Versão vigente: 08/2026
Modificado por: Acácio Roboredo (revisão de conformidade)

Política de Regras, Procedimentos e Controles Internos

LAPB Gestão de Recursos Financeiros Ltda.

08.2026

backoffice@lapb.com.br
www.lapb.com.br

1. INTRODUÇÃO

Esta Política tem como objetivo estabelecer os conceitos, as regras e os procedimentos dos controles internos da LAPB Gestão de Recursos Financeiros Ltda. ("LAPB" ou "Gestora"), em observância à Resolução CVM nº 21, de 25 de fevereiro de 2021, ao Código ANBIMA de Regulação e Melhores Práticas para a Administração de Recursos de Terceiros e às demais normas aplicáveis à atividade de gestão de recursos de terceiros.

A LAPB busca, por meio de controles internos adequados, o permanente atendimento às normas, políticas e regulamentações vigentes, observando elevados padrões éticos e profissionais.

O Departamento de Compliance é o responsável por administrar esta Política, verificar a correta aderência dos colaboradores às políticas e códigos, mantê-la atualizada em relação à legislação em vigor e realizar testes periódicos dos processos e controles internos, efetuando as correções de quaisquer falhas detectadas. O Departamento de Compliance também oferece suporte às demais áreas, esclarecendo dúvidas sobre as políticas, os manuais e os regulamentos internos.

As políticas aqui apresentadas poderão ser atualizadas e complementadas. É responsabilidade de todos os colaboradores conhecer e cumprir 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 Compliance em casos de condutas indevidas sob o ponto de vista legal, ético ou regulatório.

2. ESTRUTURA

O Departamento de Controles Internos é independente e não está subordinado a nenhum outro departamento da LAPB. O Diretor responsável pela implementação e cumprimento de regras, políticas, procedimentos e controles internos, indicado no Contrato Social e perante a Comissão de Valores Mobiliários (CVM), está subordinado apenas ao Comitê Executivo, possuindo comunicação direta para a divulgação dos resultados decorrentes das atividades de compliance, incluindo irregularidades ou falhas identificadas.

Nos termos permitidos pela Resolução CVM nº 21/2021, o Diretor de Compliance da LAPB acumula as funções de compliance, de gestão de riscos e de prevenção à lavagem de dinheiro e ao financiamento do terrorismo (PLD/FTP). O exercício acumulado dessas funções observa a vedação de atuação em atividades de gestão de carteiras de valores mobiliários, de intermediação, de distribuição ou de consultoria de valores mobiliários, preservada a independência exigida pela regulação.

O Diretor de Compliance é responsável pela implementação geral dos procedimentos e pela adesão das políticas da LAPB e das normas regulamentares em vigor por todos os departamentos. Além de supervisionar as atividades dos colaboradores, o Departamento de Compliance oferece os esclarecimentos e suportes requisitados pelos próprios colaboradores.

O Departamento de Compliance possui autonomia e autoridade para questionar os riscos assumidos nas operações realizadas pela mesa de operações, podendo buscar embasamento junto ao Departamento de Risco.

É vedado ao Diretor de Compliance atuar em funções e atividades relacionadas à administração de recursos de terceiros e à distribuição ou consultoria de valores mobiliários, bem como em qualquer atividade que limite sua independência.

3. CONTROLES INTERNOS

O Departamento de Compliance supervisiona a estrita obediência de todos os colaboradores ao Código de Ética. Anualmente, todos os colaboradores devem preencher e assinar a Declaração Anual de Investimento e Endividamento Pessoal. Também deve haver preciso cumprimento à Política de Prevenção à Lavagem de Dinheiro e à Política de Combate ao Suborno e à Corrupção.

Ocasionalmente, o Departamento de Compliance acompanha a rotina dos colaboradores de modo a garantir o cumprimento dos manuais e políticas internas, a devida realização de suas atividades profissionais e a correta utilização dos sistemas e planilhas, bem como para identificar possíveis melhorias. A supervisão dos colaboradores que desempenham funções relacionadas à administração de carteiras de valores mobiliários inclui a observância de que atuem com imparcialidade, evitando qualquer potencial conflito de interesse.

Caso o Departamento de Compliance verifique algum desvio ou defeito nas atividades internas da LAPB, deve elaborar um plano de ação definindo prazo e as melhorias a serem implementadas. Ao mesmo tempo, deve atuar para mitigar as ocorrências de ilícitos ou atividades contrárias à regulação.

O Diretor de Compliance pode, a qualquer momento, requisitar a estação de trabalho de um colaborador com o propósito de efetuar exames e análises quando houver suspeita de descumprimento dos regulamentos internos ou de atividades ilegais. A solicitação é válida apenas com a finalidade de averiguar a correta observância das normas internas e a utilização adequada dos recursos disponibilizados pela LAPB, devendo o Diretor de Compliance evitar qualquer exame que fira as regras e leis trabalhistas.

Cada colaborador possui acesso eletrônico ao servidor apenas nas pastas e arquivos relacionados à sua atividade. Apenas o Departamento de Compliance e os principais executivos que compõem o Comitê Executivo possuem acesso irrestrito aos arquivos do servidor. Periodicamente, o Departamento de Compliance apura se os acessos estão adequados e sendo respeitados. Prudência maior é dada às informações confidenciais de clientes, cujos dados pessoais não podem ser copiados e devem ser utilizados apenas nas dependências da LAPB. O Departamento de Compliance observa acessos não autorizados e investiga os motivos, gerenciando 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 às tarefas desempenhadas na LAPB. Apenas colaboradores do Departamento Comercial, do Departamento de Compliance e os principais executivos recebem e-mails enviados pelos clientes com solicitações de movimentações.

Os colaboradores são responsáveis pelas suas estações de trabalho, devendo protegê-las adequadamente. Senhas, acessos pessoais e informações confidenciais devem ser guardados e utilizados adequadamente e podem ser requisitados pelo Departamento de Compliance quando da necessidade de inspeção.

A LAPB possui servidor fisicamente separado, em sala com acesso restrito e sistema de refrigeração. Toda a rede computacional da LAPB é protegida por firewalls, antivírus e filtros de spam. Testes periódicos são realizados com o propósito de avaliar possíveis vulnerabilidades e falhas nos sistemas operacionais, softwares e rede, incluindo avaliações de aplicativos e programas instalados, testes de "Ethical Hacking" e testes de penetração de rede.

O Departamento de Compliance tem acesso a todas as mensagens trocadas por e-mail e mantém atenção àquelas que contenham anexos de grandes tamanhos. Todas as ligações telefônicas são gravadas e podem ser acessadas para esclarecer dúvidas ou quando houver suspeita de descumprimento das políticas internas.

Diariamente, são realizados dois tipos de backup dos arquivos salvos no servidor: um armazenado fisicamente no escritório e outro armazenado em nuvem, em local diverso do escritório da LAPB. Áreas e departamentos com potenciais conflitos de interesse recebem atenção especial, com supervisões in loco mais frequentes.

Anualmente, o Diretor de Compliance prepara relatório relativo ao ano civil imediatamente anterior à data de entrega, contendo a conclusão dos exames efetuados e recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando necessário, nos termos do art. 22 da Resolução CVM nº 21/2021.

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

A LAPB mantém regras, procedimentos e controles internos destinados à prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa (PLD/FTP), em conformidade com a Resolução CVM nº 50, de 31 de agosto de 2021, com a Lei nº 9.613/1998 e com as diretrizes da ANBIMA aplicáveis à administração de recursos de terceiros.

Os procedimentos abrangem a política de "Conheça seu Cliente" (KYC), a avaliação de novos e atuais clientes com base em abordagem baseada em risco, a identificação de pessoas expostas politicamente (PEP), o monitoramento de operações atípicas e a comunicação de operações suspeitas ao Conselho de Controle de Atividades Financeiras (COAF), quando aplicável. O detalhamento dos procedimentos consta da Política de PLD/FTP da LAPB.

5. PROTEÇÃO DE DADOS PESSOAIS (LGPD)

O tratamento de dados pessoais pela LAPB observa a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e as orientações da Autoridade Nacional de Proteção de Dados (ANPD).

A coleta de informações de clientes restringe-se ao necessário para a manutenção dos investimentos e ao que é determinado pela legislação e pelos órgãos reguladores. Quando necessário ao cumprimento das Políticas de Combate à Corrupção e de Prevenção à Lavagem de Dinheiro, a LAPB pode solicitar informações adicionais para verificar a idoneidade do cliente. A LAPB observa, como melhor prática, também as normas internacionais de proteção de dados aplicáveis, sem prejuízo da prevalência da legislação brasileira.

O tratamento de dados pessoais pela LAPB apoia-se nas bases legais previstas no art. 7º da LGPD, notadamente o cumprimento de obrigação legal ou regulatória, a execução de contrato, o legítimo interesse e o consentimento do titular, conforme o caso. São assegurados aos titulares os direitos previstos no art. 18 da LGPD, incluindo confirmação, acesso, correção, anonimização, portabilidade, eliminação e revogação do consentimento.

Os dados dos clientes só podem ser acessados pelos colaboradores demandados por suas atividades. É expressamente proibida a divulgação parcial ou total de dados pessoais dos clientes, exceto quando requisitada por órgãos reguladores ou pela justiça, bem como é vedada a negociação ou venda desses dados. É permitida a utilização de dados de forma não individualizada para análises estatísticas, desde que não seja possível identificar o indivíduo originário dos dados.

A LAPB designará um Encarregado pelo Tratamento de Dados Pessoais (DPO) ou canal de comunicação com os titulares, cuja identificação e contato serão divulgados de forma clara e objetiva, nos termos do art. 41 da LGPD e da regulamentação da ANPD aplicável aos agentes de tratamento de pequeno porte.

6. INCIDENTES DE SEGURANÇA

Na hipótese de divulgação de dado confidencial interno da LAPB ou de incidente de segurança envolvendo dados pessoais, deve-se, primeiramente, verificar a potencial extensão dos danos e avaliar a necessidade de comunicação privada ou pública do evento, a reavaliação das medidas de segurança da informação e, quando cabível, a comunicação aos órgãos competentes. Tratando-se de incidente que possa acarretar risco ou dano relevante aos titulares, a LAPB comunicará a ANPD e os titulares afetados, nos termos do art. 48 da LGPD, em prazo razoável conforme regulamentação vigente.

7. PLANO DE CONTINUIDADE DE NEGÓCIOS

A LAPB possui Plano de Continuidade de Negócios de forma a garantir a linearidade das operações, prevendo recursos alternativos e estratégias de continuidade em casos de ocorrências inesperadas. Para tornar efetivo o Plano, todos os colaboradores da LAPB devem conhecer as suas práticas.

Uma vez identificada a interrupção de quaisquer recursos essenciais às atividades, os responsáveis pela área de TI devem ser imediatamente comunicados, a fim de adotar as providências cabíveis. Todos os colaboradores devem possuir os contatos telefônicos e de e-mail dos responsáveis pela área de TI, de modo a possibilitar a comunicação da contingência e

a solução mais rápida do problema ou, quando não for possível solução imediata, a adoção do fluxo alternativo mais viável.

Em caso de falha de fornecimento de energia, a LAPB possui nobreak para suportar o funcionamento do ambiente até o restabelecimento do fornecimento ou, em caso de longa interrupção, a utilização do servidor de contingência em nuvem associado aos notebooks permite a continuidade da mesma infraestrutura.

Em caso de evacuação, impedimento de entrada no escritório ou incêndio com danos à infraestrutura local, os recursos de TI e as aplicações podem ser acessados remotamente por meio de notebooks configurados especificamente para a LAPB e mantidos fora do escritório. Quando a infraestrutura de TI localizada no Data Center ou escritório é afetada e não pode ser utilizada, é possível dar continuidade à operação por meio do servidor de contingência em nuvem, que possui a mesma estrutura lógica do servidor em uso, com cópia atualizada das aplicações e arquivos da LAPB.

Links de internet de diferentes provedores garantem a redundância da rede e a alta disponibilidade entre sistemas e informações da LAPB, clientes e fornecedores. A disponibilidade dos links principal e redundante é monitorada 24/7, com alertas em casos de indisponibilidade. A rede cabeada interna e a distribuída via Wi-Fi são segregadas da rede de visitantes.

Backups de arquivos, estratégias e modelos de negócios são realizados diariamente para servidor de backup em nuvem, de maneira automática, com criptografia em todas as pontas da comunicação, e com plataforma para recuperação imediata de qualquer arquivo, quando necessário. Em complemento, realiza-se backup local em discos de armazenamento externo, com a restauração de informações testada periodicamente.

Serviços utilizados pela equipe de gestão, como “Bloomberg Professional” e “Broadcast”, podem ser acessados via dispositivos móveis ou notebooks previamente configurados, possuindo tais serviços seus próprios planos de contingência. O acesso à rede é controlado por login e senha única por usuário, com alterações periódicas, podendo ser disponibilizado acesso remoto via Virtual Private Network (VPN) para determinados usuários. O serviço de e-mail é garantido por parceiro terceirizado com suporte 24/7, serviço anti-spam, acesso via Web Mail e autenticação em dois fatores (Two Factor Authentication) para usuários administradores.

Todas as atividades dos colaboradores são compartilhadas de forma a evitar que a ausência de um colaborador impeça as atividades rotineiras do departamento ou da LAPB, sendo mantidos manuais dos sistemas e planilhas proprietárias. Em situações não previstas neste Plano, será feita a mobilização prioritária de recursos humanos e eventuais aquisições de software ou hardware para manutenção do fluxo de operações da Gestora.

8. POLÍTICA CIBERNÉTICA

A LAPB estabelece a presente Política Cibernética 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, em linha com o Código ANBIMA de Administração de Recursos de

Terceiros e com as melhores práticas de segurança da informação. Considerando a rápida evolução das práticas e soluções de cibersegurança, esta Política é atualizada e reavaliada periodicamente.

A Política Cibernética visa garantir a confidencialidade, a disponibilidade e a integridade das informações, sejam elas de terceiros ou da própria LAPB:

- Confidencialidade: garante que as informações tratadas pela LAPB sejam restritas a um grupo de usuários autorizados, impedindo a exposição de dados restritos e acessos não autorizados;
- Disponibilidade: garante a disponibilidade das informações aos usuários autorizados sempre que necessário;
- Integridade: garante a veracidade e a completude das informações, de forma que sejam íntegras e sem alterações não autorizadas.

Toda informação relacionada às operações da LAPB, gerada ou desenvolvida nas suas dependências, constitui ativo da instituição, essencial à condução dos negócios. 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 ou destruição não autorizadas — decorrentes de erros, fraudes, vandalismo, espionagem ou sabotagem — causam danos aos negócios da LAPB. É diretriz que toda informação de propriedade da LAPB seja protegida de riscos e ameaças que possam comprometer sua confidencialidade, integridade ou disponibilidade.

As diretrizes adotadas são:

a. As informações da LAPB, 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 indevidamente; senhas de acesso de estações de trabalho podem ser compartilhadas, quando necessário à continuidade da atividade, com o Diretor de Compliance e com colegas da mesma área, de forma a evitar a paralisação das atividades na ausência do usuário, devendo tal acesso ser pontual, parcimonioso e restrito à continuidade da atividade em curso;
c. O acesso a dados confidenciais é restrito a determinados usuários e bloqueado com base no login; acessos indevidos devem ser comunicados imediatamente ao Departamento de Compliance;
d. As responsabilidades quanto à Segurança da Informação devem ser amplamente divulgadas aos colaboradores, que devem compreendê-las e assegurá-las;
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 desempenho das funções na LAPB ou para outras situações formalmente permitidas;

g. O computador disponibilizado para o usuário é de propriedade da LAPB;

h. A concessão de acesso às informações e sistemas deve observar a regra do mínimo acesso necessário ao desempenho da função;

i. Apenas os equipamentos e softwares disponibilizados e/ou homologados pela LAPB podem ser instalados e conectados à rede;

j. Deve-se solicitar alteração de senha sempre que exista a possibilidade de ter sido comprometida;

k. Alterações nas diretrizes de segurança do computador são bloqueadas por senha, impossibilitando, por exemplo, a desativação do firewall;

l. Em caso de não funcionamento do software antivírus instalado em cada computador, é obrigação do usuário notificar prontamente a equipe de TI;

m. Equipamentos particulares que possam armazenar e/ou processar dados não devem ser usados para armazenar ou processar informações do negócio e só podem ser conectados à rede Wi-Fi de visitantes, exceto quando o Plano de Continuidade requeira e haja autorização explícita do Departamento de Compliance;

n. A senha da rede de internet principal da LAPB e das respectivas camadas de segurança é mantida de forma segura e não é compartilhada indistintamente; e

o. Toda violação ou desvio — tais como instalação (intencional ou não) de vírus, uso de software ilegal e tentativas de acesso a informações restritas — é investigada para a determinação das medidas necessárias e definição de possíveis sanções, visando à correção da falha ou à reestruturação de processos.

9. TREINAMENTO

O Departamento de Compliance repassa a todos os colaboradores as políticas e os manuais da LAPB, de forma que todos tenham conhecimento das melhores práticas e condutas. A LAPB incentiva que todos os colaboradores busquem atualização em suas respectivas atividades. Havendo necessidade, a LAPB promove treinamentos abertos aos colaboradores a respeito das melhores práticas de mercado.

10. FREQUÊNCIA DE ATUALIZAÇÃO DESTA POLÍTICA

Esta Política deverá ser atualizada, no mínimo, a cada 24 (vinte e quatro) meses. Poderá ser atualizada com frequência menor em razão de: (i) criação ou descontinuação de produtos; (ii) alterações na estrutura, nos processos ou nos sistemas de controles internos; (iii) nova lei, norma ou dispositivo regulatório/autorregulatório que enseje sua alteração; e (iv) contratação ou descontinuidade de prestador de serviços relevante.

Caberá ao Diretor de Compliance a atualização desta Política, bem como verificar se ela está sendo cumprida e incluir o resultado da verificação no Relatório Anual de Compliance.