AV1 GESTORA DE RECURSOS LTDA.

Política de *Compliance*, Controles Internos e Segregação de Atividades

Versão	Data de Atualização
1ª	Julho/2025

SUMÁRIO

1. Introdução

A presente Política de *Compliance*, Controles Internos e Segregação de Atividades ("Política") tem como objetivo estabelecer os conceitos, regras e procedimentos dos controles internos da **AV1 Gestora de Recursos LTDA** ("AV1") na condução de suas atividades inerentes à administração de carteiras de valores mobiliários, conforme estabelecido pela Resolução da Comissão de Valores Mobiliários ("CVM") nº 21, de 25 de fevereiro de 2021 ("Resolução CVM 21"), pelo Código de Melhores Práticas para Administração de Recursos de Terceiros da Associação Brasileira das Entidades dos Mercados Financeiros e de Capitais ("ANBIMA") ("Código ANBIMA"), e demais regulamentações aplicáveis. A AV1 busca, por meio de controles internos adequados, o permanente atendimento às normas, políticas e regulamentações vigentes, bem como a elevados padrões éticos e profissionais.

A Política apresentada poderá ser atualizada e complementada, e é de responsabilidade de todos os Colaboradores (conforme abaixo definido) conhecer e cumprir todas as obrigações legais e regulatórias em suas atividades, prezando por altos padrões de conduta profissional. Também é obrigação de todos os Colaboradores notificar o Departamento de Risco e Compliance em casos de condutas indevidas sob o ponto de vista legal, ético ou regulatório.

2. Abrangência

Esta Política aplica-se a todos os colaboradores da AV1, incluindo sócios, administradores, diretores, funcionários, estagiários, consultores e colaboradores temporários ("Colaboradores") que deverão compreender o seu conteúdo e aderir formalmente à presente Política por meio da assinatura do "Termo de Compromisso" anexo ao Código de Ética e Conduta da AV1.

3. Estrutura de Compliance

A política de compliance da AV1 tem como princípios: (i) assegurar que todo profissional atue com imparcialidade e conheça o código de ética, bem como as normas aplicáveis ao exercício de suas atividades; (ii) garantir a confidencialidade de informações que a AV1 e seus colaboradores têm acesso no exercício de suas atividades; e (iii) implementar e manter programa de treinamento de sócios e colaboradores da AV1.

3.1. Departamento de Risco e Compliance

O Departamento de Risco e Compliance é independente e não está subordinado a nenhum outro departamento da AV1. O referido departamento é liderado pelo Diretor responsável, perante a CVM, designado no contrato social possuindo comunicação direta para a divulgação dos resultados decorrentes das atividades de *compliance* incluindo irregularidades ou falhas identificadas.

Entre as atividades aplicáveis ao Departamento de Risco e Compliance da AV1, estão as seguintes:

(1) administração da presente Política;
(2) verificação da correta aderência dos Colaboradores às políticas e códigos;
(3) atualização em relação às legislações em vigor e organizar evidências do cumprimento dos processos e controles internos, efetuando as correções de quaisquer falhas detectadas; e
(4) oferecimento de suporte às outras áreas da AV1 para esclarecer eventuais dúvidas sobre as políticas, manuais e regulamentos internos.

O Departamento de Risco e Compliance possui autonomia e autoridade para questionar os riscos assumidos nas operações realizadas pela mesa de operações.

Além disso, em atendimento ao artigo 22 da Resolução CVM 21, caberá ao Departamento de Risco e *Compliance* elaborar o "Relatório de Compliance e Controles Internos", até o último dia útil de abril, mantendo-o à disposição da CVM, arquivado na sede da AV1. O Relatório de Compliance e Controles Internos faz referência às operações do ano anterior ao de sua elaboração e contém: (a) os resultados dos testes periódicos de controle e aderência executados; (b) recomendações para solucionar quaisquer deficiências e cronograma de plano relevante para soluciona-las; e (c) comentários do responsável pelas atividades de gestão de ativos perante a CVM com relação a essas deficiências ou quaisquer deficiências encontradas em verificações anteriores, se houver, bem como o plano de solução do problema ou as atuais medidas tomadas para resolver tais deficiências de acordo com o cronograma de plano estabelecido para tal propósito.

4. Controles Internos

O Departamento de Risco e Compliance é responsável por garantir o cumprimento das regras, procedimentos e controles internos a que se refere esta Política e, consequentemente, deverá elaborar, em conjunto com as demais áreas aplicáveis, os planos de ação necessários a falhas de execução identificadas nos processos ou controles. Ao mesmo tempo, o Departamento de Risco e Compliance deve mitigar as ocorrências de ilícitos ou atividades contrárias à regulação.

A AV1 possui controles internos adequados para garantir o permanente atendimento às normas e regulamentações vigentes aplicáveis às atividades por ela desempenhadas, de forma a:

(i) Estabelecer o conceito de controles internos através do estabelecimento de cultura de Compliance, visando melhoria nos controles;
(ii) Realizar os reportes regulatórios periódicos exigidos pela Resolução CVM 21 e demais regulamentações aplicáveis;
(iii) Assegurar que todos os Colaboradores atuem com imparcialidade e conheçam as Políticas Locais, normas aplicáveis às atividades desempenhadas;
(iv) Apoiar as áreas de 1ª linha de defesa no processo de gestão dos riscos operacionais com o desenvolvimento de processos, métodos, ferramentas e Políticas Locais; e

(v) Identificar, administrar e eliminar eventuais conflitos de interesses que possam afetar a imparcialidade dos Colaboradores que desempenhem funções ligadas à administração de carteiras de valores mobiliários.

4.1. Procedimentos da AV1

A supervisão dos Colaboradores que desempenham funções relacionadas à administração de carteiras de valores mobiliários ainda inclui a observância de que atuem com imparcialidade evitando qualquer potencial conflito de interesse. O Diretor de Risco e Compliance pode a qualquer momento requisitar a estação de trabalho de um Colaborador com o propósito de efetuar exames e análises quando houver suspeitas de descumprimento dos regulamentos internos ou atividades ilegais. A solicitação do computador é válida apenas com a finalidade de averiguar a correta observância das normas internas e utilização adequada dos recursos disponibilizados pela AV1, devendo o Diretor de Risco e Compliance evitar qualquer exame que fira as regras e leis trabalhistas. Cada colaborador possui acesso eletrônico ao servidor apenas no que se referem às pastas e aos arquivos relacionados à sua atividade.

Apenas o Departamento de Risco e Compliance e os principais executivos da AV1 que compõem o Comitê Executivo possuem acesso irrestrito aos arquivos do servidor. O Departamento de Risco e Compliance também deve apurar se os acessos estão adequados e sendo respeitados pelos Colaboradores. Prudência maior é dada para informações confidenciais de clientes cujos dados pessoais não podem ser copiados e devem ser utilizados apenas nas dependências da AV1. O Departamento de Risco e Compliance deve observar acessos não autorizados e investigar os motivos. O Departamento de Risco e Compliance gerencia uma ficha com a lista de pastas eletrônicas a que cada Colaborador tem acesso. Os Colaboradores recebem e-mails e fazem parte de grupos de distribuição relativos à suas tarefas desempenhadas na AV1.

Os Colaboradores são responsáveis pelas suas estações de trabalho, devendo protegê-las corretamente. As senhas, os acessos pessoais e as informações confidenciais devem ser guardadas e utilizadas adequadamente e podem ser requisitados pelo Departamento de Risco e Compliance quando da necessidade de alguma inspeção.

Toda rede computacional da AV1 está protegida por firewalls, antivírus e filtros de spans. Testes periódicos são feitos com propósito de avaliar possíveis vulnerabilidades e falhas nos sistemas operacionais, softwares e rede. São feitos (i) testes de penetração, de modo a identificar possíveis falhas sistêmicas e (ii) armazenamento de informações confidenciais protegidas por criptografia. O Departamento de Risco e Compliance tem acesso a todas as mensagens trocadas via e-mail e deve ficar atento quanto aqueles contendo anexos de arquivos de grandes tamanhos. Todas as ligações telefônicas são gravadas e podem ser acessadas pelo Departamento de Risco e Compliance para esclarecer dúvidas ou quando houver suspeitas de descumprimento das políticas internas. Diariamente é feito *backup* dos arquivos salvos em nuvem em um local diferente do escritório da AV1.

Anualmente o Diretor de Risco e Compliance deverá preparar um relatório relativo ao ano civil anterior contendo a conclusão dos exames efetuados e recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando necessário.

4.2. Reportes Regulatórios

O Departamento de Risco e Compliance será obrigado a apresentar o Formulário de Referência à CVM, até 31 de março de cada ano, nos termos do Anexo E, da Resolução CVM 21. Além disso, deverá cumprir com outros reportes regulatórios previstos na regulação aplicável, como o Relatório de Compliance e Controles Internos referido no item 3.1 acima, bem como a comunicação de não ocorrência (CNO) devida ao Conselho de Controle de Atividades Financeiras (COAF) até o dia 31 de janeiro de cada ano, entre outros.

Além disso, a AV1 deve manter os registros na CVM e o Formulário de Referência atualizados com relação a seus dados societários, informando à CVM, o mais rápido possível, de qualquer alteração dessas informações. O Formulário de Referência, juntamente com essa Política e todas as demais políticas da AV1 exigidas pela CVM, estarão disponíveis no site da AV1.

5. Incidentes de Segurança

Na hipótese de ocorrência do vazamento de algum dado confidencial interno da AV1, o Departamento de Risco e Compliance deverá verificar a potencial extensão dos danos, bem como avaliar a necessidade de comunicação privada ou pública do vazamento das informações, a reavaliação das medidas de segurança da informação e, caso necessário, comunicar o vazamento aos órgãos competentes.

6. Segregação de Atividades

A política de segregação física de atividades tem como objetivo estabelecer as regras que orientam a segregação física das instalações entre áreas responsáveis pelas atividades prestadas pela empresa, em particular, as atividades de administração de carteiras das demais atividades desenvolvidas. A empresa estará focada somente nos serviços de gestão de recursos de terceiros.

A AV1 Gestora de Recursos Ltda. tem como objeto social a administração e gestão de carteiras de valores mobiliários, bem como a constituição, administração e gestão de fundos de investimento, conforme disposto em seu contrato social arquivado na Junta Comercial do Estado de São Paulo.
O plano de negócios da AV1 contempla a gestão de recursos de terceiros por meio de veículos como Fundos de Investimento em Direitos Creditórios (FIDC), Fundos de Investimento em Participações (FIP), Fundos de Investimento Imobiliário (FII) e carteiras administradas voltadas a investidores qualificados e profissionais.

Todas as atividades descritas são exercidas de forma segregada e independente das demais empresas do grupo econômico, garantindo a inexistência de interferência operacional, decisória ou comercial.

O acesso aos sistemas utilizados pela **AV1** é restrito, regido por perfis de acesso e controlado por senhas e registros de log. Da mesma forma, toda a informação em guardada em nuvem, com controle de acesso pelos colaboradores.

O Departamento de Risco e Compliance deverá monitorar os acessos concedidos aos Colaboradores, e cabe ao supervisor a responsabilidade pela análise da necessidade e verificação da correta utilização dos acessos e ferramentas concedidas.

Além da segregação dos itens listados acima, há também a devida segregação fisíca da Gestora e suas atividades, sendo esta devidamente segregada com portas e fechaduras eletrônicas com as digitais salvas, somente dos colaboradores da **AV1,** garantindo a efetiva independência e segregação fisíca das atividades da Gestora.

7. Treinamento

O Departamento de Risco e Compliance repassa a todos os Colaboradores as políticas e manuais da AV1 de forma que todos tenham conhecimento das melhores práticas e condutas, através dos treinamentos internos, para os novos Colaboradores, e de reciclagem, para os demais colaboradores. A AV1 incentiva que todos os colaboradores busquem atualizações em suas respectivas atividades de trabalho e que esclareçam dúvidas no ambiente interno.

Havendo necessidade, A AV1 promove treinamentos abertos aos colaboradores a respeito das melhores práticas de mercado.

8. Política de Certificação

A AV1 não realiza a distribuição das cotas dos fundos por ela geridos. No entanto, é obrigatória a obtenção do CGA, ou de equivalentes para fins de autorização da função de administrador de recursos, conforme ANEXO A À RESOLUÇÃO CVM Nº 21, para aqueles Colaboradores que trabalhem na área de gestão de recursos e que tenham alçada/poder discricionário de investimento (compra e venda) dos ativos dos fundos de investimentos sob gestão.

A exigibilidade de certificação obrigatória não está relacionada ao cargo formal do profissional, mas sim às atividades efetivamente exercidas por ele.

O profissional contratado (não certificado) receberá, no momento da contratação, as instruções sobre a necessidade de certificação, a depender da atividade que exercerá dentro da AV1. O Departamento de Risco e Compliance efetuará os devidos registros junto às entidades pertinentes.

O profissional que não apresentar a certificação necessária, deve ser impedido de iniciar as suas atividades. Se completado o prazo estabelecido pelo Departamento de Risco e Compliance para a retirada da certificação e o profissional não tiver apresentado, cabe ao Departamento de Risco e Compliance a comunicação ao responsável pela área em que o Colaborador foi contratado de que o profissional ainda não está habilitado a exercer as atividades pelas quais foi contratado.

Cabe ao responsável pela área que fez a contratação do novo Colaborador, a definição sobre o eventual remanejamento para uma outra área ou a sua manutenção em atividades não elegíveis, devidamente supervisionado por funcionários que possuem a certificação.

9. Plano de Continuidade de Negócios

A AV1 possui um Plano de Contingência de forma a garantir a linearidade das operações, prevendo recursos alternativos e estratégias de continuidade em casos de ocorrências inesperadas.

Observados os Evento de Contingência, a estratégia de continuidade a ser adotada pela AV1 poderá conter, entre outras, as seguintes soluções para viabilizar a manutenção de seus negócios:

- Controle de acesso as dependências por meio do uso de (i) crachás e/ou (ii) chaves;
- Controle de acesso aos sistemas da gestora por meio de login e senha;
- Revezamento de Colaboradores (trabalho remoto);
- Planejamento de sucessão das atribuições dos Colaboradores;
- Uso de recursos humanos terceirizados;
- Contratação de novas tecnologias da informação e segurança da informação;
- Contratação de serviços de assinatura eletrônica;
- Contratação de serviços de guarda de documentação;
- Manutenção dos sistemas através de equipamentos geradores instalados no condomínio do prédio e notebook com bateria para suprir o fornecimento de energia nos equipamentos principais para a manutenção das comunicações e atividades mínimas da AV1;
- Prédio onde se localiza o provedor de em nuvem da AV1 conta com geradores próprios.

Além disso, para garantir a continuidade das atividades, a AV1 realiza o backup das informações digitais e dos sistemas existentes no escritório armazenados em (i) disco externo ao servidor de produção; ou (ii) em sistema de armazenamento em nuvem.

Por fim, convém ressaltar que a AV1 conta com uma estrutura de tecnologia da informação compatível com o volume e complexidade de suas operações, bem como com sistemas contratados para arquivamento, firewall e VOIP centralizado em servidor com controle total de monitoramento e bloqueio de acesso. Ressalta-se que os sistemas contratados pela AV1 asseguram proteção integral contra adulterações e permitem a realização de auditorias e inspeções.

Após a ocorrência de qualquer Evento de Contingência, o Comitê de Compliance deverá avaliar os prejuízos decorrentes da ocorrência e propor melhorias e investimentos para a redução dos riscos.

9.1 Testes De Contingência

Os testes de contingência serão realizados no mínimo a cada 12 (doze) meses, ou em prazo inferior se exigido pela regulação em vigor e/ou se constatada necessidade pela AV1.

Os testes a serem realizados têm como objetivo avaliar o presente Plano e se ele é capaz de suportar, de modo satisfatório, os processos operacionais críticos para a continuidade dos negócios da AV1, de modo a manter a integridade, a segurança e a consistência dos bancos de dados criados pela alternativa adotado pelo Plano, bem como se o Plano pode ser ativado tempestivamente considerando o Evento de Contingência.

Os testes serão:

- Testes dos no breaks, verificando o status de funcionamento e do tempo de suporte das baterias com carga;
- Acesso aos sistemas e aos e-mails remotamente;
- Acesso aos dados armazenados externamente e/ou em nuvens; e
- Testes e atualizações nos equipamentos dos Colaboradores assegurando seu bom funcionamento.

10. Política de Segurança da Informação

A AV1 estabelece a presente Política de Segurança da Informação, a fim de garantir a aplicação dos princípios e diretrizes de proteção das informações e da propriedade intelectual da organização, dos clientes e do público em geral. Considerando-se a rápida evolução das práticas e soluções de segurança da informação, exigindo constante adaptações, esta Política será atualizada e reavaliada por diretrizes e materiais adicionais ao longo do tempo.

A Política de Segurança da Informação visa garantir a confidencialidade, disponibilidade e integridade das informações, sejam elas de terceiros ou dados da própria AV1.

- Confidencialidade: garante que as informações tratadas pela AV1 sejam restritas a um grupo restrito de usuários autorizados, impedindo a exposição de dados restritos e acessos não autorizados.
- Disponibilidade: garante a disponibilidade de informações aos usuários autorizados sempre que necessário.
- Integridade: garante a veracidade e completude das informações, de forma que elas sejam íntegras e sem alterações à dados por pessoas não autorizadas que possam efetuar modificações não aprovadas.

Toda informação relacionada às operações da AV1, gerada ou desenvolvida nas dependências da AV1, durante a execução das atividades de prestador de serviços de correspondente no país para A AV1, constitui ativo desta instituição financeira, essencial à condução de negócios, e em última análise, à sua existência. Independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada. A modificação, divulgação e destruição não autorizadas e oriundas de erros, fraudes, vandalismo, espionagem ou sabotagem causam danos aos negócios da AV1.

Toda informação de propriedade da AV1 deve ser protegida de riscos e ameaças que possam comprometer a confidencialidade, integridade ou disponibilidade destas. As diretrizes adotadas são:

a) As informações da AV1, dos clientes e do público em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida;

b) As senhas são utilizadas como assinatura eletrônica e não devem ser divulgadas para todos. A senha e login para acesso aos dados contidos em todos os computadores e equipamentos da AV1, bem como nos e-mails que também possam ser acessados via webmail, devem ser conhecidas somente pelo respectivo usuário do equipamento ou do sistema e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros. O Colaborador se responsabiliza pessoalmente por qualquer conduta realizada por meio de suas credenciais de acesso aos equipamentos e sistemas da AV1.
c) Acesso a dados confidenciais são restritos a determinados usuários e bloqueados com base no login de usuário. Acessos indevidos devem ser comunicados imediatamente ao Departamento de Risco e Compliance;
d) As responsabilidades quanto à Segurança da Informação devem ser amplamente divulgadas aos Colaboradores, que devem entender e assegurar estas diretrizes;
e) Cada usuário é responsável pelo uso dos recursos que lhe foram entregues, e estão sob sua custódia, garantindo a conservação, guarda e legalidade dos programas (softwares) instalados;
f) Os recursos que permitem o acesso à informação são autorizados e disponibilizados exclusivamente para o usuário desempenhar suas funções na AV1 ou para outras situações formalmente permitidas;
g) É proibida a conexão de equipamentos na rede da AV1 que não estejam previamente autorizados.;
h) Equipamentos eletrônicos corporativos ou nos quais circulem informações internas ou confidenciais da AV1 devem ter seu acesso protegido por, no mínimo, login e senha;
i) Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade;
j) A concessão de acesso às informações e sistemas deve ser autorizada com base na regra de mínimo acesso necessário para o desempenho da função;
k) Apenas os equipamentos e softwares disponibilizados e/ou homologados autorizados pela AV1 podem ser instalados e conectados à rede;
l) Solicitar alterações de senha sempre que exista a possibilidade de a mesma ter sido comprometida;
m) Alterações em diretrizes de segurança do computador são bloqueadas por senha, impossibilitando a desativação do firewall, por exemplo;
n) Em caso de não funcionamento do software antivírus instalado em cada computador, deverá o usuário notificar prontamente a equipe de TI;
o) Equipamentos particulares/privados, como computadores ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, não devem ser usados para armazenar ou processar informações relacionadas com o negócio da AV1, e só podem ser conectados à rede Wi-Fi de visitantes, exceto em casos em que o Plano de Contingência requeira essa prática e em que exista autorização explícita do Departamento de Risco e Compliance;
p) Os Colaboradores deverão manter arquivada na rede da AV1 toda e qualquer informação, bem como documentos que venham a ser necessários para a efetivação satisfatória de possível auditoria interna e/ou externa ou investigação de órgãos regulatórios em torno de possíveis atuações da AV1 em relação à esta Política e as atividades desenvolvidas pela AV1;

q) A senha da rede de internet principal da AV1 e das respectivas camadas de segurança são mantidas de forma segura e não são compartilhadas com todos os usuários; e
r) Toda violação ou desvio, tais como instalação (intencional ou não) de vírus de informática, uso de software ilegal e tentativas de acesso a informações restritas, por exemplo, é investigada para a determinação das medidas necessárias e definição de possíveis sanções, visando à correção da falha ou reestruturação de processos e evitando que casos análogos se repitam.

11. Revisão da Política

A presente Política será revisada anualmente, ou a qualquer momento, sempre que se observarem mudanças relevantes nas normas, regras, formato das atividades ou em qualquer outro aspecto intrínseco ao dia a dia da AV1, nos termos da regulamentação e diretrizes aplicáveis.

* * *