GEWIN CAPITAL GESTORA DE RECURSOS LTDA.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

Gestão de Recursos de Terceiros

Versão 1.0

Classificação: Pública

SUMÁRIO

1. OBJETIVO E APLICAÇÃO

Esta Política de Segurança da Informação e Cibernética (a **"Política"**) estabelece os princípios, diretrizes e responsabilidades que orientam a proteção das informações e dos recursos tecnológicos da **GEWIN Capital Gestora de Recursos Ltda.**, inscrita no CNPJ/MF sob o nº 59.272.985/0001-57 (a **"Gestora"**), em todo o ciclo de vida da informação — da coleta ao descarte —, independentemente do meio ou do local em que esteja armazenada ou processada, inclusive em ambientes de nuvem e de prestadores de serviço.

Sujeitam-se a esta Política os sócios, administradores, empregados, estagiários e prestadores de serviço que acessem informações, sistemas ou o ambiente tecnológico da Gestora (os "Colaboradores e usuários"). Suas disposições complementam a Política de Controles Internos e Compliance e a Política de Seleção e Monitoramento de Prestadores de Serviço.

2. PRINCÍPIOS

A informação é um ativo essencial à atividade da Gestora. Sua proteção apoia-se em três atributos fundamentais, preservados ao longo de todo o ciclo de vida da informação:

- **Confidencialidade —** a informação é acessível apenas a quem esteja devidamente autorizado;
- **Integridade —** a informação é mantida exata e completa, preservados os métodos de seu processamento;
- **Disponibilidade —** a informação está acessível, de forma íntegra, sempre que necessária a quem dela dependa.

A escolha dos mecanismos de proteção pondera, de forma equilibrada, o risco envolvido, a tecnologia disponível e o custo, em medida compatível com o porte, a natureza e a complexidade das atividades da Gestora.

3. REFERÊNCIAS NORMATIVAS

Esta Política observa, no que aplicável à atividade de gestão de recursos de terceiros, o seguinte arcabouço, bem como suas alterações posteriores:

- **Resolução CVM nº 21/2021**, quanto aos controles e à segurança no exercício da administração de carteiras;
- **Resolução CVM nº 35/2021**, no que tange a requisitos de segurança aplicáveis a sistemas e plataformas;
- **Lei nº 13.709/2018 (LGPD)** e regulamentação da Autoridade Nacional de Proteção de Dados (ANPD);
- **Código ANBIMA de Administração e Gestão de Recursos de Terceiros (Código AGRT)**, vigente desde 02/01/2025; e

- referências de mercado em segurança da informação, com inspiração nos requisitos da família **ABNT NBR ISO/IEC 27001 e 27701**.

4. PAPÉIS E RESPONSABILIDADES

Responsável	Atribuições principais
Diretoria	Patrocina o tema, aprova esta Política, provê recursos e demonstra comprometimento com a melhoria contínua da segurança da informação.
Diretor de Compliance e Risco	Responde pela governança de segurança da informação na Gestora, coordena a implementação desta Política, avalia riscos e autoriza exceções formalizadas.
Colaboradores e usuários	Cumprem as diretrizes, zelam pela proteção das informações e dos equipamentos sob sua guarda e comunicam de imediato incidentes e fragilidades.
Prestadores de serviço	Observam os requisitos do item 8 e comunicam incidentes que envolvam informações da Gestora ou dos Fundos.

Responsável pela governança de SI: **Mariana Girade** — Contato: **mariana.girade@gewincapital.com.br**

5. PILARES DE PROTEÇÃO

A proteção das informações organiza-se em torno dos pilares descritos a seguir, implementados por normas e procedimentos internos complementares.

5.1. Gestão de Ativos e Classificação da Informação

Os ativos relevantes — tecnológicos ou não — são identificados e mantêm um responsável. As informações são classificadas conforme seu grau de confidencialidade, recebendo proteção proporcional em todas as fases do ciclo de vida (geração, manuseio, armazenamento, transporte e descarte). O descarte de informações observa procedimentos seguros de exclusão, tanto em meio digital quanto físico.

5.2. Gestão de Acessos

O acesso às informações e sistemas rege-se pelo princípio do menor privilégio: cada usuário recebe apenas os acessos imprescindíveis às suas atribuições. A identificação é única, pessoal e intransferível, e a senha, de uso exclusivo, não pode ser compartilhada. As concessões, revisões e revogações de acesso são formalizadas e rastreáveis, com revogação imediata no desligamento ou ao término da necessidade. A segregação de funções permeia os processos críticos, evitando que uma mesma pessoa concentre execução e controle.

5.3. Proteção do Ambiente Tecnológico

A Gestora adota controles destinados a prevenir, detectar e responder a ameaças cibernéticas, contemplando, na medida aplicável à sua estrutura: autenticação robusta; criptografia de dados em repouso e em trânsito; proteção contra códigos maliciosos; gestão de correções de segurança (patches) e configuração segura (hardening); realização periódica de varreduras de vulnerabilidade; e registro de logs e trilhas de auditoria que permitam identificar quem acessou, quando, o quê e como, protegidos contra alteração.

5.4. Cópias de Segurança e Continuidade

São mantidas cópias de segurança (backups) periódicas das informações relevantes, de modo a minimizar perdas diante de incidentes, com testes que verifiquem a capacidade de recuperação. A Gestora mantém medidas de continuidade que lhe permitam preservar suas atividades essenciais e a integridade das informações dos Fundos em cenários de indisponibilidade.

5.5. Segurança Física

O acesso físico aos ambientes que abrigam informações ou ativos críticos é controlado conforme a criticidade das informações neles tratadas.

5.6. Uso Aceitável e Propriedade da Informação

Os recursos de tecnologia são utilizados exclusivamente para as finalidades aprovadas pela Gestora e estão sujeitos a monitoração, rastreabilidade e auditoria, nos limites da lei. As informações produzidas no exercício das atividades, bem como a propriedade intelectual delas decorrente, pertencem à Gestora e não podem ser utilizadas para fins particulares nem repassadas a terceiros sem autorização expressa.

6. PROTEÇÃO DE DADOS PESSOAIS

O tratamento de dados pessoais observa a LGPD e os princípios de privacidade desde a concepção (privacy by design), limitando-se às finalidades informadas e à hipótese legal aplicável, com minimização da coleta. Incidentes que possam acarretar risco ou dano relevante aos titulares são tratados conforme o item 7, com comunicação à ANPD e aos titulares quando a regulação assim exigir.

7. GESTÃO DE INCIDENTES E RESILIÊNCIA CIBERNÉTICA

A Gestora mantém processo de gestão de incidentes que lhe permita antecipar, resistir, responder, recuperar-se e adaptar-se a eventos adversos. Considera-se incidente qualquer evento, confirmado ou sob suspeita, que afete a confidencialidade, a integridade, a disponibilidade ou a autenticidade de informações e sistemas, ou que represente violação a esta Política.

Identificado um incidente, ele é registrado, avaliado quanto à causa e ao impacto, classificado por relevância e tratado de forma coordenada entre as áreas envolvidas e a Diretoria. Os

incidentes relevantes ensejam comunicação tempestiva aos reguladores, aos titulares de dados e a demais partes interessadas, quando aplicável. O quadro a seguir orienta a classificação:

Nível	Caracterização	Reporte interno
Crítico	Potencial de interromper operações essenciais por período prolongado, dano financeiro significativo ou comprometimento massivo de dados.	Imediato
Alto	Degradação relevante de serviços críticos, com potencial impacto reputacional ou comprometimento pontual de dados sensíveis.	Até 6 horas
Médio	Impacto mensurável, porém limitado; evento que, sem tratamento, pode evoluir para nível superior.	Até 24 horas
Baixo	Evento de impacto reduzido, tratável na rotina operacional.	Conforme rotina

As vulnerabilidades identificadas — sistêmicas ou de processo — são endereçadas com priorização conforme o risco e o impacto ao negócio, observadas as responsabilidades de cada área.

8. SEGURANÇA NO RELACIONAMENTO COM TERCEIROS

Os riscos de segurança da informação decorrentes da contratação de prestadores de serviço e parceiros são identificados, avaliados, classificados, mitigados e monitorados conforme a criticidade do serviço e os requisitos regulatórios e contratuais, de forma integrada à Política de Seleção e Monitoramento de Prestadores de Serviço. Aplicam-se, em especial, aos terceiros que acessem o ambiente da Gestora ou tratem informações dos Fundos ou de seus cotistas:

- acesso individualizado, mediante credenciais próprias e limitado ao estritamente necessário, com revogação ao término da relação;
- compromisso contratual de confidencialidade e de aderência à legislação de segurança e proteção de dados;
- comunicação imediata à Gestora de incidentes que envolvam suas informações;
- manutenção de controles de proteção compatíveis com a criticidade do serviço, incluindo, quando cabível, backups, criptografia e trilhas de auditoria; e
- apresentação, quando aplicável e a critério da Gestora, de certificações ou relatórios de auditoria independente que evidenciem a adequação de seus controles.

A contratação de serviços de nuvem ou de processamento de dados no exterior observa os requisitos regulatórios aplicáveis. A subcontratação de serviços relevantes deve ser previamente comunicada à Gestora.

9. CONSCIENTIZAÇÃO E CULTURA

A Gestora promove cultura de segurança da informação por meio de ações periódicas de capacitação e conscientização — no mínimo anuais e por ocasião do ingresso de novos Colaboradores —, abrangendo temas como proteção de dados, uso seguro de recursos, reconhecimento de tentativas de fraude (phishing e engenharia social) e procedimentos de resposta a incidentes. Não se admite a alegação de desconhecimento desta Política para justificar o seu descumprimento.

Periodicamente, os Colaboradores aderem formalmente a termo de comprometimento com as diretrizes de segurança da informação. A Gestora informa, ainda, seus clientes e usuários sobre precauções de segurança pertinentes ao uso de seus produtos e serviços.

10. DESCUMPRIMENTO

O descumprimento desta Política enseja a abertura de procedimento para apuração e, conforme a gravidade, a aplicação das medidas cabíveis — de orientação e advertência até o desligamento ou a rescisão contratual —, sem prejuízo das sanções legais e regulatórias aplicáveis. Acessos ou permissões em desacordo com estas diretrizes somente são admitidos em caráter excepcional, mediante autorização formal do Diretor de Compliance e Risco.

11. VIGÊNCIA E REVISÃO

Esta Política entra em vigor na data de sua aprovação pela Diretoria e é revisada, no mínimo, anualmente, ou antes, sempre que mudanças regulatórias, tecnológicas ou de negócio assim exigirem. Suas diretrizes são amplamente divulgadas aos Colaboradores e disponibilizadas conforme sua classificação.

12. DISPOSIÇÕES FINAIS

Casos omissos e dúvidas são resolvidos pelo Diretor de Compliance e Risco da Gestora. Esta Política é complementada por normas e procedimentos internos específicos de segurança da informação. Contato: **mariana.girade@gewincapital.com.br.**

13. HISTÓRICO DE REVISÕES E APROVAÇÃO

Versão	Data	Descrição	Elaboração	Aprovação
1.0	[mês/ano]	Elaboração e publicação inicial	Compliance	Diretoria