POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

THERAS CAPITAL GESTÃO DE INVESTIMENTOS LTDA
CNPJ nº 62.051.574/0001-46

Data de Elaboração: 01 de setembro de 2025
Data da Última Atualização: 01 de setembro de 2025

Conteúdo

1. Finalidade

A presente Política de Segurança Cibernética e da Informação ("**Política**") tem por finalidade estabelecer os princípios, diretrizes, procedimentos e responsabilidades destinados a proteger os ativos tecnológicos, os dados pessoais e corporativos, os registros operacionais e qualquer informação crítica pertencente ou sob a guarda da **Theras Capital Gestão de Investimentos Ltda.** ("**Theras Capital**" ou "**Gestora**"). Busca-se assegurar, de forma contínua e sistemática, a **confidencialidade, integridade, disponibilidade e autenticidade** das informações, prevenindo incidentes que possam comprometer a operação da Gestora, a proteção dos cotistas, o cumprimento regulatório ou a continuidade dos negócios.

Esta Política foi elaborada em conformidade com a **Resolução CVM nº 21/2021**, que exige controles internos compatíveis com o porte e complexidade do administrador de carteiras, e com o **Código ANBIMA de Administração e Gestão de Recursos de Terceiros – AGRT**, em sua versão atualizada, que determina padrões mínimos de segurança da informação, cibersegurança, continuidade operacional, governança tecnológica, diligência de terceiros e monitoramento permanente. Integram-se, ainda, os requisitos previstos na **Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018)**, que disciplina o tratamento de dados pessoais e estabelece obrigações relativas à segurança e prevenção a incidentes.

Por meio desta Política, a Theras Capital reafirma seu compromisso institucional com a segurança tecnológica, com a governança de riscos cibernéticos e com a adoção de controles proporcionais ao seu modelo de negócios, assegurando que suas atividades sejam conduzidas em ambiente seguro, competente e resiliente.

2. Abrangência

Esta Política aplica-se integralmente a todos os **sócios, diretores, colaboradores, estagiários e prestadores de serviços relevantes** que, de forma permanente ou eventual, tenham acesso aos sistemas, dados, informações ou infraestrutura da Theras Capital. Incluem-se nesta abrangência, ainda, **terceiros críticos**, tais como provedores de computação em nuvem, empresas de tecnologia, consultorias de segurança, administradores fiduciários, custodiantes, contadores e quaisquer outros que tratem informações em nome da Gestora.

As diretrizes desta Política aplicam-se ao ambiente físico da Gestora, ao ambiente virtual, aos servidores em nuvem, aos dispositivos corporativos, aos sistemas licenciados, às plataformas internas e externas de gestão, aos e-mails e aos meios remotos de trabalho, incluindo **home office** e **escritórios de contingência**, assegurando alinhamento completo com o **Plano de Continuidade de Negócios** ("PCN").

3. Programa de Segurança Cibernética

A Theras Capital adota um **Programa Estruturado de Segurança Cibernética**, integrado às suas políticas internas, ao PCN e aos controles de riscos e compliance. Esse programa compreende o conjunto de normas e procedimentos destinados a identificar, prevenir, mitigar, monitorar e responder a ameaças cibernéticas. Entre os riscos considerados incluem-se, mas não se limitam a:

- **Malware** (vírus, trojans, spyware, ransomware);
- **Engenharia social** (phishing, spear phishing, pharming, vishing, smishing);
- **Ataques de DDoS e botnets**, que possam impedir o acesso aos sistemas;
- **Ameaças persistentes avançadas (APT)**, conduzidas por agentes sofisticados;
- **Ataques a credenciais**, como credential stuffing e brute force;
- **Tentativas de exploração de vulnerabilidades** em softwares,

servidores ou aplicações;
• **Acesso indevido** por falhas humanas ou violações de segurança.

O Programa tem três pilares básicos:
(i) **Prevenção**, com foco em controles robustos;
(ii) **Monitoramento**, com vigilância permanente de atividades suspeitas;
(iii) **Resposta a incidentes**, com procedimentos previamente definidos para isolar, mitigar e reportar eventos.

4. Ações de Prevenção e Medidas de Proteção

A Theras Capital adota ações preventivas orientadas às melhores práticas de mercado, considerando princípios de governança, proporcionalidade e defesa em profundidade. Entre os controles utilizados incluem-se:

A Gestora adota sistemas robustos de **identificação, autenticação e autorização**, com credenciais individuais, senhas complexas e prazos de renovação compatíveis com o risco do ativo acessado. Em sistemas críticos, aplica-se **autenticação multifator**, complementada por regras de segregação de credenciais entre serviços e proibição de compartilhamento de senhas.

Os acessos são concedidos de acordo com o princípio do **menor privilégio**, limitando-se ao estritamente necessário para o desempenho das funções. Tais acessos podem ser modificados, ampliados ou revogados de forma imediata sempre que houver mudança funcional, desligamento ou identificação de risco. Todos os eventos de login, falhas de autenticação, alterações de senha e tentativas de acesso indevido são **auditáveis e rastreáveis**.

A inclusão de novos sistemas, softwares ou dispositivos em produção segue procedimento formal com avaliação de segurança, configurando-se padrões mínimos de proteção e bloqueios contra

instalação de softwares não autorizados (**whitelisting**). O acesso físico às áreas críticas é restrito por controles apropriados.

A contratação de terceiros segue processo de **due diligence**, que inclui verificação de requisitos de confidencialidade, segurança, disponibilidade, responsabilidade pelo tratamento de dados pessoais e mecanismos próprios de cibersegurança. Tais contratos devem conter **cláusulas específicas de proteção de dados**, controles mínimos, obrigações de reporte e dever de confidencialidade.

A infraestrutura de rede é protegida por **firewalls**, filtros de pacotes, sistemas antivírus atualizados, mecanismos antimalware, segregação de ambientes e controles de compartimentação. A transmissão de informações confidenciais, por meios eletrônicos, é realizada apenas por canais seguros.

Os bancos de dados, arquivos corporativos e documentos críticos são armazenados em **servidores em nuvem** com mecanismos de replicação e **backups periódicos**. A política de backups é monitorada diariamente, assegurando integridade e recuperação rápida em caso de falhas.

5. Monitoramento, Detecção e Resposta a Incidentes

Em conformidade com as práticas recomendadas pela ANBIMA, a Theras Capital mantém mecanismos contínuos de **monitoramento**, capazes de detectar, registrar e reportar atividades suspeitas ou incidentes de segurança. Esse monitoramento inclui:

inventário atualizado de hardware e software, com controle de versões e verificação frequente para identificação de elementos desconhecidos;

atualizações permanentes de sistemas operacionais e aplicações, com aplicação tempestiva de **patches de segurança**;

verificação diária das rotinas de backup e testes periódicos de restauração;

realização de **análises de vulnerabilidades** com periodicidade compatível com o risco e sempre que houver mudança relevante na infraestrutura tecnológica;

observação de alertas emitidos por provedores de nuvem, fornecedores críticos, CERT.br e demais órgãos relevantes.

Em caso de **incidente de segurança cibernética**, o Diretor de Compliance deverá ser imediatamente informado. A Gestora seguirá procedimentos formais de resposta, incluindo: isolamento do incidente, investigação preliminar, preservação de evidências, mitigação de riscos, comunicação a terceiros afetados e, quando aplicável, **comunicação à ANBIMA, CVM, administradores fiduciários, titulares de dados (conforme LGPD)** e demais envolvidos.

A gravidade, o impacto operacional e a necessidade de acionamento do **Plano de Continuidade de Negócios** serão avaliados caso a caso. Incidentes com potencial de comprometer dados pessoais seguirão os requisitos legais previstos na LGPD quanto a comunicação e mitigação.

6. Vigência, Treinamentos e Revisão da Política

Esta Política entra em vigor na data de sua publicação e deverá ser revisada ao menos **uma vez por ano**, ou sempre que houver alterações relevantes nas exigências regulatórias, nas melhores práticas de mercado, na infraestrutura tecnológica da Gestora ou nos riscos identificados.

A Theras Capital realizará **treinamentos periódicos**, com periodicidade mínima anual, abordando segurança da informação, boas práticas de cibersegurança, prevenção a engenharia social, uso adequado dos

recursos tecnológicos, tratamento de dados pessoais e procedimentos aplicáveis em situações de incidente.

Todos os colaboradores devem assinar **Termo de Ciência e Comprometimento**, confirmando que leram, compreenderam e se comprometem a cumprir esta Política. Violações injustificadas poderão resultar em medidas disciplinares, contratuais e legais cabíveis.

TERMO DE CIÊNCIA E COMPROMISSO

Política de Segurança Cibernética e da Informação
Theras Capital Gestão de Investimentos Ltda.
CNPJ 62.051.574/0001-46

Eu, _____,
nacionalidade _____, estado civil _____,
portador(a) do RG nº _____, CPF nº _____,
na qualidade de _____,

DECLARO, para todos os fins, que:

Recebi, em //_____, uma via da **Política de Segurança Cibernética e da Informação da Theras Capital Gestão de Investimentos Ltda.**, passando a ter pleno e integral acesso ao seu teor.

Li integralmente, compreendi e estou plenamente ciente das normas, procedimentos, diretrizes, controles, obrigações e responsabilidades previstos na referida Política, incluindo aqueles relacionados

a. proteção de dados pessoais (LGPD – Lei 13.709/2018);
b. confidencialidade de informações internas e de terceiros;
c. regras de uso adequado dos sistemas, redes, dispositivos e aplicações;
d. prevenção a incidentes cibernéticos e engenharia social;

e. reporte imediato de anomalias, violações ou suspeitas de incidentes;
f. monitoramento, auditoria e rastreabilidade de acessos e atividades.

Comprometo-me a cumprir integralmente todas as normas e exigências previstas na Política, responsabilizando-me pelo uso seguro e adequado:

a. dos sistemas corporativos;
b. dos dispositivo fornecidos pela empresa;
c. do acesso remoto;
d. dos dados e informações sob minha guarda.

Reconheço que:

i. o descumprimento, negligência ou violação às normas da Política pode gerar consequências disciplinares, contratuais, civis, administrativas e criminais;
ii. incidentes e violações devem ser imediatamente comunicados ao Diretor de Compliance ou ao canal formal da Theras Capital;
iii. meus acessos, registros e atividades podem ser **auditados e monitorados**, conforme previsto em lei e nas políticas internas.

Assumo plena responsabilidade por:

1. manter sigilo e proteger informações internas, estratégicas, pessoais ou confidenciais;
2. não compartilhar senhas, credenciais ou acessos;
3. não instalar softwares não autorizados;
4. seguir práticas seguras de navegação e comunicação;
5. evitar condutas que elevem o risco cibernético da organização.

Estou ciente de que esta Política poderá ser atualizada periodicamente, devendo eu acompanhar e cumprir as versões mais recentes, que serão disponibilizadas pela área de Compliance.

E, por estar de pleno acordo, firmo o presente Termo.

São Paulo, _____ de _____ de 20____.

Assinatura do Colaborador

Nome completo

Cargo / Área