

MANUAL DE COMPLIANCE

Multiplike Securitizadora S.A



MULTIPLIKE

JUNHO/2026

Sumário

1. INTRODUÇÃO.....	2
Aplicabilidade do Manual.....	3
Ambiente Regulatório	3
Termo de Compromisso	3
2. POLÍTICA DE COMPLIANCE	4
Responsabilidades e Obrigações.....	4
Garantia de Independência.....	5
Dúvidas ou Ações Contrárias aos Princípios e Normas do Manual.....	5
Acompanhamento das Políticas Descritas neste Manual	5
Sanções.....	5
Dever de Reportar.....	5
3. POLÍTICA DE CONFIDENCIALIDADE.....	6
Sigilo e Conduta.....	6
4. POLÍTICA DE SEGREGAÇÃO DAS ATIVIDADES.....	7
Objetivo e Definição.....	7
5. POLÍTICA DE SEGURANÇA E SEGURANÇA CIBERNÉTICA	7
Identificação de Riscos	7
Ações de Prevenção e Proteção.....	8
Acesso Remoto e Controle de Acesso.....	8
Firewall, Software, Varreduras e Backup	8
Plano de Identificação e Resposta	8
6. POLÍTICA ANTICORRUPÇÃO.....	8
Introdução.....	8
Abrangência	9
7. VIGÊNCIA E ATUALIZAÇÃO	9

1. INTRODUÇÃO

Este Manual de Regras, Procedimentos e Controles Internos (“Manual”), elaborado em conformidade com a Resolução CVM nº 60, de 23 de dezembro de 2021, conforme alterada (“Resolução CVM nº 60”), com a Lei nº 14.430, de 3 de agosto de 2022 (“Lei nº 14.430”), com o Código ANBIMA de Securitização e Estruturação de Mercado de Capitais (“Código ANBIMA de Securitização”) e com as demais orientações da Comissão de Valores Mobiliários (“CVM”), tem por objetivo estabelecer normas, princípios, conceitos e valores que orientam a conduta de

todos aqueles que possuam cargo, função, posição, relação societária, empregatícia, comercial, profissional, contratual ou de confiança (“Colaboradores”) com a securitizadora do Grupo Multiplike (“Securitizadora”), tanto na sua atuação interna quanto na comunicação com os diversos públicos.

Na busca incessante da satisfação dos investidores e demais participantes das operações de securitização, a Securitizadora atua com total transparência, respeito às leis, às normas e aos demais participantes do mercado financeiro e de capitais.

Dessa forma, este Manual reúne as diretrizes que devem ser observadas pelos Colaboradores no desempenho da atividade profissional, visando ao atendimento de padrões éticos cada vez mais elevados, refletindo a identidade cultural e os compromissos que a Securitizadora assume nos mercados em que atua.

A Securitizadora e seus Colaboradores não admitem e repudiam qualquer manifestação de preconceito relacionada à origem, etnia, religião, classe social, sexo, deficiência física ou qualquer outra forma de discriminação.

Aplicabilidade do Manual

Este Manual aplica-se a todos os Colaboradores que, por meio de suas relações com ou funções na Securitizadora, possam ter ou vir a ter acesso a informações confidenciais ou privilegiadas de natureza financeira, técnica, comercial, estratégica, negocial ou econômica, dentre outras, relativas às emissões de Certificados de Recebíveis (CRI, CRA e CR), aos direitos creditórios que lastreiam tais emissões, aos cedentes, devedores e investidores.

Ambiente Regulatório

Este Manual é parte integrante das regras que regem a relação societária ou de trabalho dos Colaboradores, os quais, ao assinar o termo de recebimento e compromisso, aceitam expressamente as normas, princípios, conceitos e valores aqui estabelecidos.

Todos os Colaboradores devem assegurar-se do perfeito entendimento das leis e normas aplicáveis à Securitizadora, em especial a Resolução CVM nº 60, a Lei nº 14.430 e o Código ANBIMA de Securitização, bem como do completo conteúdo deste Manual.

Termo de Compromisso

Todo Colaborador, ao receber este Manual, firmará o Termo de Recebimento e Compromisso, por meio do qual reconhece e confirma seu conhecimento e concordância com os termos deste Manual, comprometendo-se a zelar pela aplicação das normas de compliance e princípios nele expostos. Periodicamente, poderá ser requisitada a assinatura de novos termos.

O descumprimento, suspeita ou indício de descumprimento de quaisquer das normas estabelecidas neste Manual ou das demais normas aplicáveis às atividades da Securitizadora deverá ser levado à apreciação do Diretor responsável pelo compliance, a quem competirá aplicar as sanções decorrentes de tais desvios, garantido ao Colaborador amplo direito de defesa.

É dever de todo Colaborador informar ao Diretor responsável pelo compliance sobre violações ou possíveis violações dos princípios e normas aqui dispostos. Caso a violação ou suspeita recaia sobre o próprio Diretor responsável pelo compliance, o Colaborador deverá informar diretamente aos demais administradores da Securitizadora.

2. POLÍTICA DE COMPLIANCE

Responsabilidades e Obrigações

A coordenação direta das atividades relacionadas a este Manual é atribuição do diretor estatutário da Securitizadora indicado como responsável pelo cumprimento de regras, políticas, procedimentos e controles internos (“Diretor responsável pelo Compliance”), nos termos da Resolução CVM nº 60.

São obrigações do Diretor responsável pelo compliance:

- acompanhar as políticas descritas neste Manual;
- levar quaisquer pedidos de autorização, orientação ou esclarecimento, bem como casos de ocorrência, suspeita ou indício de prática em desacordo com este Manual, para apreciação dos administradores da Securitizadora;
- atender prontamente todos os Colaboradores e identificar possíveis condutas contrárias a este Manual;
- centralizar informações e revisões periódicas dos processos de compliance, principalmente quando houver alteração nas políticas vigentes;
- assessorar a administração quanto ao entendimento, interpretação e impacto da legislação, analisando periodicamente as normas emitidas pela CVM e demais órgãos competentes;
- elaborar relatório anual das operações identificadas como suspeitas e comunicadas às autoridades competentes, no âmbito da política de prevenção à lavagem de dinheiro;
- encaminhar aos órgãos de administração, anualmente, relatório contendo as conclusões dos exames efetuados, as recomendações a respeito de eventuais deficiências com cronograma de saneamento, e a manifestação dos diretores responsáveis a respeito das deficiências encontradas em verificações anteriores, devendo o relatório permanecer à disposição da CVM na sede da Securitizadora;
- definir os princípios éticos a serem observados por todos os Colaboradores e promover sua ampla divulgação, inclusive por meio de treinamentos periódicos;
- apreciar os casos de potencial descumprimento dos preceitos éticos e de compliance, bem como analisar situações não previstas;
- garantir o sigilo de eventuais denunciadores de delitos ou infrações, exceto nos casos de necessidade de testemunho judicial;
- solicitar, sempre que necessário, o apoio de auditoria interna ou externa ou de outros assessores profissionais;
- aplicar as eventuais sanções aos Colaboradores; e
- analisar situações que possam ser caracterizadas como conflitos de interesse, pessoais ou profissionais, inclusive, mas não limitadamente, as que envolvam: relacionamento com cedentes, devedores ou prestadores de serviço das operações; recebimento de favores ou presentes de contrapartes; análise de operações com empresas com as quais o Colaborador possua relação pessoal ou investimento próprio; e participação em atividade política.

Todo Colaborador que tomar conhecimento de informações ou situações que possam afetar os interesses da Securitizadora, gerar conflitos ou se revelarem contrárias a este Manual deverá informar ao Diretor para a adoção das providências cabíveis.

A Securitizadora poderá manter um Comitê de Compliance, responsável por averiguar e debater possíveis falhas e oportunidades de aprimoramento nos controles internos, além de outros assuntos pertinentes à área.

Garantia de Independência

A área de compliance atua com independência em relação às demais áreas da Securitizadora, devendo ser envolvida na análise das operações sob a ótica de conformidade e riscos. Compete a essa área avaliar e questionar os riscos das operações, inclusive podendo exercer poder de veto prévio à formalização de emissões ou operações sempre que identificar potenciais riscos regulatórios, reputacionais, de prevenção à lavagem de dinheiro (PLD) ou quaisquer outros que possam comprometer a integridade e a conformidade da atividade.

A área de compliance exerce suas atividades de forma completamente independente das demais áreas e poderá exercer seus poderes e autoridade com relação a qualquer Colaborador.

Dúvidas ou Ações Contrárias aos Princípios e Normas do Manual

Em caso de dúvida em relação a quaisquer das matérias constantes deste Manual, é imprescindível que se busque auxílio imediato junto ao Diretor responsável. Mesmo a simples suspeita de potencial conflito ou de ação que possa afetar os interesses da Securitizadora deve seguir essa orientação.

Toda solicitação que dependa de autorização, orientação ou esclarecimento do Diretor, bem como eventual ocorrência, suspeita ou indício de prática em desacordo com este Manual, deve ser dirigida ao Diretor de Compliance, preferencialmente por e-mail.

Acompanhamento das Políticas Descritas neste Manual

Mediante ocorrência, suspeita ou indício de descumprimento de quaisquer das regras estabelecidas neste Manual, o Diretor responsável pelo compliance utilizará os registros e sistemas de monitoramento eletrônico para verificar a conduta dos Colaboradores envolvidos. As ferramentas de trabalho disponibilizadas pela Securitizadora, incluindo correio eletrônico, poderão ser monitoradas, sem que isso represente invasão de privacidade.

Será realizado monitoramento periódico, sobre amostragem dos Colaboradores escolhida aleatoriamente, para verificação dos arquivos eletrônicos, com o objetivo de identificar possíveis situações de descumprimento. O Diretor de Compliance verificará rotineiramente os níveis de controles internos junto a todas as áreas, propondo a criação de novos controles e melhorias naqueles considerados deficientes.

Sanções

A eventual aplicação de sanções decorrentes do descumprimento dos princípios estabelecidos neste Manual é de responsabilidade do Diretor responsável pelo compliance, garantido ao Colaborador amplo direito de defesa. Podem ser aplicadas, entre outras, penas de advertência, suspensão, desligamento ou exclusão por justa causa, no caso de sócios, ou demissão por justa causa, no caso de empregados, nos termos do artigo 482 da Consolidação das Leis do Trabalho, sem prejuízo do direito da Securitizadora de pleitear indenização pelos prejuízos suportados.

Dever de Reportar

O Colaborador que tiver conhecimento ou suspeita de ato incompatível com este Manual deverá reportá-lo imediatamente ao Diretor de Compliance. Nenhum Colaborador sofrerá

retaliação por comunicar, de boa-fé, violações ou potenciais violações. Os comunicados e investigações serão tratados de maneira confidencial. O Colaborador que se omitir de tal obrigação poderá sofrer ação disciplinar.

3. POLÍTICA DE CONFIDENCIALIDADE

Sigilo e Conduta

As disposições deste capítulo aplicam-se aos Colaboradores que, por meio de suas funções na Securitizadora, possam ter ou vir a ter acesso a informações confidenciais, reservadas ou privilegiadas de natureza financeira, técnica, comercial, estratégica, negocial ou econômica, dentre outras. Todos os Colaboradores deverão firmar o Termo de Confidencialidade.

Nenhuma Informação Confidencial deve, em qualquer hipótese, ser divulgada fora da Securitizadora em desacordo com as normas legais e de compliance. São consideradas Informações Confidenciais, independentemente do meio em que estejam contidas, quaisquer informações sobre a Securitizadora, sobre as empresas do seu conglomerado, seus sócios, investidores, cedentes e devedores, incluindo:

- know-how, técnicas, diagramas, modelos e programas de computador;
- informações técnicas e financeiras relacionadas às operações de securitização, incluindo dados de cedentes, devedores, direitos creditórios e investidores;
- estruturas de operações, lastros, valores, garantias e demais condições de emissões analisadas ou realizadas;
- relação de cedentes, devedores, contrapartes comerciais, fornecedores e prestadores de serviço;
- informações estratégicas ou mercadológicas relativas à atividade da Securitizadora, inclusive alterações societárias, operações ainda não divulgadas e resultados financeiros antes de sua publicação; e
- demais informações obtidas junto a sócios, diretores, funcionários, estagiários, representantes, consultores, cedentes, devedores, fornecedores e prestadores de serviço.

A Informação Confidencial não pode ser divulgada, em hipótese alguma, a terceiros não Colaboradores ou a Colaboradores não autorizados. A revelação de Informações Confidenciais a autoridades governamentais ou em virtude de decisão judicial deverá ser previamente informada ao Diretor responsável pelo compliance.

Em nenhuma hipótese as Informações Confidenciais poderão ser utilizadas para a prática de Insider Trading, Dicas ou Front-running:

- **Insider Trading:** compra e venda de títulos ou valores mobiliários com base no uso de Informação Confidencial, com o objetivo de obter benefício próprio ou de terceiros.
- **Dica:** transmissão, a qualquer terceiro estranho às atividades da Securitizadora, de Informação Confidencial que possa ser usada na compra e venda de títulos ou valores mobiliários.
- **Front-running:** prática que envolve aproveitar Informação Confidencial para realizar ou concluir uma operação antes de outros.

Os Colaboradores deverão guardar sigilo sobre qualquer Informação Confidencial à qual tenham acesso, durante e após o término do relacionamento profissional, respondendo pelos danos causados em caso de descumprimento. O acesso acidental a Informação Confidencial deverá ser imediatamente comunicado ao Diretor responsável pelo compliance.

4. POLÍTICA DE SEGREGAÇÃO DAS ATIVIDADES

Objetivo e Definição

Todas as empresas do Grupo Multiplike estão devidamente segregadas, física e funcionalmente, da Securitizadora, não havendo compartilhamento de equipes, sistemas, diretórios ou quaisquer outros elementos que possam possibilitar conflito de interesses.

A Securitizadora deve exercer suas atividades com lealdade e boa-fé em relação aos investidores das emissões, evitando práticas que possam ferir a relação fiduciária. Diante de uma situação de potencial conflito de interesses, a Securitizadora informará aos investidores que está agindo em conflito e as fontes desse conflito, sem prejuízo do dever de informar após o surgimento de novos conflitos. As informações confidenciais relativas às operações não deverão ser divulgadas a terceiros sem a prévia e expressa autorização do Diretor responsável pelo compliance.

5. POLÍTICA DE SEGURANÇA E SEGURANÇA CIBERNÉTICA

As medidas de segurança da informação têm por finalidade minimizar as ameaças aos negócios da Securitizadora e às disposições deste Manual, buscando, principalmente, a proteção de Informações Confidenciais. A política leva em consideração o porte, o perfil de risco, o modelo de negócio e a complexidade das atividades desenvolvidas. A coordenação ficará a cargo do Diretor responsável pelo compliance, responsável por sua revisão, pela realização de testes e pelo treinamento dos Colaboradores.

Identificação de Riscos

A Securitizadora identificou os seguintes principais riscos internos e externos que precisam de proteção:

- **Dados e Informações:** Dados e Informações: as Informações Confidenciais, incluindo dados de investidores, cedentes, devedores, Colaboradores e da própria Securitizadora, das operações e direitos creditórios, e as comunicações internas e externas;
- **Sistemas:** informações sobre os sistemas utilizados e as tecnologias desenvolvidas interna e externamente, suas ameaças e vulnerabilidades;
- **Processos e Controles:** processos e controles internos que sejam parte da rotina das áreas de negócio; e
- **Governança da Gestão de Risco:** a eficácia da gestão de risco quanto às ameaças e planos de ação, contingência e continuidade de negócios.

No que se refere especificamente à segurança cibernética, a Securitizadora identificou:

- Malware – softwares desenvolvidos para corromper computadores e redes (vírus, cavalo de troia, spyware e ransomware);
- Engenharia social – métodos de manipulação para obter informações confidenciais (pharming, phishing, vishing, smishing e acesso pessoal);

- Ataques de DDoS e botnets – ataques que visam negar ou atrasar o acesso aos serviços ou sistemas; e
- Invasões (advanced persistent threats) – ataques realizados por invasores sofisticados para detectar e explorar fragilidades específicas no ambiente tecnológico.

Ações de Prevenção e Proteção

A Securitizadora realiza controle efetivo do acesso a arquivos que contenham Informações Confidenciais, disponibilizando-os somente aos Colaboradores efetivamente envolvidos na operação que demanda seu conhecimento. A troca de informações deve pautar-se no conceito de que o receptor necessita da informação para o desempenho de suas atividades.

O descarte de informações confidenciais, físicas ou digitais, deve ser feito de forma a impossibilitar sua recuperação. É proibida a conexão de equipamentos não autorizados à rede.

Acesso Remoto e Controle de Acesso

Os Colaboradores autorizados deverão manter a utilização apenas em dispositivos com login e senha, manter softwares de proteção contra malware atualizados, relatar qualquer violação ou ameaça de segurança e não armazenar Informações Confidenciais em dispositivos pessoais.

Firewall, Software, Varreduras e Backup

A Securitizadora utiliza firewall projetado para evitar e detectar conexões não autorizadas, mantém proteção atualizada contra malware e conduz varreduras periódicas. Mantém, ainda, plano de manutenção com varreduras e patches regulares, bem como medidas de backup testadas regularmente, atualmente objeto de backup diário com uso de computação em nuvem.

Plano de Identificação e Resposta

Qualquer suspeita de infecção, acesso não autorizado, comprometimento da rede ou vazamento de Informações Confidenciais, ainda que involuntário, deverá ser informada prontamente ao CEO, que determinará os membros da administração e, se aplicável, as agências reguladoras e os investidores que deverão ser notificados.

A resposta observará os seguintes critérios: avaliação do tipo de incidente e das informações acessadas; identificação dos sistemas a desconectar; determinação dos papéis e responsabilidades; avaliação da necessidade de recuperação dos serviços; avaliação da necessidade de notificação das partes internas e externas; avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente, a fim de garantir o tratamento equânime da informação aos investidores; e determinação do responsável pelas perdas decorrentes do incidente.

6. POLÍTICA ANTICORRUPÇÃO

Introdução

A Securitizadora está sujeita às leis e normas de anticorrupção, incluindo, mas não se limitando, à Lei nº 12.846/13 e ao Decreto nº 11.129/22 (“Normas de Anticorrupção”). Qualquer violação desta Política e das Normas de Anticorrupção pode resultar em penalidades civis e administrativas severas para a Securitizadora e seus Colaboradores, além de impactos reputacionais, sem prejuízo de eventual responsabilidade criminal dos indivíduos envolvidos.

Abrangência

As Normas de Anticorrupção estabelecem que as pessoas jurídicas serão responsabilizadas objetivamente, nos âmbitos administrativo e civil, pelos atos lesivos praticados por seus sócios e colaboradores contra a administração pública, nacional ou estrangeira, sem prejuízo da responsabilidade individual do autor, coautor ou partícipe. Considera-se agente público, sem limitação, qualquer indivíduo a serviço, empregado ou em função pública, candidato ou ocupante de cargo público, e qualquer partido político ou seu representante, estendendo-se as exigências aos familiares de funcionários públicos até o segundo grau.

7. VIGÊNCIA E ATUALIZAÇÃO

Este Manual será revisado anualmente, e sua alteração ocorrerá sempre que constatada a necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterado a qualquer tempo em razão de circunstâncias que demandem tal providência, devendo permanecer à disposição da CVM na sede da Securitizadora.