POLÍTICA DE *COMPLIANCE*, GERENCIAMENTO DE RISCO OPERACIONAL E CONTROLES INTERNOS

Atualizada em maio de 2025

ÍNDICE

1. OBJETIVO

A Política de *Compliance*, Gerenciamento de Risco Operacional e Controles Internos ("Política") da Playsec Securitizadora S.A. ("Playsec Securitizadora", "Playsec" ou "Companhia") consiste em um conjunto de diretrizes, responsabilidades e instrumentos que devem ser adotados para garantir o devido gerenciamento dos riscos de conformidade ou *compliance* da Companhia ("Gerenciamento de Compliance") e não constitui tratamento exaustivo de todas as leis, regulamentos e políticas aplicáveis às atividades da Playsec Securitizadora.

Esta Política também objetiva estabelecer os conceitos, definições e processos que devem ser adotados para o gerenciamento dos riscos operacionais na Playsec visando estabelecer padrões mínimos para o processamento das operações, gestão dos patrimônios, processos administrativos, jurídicos e de relacionamento com clientes.

Esta Política deve orientar toda a companhia abrangendo também, as atividades de terceiros associados à processos críticos.

2. ESCOPO DE APLICAÇÃO E ABRANGÊNCIA

Todos os acionistas, membros do Conselho de Administração da Companhia ("CA"), diretores, gestores, colaboradores e terceiros, independentemente da função ou cargo, que, de forma direta ou indireta atuam nas atividades negociais da Playsec Securitizadora (em conjunto os "Colaboradores"), devem aderir às diretrizes desta Política.

É dever de todos os Colaboradores informar a respeito de inconsistências em procedimentos e práticas definidos pela Política, com a finalidade de zelar pelo cumprimento das regras ali expostas. É dever de todos os Colaboradores notificar potenciais condutas indevidas sob o ponto de vista legal, regulatório ou ético ao Diretor de Compliance.

O não cumprimento da Política sujeitará o Colaborador a ações disciplinares, que podem incluir o término do contrato de trabalho e, quando cabível, o encaminhamento às autoridades governamentais e organizações de autorregulamentação competentes.

Os Colaboradores serão considerados pessoalmente responsáveis por quaisquer atos impróprios ou ilícitos que cometerem durante suas atividades. As violações de leis, regulamentos e políticas internas também podem sujeitar os Colaboradores a medidas disciplinares, incluindo a rescisão de contrato de trabalho, bem como ações de autoridades reguladoras e/ou criminais.

3. DEFINIÇÃO DE "CONFORMIDADE" E "RISCO DE CONFORMIDADE"

Para fins desta Política, o termo "conformidade" (ou "*compliance*", em inglês) significa agir de acordo com (ou em conformidade com) leis e regulamentos externos e internos aplicáveis à Playsec Securitizadora, em especial a legislação do mercado de capitais, anticorrupção e demais regulamentações correlatas aplicáveis às companhias securitizadoras, em observância aos padrões éticos e morais adotados pela Companhia em seu Código de Ética e Conduta ("Código").

Já a expressão "risco de conformidade" diz respeito aos eventuais riscos reputacionais e de responsabilização da Companhia na hipótese em que não atenda, de forma adequada, as diretrizes definidas em normas externas e internas as quais ela se encontra submetida, o que inclui o não cumprimento, por parte do tomador ou da contraparte, de suas respectivas obrigações financeiras nos termos pactuados.

Define-se o risco operacional como a possibilidade da ocorrência de perdas resultantes de eventos externos ou de falha, deficiência ou inadequação de processos internos, pessoas ou sistemas incluindo o risco legal associado à inadequação ou deficiência em contratos firmados pela companhia, bem como a sanções em razão de descumprimento de dispositivos legais e as indenizações por danos a terceiros decorrentes das atividades desenvolvidas pela companhia.

Define-se Controles Internos como o conjunto de procedimentos, métodos ou rotinas executadas pelos Colaboradores da Companhia para garantir, com razoável certeza, a concretização dos objetivos da empresa, proteger os ativos da Instituição, verificar a exatidão e a fidedignidade de seus dados contábeis, incrementar a eficiência operacional e promover a observância das diretrizes administrativas estabelecidas, visando à condução ordenada e segura dos negócios da Playsec.

A Securitizadora adota as seguintes categorias de eventos de risco operacional:

I - Fraudes internas: Perdas ocasionadas por atos com intenção de fraudar, apropriar-se indevidamente ou burlar regulamentos, a lei ou a política da empresa praticados por colabores da Playsec, (excluindo diversidade / acontecimentos discriminatórios, que envolvam pelo menos uma parte interna

II - Fraudes externas: Perdas ocasionadas por atos de um tipo com intenção de fraudar, apropriar-se indevidamente ou burlar a lei, praticados por terceiros;

III - Demandas trabalhistas e segurança deficiente do local de trabalho: Perdas decorrentes de atos inconsistentes com contratos ou leis trabalhistas, de saúde ou segurança, do pagamento de reclamações por lesões corporais, ou de diversidade / eventos discriminatórios;

IV - Práticas inadequadas relativas a clientes, produtos e serviços: Perdas decorrentes de uma falha não-intencional ou negligência em cumprir uma obrigação com clientes específicos (incluindo exigências fiduciárias e de adequação), ou de natureza ou desenho de um produto;

V - Danos a ativos físicos próprios ou em uso pela Securitizadora: Perdas decorrentes de danos aos ativos físicos ocasionados por desastres naturais ou outros acontecimentos;

VI - Situações que acarretem a interrupção das atividades da Securitizadora: Perdas decorrentes de ruptura nos negócios;

VII - Falhas em sistemas, processos ou infraestrutura de tecnologia da informação (TI): Perdas decorrentes de falhas e/ou interrupção dos

sistemas de informação ou da infraestrutura tecnológica da organização;

VIII - Falhas na execução, no cumprimento de prazos ou no gerenciamento das atividades da Securitizadora.

4. LEIS E NORMAS APLICÁVEIS

Para fins de cumprimento desta Política, serão levadas em consideração as seguintes leis e regulamentações:

a) Normas Internas

- Plano de Continuidade do Negócio;
- Políticas internas; e
- Código de Ética e Conduta.

b) Normas Externas

- Códigos da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("ANBIMA"):
  - Código de Ética;
  - Código para Ofertas Públicas de Distribuição e Aquisição de Valores Mobiliários
  - Código para o Programa de Certificação Continuada; e
  - Código dos Processos da Regulação e Melhores Práticas.

c) Legislação Nacional

- Lei nº 12.846 de 1º de agosto de 2013 ("Lei Anticorrupção");

- Decreto nº 8.420 de 18 de março de 2015 ("Decreto n° 8.420/2015"), que regulamenta a Lei Anticorrupção;
- Lei n° 9.613 de 3 de março de 1998, conforme alterada ("Lei de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo"), que dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos na referida lei; e criou o Conselho de Controle de Atividades Financeiras ("COAF"); além de outras providências;
- Lei n° 12.683 de 9 de julho de 2012, que altera a Lei de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo, para tornar mais eficiente a persecução penal dos crimes de lavagem de dinheiro;
- Lei nº 13.260 de 17 de março de 2016, que regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal ("CF"), disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista;
- A Lei nº 11.076, de 30 de dezembro de 2004 ("Lei nº 11.076");
- A Lei nº 14.430, de 3 de agosto de 2022 ("Lei nº 14.430");
- A Lei nº 13.810 de 8 de março de 2019, que dispõe sobre o cumprimento de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas ("CSNU"), incluída a indisponibilidade de ativos de pessoas naturais e jurídicas e de entidades, e a designação nacional de pessoas investigadas ou acusadas de terrorismo, de seu financiamento ou de atos a ele correlacionados;
- Lei n° 14.133 de 1° de abril de 2021 ("Nova Lei de Licitações e Contratos Administrativos");
- Decreto-Lei n° 2.848 de 7 de dezembro de 1940 ("Código Penal");
- A Resolução COAF n° 36 de 10 de março de 2021 ("Resolução COAF n° 36/2021"), que disciplina a forma de adoção de políticas, procedimentos e controles internos de prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao financiamento da proliferação de armas de destruição em massa

que permitam o atendimento ao disposto nos arts. 10 e 11 da Lei de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo, por aqueles que se sujeitem, nos termos do seu art. 14, § 1º, à supervisão do COAF;

- A Resolução COAF nº 40 de 22 de novembro de 2021 ("Resolução COAF n° 40/2021"), que dispõe sobre procedimentos a serem observados, em relação a pessoas expostas politicamente, por aqueles que se sujeitam à supervisão do COAF;
- A Resolução da Comissão de Valores Mobiliários ("CVM") nº 160, de 13 de julho de 2022, conforme alterada, que dispõe sobre as ofertas públicas de distribuição de valores mobiliários, nos mercados primário ou secundário;
- A Resolução da CVM nº 30, de 11 de maio de 2021 ("Resolução CVM nº 30/2021"), que dispõe sobre o dever de verificação da adequação dos produtos, serviços e operações ao perfil do cliente;
- A Resolução CVM nº 31 de 19 de maio de 2021 ("Resolução CVM nº 31/2021"), que dispõe sobre a prestação de serviços de depósito centralizado de valores mobiliários;
- A Resolução CVM nº 50 de 31 de agosto de 2021 ("Resolução CVM nº 50/2021"), que dispõe sobre a prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao financiamento da proliferação de armas de destruição em massa no âmbito do mercado de valores mobiliários;
- A Resolução CVM nº 60 de 23 de dezembro de 2021 ("Resolução CVM nº 60/2021"), que dispõe sobre as companhias securitizadoras de direitos creditórios registradas na CVM;
- A Carta Circular n° 4.001 de 29 de janeiro de 2020 do Banco Central do Brasil ("Carta Circular BACEN n° 4.001/2020" e "BACEN", respectivamente), que divulga relação de operações e situações que podem configurar indícios de ocorrência dos crimes de "lavagem" ou ocultação de bens, direitos e valores, de que trata a Lei de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo, previstos na Lei nº 13.260, de 16 de março de 2016, passíveis de comunicação ao COAF;

- A Circular BACEN nº 3.978 de 23 de janeiro de 2020 ("Circular BACEN n° 3.978/2020"), que revoga a Carta Circular BACEN nº 3.350 de 12 de novembro de 2008;
- A Carta Circular BACEN n° 3.977 de 30 de setembro de 2019 ("Carta Circular BACEN n° 3.977/2019"), que especifica e esclarece aspectos operacionais dos procedimentos estabelecidos na Circular nº 3.942, de 21 de maio de 2019, para a execução de medidas determinadas pela Lei nº 13.810/2019, que dispõe sobre o cumprimento de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas, incluída a indisponibilidade de ativos de pessoas naturais e jurídicas e de entidades, bem como a designação nacional de pessoas investigadas ou acusadas de terrorismo, seu financiamento ou atos correlacionados;
- A Resolução BACEN n° 44 de 24 de novembro de 2020 ("Resolução BACEN n° 44/2020"), que estabelece procedimentos para a execução pelas instituições autorizadas a funcionar pelo BACEN das medidas determinadas pela Lei nº 13.810, de 8 de março de 2019, que dispõe sobre o cumprimento de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas, incluída a indisponibilidade de ativos de pessoas naturais e jurídicas e de entidades, e a designação nacional de pessoas investigadas ou acusadas de terrorismo, de seu financiamento ou de atos a ele correlacionados;
- A Instrução Normativa n° 1.037 de 4 de junho de 2010 da Receita Federal do Brasil ("IN RFB n° 1.037/2010" e "RFB", respectivamente), conforme alterada, que relaciona países ou dependências com tributação favorecida e regimes fiscais privilegiados;
- Resoluções da Comissão de Ética Pública do Governo Federal;
- Portaria da Controladoria-Geral da União ("CGU") n° 909 de 7 de abril de 2015 ("Portaria CGU n° 909/15"), que dispõe sobre a avaliação de programas de integridade de pessoas jurídicas;
- Portaria da CGU n° 910 de 7 de abril de 2015 ("Portaria CGU n° 910/15"), que define os procedimentos para apuração da responsabilidade administrativa e para celebração do acordo de leniência de que trata a Lei Anticorrupção;

- Instrução Normativa da CGU n° 1 de 7 de abril de 2015 ("IN CGU n° 01/2015)", que estabelece metodologia para a apuração do faturamento bruto e dos tributos a serem excluídos para fins de cálculo da multa a que se refere o art. 6º da Lei Anticorrupção;
- A Instrução Normativa da CGU nº 2 de 7 de abril de 2015 ("IN CGU n° 02/2015)", que traz regras para operacionalizar o Cadastro Nacional de Empresas Inidôneas e Suspensas ("CEIS") e do Cadastro Nacional de Empresas Punidas ("CNEP"); e
- Demais leis e regulamentos supervenientes que venham a ser aplicáveis à Playsec Securitizadora.

d) Legislação Anticorrupção Estrangeira

- *Foreign Corrupt Practices Act* ("FCPA"); e
- *U.K. Bribery Act* ("UKBA").

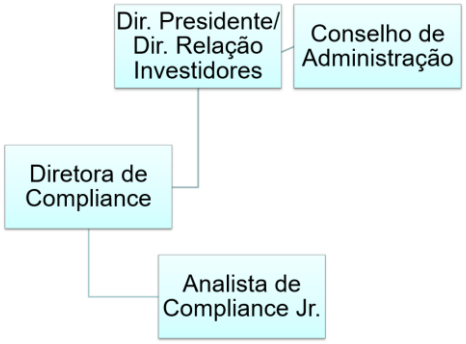
e) Guias/Diretrizes Internacionais

- *FCPA Resource Guide*; e
- *The Bribery Act 2010 Guidance*.

5. METODOLOGIA E INSTRUMENTOS

A metodologia de gestão utilizada no Gerenciamento de Risco Operacional da companhia é baseada no COSO – Recomendações de Governança em Gerenciamento de Riscos emitidos pelo "Committee of Sponsoring Organizations of the Treadway Commission"

6. ESTRUTURA ORGANIZACIONAL PARA O GERENCIAMENTO DE RISCOS E COMPLIANCE



7. MONITORAMENTO DE NORMAS EXTERNAS

A Diretoria de *Compliance* da Playsec Securitizadora acompanhará as normas e diretrizes publicadas pela CVM, ANBIMA e B3 em seus respectivos sítios eletrônicos, encaminhando as novas publicações às unidades da Companhia para a avaliação e implementação de ações a serem tomadas, caso necessário.

A Diretoria de *Compliance* também deverá acompanhar os fatos relevantes publicados pela CVM, em seu respectivo sítio eletrônico, encaminhando as informações às unidades da Playsec Securitizadora para a avaliação e implementação de ações a serem tomadas, caso necessário.

As ações a serem implementadas pelos gestores deverão ser encaminhadas para a Diretoria de *Compliance* para acompanhamento, monitoramento e para que ela avalie se as ações são suficientes e adequadas para atender às exigências das normas emitidas.

É de responsabilidade dos gestores avaliar se as normas recebidas afetam as atividades dos prestadores de serviços vinculados à suas atividades, devendo informar à Diretoria de *Compliance* tal situação.

Periodicamente a Diretoria de *Compliance* realizará treinamento acerca das normas aplicáveis às atividades da Companhia.

8. DIRETRIZES GERAIS, REGRAS E REQUERIMENTOS

a. **Diretrizes**

A Playsec Securitizadora deverá contar com uma estrutura de Gerenciamento de *Compliance* que:

i. Avalie os riscos e defina medidas de mitigação dos riscos identificados;

ii. Elabore e estabeleça as políticas e procedimentos internos;

iii. Tenha suporte da Alta Administração da Companhia;

iv. Estabeleça e gerencie os canais de comunicação da Companhia;

v. Conduza treinamentos de *compliance*;

vi. Conduza processos de *due diligence* de terceiros;

vii. Realize auditorias dos processos da Companhia;

viii. Dissemine a cultura de risco;

ix. Monitore o Programa de Integridade da Companhia;

x. Disponibilize e gerencie o Canal de Denúncia, mecanismo utilizado pela Playsec Securitizadora para reporte ou auxílio de forma anônima e/ou confidencial em relação a condutas ou suspeitas de condutas criminosas;

xi. Dê suporte às três linhas de defesa da Companhia:

- **1ª Linha de defesa:** áreas executivas representadas pelos gestores das áreas de negócios e suporte que devem gerenciar e implementar controles para monitorar e mitigar os riscos operacionais sob suas responsabilidades;
- **2ª Linha de defesa:** estrutura de Gestão de Riscos que abrange a Diretoria de *Compliance*, que é responsável pela definição e metodologia para identificar, avaliar, monitorar, controlar e mitigar os riscos e aderência regulatória dos processos; e
- **3ª Linha de defesa:** processos de auditoria para verificação e avaliação independente e periódica dos processos e áreas da Securitizadora Financeira.

b. Regra Geral

A Playsec Securitizadora deverá ter definida e operacionalizada uma estrutura eficaz de processos, técnicas, instrumentos e responsabilidades visando o gerenciamento do Risco

Operacional da Organização de forma a atender as diretrizes estabelecidas pelos órgãos normativas e melhores práticas de mercado.

c. Requerimentos Gerais

A estrutura de gerenciamento deve:

I. Disponibilizar processos para identificação, avaliação, monitoramento, controle e mitigação dos riscos operacionais relativos aos processos da companhia. Essa estrutura deve abranger também a avaliação e gerenciamento dos riscos nos contextos de:

   a. Criação ou desativação de produtos

   b. Grandes mudanças na companhia

II. Dedicar atenção específica aos processos e iniciativas executadas, por ou com fornecedores e terceiros

   a. As avaliações relacionadas a terceiros e fornecedores serão expressas no momento de sua contratação através de uma análise Know Your Partner (KYP)

   b. Garantir a formalização dos critérios de decisão quanto à terceirização de serviços e de seleção de seus prestadores, incluindo as condições contratuais mínimas necessárias para mitigar o risco operacional.

III. Implementar e manter um processo estruturado de comunicação e informação relativas ao gerenciamento de risco operacional incluindo a identificação e comunicação tempestivas à Diretoria de Compliance das falhas operacionais, exceções às políticas, normas e limites operacionais;

IV. A companhia deve contar com um processo de registro e gerenciamento das suas perdas e incidentes críticos incluindo a operacionalização do Comitê de Gerenciamento de Risco Operacional e Compliance;

   a. Esse Comitê é o colegiado onde os relatórios de risco, as perdas e os incidentes críticos ocorridos são considerados e gerenciados;

b. Ele deve ser composto pela alta administração, diretoria, gerente de todas as áreas da companhia e representante da área de Compliance

V. Periodicamente a companhia deve revisar os riscos em seus processos operacionais e gerenciais.

d. Requerimentos Detalhados

VI. O Programa de Gerenciamento de Riscos Operacionais é o conjunto de procedimentos e responsabilidades associados aos ciclos de revisão dos riscos e controles da Organização.

VII. Esses ciclos de revisão devem ocorrer:

a. quando da ocorrência de mudanças relevantes nas atividades ou processos operacionais;

b. quando da ocorrência de eventos de perdas significativas ou de incidentes críticos, neste caso como parte do processo de gerenciamento do evento.

VIII. A periodicidade da revisão dos riscos e controles (risk and control assessment) é definida em função da criticidade dos processos, e/ou riscos e/ou controles para a organização,

O nível de criticidade deve ser definido em função da dependência que a organização tem do processo e do grau em que uma falha crítica possa impactar os negócios ou representar perdas significativas para a organização.

IX. O resultado da avaliação dos riscos e controles deve ser registrado em uma Matriz de Risco permitindo a visualização e entendimento dos riscos, seus controles e mitigações.

X. Os riscos cujos controles e/ou mitigações não sejam adequados devem ser alvo de planos de ação tempestivos para sua adequação.

a. O acompanhamento dos planos de ação é de responsabilidade da Diretoria de Compliance.

XI. O não atendimento dos prazos definidos para a conclusão de um plano deve ser alvo da avaliação da hierarquia conforme sua criticidade.

   a. A prorrogação do prazo de atendimento deve ser aprovada pela diretoria;

   b. Reporte aos membros da diretoria sobre possíveis atrasos bem como seus motivos.

XII. Os controles e mitigações deverão ser testados periodicamente de acordo com o nível de criticidade inerente do processo a que ele está associado e com a classificação do controle.

XIII. As perdas significativas e incidentes críticos ocorridos no âmbito da Securitizadora devem ser registradas e gerenciadas tempestivamente de forma estruturada.

XIV. Essas perdas significativas e incidentes críticos deverão ser submetidos à avaliação do Comitê de Gerenciamento de Risco Operacional e Compliance;

XV. Caso o Comitê de Gerenciamento de Risco Operacional e Compliance ache necessário, serão definidos indicadores de gestão específicos para as perdas operacionais significativas ocorridas

A estrutura de gerenciamento do risco operacional deverá identificar e comunicar à diretoria alta administração e também acompanhar a solução das exceções, com relação às políticas e limites operacionais estabelecidos, verificadas no período.

9. ESTRUTURA ORGANIZACIONAL, ATRIBUIÇÕES E RESPONSABILIDADES

As responsabilidades relativas ao Gerenciamento de *Compliance* da Playsec Securitizadora estão definidas abaixo:

a) Alta Administração

- Aprovar, anualmente, as políticas internas e as estratégias a serem adotadas para o Gerenciamento de *Compliance* da Companhia;

- Viabilizar as condições necessárias para:
    - Garantir independência e adequada autoridade à Área de *Compliance* para o Gerenciamento de *Compliance* no âmbito da Companhia;
    - Prover e garantir o livre acesso dos responsáveis pela condução das atividades de *compliance* às informações, instrumentos e meios necessários para o devido exercício de suas atribuições;
- Assegurar:
    - A adequada gestão das políticas de *compliance* no âmbito da Companhia;
    - A efetividade e a continuidade da aplicação das políticas de *compliance*;

      A comunicação das políticas de *compliance* a todos os empregados e prestadores de serviços terceirizados relevantes; e
    - A disseminação de padrões de integridade e conduta ética como parte da cultura da Companhia; e
- Garantir que medidas corretivas sejam aplicadas quando falhas de *compliance* forem identificadas.

b) Diretoria Comercial

- Conduzir as atividades negociais da Companhia de forma a atender as normas emitidas pelos órgãos reguladores e à estrutura normativa interna;
- Garantir o fiel cumprimento das políticas de *compliance* no âmbito dos diversos níveis hierárquicos sob sua direção; e
- Promover e apoiar a aplicação da presente Política no âmbito da Companhia.

c) Área de *Compliance*

- Promover a disseminação das políticas de *compliance* no âmbito da Companhia;
- Manter as políticas de *compliance* atualizadas e monitorar o seu cumprimento;

- Manter os sistemas e atividades de *compliance* alinhados com as melhores práticas do mercado por meio de revisão e atualização periódicas, para que eventuais deficiências sejam pronta e integralmente corrigidas;
- Assegurar a existência de efetivos canais de comunicação e de divulgação das políticas e procedimentos internos para todos os níveis hierárquicos da Companhia, com o fim de garantir a disseminação de quaisquer informações relevantes;
- Testar e avaliar a aderência da Playsec Securitizadora às normas e às recomendações dos órgãos fiscalizadores e, quando aplicável, às políticas internas da Companhia;
- Garantir que os desvios às normas e políticas internas sejam prontamente identificados, comunicados e remediados conforme seu nível de gravidade;
- Garantir que informações tempestivas e adequadas relativas ao Gerenciamento de *Compliance* cheguem a todos os envolvidos no respectivo processo de gerenciamento, incluindo diretorias, gestores e Colaboradores em todos os níveis hierárquicos, bem como os terceiros que atuam em processos críticos, nos limites do seu nível de atuação;
- Informar tempestivamente os resultados obtidos no âmbito das atividades de *compliance* à Diretoria da Companhia;
- Garantir que quaisquer atualizações na legislação aplicável e nas diretrizes adotadas pela Companhia sejam divulgadas a todos os Colaboradores, alcancem os responsáveis pelo seu cumprimento e ocasionem a definição de planos de ação para garantir sua devida observância no âmbito da Playsec Securitizadora;
- Acompanhar os planos de ação eventualmente definidos pela Playsec Securitizadora para que novas demandas de *compliance* derivadas de alteração de normas, criação ou desativação de produtos, processos, serviços e áreas sejam devidamente atendidas nos prazos estabelecidos;
- Testar e avaliar a aderência da Companhia à legislação, às regulamentações normativas, às recomendações dos órgãos fiscalizadores e, quando aplicável, às políticas internas da Playsec Securitizadora;

- Elaborar relatórios anuais contendo sumário dos resultados obtidos no âmbito das atividades de *compliance*, suas principais conclusões, recomendações e providências tomadas, submetendo-os à Diretoria da Playsec Securitizadora;
- Revisar e acompanhar o endereçamento dos pontos levantados nos relatórios elaborados pelas auditorias independentes, referentes ao descumprimento da legislação e regulamentações aplicáveis;
- Prestar suporte à Diretoria da Playsec Securitizadora com relação à observância e à correta aplicação da legislação regulatória aplicável à Companhia, inclusive mantendo-a informada sobre quaisquer atualizações relevantes; e
- Auxiliar na divulgação de informações e na capacitação de todos os Colaboradores e prestadores de serviços terceirizados relevantes, com relação à assuntos relevantes de *compliance*.

d) Diretoria de *Compliance*

- Deliberar, acompanhar e discutir as estratégias, políticas e medidas adotadas pela área de *Compliance* para disseminar a cultura de *compliance* e garantir a efetividade dos controles internos;
- Analisar e discutir efetivos e potenciais conflitos de interesses, assim como eventuais falhas nos controles internos da Companhia;
- Discutir a exposição a riscos regulatórios e de reputação referentes a novos produtos, operações e clientes;
- Deliberar sobre a aplicação de medidas disciplinares com relação às violações ao Código e demais políticas internas da Companhia; e
- Acompanhar os relatórios de risco eventualmente elaborados.

e) Comitê de Gerenciamento de Risco Operacional e Compliance

Este colegiado é composto pela Alta Administração, Diretores da companhia, gerentes das áreas e um representante da área de Compliance. Suas atribuições são:

- Aprovar as políticas apresentadas;

- Decidir de forma colegiada o encaminhamento dos assuntos apresentados;
- Definir diretrizes para gestão dos riscos operacionais, bem como avaliar os resultados das atividades de controles internos, risco operacional e de Compliance;
- Discutir os apontamentos relevantes apresentados pelos gestores ou das auditorias externas;
- Discutir a situação da implementação de planos de ação requeridos;
- Avaliar e analisar mudanças nos negócios e atividades da área, assim como a necessidade de alterações nos controles;
- Supervisionar a execução das políticas e procedimentos de gestão do risco operacional e a aplicação dos princípios de governança de risco operacional;
- Acompanhar os resultados das ações do gerenciamento do risco operacional e das auditorias;
- Dar suporte à gestão ativa do risco operacional;
- Avaliar continuamente a qualidade e a adequação da estrutura de controles e o seu funcionamento;
- Fomentar a consolidação da cultura de controles internos.
- Atuar de forma colegiada nas ocorrências de perdas significativas e incidentes críticos;
- Acompanhar a Solução de Problemas relacionados às ocorrências acima.

f) Gestores

- Fortalecer e disseminar a cultura de *compliance* adotada pela Playsec Securitizadora a todos os Colaboradores sob sua supervisão;
- Garantir que os Colaboradores sob sua supervisão tenham acesso tempestivo e oportuno a todas as políticas internas da Companhia;
- Supervisionar as ações e condutas de seus subordinados;

- Evitar reincidências de violação das políticas internas da Companhia, modificando os procedimentos das atividades sob sua responsabilidade, na medida do necessário;
- Garantir que os membros de sua equipe estejam atualizados com relação às exigências legais e regulatórias aplicáveis às operações e atividades negociais da Playsec Securitizadora;
- Implementar procedimentos de controle, monitorar e mitigar todos os riscos das atividades de responsabilidade da sua área;
- Acompanhar e cobrar a regularização das ocorrências apontadas em quaisquer processos internos;
- Garantir a segregação física, lógica e de conduta entre as áreas da Playsec Securitizadora, de forma a evitar o fluxo indevido de informações confidenciais e privilegiadas; e
- Reportar tempestivamente à Diretoria de *Compliance* quaisquer ocorrências e/ou fatos relevantes relativos ao não cumprimento de normas internas ou externas, assim como quaisquer dilemas éticos.

g) Terceiro e fornecedores

- Conhecer e aderir às regras relativas às políticas e normas internas estabelecidas com relação ao processo do qual o terceiro/fornecedor estiver inserido e nosso código de ética e conduta.

h) Colaboradores

- Cumprir todas as orientações previstas nas políticas e normativos internos da Companhia;
- Buscar orientação junto ao seu gestor em caso de dúvidas associadas as suas funções e atribuições; e

- Participar ativamente dos programas de conscientização, treinamentos, testes e reciclagem relacionados a assuntos de *compliance*, sempre que requisitado pela Companhia.

i) Auditoria

- Elaborar e executar testes para avaliação do sistema de controles internos de riscos operacionais;
- Assegurar a aderência aos manuais de procedimentos estabelecidos pela área;
- Certificar que a metodologia nos papéis e responsabilidades estão de acordo com a legislação e regulamentos vigentes;
- Atestar que o risco operacional está sendo avaliado em todas as áreas;
- Verificar se os principais riscos estão sendo gerenciados.
- Verificar se a estrutura de risco operacional está implementada na companhia;
- Fornecer subsídios para a identificação e avaliação de riscos e controles de cada área / processo por meio de relatório de auditoria interna.

10. SEGREGAÇÃO DAS ATIVIDADES

A Companhia deve manter suas atividades de securitização segregadas das atividades exercidas pelas demais pessoas jurídicas do seu grupo econômico com as quais haja potencial conflito de interesses, sem prejuízo da possibilidade de compartilhamento de recursos. Adicionalmente as atividades de distribuição de valores mobiliários (de emissão ou não da Companhia) devem ser segregadas do restante das atividades da Companhia.

11. SEGURANÇA DA INFORMAÇÃO

Definição de Informações Confidenciais e Privilegiadas

A Companhia e seus Colaboradores, no desempenho de suas atividades, poderão vir a ter acesso a diversas informações classificadas como confidenciais ou privilegiadas. Nesse

sentido, para fins da presente política, 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 Companhia, 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 desempenhadas pela Companhia, mesmo que tais informações e/ou dados não estejam relacionados diretamente aos serviços ou às atividades da Companhia ("Informação Confidencial").

Não são consideradas Informações Confidenciais aquelas informações que: (a) sejam ou venham a se tornar de domínio público sem violação do disposto nesta política; (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 pela Diretoria de Compliance da Companhia.

Processo de Preservação de Informações Confidenciais e Privilegiadas

Para fins de preservação das Informações Confidenciais e privilegiadas, são adotadas as seguintes medidas, bem como adotados os seguintes mecanismos de controle e monitoramento:

(i) É proibido que os Colaboradores façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da Companhia e circulem em ambientes externos à Companhia com estes arquivos, pois constituem Informações Confidenciais;

(ii) A proibição não se aplica quando as cópias ou as impressões dos arquivos forem voltadas à execução e desenvolvimento dos negócios e dos interesses da Companhia. Nestes casos, o Colaborador que estiver na posse e guarda da cópia

ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

(iii) O descarte de Informações Confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. O descarte de documentos físicos que contenham Informações Confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso de maneira a evitar sua recuperação.

(iv) Os Colaboradores também devem se abster de utilizar pen drives, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Companhia.

(v) É proibida a conexão de equipamentos na rede da Companhia que não estejam previamente autorizados pelo Diretoria de Compliance.

(vi) Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

(vii) Todos os terceiros contratados aos quais seja concedido acesso a Informações Confidenciais deverão se comprometer, por escrito, a observar todas as medidas de segurança estabelecidas nesta política.

(viii) A utilização dos ativos da Companhia, incluindo computadores, telefones, internet, programas de mensagem instantânea, e-mail e demais aparelhos se destina a fins profissionais. O uso indiscriminado dos mesmos para fins pessoais deve ser evitado, e nunca deve ser prioridade em relação a qualquer utilização profissional.

(ix) A Companhia se reserva no direito de gravar qualquer ligação telefônica dos seus Colaboradores realizada ou recebida por meio das linhas telefônicas

disponibilizadas pela Companhia para a atividade profissional de cada Colaborador.

(x) O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem e afetar a reputação da Companhia.

(xi) O recebimento de e-mails muitas vezes não depende do próprio Colaborador, mas espera-se bom senso de todos para, se possível, evitar receber mensagens com as características descritas previamente.

(xii) Na eventualidade do recebimento de mensagens com as características acima descritas, o Colaborador deve apagá-las imediatamente, de modo que estas permaneçam o menor tempo possível nos servidores e computadores da Companhia.

(xiii) Todo Colaborador deve ser cuidadoso com seu próprio equipamento e zelar pela boa utilização dos demais equipamentos que não estejam necessariamente sob sua guarda.

(xiv) Caso algum Colaborador identifique a má conservação, uso indevido ou inadequado de qualquer ativo, deve comunicar à Diretoria de Compliance da Companhia. Os programas instalados nos computadores, principalmente via internet, sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia de um sócio-diretor e da Diretoria de Compliance. Não é permitida a instalação de nenhum software ilegal ou que possuam direitos autorais protegidos.

(xv) A instalação de novos *softwares*, com a respectiva licença, deve também ser comunicada previamente a um sócio-diretor. Este deverá aprovar ou vetar a instalação e utilização dos softwares dos Colaboradores para aspectos

profissionais e pessoais.

(xvi) A senha e login para acesso aos dados contidos em todos os computadores, devem ser conhecidas pelo respectivo usuário do computador e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros. O Colaborador poderá ser responsabilizado caso disponibilize a terceiros as senhas acima referidas para quaisquer fins.

(xvii) Todo conteúdo que está na rede pode ser acessado pela Diretoria de Compliance. Os demais Colaboradores têm acessos previamente definidos. Arquivos pessoais salvos em cada computador poderão ser acessados caso a Diretoria de Compliance julgue necessário. A confidencialidade dessas informações deve ser respeitada e seu conteúdo será divulgado somente se determinado por decisão judicial.

Vazamento de Informações – Plano de Resposta:

Na ocorrência de um evento de vazamento de informações de Informações Confidenciais, reservadas ou privilegiadas mesmo que oriundos de ações involuntárias, deverá ser seguido o procedimento abaixo:

(i) Diante de eventual identificação ou suspeita de vazamento, todos os Colaborares deverão reportar o fato à Diretoria de Compliance, a fim de que esta realize a checagem do suposto vazamento ocorrido, avalie as medidas a serem tomadas e inicie uma investigação interna para apuração de responsabilidades;

(ii) A Diretoria de Compliance, junto aos prestadores de serviço de tecnologia da informação, buscará limitar o acesso a informações ao Colaboradores ao essencialmente necessário até a apuração do fato acima;

(iii) A Diretoria de Compliance deverá, juntamente com assessores legais, avaliar e/ou realizar o ajuizamento de eventuais medidas judiciais cabíveis, visando mitigar danos e resguardar a Companhia e seus Colaboradores;

(iv) Em ocorrendo vazamento de dados pessoais, a Diretoria de Compliance deverá realizar a comunicação à Autoridade Nacional de Proteção de Dados - ANPD e aos titulares de dados, em caso de risco ou dano relevante aos titulares, nos termos da Lei Geral de Proteção de Dados – LGPD; e

(v) Por fim, a Diretoria de Compliance de Compliance deverá elaborar documentação com a avaliação interna do incidente, medidas tomadas e análise de risco, para fins de cumprimento do princípio de responsabilização e prestação de contas.

Testes de segurança:

A Diretoria de Compliance realizará, em periodicidade no mínimo anual, testes de verificação do cumprimento dos processos e procedimentos previstos nesta política, contando com o auxílio dos prestadores de serviço de tecnologia da informação. Em caso de verificação de necessidade de adequações ou mudanças nos procedimentos acima descritos, a presente política será devidamente atualizada e informada a todos os Colaboradores da Companhia.

12. GARANTIA DE INDEPENDÊNCIA DA ÁREA DE COMPLIANCE

A área de *Compliance* da Playsec Securitizadora deverá ter amplo acesso a documentos, sistemas de informação, instrumentos e pessoas no desempenho de suas funções e atribuições, podendo solicitar o compartilhamento de relatórios e demais informações necessárias para o devido exercício de suas atividades.

A estrutura da área de *Compliance* deverá ser composta por Colaboradores da Companhia, e deverá ser segregada de áreas com possíveis conflitos de interesses (áreas operacionais, comerciais, administrativas e de auditoria interna), assegurando que observem estritamente os procedimentos internos e as normas aplicáveis à Companhia.

Hierarquicamente, a área de *Compliance* reporta-se ao Presidente da Companhia.

13. REMUNERAÇÃO DA ÁREA DE COMPLIANCE

A remuneração dos responsáveis pela condução das atividades de *compliance* da Playsec Securitizadora deverá ser determinada independentemente do desempenho das áreas de negócios da Companhia, de forma a não gerar quaisquer conflitos de interesses.

14. CONTATO PARA DÚVIDAS E QUESTIONAMENTOS

Todo administrador e Colaborador deve ler e seguir as diretrizes desta Política, incluindo qualquer atualização futura. Todas as Políticas e Procedimentos Internos integrantes do Programa de Integridade estão disponíveis na *intranet* da Playsec Securitizadora.

- A Playsec Securitizadora está à disposição para dirimir quaisquer questões envolvendo sua atuação e o seu Programa de Integridade por meio do e-mail compliance@Playsec.com.br;diana.arruda@playsec.com.br.

***