sobre o tema.

9.5 Obrigações do Distribuidor

A Solidus cadastra todos os seus Clientes e mantêm seus cadastros, documentos e dados devidamente preenchidos e atualizados, conforme seus Manuais próprios, e os mantém arquivados pelo prazo de 5 (cinco) anos, mesmo após o encerramento da conta.

Além das informações cadastrais, requeridas quando do cadastramento, constam no cadastro dados relativos à capacidade econômica e rendimentos do Cliente.

A Solidus mantém registro de todas as operações realizadas pelos seus Clientes, continuando com os mesmos arquivados pelo prazo de 5 (cinco) anos, após a data da conclusão da operação.

A SAP mantém todos os registros e documentação das operações de suas Carteiras Administradas pelo mesmo prazo.

9.6 Do Dever de Comunicar

A SAP comunicará ao COAF, no prazo de 24 (vinte e quatro horas) após a efetiva análise da documentação pelo Comitê de PLD, qualquer proposta ou realização de operações em que se constatem indícios de lavagem de dinheiro.

A decisão pelo envio de comunicações ao COAF será de responsabilidade do Comitê de PLD, com seu registro em ata.

9.7 Vedação da informação ao Cliente

A legislação impõe à Solidus abster-se de fornecer, aos respectivos clientes, informações sobre eventuais comunicações efetuadas em decorrência de indícios de crime de “lavagem”.

9.8 Declaração de “não ocorrência de transações passíveis de comunicação”

De acordo com a legislação vigente, no início de cada ano deve ser enviada a declaração de “não ocorrência de transações passíveis de comunicação” por meio do Siscoaf, caso a instituição não tenha realizado nenhuma comunicação no ano imediatamente anterior.

O envio desta declaração é de responsabilidade da área de Compliance e deve observar o seguinte prazo legal:

- Segmento CVM – até o último dia útil do mês de janeiro;

A SAP enviará a declaração de “não ocorrência de transações passíveis de comunicação”, sempre que cabível e deverá encaminhar o recibo de envio da declaração para que o Diretor de Compliance dê sua ciência.

9.9 Procedimentos de PLD/FT

A Área de Compliance será responsável pela análise de todos os casos de indícios de crimes de “lavagem” e financiamento ao terrorismo, e dessa forma poderá solicitar aos colaboradores, esclarecimentos e documentos, estabelecendo prazos de respostas, baseados nos níveis de responsabilidade e risco visando ter documentação e dados suficientes, para encaminhamento do dossiê ao Comitê de PLD da Solidus.

Mensalmente serão elaborados relatórios para apreciação do Comitê de PLD com os alertas gerados e posteriormente, os mesmos deverão ser arquivados para que sejam consultados se necessário e para que se possa ter um controle efetivo das inconformidades.

9.10 Das Responsabilidades das Áreas e dos Funcionários

Todos os funcionários devem observar o cumprimento da política de PLD, e ao detectarem ou tomarem conhecimento de uma operação ou receberem proposta de operação atípica ou suspeita de prática de atividades ilícitas de “lavagem” de dinheiro, deverão comunicar a Área de Compliance, que levará a análise do caso ao Comitê de PLD.

9.11 Da Política “Conheça seu Funcionário”

A empresa acompanhará a evolução financeira do funcionário através do seu cadastro de cliente na Solidus, que deverá ser mantido atualizado.

Anualmente os colaboradores devem preencher o formulário de acompanhamento da evolução patrimonial e suas atividades externas à empresa.

As operações realizadas pelos funcionários na Corretora serão acompanhadas pela área de Compliance e deverão estar de acordo com a Política de Operações para Vinculados.

10. Órgãos reguladores e autorreguladores

Todos os colaboradores devem ser diligentes no atendimento de procedimentos decorrentes de exigências de quaisquer órgãos reguladores, sempre sob a supervisão da área de Compliance.

Os colaboradores devem ter conhecimento da legislação aplicável à sua atividade, além de todas as políticas internas da SAP, que devem ser cumpridas de forma diligente, de forma que a Instituição esteja em total conformidade, mitigando o risco legal.

11. Treinamento

Os colaboradores contratados terão reputação ilibada e amplo conhecimento em suas áreas de atuação.

A Diretoria sempre participará da seleção destes profissionais.

Logo que contratados são conscientizados e treinados quanto à necessidade de confidencialidade das informações, além de assinarem termo se comprometendo, na vigência de sua prestação de serviços e também após rescisão, manter sob sigilos a exclusividade e confidencialidade de todas as informações a que tiver acesso, tais como; dados cadastrais, saldo em custódia, saldos em conta corrente, posição das carteiras administradas.

Como política, a SAP, incentiva seus colaboradores a buscarem novos conhecimentos e todas as certificações indicadas para o exercício de sua função.

Todos os colaboradores deverão também participar dos programas de treinamento e atualização sobre as regras e procedimentos deste Manual e demais políticas.

Todos os colaboradores deverão ser constantemente avaliados e suas atividades devem ser constantemente monitoradas, a fim de identificar quaisquer situações atípicas ou suspeitas no desempenho de suas atividades profissionais, bem como qualquer descumprimento das políticas da SAP.

Os programas de treinamento deverão ter conteúdos programáticos específicos (incluindo carga horária e temas abordados) definidos pelo Diretor de Compliance.

Os programas de treinamento deverão ser pautados pela clareza, acessibilidade e simplicidade na veiculação das informações.

Ao final dos respectivos programas de treinamento, os participantes deverão ter acesso ao conteúdo apresentado e assinar lista de presença para arquivo e comprovação de participação.

12. Segurança da Informação

Para manter a confidencialidade e segurança das informações e facilitar o exercício diário de suas atividades, os colaboradores devem seguir as seguintes determinações:

- Não baixar ou instalar softwares ou hardwares sem autorização do departamento de informática;
- Não utilizar *pendrives* expostos a equipamentos de terceiros, sem autorização e a devida verificação de existência de arquivos maliciosos; e
- Não receber ou enviar mensagens ou imagens com conteúdo impróprio.

A área de Tecnologia da Informação manterá a rede interna protegida contra acessos indesejados através de firewalls e restrição de acesso apenas aos colaboradores da área de administração de carteiras.

12.1 Backup

O Backup dos arquivos da rede interna e dos bancos de dados dos sistemas serão realizados diariamente e enviados para a área de contingência da empresa

12.2 Obrigações de sigilo

Informações sobre a rede interna, como endereços, portas de acesso, topografia e especificações de rede, códigos e senhas são consideradas sensíveis e estratégicas, devendo ter, portanto, tratamento sigiloso. Todos os Colaboradores têm a obrigação de zelar pela confidencialidade dessas informações, de suas senhas de acesso, identificação de portas de acesso, e informações sobre as especificações dessa rede que eventualmente venham a possuir.

12.3 Obrigações de notificação.

Caso perceba ou desconfie de anomalias no acesso ou utilização de suas senhas ou dos meios de acesso à rede interna em geral, o Colaborador deverá imediatamente comunicar o Diretor de Compliance.

12.4 Internet e e-mail

O acesso à internet é um recurso importante e inerente às atividades da SAP e por esta razão seu uso deverá ser para este fim. Acessos a outros conteúdos não são proibidos, mas devem ser realizados de forma razoável e de forma que não atrapalhe o exercício das atividades dos colaboradores.

O acesso a provedores de e-mails que não o e-mail corporativo é bloqueado e a transmissão de informações de propriedade da SAP só deve ser feita, quando cabível, através do e-mail corporativo.

O recebimento de e-mails com anexo ou de remetentes desconhecidos deve ser analisado com atenção e se houver dúvidas acerca de conteúdos maliciosos, a área de TI deve ser acionada para verificar a existência de riscos para os recursos computacionais.

12.5 Concessão de acessos e parâmetros de senhas

A área de Tecnologia da Informação concederá os acessos mediante solicitação do Diretor Responsável pelo colaborador solicitante e as senhas obedecerão aos critérios definidos em Manual próprio da área de TI.

13. Matriz de Segregação

A área de Compliance detém matriz com a definição de alçada e tipos de acessos por colaboradores, classificada conforme as atividades executadas pelos profissionais.

14. Uso de senhas

Uma vez que as senhas de acesso são de uso pessoal e intransferível, não será admitido o compartilhamento das senhas para acesso à rede e aos demais sistemas da SAP.

Todas as atividades são registradas e associadas à senha do usuário, de modo a responsabilizá-lo no caso de irregularidades.

Caso o colaborador necessite se ausentar do seu local de trabalho, deverá bloquear ou se desconectar do seu computador ou terminal evitando que outras pessoas possam utilizá-lo em seu lugar.

15. Manutenção de arquivos

A SAP deverá manter, pelo prazo mínimo de 05 (cinco) anos, ou por prazo superior quando solicitada pela CVM ou outro órgão fiscalizador, todos os documentos e informações exigidos pela legislação em vigor, bem como todas as informações produzidas no exercício da atividade de administração de carteiras e Compliance.