Capital em movimento

POLÍTICA DE
COMPLIANCE, CONTROLES INTERNOS E GOVERNANÇA CORPORATIVA

GRUPO SRM

Junho de 2026

Versão 1.0

Controle Documental

Título do Documento	POLÍTICA DE COMPLIANCE, CONTROLES INTERNOS E GOVERNANÇA CORPORATIVA
Código do Documento	*POL-GRP-COMPL-CCIG-1.0*
Tipo de Documento	*Política*
Escopo	*Corporativo*
Entidades Aplicáveis	*Grupo SRM, compreendido como suas sociedades controladoras, controladas, coligadas e aquelas sob controle comum, observadas as especificidades regulatórias aplicáveis*
Classificação do Documento	*Pública*
Versão	*1.0*
Data de Vigência	*15/06/2026*
Última Revisão	*15/06/2026*
Periodicidade de Revisão	*Anual*
Status do Documento	*Aprovado*
Local de Publicação	*Repositório Oficial - Intranet*
Elaborado por	*Compliance e Controles Internos*
Revisado por	*Compliance e Controles Internos*
Aprovado por	*Sócios e Diretores Executivos*
Área Responsável	*Compliance e Controles Internos*
Base Normativa Principal	*Ver Seção 3 deste documento*

SUMÁRIO

1. OBJETIVO

A presente Política de Compliance, Controles Internos e Governança ("Política") tem por objetivo estabelecer, de forma integrada e em instrumento normativo único de abrangência corporativa, os princípios, diretrizes, responsabilidades e parâmetros gerais de atuação que regem o Programa de Compliance, a estrutura de controles internos e a governança corporativa do Grupo SRM, compreendido por suas sociedades controladoras, controladas, coligadas e aquelas sob controle comum ("Grupo SRM" ou "Grupo").

A consolidação dessas matérias em documento único visa promover consistência sistêmica, eliminar redundâncias normativas, assegurar a coerência entre os diferentes regimes regulatórios aplicáveis às entidades do Grupo SRM e evidenciar, perante reguladores, autorreguladores, parceiros e colaboradores, o comprometimento da Alta Administração com a gestão íntegra, transparente e responsável dos negócios.

São objetivos específicos desta Política:

- estabelecer as diretrizes e os padrões mínimos de compliance aplicáveis a todas as entidades do Grupo SRM, observadas as especificidades regulatórias de cada uma;
- definir os princípios e requisitos da estrutura de controles internos do Grupo SRM, em linha com as melhores práticas e exigências regulatórias;
- fixar os pilares da governança corporativa, assegurando segregação de funções, transparência e prestação de contas (*accountability*);
- estabelecer as responsabilidades da Alta Administração, do Compliance, dos Controles Internos, das áreas de negócio e da Auditoria Interna no âmbito do Programa de Compliance;
- promover a cultura de conformidade, integridade e ética entre todos os colaboradores, administradores e terceiros que atuam em nome do Grupo SRM; e
- assegurar o atendimento às exigências legais, regulatórias e autorregulatórias aplicáveis a cada entidade regulada integrante do Grupo SRM.

2. ABRANGÊNCIA

Esta Política aplica-se a todas as sociedades integrantes do Grupo SRM, incluindo suas controladoras, controladas, coligadas, sociedades sob controle comum e demais entidades que venham a integrar o Grupo, independentemente de sua forma societária, atividade operacional ou enquadramento regulatório.

A abrangência desta Política inclui, sem limitação, as entidades do Grupo SRM que atuem nos segmentos de gestão de recursos, distribuição de valores mobiliários, securitização de créditos, prestação de serviços fiduciários, consultoria de valores mobiliários, instituição de pagamento, ativos virtuais, serviços financeiros, cobrança, holdings e participações, bem como outras atividades reguladas ou não reguladas que venham a ser desenvolvidas pelo Grupo SRM.

Esta Política aplica-se a todos os administradores, diretores, conselheiros, membros de comitês, empregados, estagiários, aprendizes, colaboradores, terceiros, prestadores de serviços, parceiros e demais pessoas que, por força contratual, regulatória, fiduciária ou de governança interna, devam observar os normativos internos do Grupo SRM, independentemente do vínculo jurídico mantido com as sociedades integrantes do Grupo SRM.

As disposições desta Política possuem caráter corporativo e aplicação transversal, sem prejuízo da observância de regras específicas aplicáveis a determinadas entidades, atividades, produtos, serviços ou estruturas reguladas. As especificidades regulatórias serão tratadas, quando necessário, em manuais,

procedimentos, matrizes, anexos ou demais documentos complementares vinculados a esta Política, observada a hierarquia normativa interna estabelecida no Manual Corporativo de Governança Normativa do Grupo SRM.

Para fins de aplicação desta Política, a identificação das sociedades abrangidas deverá observar o organograma societário, os cadastros regulatórios e/ou o inventário interno de entidades do Grupo SRM vigente à época da aplicação do normativo.

3. BASE REGULATÓRIA

Esta Política fundamenta-se nas disposições legais, regulatórias e autorregulatórias aplicáveis às atividades desempenhadas pelas sociedades integrantes do Grupo SRM, considerando seus respectivos registros, autorizações, enquadramentos regulatórios, produtos, serviços e estruturas operacionais.

A observância desta Política deverá considerar, sem limitação, as normas aplicáveis aos seguintes temas:

Norma	Regulador	Tema	Entidades
Res. CMN nº 4.595/2017 Res. BCB nº 65/2021	CMN / BCB	Política de conformidade / Compliance	DTVM · IP
Res. CMN nº 4.968/2021	CMN	Controles internos — IFs em geral (excl. DTVM/CTVM/IP)	Demais IFs
Res. BCB nº 260/2022 Res. BCB nº 431/2024	BCB	Controles internos — DTVM, CTVM, corretoras de câmbio e Instituições de Pagamento (norma específica, prevalece sobre CMN 4.968)	DTVM · IP
Res. BCB nº 432/2024	BCB	Política de remuneração de administradores — DTVM, CTVM, corretoras de câmbio e IP (vigência 1º/1/2025; exige diferimento mínimo e parte em instrumentos de longo prazo)	DTVM · IP
Lei nº 6.404/1976 Lei nº 6.385/1976	Federal / CVM	Governança societária e mercado de capitais	Todas
Res. CMN nº 4.557/2017 Res. BCB nº 265/2022	CMN / BCB	Gerenciamento de riscos e governança prudencial	DTVM · IP
Res. CVM nº 21/2021 Res. CVM nº 19/2021 Res. CVM nº 35/2021	CVM	Atividades reguladas no mercado de capitais	DTVM · Gestora · Consultoria
Res. CVM nº 60/2021	CVM	Securitização (CRI, CRA, DEB, CR) — Companhias Securitizadoras	Securitizadora
Lei nº 12.865/2013 Res. BCB nº 80/2021 Res. BCB nº 494/2025	Federal / BCB	Instituições de Pagamento — regime legal e regulatório	IP

Norma	Regulador	Tema	Entidades
Lei nº 9.613/1998 Circular BCB nº 3.978/2020 Res. BCB nº 50/2020 Res. CVM nº 50/2021	Federal / BCB / CVM	Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLD/FTP)	Todas
Res. CMN nº 4.893/2021 Res. BCB nº 85/2021	CMN / BCB	Segurança cibernética — IFs e IPs (políticas, plano de resposta, relatório anual)	DTVM · IP
Res. CMN nº 5.274/2025 Res. BCB nº 538/2025	CMN / BCB	Segurança cibernética — novo framework prescritivo com 14 controles mínimos obrigatórios (MFA, criptografia, testes de intrusão anuais, CTI). Adequação até 1º/3/2026	DTVM · IP
Lei nº 13.709/2018 (LGPD)	Federal / ANPD	Proteção de dados pessoais — designação de Encarregado (DPO), base legal para tratamento, direitos dos titulares, gestão de incidentes	Todas
Lei nº 12.846/2013 Decreto nº 11.129/2022	Federal / CGU	Lei Anticorrupção — responsabilização objetiva de PJ; programa de integridade como atenuante (art. 57 do Decreto)	Todas
Res. CMN nº 4.860/2020 Res. CMN nº 5.182/2024	CMN / BCB	Ouvidoria — obrigatória para entidades com clientes pessoas naturais e ME/EPP; prazo de resposta 10 dias úteis (prorrogável por mais 10)	DTVM · IP
Lei nº 14.457/2022	Federal / MTE	Canal de denúncias e prevenção ao assédio — obrigatório para empresas com CIPA (> 20 empregados); treinamento a cada 12 meses	Todas (com CIPA)
Res. BCB nº 519/2025 Res. BCB nº 520/2025 Res. BCB nº 521/2025	BCB	Ativos Virtuais — VASPs/PSAVs (vigência 2/2/2026; prazo para pedido de autorização 30/10/2026). Aplicável se o Grupo operar intermediação ou custódia de ativos virtuais	PSAV (se VASP)
Res. CVM nº 193/2023	CVM	Relatório de sustentabilidade ISSB — obrigatório para exercícios iniciados em/após 1º/1/2026 (companhias abertas e securitizadoras com emissão pública)	Securitizadora
Códigos ANBIMA aplicáveis às atividades do Grupo SRM	ANBIMA	Autorregulação e melhores práticas de mercado (Código de Distribuição; Código de Administração de Recursos de Terceiros — versão vigente jul/2024; Código de Serviços Qualificados; Código de Ofertas Públicas)	Todas (empresas aderentes)

Esta lista não é exaustiva. O Grupo SRM e suas entidades estão sujeitos a outras normas legais, regulamentares e autorregulatórias aplicáveis em razão de suas atividades, autorizações e registros vigentes. A área de Compliance é responsável pelo monitoramento contínuo do ambiente normativo e pela atualização desta Política e dos documentos vinculados sempre que houver alteração relevante.

4. DEFINIÇÕES

Para fins desta Política, aplicam-se as seguintes definições, sem prejuízo de outras definições constantes dos documentos normativos vinculados:

Alta Administração: Sócios Diretores Executivos, Diretores Executivos e Diretores responsáveis pela condução estratégica e supervisão das atividades das sociedades do Grupo SRM, e, quando aplicável, conselhos e comitês de governança.

Avaliação Interna de Risco (AIR) de PLD/FTP: Avaliação periódica e documentada dos riscos de lavagem de dinheiro e financiamento do terrorismo inerentes às atividades, clientes, produtos, canais de distribuição e geografias das entidades do Grupo, com abordagem baseada em risco. Deve ser aprovada pelo Diretor Responsável, revisada a cada dois anos (ou quando houver alteração significativa do perfil de risco) e encaminhada aos órgãos de administração.

Canal de Denúncias: Meio formal disponibilizado para recebimento de relatos de suspeitas ou evidências de irregularidades, fraudes, descumprimento desta Política ou das normas internas, bem como de violações éticas ou legais, garantindo a confidencialidade e a proteção do denunciante de boa-fé.

Chinese Wall (Barreira de Informação): Conjunto de procedimentos, controles físicos, lógicos e comportamentais destinados a prevenir o fluxo inadequado de informações privilegiadas, confidenciais ou relevantes entre diferentes áreas de atuação, entidades ou funções do Grupo SRM.

Compliance: Observância, pelas entidades do Grupo SRM, seus administradores e colaboradores, das leis, regulamentos, normas autorregulatórias, políticas internas e padrões éticos e de conduta aplicáveis.

Conflito de Interesse: Situação em que o interesse pessoal ou profissional de um administrador, colaborador ou terceiro, real ou potencial, diverge dos interesses do Grupo SRM, de seus clientes ou das entidades reguladas, podendo comprometer a imparcialidade, a lealdade ou a conformidade das decisões.

Controles Internos: Conjunto de processos, procedimentos, políticas e sistemas estabelecidos para assegurar a eficácia e a eficiência operacional, a confiabilidade das informações, a conformidade com leis e regulamentos e a proteção dos ativos das entidades do Grupo.

Dados Pessoais e Encarregado (DPO): Dados pessoais são informações relacionadas a pessoa natural identificada ou identificável, conforme definição da Lei Geral de Proteção de Dados (LGPD — Lei 13.709/2018). O Encarregado (Data Protection Officer — DPO) é o responsável formalmente designado para ser o canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Diretor Responsável: Diretor estatutário formalmente designado perante os reguladores (CVM, BCB, ANBIMA, conforme aplicável) como responsável pela implementação e cumprimento das obrigações regulatórias pertinentes em cada entidade do Grupo.

Governança Corporativa: Sistema pelo qual as entidades do Grupo SRM são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, Alta Administração, órgãos de fiscalização e

controle e demais partes interessadas, com base nos princípios de transparência, equidade, accountability e responsabilidade corporativa.

Informação Privilegiada: Informação relevante ainda não divulgada ao mercado que, se tornada pública, poderia influenciar significativamente a cotação de valores mobiliários ou as decisões de investimento de participantes do mercado.

KYC (Know Your Customer): Conjunto de procedimentos de identificação, verificação e monitoramento de clientes, destinados a conhecer o perfil, a natureza das atividades e os riscos associados a cada cliente, conforme exigências regulatórias.

Lavagem de Dinheiro: Conjunto de operações financeiras destinadas a ocultar ou dissimular a origem ilícita de recursos, bens ou valores, conforme definido na Lei n.º 9.613/1998 e suas alterações.

Ativos Virtuais (VASP/PSAV): Representações digitais de valor que podem ser negociadas ou transferidas por meios eletrônicos, conforme definição da Lei 14.478/2022 e da regulação do Banco Central do Brasil. Prestador de Serviços de Ativos Virtuais (VASP ou PSAV) é a entidade habilitada pelo BCB para operar intermediação, custódia ou corretagem de ativos virtuais, nos termos das Resoluções BCB 519/520/521, de novembro de 2025.

Ouvidoria: Instância de resolução de conflitos e atendimento de última instância, responsável por receber, registrar, analisar e dar tratamento a demandas de clientes e usuários que não foram solucionadas no atendimento comum, nos termos da Resolução CMN 4.860/2020 e normas correlatas.

PEP (Pessoa Politicamente Exposta): Pessoa que exerce ou exerceu, nos últimos cinco anos, cargo, emprego ou função pública relevante no Brasil ou no exterior, conforme definição da regulação de PLD/FTP aplicável.

PLD/FTP: Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa, conjunto de obrigações legais e regulatórias destinadas a evitar que o sistema financeiro seja utilizado para atividades ilícitas.

Programa de Compliance: Conjunto estruturado de políticas, procedimentos, controles, treinamentos, mecanismos de monitoramento e instâncias de governança voltados a assegurar a conformidade legal, regulatória, autorregulatória e ética das atividades do Grupo SRM.

Programa de Integridade: Conjunto de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades, bem como de aplicação efetiva de códigos de ética e de conduta, políticas e diretrizes, com o objetivo de detectar e sanar desvios, fraudes, irregularidades e atos lesivos à administração pública ou privada, nos termos da Lei 12.846/2013 e do Decreto 11.129/2022.

Risco de Compliance: Possibilidade de ocorrência de perdas, sanções regulatórias, restrições operacionais, danos reputacionais ou responsabilidades decorrentes do descumprimento de leis, regulamentos, normas autorregulatórias, políticas internas ou padrões de conduta.

Segurança Cibernética: Conjunto de práticas, tecnologias, processos e controles destinados a proteger sistemas, redes, dados e ativos digitais do Grupo SRM contra ataques, acessos não autorizados, falhas e incidentes cibernéticos, em conformidade com as normas BCB/CMN aplicáveis (Res. CMN 5.274/2025 e Res. BCB 538/2025).

Três Linhas de Defesa: Modelo de governança e controle que distribui responsabilidades entre: (i) primeira linha — áreas de negócio e operações, responsáveis pelo gerenciamento direto dos riscos; (ii) segunda linha — Compliance e Controles Internos, responsáveis pelo monitoramento e suporte; e (iii) terceira linha — Auditoria Interna, responsável pela avaliação independente.

5. DIRETRIZES

O Grupo SRM conduz seus negócios com base nos princípios de legalidade, integridade, transparência, responsabilidade e respeito às normas legais, regulatórias, autorregulatórias e aos mais elevados padrões éticos do mercado financeiro e de capitais. A conformidade não é tratada como obrigação acessória, mas como fator estratégico e elemento essencial à sustentabilidade, à reputação e à continuidade dos negócios.

São diretrizes gerais desta Política:

Tone from the Top: o comprometimento da Alta Administração com a cultura de compliance e a integridade é condição indispensável para a efetividade do Programa de Compliance do Grupo, devendo ser demonstrado de forma consistente e exemplar em todas as instâncias.

Modelo das Três Linhas de Defesa: a gestão de riscos e controles internos do Grupo SRM observa o modelo das Três Linhas de Defesa, com responsabilidades distribuídas e complementares entre as áreas de negócio, o Compliance e Controles Internos (segunda linha) e a Auditoria Interna (terceira linha).

Proporcionalidade e adequação: os controles, procedimentos e mecanismos de compliance devem ser proporcionais à natureza, ao porte, à complexidade e ao perfil de risco das atividades desenvolvidas por cada entidade do Grupo.

Abordagem baseada em risco: a priorização dos recursos, esforços e controles de compliance observa uma abordagem baseada em risco, com foco nas atividades, operações, clientes e relacionamentos de maior exposição.

Independência do Compliance: a área de Compliance deve possuir autonomia funcional, acesso direto à Alta Administração e recursos adequados para o exercício de suas funções, sendo vedada qualquer ação que comprometa sua independência ou imparcialidade.

Atualização contínua: os normativos internos do Grupo devem ser revistos e atualizados periodicamente, e sempre que houver alterações relevantes no ambiente legal, regulatório, autorregulatório, societário ou de risco.

Confidencialidade e proteção de informações: a gestão de informações privilegiadas, confidenciais e de clientes deve observar os princípios de necessidade de conhecimento, segregação de funções e proteção adequada, em linha com as exigências regulatórias e as políticas internas do Grupo.

Não tolerância a violações: O Grupo SRM não tolera condutas que violem leis, regulamentos, normas internas, padrões éticos ou que configurem conflito de interesses, uso indevido de informação confidencial ou privilegiada, corrupção, fraude, assédio, discriminação, retaliação ou qualquer outra irregularidade.

5.1 VEDAÇÕES

São expressamente vedados a todos os administradores, colaboradores e terceiros que atuam em nome do Grupo SRM:

- utilizar informações privilegiadas, confidenciais ou não públicas em proveito próprio ou de terceiros, inclusive para fins de negociação de valores mobiliários ou para obtenção de vantagens indevidas;
- realizar ou facilitar operações que configurem ou possam configurar lavagem de dinheiro, financiamento do terrorismo ou ocultação de ativos de origem ilícita;

- oferecer, prometer, dar, solicitar, receber ou aceitar, direta ou indiretamente, qualquer vantagem indevida a agentes públicos, privados, reguladores, autorreguladores, clientes ou fornecedores para influenciar decisões em benefício próprio ou do Grupo (antissuborno e anticorrupção);
- atuar em situações de conflito de interesse não devidamente identificadas, comunicadas e gerenciadas conforme os procedimentos internos, podendo comprometer a imparcialidade das decisões;
- divulgar, vazar ou utilizar informações de clientes, carteiras ou operações sem a devida autorização ou fora das hipóteses legalmente admitidas;
- interferir, pressionar ou buscar influenciar indevidamente decisões da área de Compliance, de Controles Internos ou de Auditoria Interna;
- ignorar, contornar ou burlar controles internos, procedimentos de PLD/FTP, barreiras de informação (*Chinese Walls*) ou qualquer outro mecanismo de compliance formalmente estabelecido;
- prestar informações falsas, incompletas ou enganosas a reguladores, autorreguladores, clientes, parceiros ou auditores; e
- tomar qualquer medida de retaliação contra colaborador que, de boa-fé, tenha reportado suspeita ou evidência de irregularidade ao canal de denúncias ou à área de Compliance.

5.2 PROGRAMA DE COMPLIANCE

O Grupo SRM deve implementar e manter, de forma permanente, um Programa de Compliance robusto e efetivo, capaz de identificar, avaliar, monitorar e mitigar os riscos de compliance inerentes às atividades das entidades do Grupo.

O Programa de Compliance do Grupo SRM deve contemplar, no mínimo, os seguintes elementos:

- Políticas, manuais e procedimentos internos aprovados, documentados e periodicamente revistos, organizados conforme o Manual Corporativo de Governança Normativa;
- Designação formal de Diretores Responsáveis perante os reguladores e autorreguladores aplicáveis em cada entidade, com autonomia, recursos e acesso adequados ao desempenho de suas funções;
- Estrutura de Compliance com recursos humanos, tecnológicos e financeiros adequados à complexidade e ao perfil de risco das atividades do Grupo;
- Mapeamento e avaliação periódica dos riscos de compliance das entidades, processos, produtos, serviços e relacionamentos do Grupo, com abordagem baseada em risco;
- Monitoramento contínuo das atividades das entidades e de seus colaboradores, incluindo o monitoramento de operações suspeitas, conflitos de interesse e uso de informação privilegiada;
- Mecanismos de reporte à Alta Administração com periodicidade mínima anual, contendo indicadores de compliance, ocorrências relevantes, status dos planos de ação e avaliação do ambiente de risco;
- Canal de denúncias acessível, confidencial e com proteção ao denunciante de boa-fé;
- Programa de treinamento e conscientização anual, com frequência e conteúdo adequados ao perfil e ao nível de risco de cada público;
- Gestão do relacionamento com reguladores e autorreguladores, incluindo o controle de prazos regulatórios, as respostas a demandas e a atualização normativa; e
- Avaliação periódica da efetividade do Programa, com implementação de melhorias contínuas.

5.3 PREVENÇÃO À LAVAGEM DE DINHEIRO E AO FINANCIAMENTO DO TERRORISMO (PLD/FTP)

O Grupo SRM, por meio de suas entidades reguladas, deve implementar e manter políticas, procedimentos e controles voltados à prevenção, detecção e comunicação de operações que possam estar relacionadas à lavagem de dinheiro, ao financiamento do terrorismo ou à proliferação de armas de destruição em massa, em conformidade com as exigências legais e regulatórias aplicáveis a cada entidade.

A estrutura de PLD/FTP do Grupo SRM deve contemplar, no mínimo:

- *Avaliação interna de risco de PLD/FTP:* deve ser realizada avaliação periódica e documentada dos riscos de lavagem de dinheiro e financiamento do terrorismo inerentes às atividades, clientes, produtos, canais de distribuição e geografias das entidades do Grupo, com abordagem baseada em risco;
- *Procedimentos de diligência e "Conheça seu Relacionamento" — KYC, KYP, KYE e KYS:* devem ser adotados procedimentos proporcionais ao risco para identificação, verificação, qualificação, avaliação, aprovação e monitoramento contínuo de clientes, parceiros, colaboradores, prestadores de serviços, fornecedores, contrapartes, beneficiários finais e demais partes relacionadas às atividades do Grupo SRM, conforme aplicável. Tais procedimentos devem contemplar, quando pertinente, diligência reforçada para situações de maior risco, incluindo Pessoas Politicamente Expostas — PEPs, clientes ou contrapartes estrangeiras, estruturas societárias complexas, operações não usuais, indícios de inconsistência cadastral, relacionamento com jurisdições de maior risco ou quaisquer situações que demandem análise adicional pelo Compliance.
- *Monitoramento de operações:* devem ser implementados mecanismos sistemáticos de monitoramento de operações e transações para identificação de padrões atípicos ou suspeitos, em linha com o perfil de risco e com os parâmetros estabelecidos pelas normas regulatórias de PLD/FTP;
- *Comunicações ao COAF:* as entidades do Grupo devem adotar procedimentos internos para análise, deliberação e comunicação tempestiva de operações suspeitas ao Conselho de Controle de Atividades Financeiras (COAF), nos prazos e formas estabelecidos pela regulação aplicável;
- *Registros de operações:* devem ser mantidos registros de operações em espécie e demais operações sujeitas a registro, conforme exigências regulatórias, pelo prazo mínimo previsto na legislação;
- *Treinamento específico:* todos os colaboradores que atuam em funções expostas ao risco de PLD/FTP devem receber treinamento específico com periodicidade mínima anual;
- *Responsável pelo cumprimento das obrigações de PLD/FTP:* deve ser formalmente designado em cada entidade, perante o regulador, o responsável pelas políticas e procedimentos de PLD/FTP; e
- *Registros e evidências:* devem ser mantidos registros documentais suficientes para demonstrar a efetividade dos controles de PLD/FTP e para atender a eventuais demandas dos reguladores.

As entidades do Grupo SRM que se qualificam como obrigadas nos termos da Lei n.º 9.613/1998 e das normas regulatórias de PLD/FTP devem manter, adicionalmente, política e procedimentos específicos de PLD/FTP aprovados e em vigor, nos termos das exigências de cada regulador aplicável.

5.4 SEGREGAÇÃO DE ATIVIDADES E GESTÃO DE CONFLITOS DE INTERESSE

Em razão da natureza multifacetada das atividades desenvolvidas pelas entidades do Grupo SRM no mercado financeiro e de capitais, o Grupo SRM reconhece a existência de potenciais conflitos de interesse entre suas diferentes áreas de atuação e adota a política de segregação de atividades (*Chinese Wall*) como mecanismo essencial de gestão e mitigação desses riscos.

As principais diretrizes de segregação de atividades e gestão de conflitos de interesse são:

- *Separação física e lógica:* as atividades sujeitas a potencial conflito de interesse devem ser desenvolvidas em espaços físicos separados, com restrições de acesso, e em sistemas de informação segregados, com controles de acesso individualizados;
- *Restrições de comunicação e compartilhamento de informações:* informações privilegiadas, confidenciais ou relevantes não públicas não devem ser compartilhadas entre áreas separadas pelo Chinese Wall, salvo nas hipóteses expressamente previstas na regulação e nos procedimentos internos, com registro formal da transposição da barreira;
- *Identificação e declaração de conflitos:* administradores e colaboradores devem identificar e comunicar formalmente à área de Compliance situações reais ou potenciais de conflito de interesse, antes de tomarem qualquer decisão ou praticarem qualquer ato que possa ser por elas afetado;
- *Política de investimentos pessoais:* administradores e colaboradores devem observar as restrições aplicáveis à negociação de valores mobiliários em conta própria, conforme as normas regulatórias de cada entidade e os procedimentos internos do Grupo SRM; e
- *Registro e monitoramento:* os potenciais conflitos de interesse identificados, as medidas adotadas e as situações de travessia do Chinese Wall devem ser documentados e monitorados pela área de Compliance.

5.5 CANAL DE DENÚNCIAS (WHISTLEBLOWING)

O Grupo SRM disponibiliza Canal de Denúncias (“Canal”), por meio de plataforma terceirizada e independente, para que colaboradores, administradores, membros de comitês, prestadores de serviços, parceiros, clientes, fornecedores e quaisquer terceiros possam comunicar, de forma segura, confidencial e sem receio de retaliação, suspeitas ou evidências de violações a esta Política, às normas internas, à legislação e regulamentação aplicáveis, aos padrões éticos ou às diretrizes de integridade do Grupo SRM.

O Canal deve permitir o recebimento de relatos relacionados, entre outros temas, a violações legais, regulatórias, éticas, operacionais, societárias, trabalhistas, financeiras, contábeis, de controles internos, conflitos de interesses, fraudes, corrupção, assédio, discriminação, uso indevido de informações, descumprimento de políticas internas ou qualquer outra irregularidade envolvendo o Grupo SRM, seus colaboradores, administradores, terceiros ou demais partes relacionadas.

O acesso ao Canal deverá ser disponibilizado por meio oficial definido pelo Grupo SRM, incluindo, conforme aplicável, a intranet, o site institucional e/ou link específico da plataforma terceirizada contratada.

As informações sobre o Canal, incluindo forma de acesso, orientações de utilização, escopo dos relatos, garantias de confidencialidade, possibilidade de anonimato, vedação à retaliação e demais diretrizes aplicáveis, deverão ser divulgadas por meio de comunicações internas, treinamentos, Código de Ética e Conduta, políticas internas e/ou demais documentos corporativos aplicáveis.

As informações atualizadas sobre o canal de acesso, incluindo link, endereço eletrônico, telefone, plataforma externa ou outros meios disponíveis para registro de denúncias, deverão ser mantidas em local de fácil acesso aos públicos impactados, sob responsabilidade da área competente.

As diretrizes aplicáveis ao Canal de Denúncias são:

- o Canal deve ser disponibilizado por meio oficial, adequado e acessível, com ampla divulgação aos colaboradores, administradores, prestadores de serviços, parceiros, clientes, fornecedores e demais partes interessadas;

- o Canal deve permitir o recebimento, registro e tratamento de relatos, inclusive anônimos, observadas as funcionalidades disponibilizadas pela plataforma contratada e a legislação aplicável;
- a confidencialidade da identidade do denunciante deve ser preservada, salvo quando houver autorização expressa do denunciante, necessidade legal, ordem de autoridade competente ou exigência indispensável para adequada condução da apuração;
- são expressamente vedadas quaisquer medidas de retaliação, ameaça, constrangimento, discriminação ou punição contra denunciantes que realizem relatos de boa-fé;
- todos os relatos recebidos devem ser registrados, analisados, classificados, tratados e, quando aplicável, apurados com diligência, imparcialidade, confidencialidade e tempestividade;
- as apurações deverão observar critérios de independência, ausência de conflito de interesses, preservação de evidências, proporcionalidade e proteção das pessoas envolvidas;
- quando houver potencial conflito de interesses na condução da apuração, o relato deverá ser direcionado à instância competente, de forma a preservar a independência e a imparcialidade do processo;
- as medidas corretivas, disciplinares ou de aprimoramento de controles deverão ser adotadas de acordo com a gravidade dos fatos apurados, as normas internas, os contratos aplicáveis e a legislação vigente; e
- Os resultados relevantes das apurações, os indicadores do Canal, as medidas adotadas e eventuais riscos identificados deverão ser reportados à Alta Administração ou à instância de governança competente, preservada a confidencialidade das informações sensíveis, estratégicas e identificadoras.

A gestão, o acompanhamento e a revisão periódica do Canal de Denúncias deverão observar as responsabilidades definidas internamente pelo Grupo SRM, incluindo a avaliação da adequação da plataforma terceirizada, dos fluxos de tratamento dos relatos, dos prazos de apuração, dos controles de confidencialidade e dos mecanismos de reporte à Alta Administração ou à instância de governança competente.

5.6 TREINAMENTO E DISSEMINAÇÃO DE CULTURA DE COMPLIANCE

O Grupo SRM reconhece que a efetividade do Programa de Compliance depende fundamentalmente do comprometimento e da conscientização de todos os colaboradores e administradores.

O programa de treinamento do Grupo SRM deve:

- contemplar treinamento obrigatório de compliance para todos os colaboradores e administradores no ato da admissão/posse e com periodicidade mínima anual;
- incluir módulos específicos sobre as obrigações regulatórias das entidades do Grupo SRM (PLD/FTP, conflito de interesse, uso de informação privilegiada, práticas proibidas, governança), com profundidade adequada ao perfil de risco de cada função;
- contemplar treinamentos adicionais para as áreas expostas a riscos específicos (equipes comerciais, área de PLD/FTP, área de gestão de carteiras e fundos);
- ser documentado, com registro de presença ou conclusão e avaliação de aprendizado, quando aplicável; e
- ser avaliado anualmente quanto à efetividade, com ajustes sempre que necessário.

5.7 SEGURANÇA CIBERNÉTICA E CONTINUIDADE DE NEGÓCIOS

O Grupo SRM deve implementar e manter política e plano de resposta a incidentes de segurança cibernética, em conformidade com a Resolução CMN 5.274/2025 e a Resolução BCB 538/2025 (adequação

até 1º/3/2026), bem como com a Resolução CMN 4.893/2021 e a Resolução BCB 85/2021, conforme aplicável a cada entidade regulada.

A estrutura de segurança cibernética do Grupo SRM deve contemplar, no mínimo:

- Política de Segurança Cibernética aprovada pela Alta Administração, com revisão mínima anual;
- Plano de Resposta a Incidentes Relevantes de Segurança Cibernética, documentado e testado periodicamente;
- Relatório Anual de Segurança Cibernética, com data-base 31/12, entregue ao órgão de administração responsável;
- Implementação dos 14 controles mínimos obrigatórios previstos na Resolução CMN 5.274/2025 e Resolução BCB 538/2025, incluindo autenticação multifator (MFA), criptografia de dados em trânsito e em repouso, isolamento de ambientes críticos (Pix/STR), gestão de certificados digitais, programa de inteligência de ameaças cibernéticas (CTI) e testes de intrusão anuais realizados por equipe independente;
- Gestão de riscos de terceiros e provedores de serviços em nuvem, com due diligence documentada (inclusive nos termos do Questionário ANBIMA de Due Diligence — QDD, quando aplicável);
- Designação de Diretor Responsável por segurança cibernética perante o BCB (art. 7 da Res. BCB 85/2021);
- Programa de conscientização e treinamento de colaboradores sobre segurança da informação; e
- Plano de Continuidade de Negócios (PCN) compatível com os riscos operacionais e cibernéticos das entidades do Grupo SRM.

5.8 PROTEÇÃO DE DADOS PESSOAIS (LGPD)

O Grupo SRM deve observar, em todas as suas atividades, os princípios e as obrigações estabelecidos na Lei Geral de Proteção de Dados Pessoais (LGPD — Lei 13.709/2018), assegurando o tratamento lícito, transparente e seguro dos dados pessoais de clientes, colaboradores, parceiros e demais titulares.

As diretrizes de proteção de dados pessoais do Grupo SRM incluem:

- Designação formal de Encarregado (DPO), responsável por ser o canal de comunicação entre o Grupo SRM, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD);
- Mapeamento e inventário dos dados pessoais tratados pelas entidades do Grupo SRM (Registro de Atividades de Tratamento — RAT), com identificação de bases legais para cada atividade de tratamento;
- Controles de segurança adequados à proteção dos dados pessoais, integrados à política de segurança cibernética do Grupo SRM;
- Procedimentos para atendimento dos direitos dos titulares (acesso, correção, exclusão, portabilidade, oposição), dentro dos prazos regulatórios;
- Processo de gestão de incidentes envolvendo dados pessoais, com avaliação de necessidade de comunicação à ANPD e aos titulares afetados, nos prazos legais;
- Contratos de processamento de dados com operadores terceirizados, contendo cláusulas de proteção adequadas; e
- Treinamento periódico de colaboradores sobre privacidade e proteção de dados pessoais.

5.9 PROGRAMA DE INTEGRIDADE E ANTICORRUPÇÃO

O Grupo SRM adota compromisso irrestrito com a integridade, a ética e a anticorrupção em todas as suas atividades e relacionamentos, em observância à Lei 12.846/2013 (Lei Anticorrupção) e ao Decreto 11.129/2022, que regulamenta seus parâmetros de avaliação do Programa de Integridade.

O Programa de Integridade do Grupo SRM deve contemplar, no mínimo, os parâmetros estabelecidos no art. 57 do Decreto 11.129/2022, incluindo:

- Comprometimento expresso e visível da Alta Administração com o Programa de Integridade (*tone from the top*);
- Padrões de conduta, código de ética, políticas e procedimentos de integridade aplicáveis a colaboradores, administradores e terceiros que atuam em nome do Grupo SRM;
- Due diligence de integridade na contratação e monitoramento de terceiros, parceiros e fornecedores com interação com o setor público;
- Análise periódica de riscos de corrupção e atos lesivos à administração pública, com abordagem baseada em risco;
- Canal de denúncias com garantia de anonimato, confidencialidade e proteção contra retaliação;
- Monitoramento contínuo do Programa, com auditorias e avaliações periódicas de efetividade; e
- Registros, evidências e documentação suficientes para demonstrar a existência e aplicação efetiva do Programa.

5.10 OUVIDORIA

As entidades do Grupo SRM que mantêm relacionamento com clientes pessoas naturais ou microempresas/empresas de pequeno porte devem manter estrutura de Ouvidoria em conformidade com a Resolução CMN 4.860/2020 (alterada pela Resolução CMN 5.182/2024) e demais normas aplicáveis.

As diretrizes de Ouvidoria do Grupo SRM incluem:

- Designação de Ouvidor e Diretor Responsável pela Ouvidoria perante o BCB ou CVM, conforme aplicável;
- Prazo de resposta às demandas de clientes de até 10 dias úteis, prorrogável por mais 10 dias úteis em casos devidamente justificados;
- Relatório semestral de Ouvidoria (data-base 30/6 e 31/12), com análise dos dados e encaminhamento aos órgãos de administração competentes;
- Registro de todas as demandas recebidas, com controle de prazos e indicadores de qualidade do atendimento; e
- Independência da Ouvidoria em relação às áreas de negócio, assegurando imparcialidade no tratamento das demandas.

6. CONTROLES INTERNOS

A estrutura de controles internos do Grupo SRM deve ser compatível com a natureza, o porte, a complexidade, o perfil de risco, o modelo de negócio e o ambiente regulatório aplicável a cada sociedade integrante do Grupo SRM, observando princípios de governança, segregação de funções, transparência, rastreabilidade, responsabilização e prestação de contas.

Os controles internos têm por finalidade assegurar, de forma razoável, que as atividades do Grupo SRM sejam conduzidas em conformidade com as leis, regulamentos, normas autorregulatórias, políticas internas, diretrizes da Alta Administração e boas práticas de mercado.

A estrutura de controles internos deve contribuir para:

- a efetividade e eficiência das operações;
- a confiabilidade, integridade e tempestividade das informações contábeis, financeiras, regulatórias, gerenciais e operacionais;

- a adequada identificação, avaliação, mitigação, monitoramento e reporte de riscos;
- a prevenção e detecção de falhas, irregularidades, conflitos de interesse, fraudes, desvios de conduta e descumprimentos normativos;
- a proteção de ativos, informações, sistemas, dados, documentos e registros corporativos;
- a adequada segregação de funções, alçadas, responsabilidades e níveis de aprovação; e
- a correção tempestiva de deficiências, fragilidades ou inconsistências identificadas nos processos internos.

6.1 ESTRUTURA E ABRANGÊNCIA DOS CONTROLES INTERNOS

A estrutura de controles internos deve contemplar controles preventivos, detectivos e corretivos, proporcionais aos riscos envolvidos nas atividades, processos, produtos, serviços e entidades do Grupo SRM.

Os controles devem ser formalizados, comunicados às áreas envolvidas, periodicamente revisados e suportados por evidências suficientes para fins de monitoramento, auditoria, supervisão regulatória e prestação de contas.

A aplicação dos controles internos deverá considerar, entre outros fatores:

- processo ou atividade avaliada;
- risco identificado;
- controle associado;
- natureza do controle, se preventivo, detectivo ou corretivo;
- responsável pelo controle;
- periodicidade de execução;
- evidência esperada;
- avaliação de efetividade; e
- plano de ação associado, quando necessário.

A estrutura de controles internos deverá ser continuamente aprimorada, considerando a evolução das atividades do Grupo SRM, alterações regulatórias, mudanças no ambiente de negócios, resultados de testes, auditorias, fiscalizações, incidentes, apontamentos de reguladores e necessidades identificadas pela Alta Administração.

6.2 DIRETRIZES MÍNIMAS DE CONTROLES INTERNOS

Os controles internos do Grupo SRM devem observar, no mínimo, as seguintes diretrizes:

- *Segregação de funções:* deve ser assegurada a separação adequada entre as funções de execução, aprovação, conferência, registro, liquidação, custódia, monitoramento e supervisão das atividades, de modo a reduzir riscos de conflito de interesses, erro operacional, fraude, manipulação de informações ou concentração indevida de poderes.
- *Definição de alçadas e responsabilidades:* os processos críticos devem possuir responsáveis definidos, níveis de aprovação compatíveis com a materialidade e o risco da operação, bem como trilhas de decisão que permitam a identificação dos envolvidos, das aprovações concedidas e das exceções autorizadas.
- *Controle de acesso a sistemas e informações:* o acesso a sistemas, bases de dados, carteiras, informações de clientes, dados pessoais, informações confidenciais, estratégicas ou privilegiadas deve ser concedido com base no princípio do menor privilégio necessário, devendo ser periodicamente revisado, bloqueado ou ajustado em caso de movimentação, desligamento ou alteração de função.

- *Formalização de processos e evidências:* os processos relevantes devem ser documentados por meio de políticas, manuais, procedimentos, fluxos, matrizes, checklists, registros sistêmicos ou demais documentos aplicáveis, com manutenção de evidências suficientes para demonstrar a execução dos controles e a aderência às regras internas e regulatórias.
- *Conciliações, conferências e validações:* os processos sujeitos a risco financeiro, operacional e regulatório devem prever rotinas de conferência, conciliação, validação ou dupla checagem, conforme a natureza e criticidade da atividade.
- *Gestão de exceções:* exceções às regras internas, alçadas, procedimentos ou controles estabelecidos devem ser justificadas, documentadas, aprovadas pela instância competente e monitoradas pela área responsável, especialmente quando envolverem risco financeiro, operacional, regulatório ou conflito de interesses.
- *Continuidade e rastreabilidade:* os controles devem permitir a rastreabilidade das decisões, aprovações, registros, alterações sistêmicas, comunicações relevantes e evidências produzidas no curso das atividades.

6.3 MONITORAMENTO E TESTES DE CONTROLES

Os controles internos devem ser objeto de acompanhamento contínuo pelas áreas responsáveis pelos processos e, quando aplicável, de testes periódicos pela área de Controles Internos, Compliance, Riscos ou Auditoria Interna, conforme a natureza do controle, o nível de risco e o plano anual aprovado.

Os testes de controles poderão abranger, entre outros aspectos:

- existência e formalização do controle;
- aderência do controle ao procedimento aprovado;
- aderência as regulamentações aplicáveis;
- suficiência das evidências mantidas;
- tempestividade da execução;
- efetividade na mitigação do risco;
- recorrência de falhas ou exceções; e
- necessidade de aprimoramento do processo ou do desenho do controle.

6.4 TRATAMENTO DE FALHAS, DEFICIÊNCIAS E PLANOS DE AÇÃO

Falhas, deficiências, inconsistências ou fragilidades identificadas nos controles internos devem ser formalmente registradas, avaliadas quanto à causa, impacto e risco, e endereçadas por meio de plano de ação com responsável, prazo, prioridade e acompanhamento até sua efetiva conclusão.

Os planos de ação deverão ser compatíveis com a criticidade da falha identificada e poderão envolver, conforme o caso, incluindo, mas não se limitando a:

- revisão de procedimento;
- reforço de controle existente;
- implementação de novo controle;
- ajuste sistêmico;
- treinamento ou comunicação interna;
- revisão de alçadas ou responsabilidades;
- reporte à instância de governança competente; e
- avaliação de eventual necessidade de comunicação regulatória, quando aplicável.

6.5 REPORTE E GOVERNANÇA DOS CONTROLES INTERNOS

Os resultados relevantes de monitoramento, testes, deficiências de controles, planos de ação, incidentes, exceções e riscos materiais devem ser reportados periodicamente à Alta Administração ou às instâncias de governança competentes, de forma compatível com a criticidade dos temas identificados.

A atuação em controles internos deverá observar o modelo de linhas de defesa adotado pelo Grupo SRM, cabendo:

- às áreas de negócio e áreas operacionais, a execução dos processos e controles sob sua responsabilidade;
- às áreas de Compliance, Controles Internos, Riscos e demais áreas de segunda linha, o monitoramento, orientação, avaliação, reporte e acompanhamento dos riscos e controles; e
- à Auditoria Interna, quando aplicável, a avaliação independente da efetividade da governança, do gerenciamento de riscos e dos controles internos.

6.6 MATRIZ DE RISCOS E CONTROLES

O Grupo SRM deverá manter estrutura de identificação e documentação dos principais riscos e controles associados aos processos relevantes, por meio de matriz de riscos corporativa, inventário de controles, plano de testes ou documento equivalente, conforme metodologia definida pela área responsável.

A matriz de riscos corporativa deverá contemplar, quando aplicável:

- processo ou atividade avaliada;
- risco identificado;
- controle associado;
- responsável pelo controle;
- periodicidade de execução;
- avaliação de efetividade; e
- plano de ação associado, quando necessário.

A estrutura de controles internos deverá ser continuamente aprimorada, considerando a evolução das atividades do Grupo SRM, alterações regulatórias, mudanças no ambiente de negócios, resultados de testes, auditorias, fiscalizações, incidentes, apontamentos de reguladores e necessidades identificadas pela Alta Administração.

7. GOVERNANÇA CORPORATIVA

O Grupo SRM adota os princípios de governança corporativa de transparência, equidade, prestação de contas (*accountability*) e responsabilidade corporativa como pilares da condução de suas atividades.

A estrutura de governança corporativa do Grupo SRM deve observar as seguintes diretrizes:

- *Transparência:* o Grupo SRM deve disponibilizar, de forma tempestiva e adequada, as informações relevantes sobre suas atividades, resultados, riscos e governança às partes interessadas, nos termos exigidos pela regulação aplicável e pelas melhores práticas de mercado;
- *Estrutura de decisão e alçadas:* as decisões do Grupo SRM devem ser tomadas de acordo com as alçadas e os órgãos deliberativos formalmente estabelecidos, assegurando a segregação entre as funções executivas, deliberativas e de supervisão;

- *Instâncias de governança:* o Grupo SRM deve manter instâncias de governança adequadas (Diretoria Executiva, comitês, conselho, conforme aplicável), com composição, competências, periodicidade e regras de funcionamento formalmente definidas;
- *Prestação de contas e responsabilidade dos administradores:* os administradores devem prestar contas de forma clara, completa e tempestiva, assumindo responsabilidade pelos atos praticados no exercício de suas funções;
- *Política de remuneração alinhada com compliance:* a estrutura de remuneração e incentivos não deve estimular a assunção de riscos excessivos ou comportamentos contrários às normas de compliance, às leis aplicáveis e aos padrões éticos do Grupo SRM; e
- *Relacionamento com reguladores:* o Grupo SRM deve manter relacionamento transparente, colaborativo e tempestivo com os reguladores (CVM, BCB, COAF, ANBIMA) e demais autoridades competentes.

A Governança Corporativa do Grupo SRM compreende o sistema pelo qual o Grupo SRM é dirigido, monitorado e prestado contas, envolvendo os relacionamentos entre sócios, Alta Administração, comitês de assessoramento, órgãos de controle e demais partes interessadas, com base nos princípios do Instituto Brasileiro de Governança Corporativa (IBGC) e nas exigências regulatórias aplicáveis às entidades reguladas.

7.1 ESTRUTURA DE GOVERNANÇA

A estrutura de governança do Grupo SRM compreende, em ordem hierárquica, as seguintes instâncias:

- *Sócios / Acionistas:* Compostos pelos sócios fundadores e demais sócios das entidades do Grupo SRM, conforme Estatutos e Acordos de Sócios/Acionistas aplicáveis. Competem-lhes a aprovação de reorganizações societárias e reformas estatutárias; a eleição de administradores; a aprovação ou rejeição de contas; e as demais deliberações previstas em lei, Estatuto Social e Acordo de Acionistas.
- *Assembleia Geral:* Órgão soberano das entidades constituídas sob a forma de S.A., composto pelos acionistas. Possui competência sobre reforma estatutária, eleição de membros de conselhos quando aplicável, aprovação ou rejeição de contas, reorganizações societárias e demais matérias previstas em lei, Estatuto e Acordo de Acionistas.
- *Alta Administração:* Composta pelos Sócios Diretores Executivos e Diretores Executivos das entidades do Grupo SRM. Competem-lhe a orientação geral dos negócios; a aprovação de políticas corporativas; a designação de Diretores Responsáveis; a aprovação de documentos normativos de alta criticidade; a deliberação sobre exceções relevantes e descumprimentos graves; e a garantia de recursos adequados ao Programa de Compliance.
- *Comitês:* A Alta Administração tem a responsabilidade de definir e aprovar a estrutura de governança do Grupo SRM, bem como aprovar a instituição de comitês técnicos, de assessoramento e de controle e respectivos regimentos interno, incluindo a composição, atribuições, periodicidade, quórum e forma de deliberação dos comitês.
- *Diretores Responsáveis:* A designação de Diretores Responsáveis perante os reguladores será formalizada nos respectivos processos administrativos e registros regulatórios de cada entidade, conforme as exigências da CVM, do BCB e da ANBIMA. A identidade dos Diretores Responsáveis vigentes constará dos manuais específicos de cada entidade ou de comunicações internas devidamente arquivadas pela área de Compliance.

8. PROCEDIMENTOS

Os procedimentos operacionais detalhados para implementação das diretrizes previstas nesta Política serão disciplinados em manuais, procedimentos e documentos complementares específicos, organizados conforme a hierarquia normativa do Manual Corporativo de Governança Normativa do Grupo SRM e vinculados a esta Política. Esta seção estabelece as diretrizes procedimentais de alto nível.

8.1 MONITORAMENTO E VERIFICAÇÃO DE COMPLIANCE

A área de Compliance deve conduzir atividades contínuas de monitoramento das atividades das entidades do Grupo SRM, dos colaboradores e das operações, com o objetivo de identificar tempestivamente desvios, inconformidades, riscos emergentes e situações que demandem ação corretiva. O monitoramento deve ser documentado e seus resultados registrados em sistema ou arquivo adequado.

8.2 REPORTE E COMUNICAÇÃO REGULATÓRIA

A área de Compliance é responsável por centralizar, coordenar e monitorar o cumprimento de todas as obrigações de reporte e comunicação às entidades regulatórias e autorreguladores. Os prazos regulatórios devem ser gerenciados por meio de sistema ou controle formal. Qualquer demanda recebida de regulador (ofício, questionário, inspeção) deve ser imediatamente comunicada à área de Compliance, que coordenará a elaboração e formalização da resposta.

8.3 GESTÃO DE INCIDENTES DE COMPLIANCE

Qualquer inconformidade, incidente, suspeita de irregularidade ou violação desta Política deve ser reportada à área de Compliance, que procederá com a análise preliminar, a investigação e a definição das medidas cabíveis. Os incidentes e suas resoluções devem ser documentados e, quando relevantes, reportados à Alta Administração. Situações que configurem descumprimento regulatório devem ser analisadas quanto à necessidade de comunicação voluntária ao regulador.

8.4 REVISÃO E ATUALIZAÇÃO NORMATIVA

A área de Compliance deve monitorar, de forma sistemática, o ambiente legal, regulatório e autorregulatório aplicável às entidades do Grupo SRM e comunicar tempestivamente às áreas impactadas e à Alta Administração qualquer alteração normativa relevante. As políticas, manuais e procedimentos internos devem ser atualizados sempre que necessário, em conformidade com os prazos e requisitos do Manual Corporativo de Governança Normativa.

9. MONITORAMENTO, CONTROLES E GOVERNANÇA

9.1 INSTÂNCIAS DE GOVERNANÇA DO PROGRAMA DE COMPLIANCE

O Programa de Compliance do Grupo SRM deve ser supervisionado por instâncias de governança adequadas, que assegurem visibilidade da Alta Administração sobre os riscos de compliance, as inconformidades identificadas e o status dos planos de ação. As instâncias e seus critérios de composição, competências e periodicidade serão definidos nos manuais específicos de cada entidade e no documento de governança interna do Grupo SRM.

9.2 REPORTE PERIÓDICO À ALTA ADMINISTRAÇÃO

A área de Compliance deve elaborar e apresentar relatório periódico à Alta Administração, com periodicidade mínima anual e sempre que houver ocorrência relevante, contendo, no mínimo:

- status de implementação e avaliação da efetividade do Programa de Compliance;
- sumário das principais inconformidades identificadas e dos planos de ação em andamento;
- atualização sobre alterações regulatórias relevantes e seus impactos para o Grupo SRM;
- status das comunicações com reguladores e autorreguladores;
- resultados dos programas de treinamento e indicadores de conscientização; e
- avaliação do perfil de risco de compliance do Grupo SRM e recomendações de melhoria.

9.3 INDICADORES DE COMPLIANCE E CONTROLES INTERNOS

A área de Compliance, em conjunto com Controles Internos, deverá acompanhar indicadores, ocorrências, apontamentos, planos de ação e demais informações relevantes relacionadas à aderência regulatória, à efetividade dos controles internos e ao cumprimento desta Política, reportando desvios relevantes à Alta Administração ou às instâncias de governança competentes.

9.4 AUDITORIA E AVALIAÇÃO INDEPENDENTE

A Auditoria Interna deve avaliar, de forma independente e periódica, a adequação, a suficiência e a efetividade do Programa de Compliance e da estrutura de controles internos do Grupo SRM. Os relatórios de auditoria, os planos de ação decorrentes e o acompanhamento de sua implementação devem ser formalizados e preservados como evidência.

10. ALÇADAS / CRITÉRIOS

A área de Compliance será a instância técnica responsável pela interpretação desta Política, pela avaliação de aderência regulatória, pela orientação às áreas, pela manifestação sobre exceções, pela análise de conflitos de interesse, pelo acompanhamento de inconformidades e pelo monitoramento dos planos de ação relacionados ao Programa de Compliance, Controles Internos e Governança. As decisões relacionadas à aplicação desta Política deverão observar a natureza da matéria, a criticidade do tema, o risco envolvido, a materialidade, o impacto regulatório, financeiro, operacional ou reputacional e a estrutura de governança aplicável à respectiva sociedade integrante do Grupo SRM.

As dúvidas de interpretação, orientações gerais, recomendações de conformidade e avaliações técnicas relacionadas a esta Política deverão ser submetidas à área de Compliance.

As exceções pontuais às diretrizes desta Política, quando não envolverem impacto regulatório relevante, conflito de interesses, impacto reputacional ou afastamento de controle material, deverão ser avaliadas pela área de Compliance e aprovadas pelo diretor responsável pela área impactada, conforme a natureza do tema.

As exceções que envolvam risco regulatório relevante, potencial descumprimento legal, regulatório ou autorregulatório, conflito de interesses, impacto reputacional, tratamento diferenciado ou afastamento de controle relevante deverão ser previamente avaliadas pela área de Compliance e submetidas à deliberação do Diretor responsável por Compliance, da Diretoria Executiva ou da instância de governança competente, conforme a criticidade do caso.

As inconformidades, falhas de controles ou descumprimentos internos de baixa ou média criticidade deverão ser tratadas pela área responsável pelo processo, com acompanhamento da área de Compliance e/ou de Controles Internos, quando aplicável. Inconformidades relevantes, recorrentes ou com potencial impacto regulatório, financeiro, operacional ou reputacional deverão ser escaladas à Diretoria responsável, ao Diretor responsável por Compliance, à Diretoria Executiva ou à instância de governança competente.

Os conflitos de interesse envolvendo colaboradores, terceiros, prestadores de serviço ou parceiros deverão ser avaliados pela área de Compliance, com deliberação da Diretoria responsável quando necessário. Quando o conflito envolver administradores, diretores, membros da Alta Administração, partes relacionadas ou situações de maior sensibilidade, a deliberação deverá ser submetida à Diretoria Executiva, ao Conselho de Administração, comitê ou órgão equivalente, quando existente.

As decisões relacionadas ao arquivamento, encerramento ou não prosseguimento de apurações internas relevantes deverão ser formalmente fundamentadas, registradas e aprovadas pelo Diretor responsável por Compliance, pela Diretoria Executiva ou por instância de governança definida para o caso, observadas as regras de confidencialidade, independência e ausência de conflito de interesses.

As medidas disciplinares decorrentes de apurações internas deverão ser avaliadas pela Diretoria responsável, pela área de Recursos Humanos e/ou pela Alta Administração, conforme a gravidade dos fatos apurados, com suporte da área de Compliance quando envolver descumprimento de normas internas, conduta ética, conflito de interesses, fraude, corrupção, assédio, discriminação, retaliação ou irregularidade relevante.

As comunicações regulatórias obrigatórias, inclusive aquelas relacionadas à prevenção à lavagem de dinheiro e ao financiamento do terrorismo, deverão observar os prazos, responsáveis e procedimentos previstos na legislação, na regulamentação aplicável e nos normativos internos específicos, não podendo ser indevidamente retardadas por fluxos internos de aprovação.

As alterações, revisões, revogações ou substituições desta Política e de seus documentos vinculados deverão observar o fluxo de governança normativa definido no Manual Corporativo de Governança Normativa do Grupo SRM, incluindo as alçadas de aprovação de documentos normativos nele previstas.

Todas as aprovações, exceções, deliberações, decisões de arquivamento, medidas corretivas e escalonamentos tratados nesta seção deverão ser formalmente registrados, com indicação da fundamentação, responsáveis, aprovações, medidas adotadas e evidências aplicáveis, de forma a permitir rastreabilidade, prestação de contas e verificação posterior por Compliance, Controles Internos, Auditoria Interna, Alta Administração, reguladores ou demais instâncias competentes, quando aplicável.

11. CONSEQUÊNCIAS PELO DESCUMPRIMENTO

O descumprimento das disposições desta Política, dos normativos internos vinculados, das leis e regulações aplicáveis sujeitará os responsáveis, administradores e colaboradores, às medidas disciplinares cabíveis, graduadas conforme a gravidade, a reincidência e os impactos da conduta, sem prejuízo das responsabilidades civil, penal e administrativa decorrentes.

As medidas disciplinares podem incluir, conforme o caso:

- advertência formal;
- suspensão;
- rescisão do vínculo empregatício por justa causa;

- responsabilização civil pelos danos causados ao Grupo SRM, a seus clientes ou a terceiros;
- comunicação aos órgãos regulatórios e autorreguladores competentes, quando exigida ou recomendada pela gravidade da infração; e
- aplicação das penalidades contratuais previstas em contratos com prestadores de serviço ou parceiros.

A aplicação de medidas disciplinares observará os princípios do contraditório, da ampla defesa e da proporcionalidade, nos termos da legislação trabalhista aplicável e dos procedimentos internos de Recursos Humanos. A área de Compliance comunicará à Alta Administração e, quando aplicável, ao setor de Recursos Humanos os casos que configurem descumprimento relevante desta Política, para deliberação sobre as medidas cabíveis.

12. EXCEÇÕES

Qualquer exceção às disposições desta Política deve ser previamente analisada e aprovada pela área de Compliance e, conforme a materialidade, pela Alta Administração. Não serão admitidas exceções que configurem violação a disposições legais ou regulatórias imperativas.

O processo de solicitação e aprovação de exceções deve seguir os seguintes passos:

- Solicitação formal e fundamentada pelo responsável da área peticionante à área de Compliance, com descrição da situação, dos riscos associados e das medidas de mitigação propostas;
- Análise pela área de Compliance quanto à viabilidade jurídica, regulatória e de risco da exceção solicitada;
- Aprovação formal da exceção, com registro da fundamentação, dos riscos aceitos e do prazo de validade; e
- Monitoramento pela área de Compliance do cumprimento dos termos da exceção aprovada e de sua vigência.

Exceções aprovadas devem ser documentadas e periodicamente revisadas. Não é admitida a prorrogação tácita de exceções vencidas.

13. DISPOSIÇÕES GERAIS

Esta Política deve ser interpretada em conjunto com os demais documentos normativos do Grupo SRM, respeitada a hierarquia normativa estabelecida no Manual Corporativo de Governança Normativa. Em caso de conflito aparente entre as disposições desta Política e normas externas imperativas (leis ou regulamentos), prevalecerão as normas externas, devendo a área de Compliance ser imediatamente comunicada para avaliação e atualização dos documentos internos. Casos omissos serão analisados e decididos pela área de Compliance, com registro formal da orientação adotada.

Esta Política e seus documentos vinculados são de acesso restrito a colaboradores, administradores e terceiros abrangidos por sua abrangência. A distribuição externa somente será admitida nos termos exigidos pela regulação aplicável ou mediante autorização expressa da área de Compliance.

14. REVISÃO E ATUALIZAÇÃO

Esta Política deve ser revisada com periodicidade mínima anual pela área de Compliance, com aprovação nas instâncias competentes conforme o Manual Corporativo de Governança Normativa. Adicionalmente,

revisão extraordinária deve ser realizada sempre que houver alteração relevante no ambiente legal, regulatório ou autorregulatório aplicável às entidades do Grupo SRM, mudança societária ou de controle, alteração do perfil de risco do Grupo SRM ou identificação de deficiência material no Programa de Compliance.

Toda revisão deve ser registrada no Histórico de Revisão ao final deste documento, com descrição objetiva das alterações realizadas. A versão aprovada e vigente desta Política deve ser publicada no repositório oficial do Grupo SRM, garantindo que todos os colaboradores e administradores tenham acesso à versão mais atualizada.

QUADRO DE APROVAÇÃO

Etapa	Responsável	Data / Assinatura
Elaboração	Compliance e Controles Internos	28/05/2026
Revisão	Compliance e Controles Internos	05/06/2026
Aprovação	Diretoria Executiva	15/06/2026

HISTÓRICO DE REVISÃO

Versão	Data	Responsável	Síntese da Alteração
1.0	15/06/2026	Compliance e Controles Internos	Primeira emissão da Política de Compliance, Controles Internos e Governança Corporativa.