ITER
INVESTIMENTOS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO E ABRANGÊNCIA

1.1. Esta Política estabelece as regras, os processos e os controles adotados pela ITER Gestora de Recursos S.A. ("Iter") para proteger as informações sob sua guarda, inclusive contra ameaças cibernéticas, de forma a garantir sua confidencialidade, integridade e disponibilidade, nos termos da Resolução CVM nº 21/2021, do Código ANBIMA de Administração e Gestão de Recursos de Terceiros ("Código ANBIMA"), do Guia de Cibersegurança da ANBIMA e da Lei nº 13.709/2018 ("LGPD").

1.2. Esta Política aplica-se a todos os Empregados, Parceiros e Prestadores de Serviço Terceirizados da Iter que tenham acesso a informações ou sistemas da Iter, e integra o Manual de Compliance, o Código de Ética e o Plano de Continuidade dos Negócios.

1.3. O Diretor de Compliance é o responsável pela implementação, monitoramento e cumprimento desta Política, podendo contar com o apoio de prestadores de serviços de tecnologia contratados pela Iter.

2. CONTROLE DE ACESSO

Controle de Acesso Pessoal

2.1. Informações confidenciais somente são acessadas por Empregados que necessitem ter acesso a tais informações para desempenhar atividade relacionada aos negócios da Iter.

Controle de Acesso a Arquivos Eletrônicos

2.2. O acesso às bases de dados e aos sistemas deve ser feito somente por ferramentas e tecnologias autorizadas pelo Diretor de Compliance, de forma a permitir a identificação e o rastreamento dos usuários que tiveram acesso a determinadas informações (os registros de acesso ficam armazenados nos sistemas).

2.3. Os acessos a sistemas, pastas e arquivos são controlados por logins individuais e intransferíveis, com perfis de acesso definidos por função e área e autenticação em dois fatores nos sistemas corporativos (e-mail, armazenamento em nuvem e bases de dados). Planilhas e arquivos sensíveis podem ser protegidos por senha.

2.4. Os acessos são revistos periodicamente e cancelados imediatamente em caso de desligamento do Empregado ou término do contrato com o Prestador de Serviço. Não é permitida a permanência de antigos Empregados nas dependências da Iter, salvo para conclusão do processo de desligamento.

Controle de Acesso Físico

2.5. O escritório da Iter tem acesso restrito por biometria ou cartão, com segregação física entre as áreas, nos termos do Manual de Compliance.

Acesso Remoto

2.6. O acesso remoto aos sistemas da Iter é permitido apenas a Empregados previamente autorizados pelo Diretor de Compliance, por meio de equipamentos corporativos e conexões seguras, vedado o download de informações sensíveis em equipamentos pessoais.

3. INFRAESTRUTURA E PROTEÇÃO

3.1. A Iter utiliza infraestrutura em nuvem contratada de fornecedores de mercado (Microsoft 365 e Google Cloud), com criptografia, redundância e backup diário das informações. Os equipamentos corporativos contam com antivírus, firewall e atualizações de segurança.

3.2. Os registros e documentos exigidos pela regulamentação são mantidos pelo prazo mínimo de 5 (cinco) anos.

4. IDENTIFICAÇÃO DE RISCOS (RISK ASSESSMENT)

4.1. No âmbito de suas atividades, a Iter identificou os seguintes principais ativos e riscos que precisam de proteção:

- **Dados e Informações:** Informações Confidenciais, incluindo informações sobre Investidores, cedentes, devedores, Empregados e a própria Iter, operações e ativos das carteiras sob gestão, e comunicações internas e externas;
- **Sistemas:** sistemas utilizados pela Iter e tecnologias desenvolvidas internamente ou por terceiros, suas ameaças e vulnerabilidades;
- **Processos e Controles:** processos e controles internos que integram a rotina das áreas da Iter;
- **Governança da Gestão de Risco:** eficácia da gestão de riscos quanto às ameaças e aos planos de ação, de contingência e de continuidade de negócios.

4.2. Quanto à segurança cibernética, a Iter identificou as seguintes principais ameaças, nos termos do Guia de Cibersegurança da ANBIMA:

- **Malware:** softwares desenvolvidos para corromper computadores e redes (vírus, cavalo de Troia, spyware e ransomware);
- **Engenharia social:** métodos de manipulação para obter informações confidenciais (pharming, phishing, vishing, smishing e acesso pessoal);
- **Ataques de DDoS e botnets:** ataques que visam negar ou atrasar o acesso aos serviços ou sistemas;
- **Invasões (advanced persistent threats):** ataques sofisticados destinados a explorar fragilidades específicas do ambiente tecnológico.

4.3. Com base nesses riscos, a Iter define as medidas de prevenção e acompanhamento para sua mitigação, as modificações necessárias e o plano de retomada das atividades, nos termos do Plano de Continuidade dos Negócios.

5. MONITORAMENTO E TESTES

5.1. O Diretor de Compliance (ou pessoa por ele designada) adotará as seguintes medidas para detectar acessos não autorizados ou outras violações:

(a) disponibilizará equipamento de uso exclusivo para cada Empregado, de modo a evitar o compartilhamento de equipamentos e a visualização de informações de outras áreas;

(b) manterá níveis de acesso a pastas e arquivos de acordo com a função e a área de cada Empregado, podendo monitorar tais acessos;

(c) manterá registro dos acessos aos arquivos e sistemas, que permita identificar os Empregados que acessaram cada informação;

(d) poderá monitorar o uso, pelos Empregados, de sites, webmails, redes sociais e e-mails corporativos;

(e) realizará, ao menos anualmente, testes e verificações de segurança dos sistemas, com o apoio de prestadores de tecnologia quando necessário; e

(f) verificará, por amostragem, os registros de acesso ao escritório, equipamentos, pastas e sistemas, para avaliar a aderência às regras de restrição de acesso.

5.2. O Diretor de Compliance poderá adotar medidas adicionais de monitoramento e reportará os resultados das verificações à Diretoria, permitindo a identificação dos responsáveis em caso de vazamento.

6. INCIDENTES DE SEGURANÇA

6.1. Qualquer suspeita ou ocorrência de incidente de segurança (vazamento, acesso indevido, perda de dados ou ataque cibernético) deve ser comunicada imediatamente ao Diretor de Compliance.

6.2. O Diretor de Compliance avaliará o incidente, adotará as medidas de contenção e recuperação previstas no Plano de Continuidade dos Negócios, registrará a ocorrência e, quando aplicável, comunicará os administradores fiduciários dos fundos, a Autoridade Nacional de Proteção de Dados e os titulares afetados, nos termos da LGPD.

7. PRESTADORES DE SERVIÇO E DADOS PESSOAIS

7.1. Prestadores de Serviço com acesso a informações ou sistemas da Iter são avaliados previamente quanto às suas práticas de segurança da informação e proteção de dados, nos termos do item 4.3 da Política de Decisão, Seleção e Alocação de Ativos, e devem assumir obrigação contratual de confidencialidade.

7.2. Os dados pessoais são tratados exclusivamente para as finalidades das atividades da Iter e em conformidade com a LGPD.

ITER
INVESTIMENTOS

8. TREINAMENTO

8.1. Os Empregados recebem esta Política no ingresso e são treinados anualmente em segurança da informação e prevenção a ameaças cibernéticas, no âmbito do programa de treinamento do Manual de Compliance.

9. DISPOSIÇÕES FINAIS

9.1. A presente Política foi revisada e aprovada pelo setor jurídico e entra em vigor na presente data.

9.2. Esta Política deverá ser revisada anualmente ou em menor periodicidade, à medida que ocorram alterações nos procedimentos nela previstos.

9.3. Havendo quaisquer dúvidas, favor contatar:

Lauir José Lima do Prado
Diretor de Compliance
Telefone: +55 (11) 94042-2283
E-mail: lauir@iterinvestimentos.com.br

10. CONTROLE DE APROVAÇÕES

Versão	Data
1	11 de março de 2024
2	04 de abril de 2026

* * *