

LAIC Asset Management

Política de Segurança Cibernética e Continuidade de Negócios

Documento	Política de Segurança Cibernética e Continuidade de Negócios
Versão	2.0
Data-base regulatória	27/07/2026
Responsável pela manutenção	Diretoria de Compliance, Risco e Controles Internos
Aprovação	Diretoria da LAIC, conforme registro interno e ata ou termo equivalente
Abrangência	LAIC Asset Management, administradores, sócios, colaboradores, prestadores relevantes e terceiros vinculados

1. Base regulatória e princípios de interpretação

Esta política deve ser lida em conjunto com as demais políticas internas da LAIC, o contrato social, os regulamentos dos fundos, os contratos com prestadores de serviços essenciais e terceiros contratados, e as normas legais, regulatórias e autorregulatórias aplicáveis.

- Resolução CVM nº 21/2021, texto consolidado, que regula o exercício profissional de administração de carteiras de valores mobiliários e substitui o regime da antiga Instrução CVM nº 558/2015.
- Resolução CVM nº 175/2022, texto consolidado, e seus anexos normativos aplicáveis aos fundos de investimento, especialmente regras de constituição, funcionamento, divulgação de informações, classes, subclasses, prestadores essenciais e responsabilidades do gestor.
- Anexo Normativo II da Resolução CVM nº 175/2022, aplicável aos Fundos de Investimento em Direitos Creditórios, inclusive quanto a diligência, lastro, elegibilidade, documentação, registro, custódia, cobrança, liquidação e monitoramento de direitos creditórios.
- Resolução CVM nº 50/2021, com alterações posteriores, inclusive Resolução CVM nº 245/2026, para prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa.
- Código ANBIMA de Administração e Gestão de Recursos de Terceiros, Regras e Procedimentos de Administração e Gestão de Recursos de Terceiros, Regras e Procedimentos de Deveres Básicos e Regras e Procedimentos de Certificação, conforme versões vigentes na data-base desta política.
- Demais normas CVM, ANBIMA, legislação societária, Lei nº 9.613/1998, Lei Geral de Proteção de Dados e regras aplicáveis à atividade efetivamente exercida pela LAIC.

2. Objetivo e escopo

Esta Política estabelece diretrizes de segurança cibernética, segurança da informação, proteção de dados, uso aceitável de recursos tecnológicos e continuidade de negócios da LAIC.

A política abrange sistemas próprios, plataformas de administradores, custodiantes, bancos, corretoras, registradoras, provedores de nuvem, e-mails, arquivos, dispositivos, redes, aplicativos de mensagem, bases de investidores e documentos de fundos.

3. Princípios de segurança

- Confidencialidade, garantindo que informações sejam acessadas apenas por pessoas autorizadas.
- Integridade, preservando exatidão, completude e rastreabilidade dos dados e documentos.
- Disponibilidade, assegurando acesso tempestivo a sistemas e documentos críticos.
- Menor privilégio, concedendo acessos apenas na medida necessária à função.
- Autenticação forte, especialmente em e-mail, sistemas financeiros, nuvem, bancos e plataformas de prestadores.
- Registro e auditoria, mantendo trilha de acessos, alterações, conciliações e incidentes relevantes.

4. Classificação da informação e acessos

As informações devem ser classificadas, no mínimo, como públicas, internas, confidenciais ou restritas. Posições de fundos, dados de investidores, documentos de crédito, informações de cedentes e sacados, modelos proprietários, senhas, tokens e estratégias são considerados restritos ou confidenciais.

1. Conceder acesso mediante solicitação formal ou registro equivalente.
2. Revisar acessos periodicamente e em caso de mudança de função ou desligamento.
3. Revogar imediatamente acessos de colaboradores desligados ou prestadores encerrados.
4. Proibir compartilhamento de senhas, tokens, certificados digitais e credenciais pessoais.
5. Registrar exceções e acessos emergenciais.

5. Uso aceitável e proteção de dados

- Dados e documentos da LAIC devem ser armazenados em ambientes corporativos autorizados, evitando cópias locais desnecessárias.
- Dispositivos pessoais somente podem ser usados quando autorizados e protegidos por senha, biometria, criptografia e bloqueio automático.
- E-mails e mensagens com anexos sensíveis devem ser enviados apenas a destinatários validados e com cuidado redobrado em listas de distribuição.
- Dados pessoais devem ser tratados conforme finalidade legítima, necessidade, segurança, retenção adequada e direitos dos titulares.
- Arquivos de borderô, carteira, cadastro, conciliação, contratos e documentos de crédito devem ter controle de versão e backup.

6. Prestadores de tecnologia e nuvem

Antes da contratação de provedores críticos de tecnologia, nuvem, armazenamento, comunicação, segurança ou processamento de dados, a LAIC deve avaliar risco, reputação, segurança, continuidade, confidencialidade, localização de dados, subcontratação, suporte, reversibilidade e reporte de incidentes.

- Contratos devem prever confidencialidade, proteção de dados, níveis mínimos de serviço, backup, recuperação, comunicação de incidentes e rescisão segura.
- Prestadores críticos devem ser reavaliados periodicamente ou após incidente relevante.
- A LAIC deve manter inventário de sistemas e prestadores críticos.

7. Incidentes cibernéticos

Incidentes incluem perda, vazamento, alteração indevida, indisponibilidade, acesso não autorizado, phishing, ransomware, fraude, envio errado de informação, uso indevido de credenciais e falhas relevantes de prestadores.

6. Conter o incidente e preservar evidências.
7. Classificar impacto sobre confidencialidade, integridade, disponibilidade, fundos, clientes e dados pessoais.
8. Comunicar Compliance, Diretoria e responsáveis técnicos.
9. Avaliar obrigação de comunicação a investidores, administradores fiduciários, CVM, ANBIMA, ANPD ou demais autoridades.
10. Corrigir vulnerabilidade, revisar controles e registrar relatório pós-incidente.

8. Continuidade de negócios

A LAIC deve manter plano de continuidade para indisponibilidade de sistemas, pessoas-chave, escritório, internet, bancos, administradores, custodiantes e fornecedores críticos.

- Definir processos críticos, responsáveis, substitutos, contatos de emergência e prioridades de recuperação.
- Manter backups e rotinas alternativas para acesso a documentos essenciais.
- Testar periodicamente o plano ou, no mínimo, revisar sua viabilidade operacional.
- Documentar indisponibilidades e decisões tomadas durante contingência.

Disposições finais e aprovação

Esta política entra em vigor na data de sua aprovação formal e deverá ser revisada, no mínimo, anualmente ou sempre que houver alteração relevante na legislação, na regulação, nas regras ANBIMA, na estrutura da LAIC, nos produtos sob gestão ou em seus processos operacionais.

A versão aprovada deve permanecer arquivada em repositório interno controlado e, quando aplicável, disponibilizada no site institucional da LAIC ou encaminhada a administradores fiduciários, distribuidores, auditores, reguladores e autorreguladores.

Elaboração	Revisão	Aprovação
Nome, cargo e data	Nome, cargo e data	Nome, cargo e data