MANUAL DE CONTROLES INTERNOS E COMPLIANCE

Versão:
31/05/2022

leads
SECURITIZADORA

SUMÁRIO

***** ***** ***** ***** *****

1. | OBJETIVO

1.1. Este manual tem por objetivo disciplinar e padronizar as políticas de controles internos, *compliance*, prevenção e combate à lavagem de dinheiro, práticas abusivas de ofertas e financiamento ao terrorismo, e o plano de contingências no caso de risco de continuidade dos negócios, todas em conjunto doravante designada como "Manual de Compliance" ("Manual de Compliance" ou "Manual").

1.2. Este Manual de Compliance abrange os princípios necessários para aderir ao disposto no que dispõe sobre a atividade de securitização da Leads Companhia Securitizadora. ("Leads"), nos termos da Resolução da Comissão de Valores Mobiliários nº 60, de 23 de dezembro de 2021 ("RCVM 60") e demais disposições legislativas e normativas vigentes.

1.3. A Leads tem como princípio basilar exercer suas atividades com boa-fé, transparência, diligência e lealdade, dispendendo no exercício de suas atividades, todo o cuidado que toda pessoa prudente e diligente costuma dispensar à administração de seus próprios negócios.

1.4. Com a finalidade de evitar práticas que possam vir a prejudicar os clientes, investidores, parceiros e a Leads, os Colaboradores (definido abaixo) devem envidar seus melhores esforços para evitar quaisquer práticas que infrinjam ou estejam em conflito com este Manual de Compliance, ou os princípios adotados pela Leads razão pela qual, com a ocorrência de qualquer caso que na percepção do Colaborador possa ser caracterizado como uma violação, este deverá reportar-se ao Diretor responsável pelo Compliance, com a finalidade de obter a orientação sobre qual procedimento adotar.

1.5. O presente Manual de Compliance entrará em vigor em maio de 2022 e vigorará por prazo indeterminado.

2. | ABRANGÊNCIA

2.1. O Manual de Compliance em conjunto, com a legislação e regulamentação aplicável, disciplina a relação de todos os acionistas, administradores, fornecedores, funcionários, parceiros ou empregados da Leads ("Colaboradores") entre si e com terceiros.

2.2. Posto isto, antes do início do exercício de suas funções perante à Leads, os Colaboradores deverão receber uma cópia deste Manual de Compliance, bem como, firmar o Termo de Adesão abaixo, declarando se encontrar totalmente familiarizado o Manual de Compliance e os procedimentos aqui contidos, devendo estar sempre atento às situações que poderão ensejar condutas inadvertidas, por ele ou por qualquer outro Colaborador, isto é, condutas e/ou ações que pareçam ser uma violação direta ou indireta deste Manual de Compliance ou de qualquer lei, ou regulamentação aplicável.

2.3. O Diretor de Compliance manterá em arquivo digital e físico uma via do Termo de Adesão devidamente assinado por seus Colaboradores, bem como, disponibilizará uma cópia deste Manual na sede da Leads e na rede mundial de computadores.

2.4. O descumprimento das regras estabelecidas neste Manual de Compliance ou em normas e/ou regulamentações aplicáveis, será caracterizado como uma infração contratual e poderá resultar na imposição de penas de advertência, suspensão, desligamento ou exclusão por justa causa dos Colaboradores da Leads.

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

2.6. O Diretor de Compliance da Leads é o responsável pela implementação, revisão dos processos e procedimentos, manutenção e atualização desse Manual de Compliance.

3. | CONDIÇÕES GERAIS DA POLÍTICA DE CONTROLES INTERNOS E COMPLIANCE

3.1. **Estrutura da Diretoria de Compliance**: A área de controles internos e compliance da Leads é de responsabilidade do Diretor de Compliance, incluindo entre suas atribuições, o controle e a supervisão das práticas profissionais de todos os Colaboradores para atendimento das regras previstas no presente Manual, na regulamentação e na legislação vigente. Tendo isso em vista, o Diretor de Compliance atua com o objetivo de:

i. assegurar a conformidade das operações e atividades desenvolvidas pela Leads com as disposições legais e regulamentares aplicáveis, bem como às políticas internas e instrumentos de autorregulação adotados;

ii. monitorar e supervisionar, com independência e eficiência, as operações e atividades desenvolvidas pela Leads e o cumprimento das normas aplicáveis, especialmente as regras contidas neste Manual;

iii. implementar os Programas de Treinamento dos Colaboradores e demais procedimentos operacionais que deem cumprimento às normas previstas neste Manual; e

iv. esclarecer eventuais dúvidas dos Colaboradores a respeito da legislação e regulamentação aplicável, assim como sobre as disposições deste Manual.

3.1.1. O Diretor de Compliance, nos termos do artigo 5º, parágrafo 2º, da Resolução CVM n º 60: **(i)** exercer suas funções com independência em relação às demais áreas da Leads; e (ii) não atuar em funções relacionadas às companhias securitizadoras e que limite a sua independência, na instituição ou fora dela.

3.1.2. O Diretor de Compliance, visando a assegurar que a Leads opere em conformidade com as regras, normas e orientações aos quais está sujeita, deverá, ao menos uma vez por ano, avaliar e revisar os seus procedimentos relativos a controles internos e compliance, de modo a implementar eventuais atualizações ou aprimoramentos.

3.2. O presente Manual contém as seguintes políticas internas da Leads: **(i)** Política de Segregação Física de Atividades; **(ii)** Conflito de Interesses; **(iii)** Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo; **(iv)** Política de Contratação de Prestadores de Serviços; **(v)** Política de Segurança das Informações; **(vi)** Política de Segurança Cibernética; e **(v)** Plano de Contingências no Caso de Risco de Continuidade dos Negócios.

4. | POLÍTICA DE SEGREGAÇÃO FÍSICA DE ATIVIDADES

4.1. A Política de Segregação Física de Atividades tem como objetivo estabelecer as regras que orientam a segregação física das instalações entre áreas responsáveis pelas atividades prestadas pela Leads. Atualmente, a Leads exerce apenas a atividade de securitizadora, não atuando, neste momento com a distribuição dos ativos securitizados.

4.2. Para que exista a efetividade na segregação de atividades é necessário:

i. garantir a segregação física de instalações entre a área responsável pela securitização e as demais áreas da Leads;

ii. assegurar o bom uso de instalações, equipamentos e informações comuns a mais de um setor da Leads;

iii. preservar informações confidenciais e permitir a identificação das pessoas que tenham acesso a elas;

iv. restringir o acesso a arquivos e permitir a identificação das pessoas que tenham acesso a informações confidenciais; e,

v. implantação e manutenção de programa de treinamento que tenham acesso a informações confidenciais e/ou participem de processo de estruturação dos ativos.

4.3. Buscando mitigar riscos de potenciais conflitos de interesse na condução de sua atividade, a Leads possui segregação física da área de estruturação de ativos e securitização da área de compliance.

4.4. A Leads assegura, por meio de acesso controlado, que apenas os Colaboradores diretamente envolvidos na securitização tenham acesso ao ambiente segregado. Adicionalmente, são disponibilizados linhas telefônicas específicas e diretórios de rede privativos e restritos, devidamente segregados dos equipamentos dos demais colaboradores.

4.5. O controle de acesso é efetuado por meio de identificação funcional, sendo o acesso ao local permitido apenas para pessoas autorizadas. O acesso a dados e informações eletrônicas é totalmente controlado e feito mediante uso de dados de acesso (login e senha) pessoais e intransferíveis,

respondendo o Colaborador pelo uso indevido e/ou pela disponibilização de tais dados de acesso a quaisquer pessoas.

4.6. O acesso às instalações físicas da Leads é controlado. O acesso de terceiros à Leads somente é permitido na recepção e em sala de reunião, e somente enquanto acompanhados de pelo menos um Colaborador.

4.7. O Diretor de Compliance é responsável por promover a aplicação das regras aqui contidas, de forma a assegurar a segregação física das instalações entre áreas responsáveis pelas atividades prestadas pela Leads.

4.8. Os controles lógicos são controles estabelecidos sobre os sistemas eletrônicos e de comunicação, estes controles limitam e/ou monitoram o acesso à informação, como controle de acesso aos servidores e arquivos via rede, com o objetivo de preservar as informações confidenciais e permitir a identificação das pessoas com acesso a elas. Os controles lógicos sobre os sistemas eletrônicos auxiliam a segregação de funções ao restringir o acesso a determinadas operações. Os acessos são concedidos através de perfis de função previamente estabelecidos em matrizes de segregação de funções, e sua efetividade é mensurada periodicamente através de testes realizados pelas áreas de compliance e tecnologia.

5. | CONFLITO DE INTERESSES

5.1. A Leads tem como objetivo conduzir seus negócios buscando sempre identificar, administrar e eliminar a existência de potencial conflitos de interesses. Há potencial conflito de interesses quando há indício de que o interesse pessoal dos Colaboradores (ou grupo de Colaboradores) e/ou da própria Leads sobrepõe-se, direta ou indiretamente, aos interesses dos clientes da Leads.

5.2. Qualquer circunstância que represente conflito de interesses real ou potencial deve sempre ser resolvida priorizando-se o cliente em detrimento da Leads e/ou seus Colaboradores. Todos os Colaboradores devem evitar engajar-se em negócios externos que possam representar potenciais ou reais conflitos de interesses, que possam prejudicar a imagem da Leads.

5.3. Os Colaboradores compreendem que o conflito de interesses se estende também aos seus familiares, cônjuges e relacionados devendo observar as regras estabelecidas neste Manual, também como forma de prevenir conflitos de interesses.

5.4. Os Colaboradores não poderão manter relações comerciais privados com clientes, prestadores de serviços, parceiros e concorrentes nas quais venham a obter privilégios pessoais em razão de cargo ou função ocupada.

5.5. Entendendo ser difícil prever toda e qualquer situação de conflito, os profissionais devem ser sensíveis a potenciais conflitos e trazer dúvidas à atenção do Diretor de Compliance. Se um conflito não puder ser evitado, o mesmo deve ser gerido de forma ética e responsável, sempre priorizando os interesses dos clientes.

6. | POLÍTICA DE PREVENÇÃO A LAVAGEM DE DINHEIRO E AO FINANCIAMENTO DO TERRORISMO ("PLDFT")

6.1. A Leads deverá conduzir seus negócios e operações em conformidade com certas disposições das normas de combate à Lavagem de Dinheiro e Financiamento ao Terrorismo ("PLDFT"), buscando impedir, detectar e reportar qualquer suspeita de operações que apresentem indícios ou evidências de envolverem atividades relacionadas aos crimes de lavagem de dinheiro, ocultação de bens, direitos e valores provenientes direta ou indiretamente de infração penal e financiamento ao terrorismo.

6.2. Qualquer Colaborador deverá imediatamente notificar o Diretor de Compliance, quando verificada a ocorrência de um evento que pode ser considerado suspeito para fins da Lei nº 9.613, de 03 de março de 1998, e pela Resolução CVM nº 50 de 02 de setembro de 2021 ("RCVM 50").

6.3. O Diretor de Compliance analisará a atividade suspeita, em conjunto com outros fatores, tais como, a forma de realização, as partes e valores envolvidos, a capacidade financeira e a atividade econômica do cliente e qualquer indicativo de irregularidade ou ilegalidade envolvendo o cliente e/ou suas operações.

6.4. O Diretor de Compliance analisará a atividade suspeita e irá preparar um dossiê com as evidências colhidas e o histórico das operações, bem como analisará a documentação apresentada, que deve confirmar a suspeita após análise e assinar a carta de comunicação aos órgãos reguladores.

6.5. A Leads se compromete a priorizar a comunicação de suspeita de crime de lavagem de dinheiro e de financiamento de atividades terroristas aos órgãos reguladores, encaminhando a documentação comprobatória imediatamente após sua identificação. As comunicações acima citadas serão efetivadas com a utilização, no que couber, de meio magnético dentre outros materiais e registros comprobatórios, havendo a postura de manter a informação em estrito sigilo, inclusive não sendo efetuada comunicação ou ciência de tais atos aos respectivos clientes.

6.6. No caso de envolvimento de Colaborador(es) em operações dessa natureza, os envolvidos ficarão sujeitos às sanções previstas neste Manual, inclusive desligamento ou demissão por justa causa, no caso de Colaborador(es) que sejam empregados, administradores ou terceiros ligados a Leads, e ainda às demais consequências legais cabíveis.

6.7. Caberá ao Diretor de Compliance a responsabilidade e a realização das seguintes atividades: **(i)** monitoração e fiscalização periódica do cumprimento, pelos Colaboradores, da presente política de PLDFT; **(ii)** definição de políticas, procedimentos e treinamento de Colaboradores visando à prevenção e combate à lavagem de dinheiro; e **(iii)** procedimento de identificação de atividades suspeitas, incluindo comunicação ao Conselho de Controle de Atividades Financeiras - COAF.

7. | PROCEDIMENTOS DE CONHEÇA SEU COLABORADOR ("KNOW YOUR EMPLOYEE – KYE")

7.1. Os procedimentos de "Conheça seu Colaborador" têm por objetivo fornecer à Leads informações detalhadas sobre seus Colaboradores, os quais incluem critérios para a sua contratação e verificação de suas condutas.

7.2. A Leads adota uma postura rígida e transparente na contratação de seus Colaboradores e, portanto, além dos requisitos técnicos e profissionais, serão avaliados os requisitos ligados à reputação dos Colaboradores no mercado e ao perfil profissional, bem como os antecedentes profissionais do candidato.

7.3. Para este fim, a Leads obterá, junto aos meios legais aplicáveis, as informações relativas à situação econômico-financeira de seus Colaboradores.

8. | PROCEDIMENTOS DE CONHEÇA SEU PARCEIRO ("KNOW YOUR PARTNER – KYP")

8.1. Os procedimentos de "Conheça seu Parceiro" abrangem todos os parceiros de negócios da Leads, no Brasil ou no exterior, bem como todos os seus fornecedores e prestadores de serviços.

8.2. Os procedimentos de "Conheça seu Parceiro" têm como objetivo a prevenção do envolvimento da Leads em situações que possam acarretar a riscos legais e à sua reputação perante o mercado.

8.3. O processo de análise de contrapartes da Leads está inserido dentro do âmbito das obrigações enquanto securitizadora, devendo ser averiguada as seguintes questões:

i. Estabelecer a identidade de cada contraparte;

ii. Conhecer a atividade da contraparte;

iii. Conhecer a origem do patrimônio da contraparte; e

iv. Averiguar a origem e destino dos recursos movimentados pela contraparte.

8.4. A Leads entende que para prevenir de maneira eficaz a lavagem de dinheiro é necessária a avaliação do risco oferecido por suas contrapartes, antes da efetiva transação do negócio.

8.5. No auxílio a essa averiguação, a Leads poderá se utilizar de um Questionário de Due Diligencie próprio, ou até mesmo efetuar visitas de diligência, de forma a assegurar que os parceiros comerciais possuam práticas adequadas de prevenção à lavagem de dinheiro.

8.6. Antes do início do relacionamento com parceiros de negócios, a Leads e seus Colaboradores farão pesquisas, através dos meios públicos disponíveis, sobre a reputação de potenciais parceiros e

sobre seu histórico econômico-financeiro, por meio das informações disponíveis nos serviços de proteção ao crédito, nos órgãos judiciais, em mecanismos de busca online e demais fontes de informação pública.

8.7. No sentido de cooperar, conforme previsto acima, a Leads irá rever periodicamente as políticas de PLDFT dos seus prestadores de serviços para verificar se adotam regras e controles internacionalmente aceitos e recomendados.

8.8. Para os fins desta Política, entende-se como "Contraparte" a pessoa natural ou jurídica, que atua como contraparte nas operações de securitização.

9. | MONITORAMENTO DE OPERAÇÕES

9.1. A Leads manterá registro de todas as operações que realizar em nome de seus clientes e investidores. Os registros das operações ficarão arquivados na sede da Leads e à disposição dos órgãos reguladores por, no mínimo, 05 (cinco) anos contados do encerramento da relação contratual com o cliente, podendo ser descartados após este prazo.

9.2. Ainda, a Leads também realizará o monitoramento de notícias e eventos negativos ou relacionados à lavagem de dinheiro com seus parceiros comerciais/contrapartes, que permite a Leads cessar o vínculo imediato com a eventual instituição, bem como apurar o cometimento de algum ilícito que possa afetar a Leads.

10. | COMUNICAÇÃO AOS ÓRGÃOS REGULADORES

10.1. O Diretor de Compliance comunicará ao COAF, em até de 24 (vinte e quatro) horas a contar da conclusão da operação ou da proposta de operação suspeitas.

10.2. Quando a verificação de clientes potenciais quanto à indício de lavagem de dinheiro ou financiamento de atividades terroristas, a área de Compliance realizará uma análise das operações bem como do cliente, de acordo com o procedimento interno da Leads, e ao final da análise verificarmos qualquer incompatibilidade que possa configurar suspeita de indícios à lavagem de dinheiro ou financiamento de atividades terroristas, Leads informará imediatamente ao COAF.

10.3. Nos termos da Lei 9.613/98 e alterações dadas pela Lei nº 12.683/2012 e do parágrafo a Instrução RCVM 50, alterações posteriores, as comunicações feitas de boa-fé não darão origem a qualquer responsabilidade civil ou administrativa para a pessoa que comunicou tal evento.

10.4. As comunicações realizadas têm caráter confidencial e devem ser restritas aos Colaboradores envolvidos no processo de análise. Todos os registros deverão ser arquivados pelo prazo de 05 (cinco) anos.

11. | POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

11.1. Os Colaboradores da Leads, no desempenho de suas funções, poderão vir a ter acesso a diversas informações classificadas como confidenciais.

11.2. Para fins da presente Política de Segurança da Informação, serão consideradas informações confidenciais todas e quaisquer informações e/ou dados de natureza sigilosa (incluindo, sem limitação, todas as informações técnicas, financeiras, operacionais, econômicas, bem como demais informações comerciais) referentes à Leads, suas atividades e seus clientes e quaisquer cópias ou registros dos mesmos, orais ou escritos, contidos em qualquer meio físico ou eletrônico, que tenham sido direta ou indiretamente fornecidos ou divulgados em razão das atividades de securitização desenvolvida pela Leads, mesmo que tais informações e/ou dados não estejam relacionados diretamente aos serviços ou às transações aqui contempladas ("Informação Confidencial").

11.3. Não são consideradas informações confidenciais aquelas informações que: (a) sejam ou venham a se tornar de domínio público sem violação do disposto nesta Política de Segurança da Informação; (b) tenham sido recebidas de boa-fé pelo Colaborador, de terceiros que tenham o direito de divulgá-las, sem obrigação de confidencialidade; (c) em virtude de lei, decisão judicial ou administrativa, devam ser divulgadas a qualquer pessoa; ou (d) cuja divulgação tenha sido aprovada pelo Diretor de Compliance.

11.4. Nesse sentido, todos os Colaboradores, ao firmar o Termo de Adesão anexo ao presente Manual na forma do "Anexo I", deverão tomar conhecimento e expressamente anuir com o quanto segue:

i. Os Colaboradores expressamente obrigam-se a manter o sigilo das Informações Confidenciais que lhes tenham sido transmitidas, fornecidas e/ou divulgadas sob ou em função de seu vínculo com a Leads ou de relacionamento com clientes da Leads, se comprometendo a não utilizar, reproduzir ou divulgar as referidas Informações Confidenciais, inclusive à pessoas não habilitadas ou que possam vir a utilizá-las indevidamente em processo de decisão de investimento próprio ou de terceiros, exceto mediante autorização expressa e escrita do respectivo titular e na medida do estritamente necessário para o desempenho de suas atividades e/ou obrigações;

ii. Todos os negócios, técnicas, materiais, planilhas, formulários, projetos, desenvolvimentos de estratégias, produtos ou serviços elaborados, desenvolvidos e/ou utilizados pela Leads e/ou por seus clientes, mesmo que tenham significativa participação de qualquer Colaborador, sempre serão de propriedade da Leads, sendo vedado a qualquer Colaborador os divulgar, utilizá-los para si ou terceiros, cedê-los ou aliená-los, seja a que título for;

iii. Os Colaboradores expressamente reconhecem ser de propriedade da Leads todos os direitos autorais e/ou intelectuais existentes e advindos de projetos, técnicas, estratégias, materiais, planilhas, formulários, desenvolvimentos de contratos ou serviços, métodos e/ou

sistemas atualmente existentes ou que vierem a ser desenvolvidos durante seus respectivos vínculos com a Leads, nada podendo vir a reclamar a esse título;

iv. Caso qualquer Colaborador seja obrigado a divulgar Informações Confidenciais por determinação judicial ou de autoridade competente, o Colaborador deverá comunicar a Leads da existência de tal determinação previamente à divulgação e se limitar estritamente à divulgação da Informação Confidencial requisitada;

v. Para os propósitos do disposto nesta política, caberá ao Colaborador o ônus de provar o caráter não confidencial de qualquer informação; e

vi. O acesso às Informações Confidenciais será restrito e poderá ser diferenciado conforme os níveis hierárquicos e as funções desempenhadas pelos Colaboradores da Leads, a critério do gestor de cada área e com anuência do Diretor de Compliance. O controle de acesso a tais informações será realizado por meio das senhas pessoais dos Colaboradores, que, conforme exposto aqui, seguirá o critério definido pelo gestor de cada área, o responsável de TI, juntamente com o Diretor de Compliance, respeitando uma ordem de graduação com diferentes níveis de acessibilidade a arquivos, pastas e diretórios da rede corporativa.

11.5. Caso tenham conhecimento de que qualquer Colaborador tenha infringido a presente política, os demais colaboradores obrigam-se a reportar tal falta ao Diretor de Compliance, sob pena de ser considerado corresponsável com o infrator.

11.6. O Diretor de Compliance visa a promover a aplicação da presente política, bem como o controle, a supervisão e a aprovação de exceções em relação à mesma, sendo responsabilidade desta Diretoria assegurar a implementação de mecanismos eficientes capazes de resguardar o sigilo das Informações Confidenciais, bem como a identificação de quaisquer infrações às regras aprovadas na forma da presente política.

11.7. Todos os Colaboradores da Leads têm a obrigação de zelar pelo sigilo das Informações Confidenciais, devendo observar as seguintes regras para tanto:

i. Em nenhuma hipótese o profissional deverá, durante a vigência de sua prestação de serviços à Leads e mesmo após o término de seu contrato, transmitir ou revelar a qualquer pessoa, empresa, sociedade ou negócio, nem usar por sua própria conta, sem a aprovação escrita da Leads, qualquer informação relativa aos negócios e clientes recebida durante seu vínculo com a Leads, ou recebida de qualquer empresa direta ou indiretamente a ela relacionada;

ii. Todos os dados recebidos serão tratados como Informações Confidenciais, devendo manter sigilo sobre as operações realizadas e os nomes de clientes;

iii. Todas as listas de clientes, orientações e dados sobre vendas e serviços, operações e negócios, bem como todos os demais papéis, registros e documentos elaborados seja pela

empresa, pelo profissional, ou que estejam em poder desse durante seu vínculo empregatício ou de alguma forma a ele pertinente, deverão ser devolvidos a Leads por ocasião do término do contrato de trabalho ou em qualquer tempo, sendo vedada a reprodução de cópias ou de arquivos eletrônicos com tais conteúdos;

iv. O profissional é responsável pela guarda e boa conservação de todos e quaisquer documentos que estiverem sob sua responsabilidade durante a execução de seu trabalho. O profissional será pessoalmente responsável no caso de quebra de sigilo a pessoas não autorizadas;

v. A Leads mantém arquivos separados eletronicamente, para cada área. Os diretórios de cada área são acessados conforme a configuração de acesso de cada Colaborador, sendo que os Colaboradores de uma área não têm permissão para criar, editar, alterar ou salvar arquivos armazenados nos diretórios de outras áreas;

vi. A senha fornecida para acesso às redes de dados institucionais, incluindo os diretórios de acesso restrito, é pessoal e intransferível, sendo vedada a sua divulgação a outras Colaboradores ou terceiros;

vii. Tendo em vista a alta especialização da atividade desenvolvida pela Leads, assim como os princípios que regem o mercado de valores mobiliários, é absolutamente vedada a revelação de carteiras, operação e estratégias de todo e qualquer produto de securitização à qualquer não integrante da Leads, seja da Imprensa, de círculo pessoal de convívio, de Leads ação imediata de parentesco ou de estado civil, exceto nas formas da lei e com autorização da diretoria;

viii. É também vedada a utilização de informações privilegiadas ("*Inside Information*"), assim entendidas informações não públicas a respeito de empresas de capital aberto e negociadas em bolsas de valores, e que façam parte do universo potencial de operações das estratégias da Leads. Todo Colaborador que, mesmo que involuntariamente, obtiver acesso a informações privilegiadas, deverá comunicá-las imediatamente à Diretoria, que poderá restringir a negociação com ativos relacionados à informação obtida até que sejam confirmadas publicamente ou desmentidas;

ix. Os profissionais devem proteger os ativos da empresa e assegurar o seu uso eficiente. Os ativos serão utilizados prioritariamente para fins do negócio. Qualquer suspeita de fraude ou roubo de ativos deve ser reportado à Diretoria imediatamente. Ativos da Leads incluem o seu capital, suas instalações, seus equipamentos, informação proprietária e intelectual, tecnologia, seu "*business plan*", ideais de novos produtos ou negócios, material e lista de clientes entre outros;

x. Os equipamentos e computadores disponibilizados aos Colaboradores da Leads devem ser utilizados com a finalidade prioritária de atender aos interesses comerciais legítimos da Leads;

xi. A obtenção de cópias de arquivos de qualquer extensão, de forma gratuita ou remunerada, em computadores da Leads, originados em máquina remota ("Download") deverá observar os direitos de propriedade intelectual pertinentes tais como copyright, licenças e patentes. Arquivos eletrônicos, programas ou quaisquer outros materiais mantidos na rede são considerados ativos da sociedade e estão sujeitos a revisões periódicas, monitoramento ou vigilância por parte da empresa; e

xii. A Leads só autoriza o acesso à internet através de conexões aprovadas, não podendo o profissional fazer uso de conexões dial-up ou outros meios não aprovados. O profissional deve usar o bom senso e julgamento quando fizer uso de internet durante o horário de trabalho, quando o mesmo não for por interesse da sociedade.

11.8. Aos Colaboradores da Leads, é vedado:

i. Transmitir, copiar ou fazer download de quaisquer materiais, incluindo imagens, com conotações sexuais explícitas ou não, ou mensagens ou materiais que tragam conteúdo racista ou sexista, que possam embaraçar, ofender, ameaçar ou prejudicar um profissional, um cliente ou o público em geral;

ii. Transmitir, postar, copiar, ou fazer download de "copyright" sem o devido consentimento do proprietário do material;

iii. Transmitir ou postar informações não públicas sobre a Leads;

iv. Tentar conseguir acesso a qualquer computador, base de dados ou rede sem a devida autorização;

v. Transmitir vírus de forma intencional ou outros programas não autorizados;

vi. Distribuir mensagens de e-mails que configurem correntes, spam, propagandas, etc.;

vii. Criar um endereço de e-mail ou um domínio que seja derivado ou similar ao nome da Leads;

viii. O uso de senhas é confidencial e as mesmas, não devem ser distribuídas ou comunicadas a terceiros sob nenhuma hipótese;

ix. Uso de e-mail da Leads deve ser feito com bom senso e julgamento; e

x. Toda comunicação eletrônica relacionada ao negócio deve ser feita através da rede de comunicação da Leads, não sendo permitido o envio de documentos por outros servidores que possam ser acessados através da Internet.

11.9. O correio eletrônico disponibilizado pela Leads caracteriza-se como correio eletrônico corporativo para todos os efeitos legais, especialmente os relacionados aos direitos trabalhistas, sendo de utilização preferencial para alcançar os fins comerciais aos quais se destina. É permitida a utilização pessoal de forma moderada, desde que tais comunicações estejam de acordo com as regras descritas neste documento.

11.10. Não obstante, mensagens enviadas ou recebidas através do correio eletrônico corporativo, seus respectivos anexos, e a navegação na internet através de equipamentos da Leads poderão ser monitoradas sem qualquer aviso ao profissional.

11.11. Nenhum profissional está autorizado falar com o público, dar entrevistas, prestar informações ou afins, seja a Imprensa, escrita ou falada, reguladores, fiscais, ficando essa função de responsabilidade exclusiva da Diretoria ou por alguém explicitamente aprovado pela diretoria.

11.12. As regras dispostas nesta política visam a estabelecer regras que orientem o controle de acesso a Informações Confidenciais pelos Colaboradores, inclusive através do estabelecimento de regras para a utilização de equipamentos e e-mails da empresa, para gravação de cópias de arquivos, para download e instalação de programas nos computadores da empresa dentre outras.

12. | POLÍTICA DE SEGURANÇA CIBERNÉTICA

12.1. Os avanços tecnológicos criam facilidades e possibilitam o uso de novas ferramentas para a atuação da Leads, permitindo agilidade na construção e disponibilização de serviços, ampliação dos meios de comunicação, entre outros avanços. Por outro lado, o aumento do uso de tais ferramentas potencializa os riscos de ataques cibernéticos, ameaçando a confidencialidade, a integridade e a disponibilidade dos dados ou dos sistemas da Leads.

12.2. Tendo isso em vista, esta Política de Segurança Cibernética tem por objetivo mitigar os riscos de uma ameaça cibernética por meio da implementação de um programa de segurança cibernética que contempla os seguintes aspectos: (i) identificação e avaliação dos riscos internos e externos aos quais a Leads está sujeita, os ativos de hardware e software e os processos que precisam de proteção; (ii) estabelecimento de ações de prevenção e proteção; (iii) monitoramento das ameaças em tempo hábil; (iv) criação de um plano de resposta; e (v) reciclagem e revisão do programa de segurança cibernética.

12.3. O Diretor de Compliance será o responsável para tratar e responder questões relacionadas à segurança cibernética.

12.4. Qualquer processo ou ativo classificado como Informação Confidencial serão considerados vulneráveis para fins de segurança cibernética, sendo classificados internamente com alto grau de ameaça institucional em caso de eventual ataque cibernético.

12.5. Nesse sentido, o Compliance, juntamente com o departamento de tecnologia da Leads realiza ações de prevenção e proteção de tais ativos, por meio dos procedimentos elencados na Política

de Segurança de Sigilo das Informações. Adicionalmente, ressalta-se que a Leads trabalha com (i) backup dos seus arquivos; (ii) sistema de firewall e antivírus; (iii) restrição de instalação e execução de softwares e aplicações não autorizadas por meio de controles de execução de processos; e (iv) acesso restrito a páginas na rede mundial de computadores.

12.6. Para fins de monitoramento, o departamento de tecnologia da Leads realiza, periodicamente, testes de segurança e procedimentos para detectar falhas e vulnerabilidades.

12.7. Adicionalmente, a Leads (i) mantém inventários atualizados de hardware e software por ela detidos; (ii) mantém os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizados; (iii) monitora e as rotinas de backup, executando testes regulares de restauração dos dados; e (iv) analisa regularmente os logs e trilhas de auditoria criadas, de forma a permitir a rápida identificação de ataques, sejam internos, sejam externos.

12.8. No caso concreto de um ataque cibernético amplo nas redes da Leads, o Compliance e o departamento de tecnologia da Leads deverão contatar imediatamente os Colaboradores chaves da Leads, bem como empresa especializada para resolver a questão no menor tempo possível. Neste cenário, os Colaboradores da Leads deverão utilizar instalações de contingência até a normalização dos serviços, as quais obedecerão às regras de controle de acesso previstas na Política de Segurança e Sigilo de Informações.

12.9. Em se tratando de um ataque individual a um determinado Colaborador, a Leads deverá disponibilizar novos equipamentos para a continuidade da prestação dos serviços por parte daquele Colaborador.

12.10. Todo e eventual incidente cibernético deverá ser documentado por escrito em relatório elaborado pelo Compliance, no qual constarão as descrições do incidente e as medidas tomadas pela Leads para resolver tal incidente, e deverá ser arquivado na sede da Leads para fins de evidência em eventuais questionamentos.

12.11. Os procedimentos previstos nesta Política de Segurança Cibernética, conforme mencionados anteriormente, serão revisados anualmente pela Leads, ou quando houver alteração na regulação referente à segurança cibernética. Em tais revisões, serão atualizadas as avaliações de riscos, vulnerabilidades e ameaças identificadas originalmente.

13. | RISCOS DE CONTINUIDADE DE NEGÓCIOS

13.1. Os principais riscos aos quais a Leads está sujeita são aqueles relacionados ao uso adequado de suas instalações físicas, incluindo: (i) Falhas de energia; (ii) Falhas no provedor de internet; (iii) Vandalismo nas suas instalações; (iv) Ataques cibernéticos; e (v) Acidentes que impeçam o acesso físico à Leads, incluindo desastres naturais. Para mitigar estes possíveis risco a Leads adota as seguintes contingências:

13.1.1. Cópia e Recuperação de Dados: A Leads mantém cópias eletrônicas de todas as informações fundamentais relacionadas às emissões em um ambiente seguro na "nuvem". Toda informação eletrônica é arquivada diariamente e salva em meio eletrônico no ambiente de contingência na nuvem. O Diretor de Compliance está incumbido de desenvolver o arquivamento detalhado de dados e pelo plano de recuperação de desastres referente a todos os serviços de informações da Leads e supervisionar a análise periódica deste plano.

Além disso, os recursos computacionais da Leads devem ser: (i) protegidos contra adulterações; e (ii) objeto de realização de auditorias e inspeções por empresas e funcionários especializados para tanto. Todos os registros eletrônicos realizados pela Leads deverão ser mantidos e estar disponíveis para atender os prazos legais e regulatórios praticados pelos órgãos reguladores locais e jurisdições que a Leads atue em mercado regulado.

As informações mantidas em meios eletrônicos devem ser salvas em bases replicadas (backups) e devem permanecer íntegras e acessíveis por prazo não inferior a 5 (cinco) anos. O acesso a essas bases devem ser limitadas somente a pessoas autorizadas pelo Diretor de Compliance.

13.1.2. Sistemas Críticos: Todos os sistemas que são cruciais para as operações de negócios da Leads, são considerados sistemas críticos. Alguns Colaboradores, mediante supervisão, poderão ter acesso a determinados sistemas críticos de forma remota (acesso em casa), mediante prévia e expressa autorização do Diretor de Compliance.

13.1.3. Centro de Comando Operacional: Na impossibilidade de acesso ou permanência dos Colaboradores nas dependências da Leads será disponibilizado um escritório de trabalho contingencial para onde os Colaboradores deverão se deslocar, onde terão acesso aos sistemas fundamentais para a manutenção das atividades. O escritório contingencial proporcionará condições mínimas de operação e segurança para a continuidade operacional dos negócios.

O Diretor de Compliance indicará os Colaboradores responsáveis pelas funções mínimas necessárias para a continuidade dos negócios, em momentos de recuperação de crise, de tal forma que a Leads possa continuar funcionando, atendendo aos seus clientes e dando prosseguimento às suas atividades normalmente.

Uma vez detectada a situação de contingência, o Diretor de Compliance orientará os Colaboradores da Leads (pessoalmente ou por telefone móvel) a se dirigirem ao escritório de trabalho contingencial.

13.1.4. Vazamento de Informações Confidenciais: Os Colaboradores deverão comunicar ao Diretor de Compliance quaisquer casos de violações às normas de segurança da informação que tenham conhecimento. Toda violação ou desvio é investigado para a determinação das

medidas necessárias, visando à correção da falha, ou reestruturação de processo. Em caso de vazamento de informação confidencial, o Diretor de Compliance discutirá com a equipe interna de tecnologia da informação ("TI"), ou com funcionários terceirizados e contratados para essas funções, qual o melhor plano efetivo de recuperação e medidas para minimizar e prevenir danos, levando o assunto ao Diretor de Compliance, conforme o caso.

13.1.5. Testes Financeiros e Operacionais: Semestralmente, a Leads realiza teste de eficiência e rapidez de acesso para garantir que os sistemas fundamentais da securitizadora estão aptos a operar de forma remota. A Leads também verifica se as cópias eletrônicas das informações que são mantidas no escritório da securitizadora e na "nuvem" se mantêm em boas condições e se estão disponíveis para uso da securitizadora.

13.1.6. Métodos Alternativos de Comunicação: A Leads possui diversos meios disponíveis pelos quais os emissores e clientes podem contatar Colaboradores e pelos quais os Colaboradores podem contatar uns aos outros, incluindo endereços de e-mails de trabalho, endereços de e-mails alternativos, números de telefones de trabalho, números de telefones domésticos e números de telefones celulares. Tais informações são mantidas no escritório da Leads

13.1.7. Infraestrutura: A Leads tem à sua disposição um *no-break* interno com gerador que permite o escritório funcionar por várias horas em caso de queda de energia, e, também diversos links de internet que permitem o funcionamento contínuo em caso de queda ou lentidão em algum deles

13.1.8. Contingências Com Servidor de e-mail: O servidor de e-mail da Leads é baseado na "nuvem", o que implica acesso a qualquer ponto com internet, independentemente da localização. O serviço utilizado tem backups online protegidos por sistema de encriptação.

13.2. A equipe de Compliance da Leads será responsável por verificar a volta à normalidade das instalações físicas, observando-se os seguintes critérios: (i) Quando as instalações estiverem em condições de serem utilizadas; (ii) Quando não há risco para os funcionários para regresso às instalações; (iii) Quando há condições de serem desenvolvidos os procedimentos habituais de trabalhos; e (iv) Quando o suporte de TI estiver pronto para iniciar o processo de retorno verificando equipamentos, restaurando os acessos na rede, restabelecendo os acessos de código de segurança.

13.3. Ainda, todos os funcionários que permaneceram em suas residências ou em local designado pela equipe de Compliance serão avisados, pela própria equipe de Compliance, para o retorno às instalações da Leads.

13.4. No caso em que se decida que não é oportuno desativar o plano de contingência em aberto, o plano será mantido e os procedimentos de recuperação serão reavaliados. Uma vez aprovado o retorno ao ambiente normal de trabalho, a equipe de Compliance informará a todos os funcionários, e coordenará a comunicação externa sobre o fim do processo de contingência.

13.5. Quaisquer dúvidas ou questões pertinentes aos temas elencados neste código, devem ser encaminhadas ou esclarecidas com o Diretor de Compliance.

***** ***** ***** ***** *****

ANEXO I – TERMO DE ADESÃO

Manual de Controles Internos e Compliance

DE ACORDO:

Declaro que li, compreendi e concordei com todas as políticas integrantes do presente **Manual de Controles Internos e Compliance** ("Manual de Compliance"), aderindo de forma expressa e inequívoca aos seus termos. Declaro ainda que não tive conhecimento de quaisquer circunstâncias que não foram reportadas ao Diretor de Compliance ("Diretor de Compliance") que poderiam vir a conflitar com este Manual de Compliance, seja de natureza pessoal ou familiar, bem como referente a qualquer outro Colaborador. Afirmo ter conhecimento das responsabilidades relativas a este Manual de Compliance conforme descrito neste documento.

Data: ___/___/20___

_____

Colaborador

Nome:

Identidade:

***** ***** ***** ***** *****