

Manual de Compliance e Controles Internos

Endurant Consultoria de Investimentos Ltda.

CNPJ 66.047.508/0001-53



Ficha técnica

Título: Manual de Compliance e Controles Internos

Descrição: Este manual descreve como a Endurant garante que seu trabalho de consultoria de investimentos seja feito de forma ética, segura e em conformidade com as regras.

- Define as responsabilidades dos diretores e a forma como as decisões importantes devem ser aprovadas em conjunto.
- Explica como a empresa protege informações confidenciais e evita conflitos de interesse, garantindo que o cliente seja sempre prioridade.
- Detalha a forma como os sistemas automatizados são desenvolvidos, monitorados e revisados para que as recomendações sejam corretas e rastreáveis.
- Descreve as medidas de segurança da informação, como autenticação forte, criptografia e testes regulares de vulnerabilidade.
- Estabelece o prazo mínimo de cinco anos para guardar registros de recomendações, comunicações e incidentes, e indica que o relatório anual de conformidade deve ser apresentado até o fim de abril.

Autor: Compliance

Aprovado por: Diretoria

Vigência: 11/05/2026

Versão: 2026.1

Sumário

1. Objetivo, Âmbito e Documentos Relacionados	5
1.1. Mapa de documentos	5
2. Governança e Atribuições Regulatórias.....	5
3. Segregação de Atividades e Confidencialidade.....	6
4. Conflitos de Interesse	7
4.1. Remuneração por terceiros	7
4.2. Produtos de partes relacionadas	7
4.3. Operações pessoais	7
4.4. Indicação de prestadores	7
4.5. Escalonamento.....	7
5. Governança de Sistemas Automatizados.....	8
5.1. Responsabilidade	8
5.2. Disponibilidade para inspeção.....	8
5.3. Versionamento e rastreabilidade	8
5.4. Controles pré-entrega	8
5.5. Supervisão humana.....	9
5.6. Governança de mudanças	9
5.7. Modelos externos	9
6. Segurança da Informação e Testes Periódicos	9
6.1. Controles técnicos transversais.....	10
6.2. Testes periódicos.....	10
6.3. Resposta a incidentes.....	10
6.4. Aceite eletrônico	10
6.5. Fornecedores críticos	11
7. Registros, Retenção e Arquivamento.....	11
7.1. Registro das recomendações	11
7.2. Retenção mínima	11
7.3. Meio de arquivamento	12

8. Monitoramento, Relatório Anual e Revisão	12
8.1. Monitoramento contínuo	12
8.2. Relatório anual de Compliance	12
8.3. Revisão deste Manual	12
9. Vigência, Publicação e Adesão	12

1. Objetivo, Âmbito e Documentos Relacionados

Este Manual de Compliance e Controles Internos ("Manual") cumpre o art. 14, III, da Res. CVM nº 19/2021 ao descrever as regras, procedimentos e controles internos adotados pela **Endurant Consultoria de Investimentos Ltda.** (CNPJ nº 66.047.508/0001-53, "Endurant" ou "Sociedade") no exercício da atividade de consultoria de valores mobiliários.

O Manual consolida o regime interno de controles e remete às políticas dedicadas listadas abaixo sempre que o tema esteja nelas detalhado, evitando duplicação normativa. Aplica-se a todos os sócios, diretores, colaboradores e prestadores de serviços que atuem em nome da Endurant ou tenham acesso a seus sistemas, dados ou informações de clientes ("Colaboradores").

1.1. Mapa de documentos

- **Código de Ética e Conduta:** valores, princípios, normas de conduta, sigilo e classificação da informação, segurança no manuseio de equipamentos, comunicação pública, canal de violações, sanções, treinamento e composição da equipe;
- **Política de PLD/FTP e Manual de Procedimentos de PLD/FTP:** programa de PLD/FTP, KYC, KYE, KYP/KYS, AIR, indicadores de suspeição e comunicação ao COAF;
- **Política de Negociação de Valores Mobiliários:** regime de operações pessoais, *Restricted List*, *Watch List*, *Blackout Periods* e pré-autorização;
- **Política de Suitability:** metodologia de API, classificação de produtos, atualização do perfil e governança específica do *pipeline* automatizado de Suitability;
- **Política de Privacidade e Proteção de Dados:** LGPD, direitos dos titulares, Encarregado, incidentes que envolvam dados pessoais, transferência internacional e tratamento automatizado;
- **Termos de Uso da Plataforma:** relação contratual com o usuário e delimitação entre Plataforma e Serviços de Consultoria de Investimentos;
- **Contrato de Consultoria de Investimentos:** instrumento contratual com o cliente que rege a prestação dos Serviços de Consultoria de Investimentos, observados os deveres regulatórios e o regime *fee-based* descritos nas políticas internas.

2. Governança e Atribuições Regulatórias

A Endurant tem dois diretores estatutários, com atribuições não acumuláveis nos termos do art. 4º, § 4º, da Res. CVM nº 19/2021:

- **Lucas Fontenla — Diretor de Consultoria e Suitability** (art. 4º, II): atividade de consultoria de valores mobiliários e verificação da adequação do perfil, com responsabilidades detalhadas no cap. 11 da *Política de Suitability*.
- **Martim José — Diretor de Controles Internos, Compliance e PLD/FTP** ('Diretor de Compliance') (art. 4º, III): implementação e cumprimento das regras, procedimentos e controles internos descritos neste Manual e do programa de PLD/FTP, nos termos do cap. 4 da *Política de PLD/FTP*. Acumula a função de Encarregado pelo Tratamento de Dados Pessoais, conforme cap. 10 da *Política de Privacidade e Proteção de Dados* e regime da Res. CD/ANPD nº 2/2022 para agentes de pequeno porte.

A independência funcional do Compliance é reforçada por procedimentos formais: deliberação conjunta para decisões materiais, *cross-review* das operações pessoais do Diretor de Compliance pelo Diretor de Consultoria (Seção 4 da *Política de Negociação de Valores Mobiliários*) e registro escrito de cada deliberação relevante.

Decisões que envolvam alteração do modelo de negócios, introdução de novos produtos, contratação de prestadores críticos, alteração material de sistemas automatizados ou modificação das políticas internas exigem aprovação conjunta dos diretores.

3. Segregação de Atividades e Confidencialidade

A Endurant exerce exclusivamente consultoria de valores mobiliários. Não realiza gestão discricionária, distribuição, custódia, intermediação, execução de ordens ou recebimento de valores dos clientes. Todo movimento financeiro do cliente ocorre em conta de sua titularidade, em instituições autorizadas. Expansão do escopo depende de autorização prévia da CVM e de revisão deste Manual.

A classificação da informação em quatro níveis (Pública, Interna, Confidencial, Restrita), os deveres gerais de sigilo, as barreiras de informação, a vedação a *insider trading* e *tipping*, a confidencialidade extensiva a prestadores e as regras de manuseio de equipamentos aprovados estão consolidados nas Seções 5.3, 6 e 7 do *Código de Ética e Conduta*. Este Manual não os repete.

A barreira de informação temporária ou permanente, quando instituída pelo Diretor de Compliance, sujeita-se a registro em trilha de auditoria das pessoas com acesso e à vedação de negociação nos ativos relacionados, integrando a *Restricted List* prevista na Seção 10.3 da *Política de Negociação de Valores Mobiliários*.

4. Conflitos de Interesse

A Endurant identifica, administra e mitiga conflitos de interesse com prioridade integral ao interesse do cliente, em cumprimento ao art. 19, § 1º, III e IV, da Res. CVM nº 19/2021.

4.1. Remuneração por terceiros

A Sociedade adota modelo *fee-based*, descrito na Seção 5.6 do *Código de Ética e Conduta* e na Cláusula 4 dos *Termos de Uso da Plataforma*. Qualquer valor recebido de terceiros em razão da atividade de consultoria, sob qualquer rubrica, é integralmente repassado ao cliente titular, conforme orientação do Ofício-Circular nº 2/2026/CVM/SIN, com comunicação documentada ao cliente e registro pela Diretoria de Compliance.

4.2. Produtos de partes relacionadas

É vedada a recomendação de produtos geridos, administrados, estruturados, originados ou distribuídos por sócios, diretores, colaboradores ou partes a eles relacionadas, enquanto a Sociedade operar em escopo exclusivo de consultoria, sem as estruturas de segregação física do art. 21 da Res. CVM nº 19/2021.

4.3. Operações pessoais

O regime de operações pessoais dos Colaboradores está consolidado na *Política de Negociação de Valores Mobiliários*, incluindo pré-autorização, *Holding Period*, *Blackout Periods*, *Restricted List* e vedações específicas (*front running*, *insider trading*, *day trade*).

4.4. Indicação de prestadores

Aplica-se a Seção 5.6 do *Código de Ética e Conduta*: divulgação prévia de qualquer relação comercial com prestador indicado e vedação de remuneração, comissão ou benefício pela indicação, nos termos do art. 16, XII, da Res. CVM nº 19/2021.

4.5. Escalonamento

Conflito potencial ou consumado é comunicado pelo Colaborador à Diretoria de Compliance, que delibera, registra a ocorrência e adota a medida aplicável. Regras correlatas de conduta pessoal — presentes, atividades externas, anticorrupção — estão nas Seções 5.5 a 5.9 do *Código de Ética e Conduta*.

5. Governança de Sistemas Automatizados

A Endurant emprega sistemas automatizados, incluindo modelos de inteligência artificial e *pipelines* de processamento de dados, em todas as etapas da prestação do serviço, do *onboarding* à entrega de recomendações. Esta seção operacionaliza o art. 17 da Res. CVM nº 19/2021 e disciplina a governança aplicável ao sistema como um todo. A governança específica do *pipeline* de Suitability está nas Seções 4.1, 4.3 e 11 da *Política de Suitability*; o regime de tratamento automatizado e o direito de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado (LGPD, art. 20, na redação dada pela Lei nº 13.853/2019) estão nas Seções 9 e 13 da *Política de Privacidade e Proteção de Dados*.

5.1. Responsabilidade

Os sistemas podem entregar recomendações diretamente ao cliente, sem revisão individual prévia por consultor humano em cada interação, observados os controles desta seção. A responsabilidade regulatória pelas recomendações, automatizadas ou não, permanece com o Diretor de Consultoria.

5.2. Disponibilidade para inspeção

Em cumprimento ao art. 17, parágrafo único, da Res. CVM nº 19/2021, o código-fonte e os algoritmos utilizados são mantidos, em versão não compilada, disponíveis para inspeção da CVM na sede, inclusive mediante acesso às instâncias remotas dos repositórios a partir das instalações.

A Diretoria de Compliance retém, em repositório de código versionado e em acervo próprio: histórico completo de versões do código-fonte, *prompts* e parâmetros de modelos, *pipelines* de processamento e logs de operações críticas. O Diretor de Compliance produz qualquer documento solicitado pela CVM no prazo do respectivo ofício ou, na ausência de prazo, em até 10 dias úteis.

5.3. Versionamento e rastreabilidade

Cada versão de modelo, *prompt* e *pipeline* tem identificador único, data de vigência e responsável pelo *deploy*. Para cada interação com cliente, são registrados insumos recebidos, versão do modelo, versão do *prompt*, parâmetros de inferência e saída entregue, permitindo reconstruir o contexto decisório de qualquer recomendação. A saída entregue é preservada nos termos do Capítulo 7.

5.4. Controles pré-entrega

Antes da entrega ao cliente, toda recomendação automatizada passa por camada determinística sob a Diretoria de Consultoria, contendo, no mínimo: validação de aderência

ao perfil; aplicação de *blocklist* de instrumentos vedados, incluindo *Restricted List* e produtos incompatíveis; aplicação de limiares de confiança abaixo dos quais a recomendação é bloqueada ou escalada para revisão humana; e disponibilização de *circuit breaker* acionável por qualquer dos diretores para suspender em tempo real a entrega automatizada. Recomendação que não atenda integralmente aos controles não é entregue.

5.5. Supervisão humana

Enquanto o volume de recomendações automatizadas entregues for inferior a 50 por trimestre, a revisão pelo Diretor de Consultoria é integral. Acima desse limiar, a revisão passa a ser amostral, com critérios e tamanho da amostra calibrados com base nos achados das revisões anteriores e registrados a cada ciclo. Falha material identificada em revisão, reclamação de cliente cuja procedência seja confirmada na análise inicial pela Diretoria de Compliance ou alerta operacional acionam o *circuit breaker* da Seção 5.4. Em qualquer dessas hipóteses, é desencadeada revisão direcionada do domínio afetado, com retorno ao regime manual naquele domínio até a correção.

5.6. Governança de mudanças

Alteração relevante — troca de modelo base ou de provedor, alteração do *prompt* de sistema, alteração de parâmetros de inferência, nova integração externa, mudança de *pipeline* — exige aprovação prévia do Diretor de Compliance e é registrada no histórico de versões. Demais alterações são registradas pelo responsável pelo *deploy*. Incidentes de IA com impacto material, como alucinação, vazamento via *prompt* ou violação de *guardrails*, acionam o protocolo de incidentes do Capítulo 6.

5.7. Modelos externos

Modelo externo é utilizado apenas após avaliação prévia, pelo Diretor de Compliance, das políticas de privacidade, retenção e uso de dados do fornecedor, incluindo o regime de transferência internacional nos termos do Capítulo V da LGPD e da Res. CD/ANPD nº 19/2024. O contrato com o fornecedor prevê, no mínimo, vedação de uso dos dados para treinamento, prazo definido de retenção e dever de sigilo. Antes do envio, dados pessoais são minimizados ao estritamente necessário; dados sensíveis (art. 5º, II, da LGPD) não são enviados sem base legal específica.

6. Segurança da Informação e Testes Periódicos

Esta seção operacionaliza o art. 19, § 1º, VI, da Res. CVM nº 19/2021. Os controles relativos a dados pessoais — bases legais, direitos dos titulares, regime do Encarregado e notificação à ANPD — estão nas Seções 8 e 11 da *Política de Privacidade e Proteção de Dados*.

6.1. Controles técnicos transversais

- Autenticação multifator obrigatória para acesso a sistemas com dados de clientes;
- *Least privilege*: cada usuário acessa apenas o necessário à sua função, com revisão formal de permissões a cada seis meses e imediatamente após desligamento;
- Dados em trânsito: TLS 1.2 ou superior. Dados em repouso: AES-256;
- *Patches* de segurança críticos aplicados em até 72 horas após disponibilização;
- Logs de acesso, autenticação e operações críticas retidos por no mínimo cinco anos, com alertas para acessos anômalos e revisão amostral mensal pela Diretoria de Compliance.

6.2. Testes periódicos

Em cumprimento ao art. 19, § 1º, VI, da Res. CVM nº 19/2021, com calibragem proporcional ao porte da Sociedade:

- Varredura anual de vulnerabilidades em dependências de software, com ferramentas automatizadas adequadas ao *stack* utilizado;
- Teste funcional dos controles após mudança material de infraestrutura;
- Revisão anual da matriz de controles internos pela Diretoria de Compliance.

Resultados e planos de remediação são documentados e arquivados.

6.3. Resposta a incidentes

- **Deteção** por alerta automatizado ou comunicação de Colaborador.
- **Contenção** com isolamento do sistema afetado e preservação de evidências.
- **Avaliação** da gravidade e do impacto.
- **Notificação** à CVM quando o incidente afetar o serviço regulado e à ANPD quando envolver dados pessoais com risco relevante, nos termos da Seção 11 da *Política de Privacidade e Proteção de Dados*.
- **Remediação** com correção da vulnerabilidade e revisão dos controles.
- **Documentação** completa do incidente e das medidas, retida pelo prazo do Capítulo 7.

6.4. Aceite eletrônico

Para a validade jurídica dos aceites eletrônicos (art. 10, § 2º, da MP 2.200-2/2001 c/c o Código Civil), o sistema captura e armazena, por documento aceite: autenticação multifator do usuário (e-mail e telefone validados por OTP); IP, *user agent*, tipo de dispositivo e geolocalização aproximada; carimbo de tempo criptográfico; hash SHA-256 da versão exata do documento apresentada ao usuário; trilha de auditoria imutável. Alteração substantiva do documento exige reaceite.

6.5. Fornecedores críticos

Provedor de *cloud*, provedor de LLM e plataforma de mensageria mantêm certificações reconhecidas (SOC 2 Tipo II, ISO 27001 ou equivalente), são avaliados anualmente quanto ao estado das certificações e quanto a incidentes públicos, e operam sob contrato com cláusulas de segurança e notificação. A diligência sobre fornecedores com acesso a dados de clientes ou ao *pipeline* de IA observa adicionalmente o regime KYP/KYS da Seção 8 do *Manual de Procedimentos de PLD/FTP*.

7. Registros, Retenção e Arquivamento

Em cumprimento aos arts. 22 e 23 da Res. CVM nº 19/2021:

7.1. Registro das recomendações

Orientações, recomendações e aconselhamentos são registrados de modo a permitir reprodução integral, garantir proteção contra adulteração e preservar trilha de auditoria.

7.2. Retenção mínima

São retidos por no mínimo cinco anos, contados da geração ou do encerramento da relação com o cliente, ou por prazo superior determinado pela CVM:

- Análises, relatórios e recomendações entregues ao cliente;
- Documentação de Suitability e KYC, conforme cap. 12 da *Política de Suitability* e cap. 16 da *Política de PLD/FTP*;
- Comunicações relacionadas à prestação do serviço, internas e externas;
- Histórico de versões dos sistemas automatizados (Capítulo 5) e registros de supervisão humana;
- Registros de conflitos, denúncias, incidentes e deliberações da Diretoria de Compliance;
- Registros do canal de comunicação de violações (Seção 10 do *Código de Ética e Conduta*).

Prazos específicos mais extensos previstos em política dedicada prevalecem; a retenção de 10 anos para o processo de comunicação ao COAF (Seção 6 do *Manual de Procedimentos de PLD/FTP*) é exemplo desse padrão superior.

7.3. Meio de arquivamento

Admite-se imagem digitalizada em substituição ao original, nos termos do art. 23, § 1º. O acervo é armazenado em sistemas aprovados pela Diretoria de Compliance, com controle de acesso, criptografia e cópia de contingência.

8. Monitoramento, Relatório Anual e Revisão

8.1. Monitoramento contínuo

A Diretoria de Compliance monitora, ao longo do ano, o cumprimento deste Manual e das demais políticas, com base em revisão amostral de logs e dos registros de supervisão humana do Capítulo 5; verificação do atendimento ao percentual mínimo de consultores certificados (Seção 9.5 do *Código de Ética e Conduta*); acompanhamento do programa de treinamento (Seção 9.4 do *Código de Ética e Conduta*); registro de conflitos, incidentes e denúncias.

8.2. Relatório anual de Compliance

Até o último dia útil de abril de cada ano, o Diretor de Compliance apresenta à alta administração relatório contendo, no mínimo: resumo das atividades de monitoramento e seus achados; incidentes, conflitos e denúncias registrados no período e seu desfecho; resultados dos testes periódicos do Capítulo 6; mudanças relevantes nos sistemas automatizados; e plano de ação para o ciclo seguinte. O relatório anual de PLD/FTP (cap. 5 da *Política de PLD/FTP* e cap. 9 do *Manual de Procedimentos de PLD/FTP*) e o relatório anual de Suitability (Seção 11.4 da *Política de Suitability*) são apresentados em separado e podem ser deliberados na mesma ocasião.

8.3. Revisão deste Manual

A revisão ocorre ao menos anualmente, ou diante de alteração regulatória relevante, mudança material no modelo de negócios, introdução ou descontinuação de sistemas automatizados ou identificação de lacuna de controle. Cada versão é aprovada conjuntamente pelos diretores, formalmente versionada e comunicada aos Colaboradores.

9. Vigência, Publicação e Adesão

Este Manual entra em vigor na data de sua aprovação conjunta pelos diretores da Endurant e permanece vigente até sua substituição ou atualização formal. A revisão observa o regime da Seção 8.3.

A versão vigente é publicada em endurant.com.br/regulatorio, em cumprimento ao art. 14, *caput* e III, da Res. CVM nº 19/2021.

A adesão dos Colaboradores ao regime descrito neste Manual é formalizada conjuntamente com a adesão ao Código de Ética e Conduta, por meio do Termo de Adesão constante do Anexo I do referido Código, ficando o presente Manual incorporado ao referido Termo.

Em caso de dúvidas, contatar a Diretoria de Compliance em compliance@endurant.com.br.