Política Institucional		
Área Gestora ***Compliance* e Gestão de Riscos**	Código	Versão **02**
Assunto **Manual de Segurança da Informação e Continuidade de Negócios**	Data Criação **08/05/2025**	Data Publicação **15/05/2025**
Abrangência **Troon Gestora de Recursos Ltda.**		

MANUAL DE SEGURANÇA DA INFORMAÇÃO E CONTINUIDADE DE NEGÓCIOS

Versão	Atualizada em	Responsável:
1	29/07/2024	Diretor de Compliance
2	08/05/2024	Diretor de Compliance

1. INTRODUÇÃO E OBJETIVO

O Manual de Segurança da Informação e Com tenuidade de Negócios ("Manual") da **TROON GESTORA DE RECURSOS LTDA.** ("Troon" ou Gestora"), aplica-se a todos os sócios, Colaboradores, prestadores de serviços e sistemas, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da Troon, ou que acesse informações a ela pertencentes. Todo e qualquer usuário de recursos computadorizados da nossa instituição tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática da Troon.

Este Manual foi elaborado para atender especificamente às atividades desempenhadas pela Gestora, de acordo com natureza, complexidade e riscos a elas inerentes, observada a obrigação de revisão e atualização periódica.

Este Manual deve ser lido em conjunto com o Código de Ética e demais políticas da Gestora, que também contém regras que visam atender aos objetivos aqui descritos.

Este Manual está de acordo com o Código ANBIMA de Regulação e Melhores Práticas para Administração e Gestão de Recursos de Terceiros, bem como com a regulamentação vigente emitida pela Comissão de Valores Mobiliários ("CVM").

2. POLÍTICA DE CONFIDENCIALIDADE E TRATAMENTO DA INFORMAÇÃO

Nos termos da Resolução CVM nº 21, de 25 de fevereiro de 2021, especialmente o Artigo 27, III e Artigo 28, II, a Gestora adota procedimentos e regras de conduta para preservar informações confidenciais e permitir a identificação das pessoas que tenham acesso a elas.

A informação alcançada em função da atividade profissional desempenhada por cada Colaborador na Gestora é considerada confidencial e não pode ser transmitida de forma alguma a terceiros não Colaboradores ou a Colaboradores não autorizados.

2.1. *Segurança da Informação Confidencial*

A Gestora mantém um inventário atualizado que identifica e documenta a existência e as principais características de todos os ativos de informação, como base de dados, arquivos, diretórios de rede, planos de continuidade, entre outros. Nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da Gestora, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

Em caso de determinado Colaborador passar a exercer atividade ligada a outra área da Gestora, tal Colaborador terá acesso apenas às informações relativas a esta área, das quais necessite para o exercício da nova atividade, deixando de ter permissão de acesso aos dados, arquivos, documentos e demais informações restritas à atividade exercida anteriormente. Em caso de desligamento da Gestora, o Colaborador deixará imediatamente de ter acesso a qualquer ativo de informação interna da Gestora.

Qualquer informação sobre a Gestora, ou de qualquer natureza relativa às atividades da Gestora, aos seus sócios e Clientes, obtida em decorrência do desempenho das atividades normais do Colaborador na Gestora, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado por escrito pela Diretoria de *Compliance*.

Todos os Colaboradores, assim como todos os terceiros contratados pela Gestora, deverão assinar documento de confidencialidade sobre as informações confidenciais, reservadas ou privilegiadas que lhes tenham sido confiadas em virtude do exercício de suas atividades profissionais.

É terminantemente proibido que os Colaboradores façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da Gestora e circulem em ambientes externos à Gestora com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas informações confidenciais.

A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Gestora e de seus Clientes. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

Ainda, qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois podem conter informações restritas e confidenciais, mesmo no ambiente interno da Gestora.

O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Todos os arquivos digitalizados em pastas temporárias serão apagados periodicamente, de modo que nenhum arquivo deverá ali permanecer. A desobediência a esta regra será considerada uma infração, sendo tratada de maneira análoga à daquele que esquece material na área de impressão.

O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso, usando uma trituradora, de maneira a evitar sua recuperação.

Adicionalmente, os Colaboradores devem se abster de utilizar *hard drives*, *pen-drives*, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Gestora.

É proibida a conexão de equipamentos na rede da Gestora que não estejam previamente autorizados pela área de informática e pela área de *compliance*.

Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

O envio ou repasse por *e-mail* de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido, conforme acima aventado, bem como o envio ou repasse de *e-mails* com opiniões, comentários ou mensagens que possam denegrir a imagem e/ou afetar a reputação da Gestora.

Em nenhuma hipótese um Colaborador pode emitir opinião por *e-mail* em nome da Gestora, ou utilizar material, marca e logotipos da Gestora para assuntos não corporativos ou após o rompimento do seu vínculo com este, salvo se expressamente autorizado para tanto.

A Diretoria de *Compliance* também monitorará e será avisada por *e-mail* em caso de tentativa de acesso aos diretórios e *logins* virtuais no servidor protegidos por senha. A Diretoria de *Compliance* elucidará as circunstâncias da ocorrência deste fato e aplicará as devidas sanções.

Programas instalados nos computadores, principalmente via *internet* (*downloads*), sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia do responsável pela área de informática na Gestora. Não é permitida a instalação de nenhum *software* ilegal ou que possua direitos autorais protegidos. A instalação de novos *softwares*, com a respectiva licença, deve também ser comunicada previamente ao responsável pela informática. Este deverá aprovar ou vetar a instalação e utilização dos *softwares* dos Colaboradores para aspectos profissionais e pessoais.

A Gestora se reserva no direito de gravar qualquer ligação telefônica e/ou qualquer comunicação dos seus Colaboradores realizada ou recebida por meio das linhas telefônicas ou qualquer outro meio disponibilizado pela Gestora para a atividade profissional de cada Colaborador.

Todas as informações do servidor da Gestora, do banco de dados dos clientes e os modelos dos analistas são enviados para o servidor em nuvem da Gestora. Nesse servidor, as informações são segregadas por área, sendo armazenadas com backup.

A rotina de backup garante a salvaguarda de todos os dados, sendo eles banco de dados, documentos, planilhas e diversos outros guardados na área de armazenamento dos servidores.

Em caso de divulgação indevida de qualquer informação confidencial, a Diretoria de *Compliance* apurará o responsável por tal divulgação, sendo certo que poderá verificar no servidor quem teve acesso ao referido documento por meio do acesso individualizado de cada Colaborador.

Serão realizados testes de segurança para os sistemas de informações utilizados pela Gestora, em periodicidade, no mínimo, anual, para garantir a efetividade dos controles internos mencionados neste Manual de *Compliance*, especialmente as informações mantidas em meio eletrônico.

2.2. *Propriedade intelectual*

Todos os documentos desenvolvidos na realização das atividades da Gestora ou a elas diretamente relacionados, tais quais, sistemas, arquivos, modelos, metodologias, fórmulas, projeções, relatórios de análise etc., são de propriedade intelectual da Gestora.

A utilização e divulgação de qualquer bem sujeito à propriedade intelectual da Gestora fora do escopo de atuação ou não destinado aos Clientes, dependerá de prévia e expressa autorização por escrito da Diretoria de *Compliance*.

Uma vez rompido com a Gestora o vínculo do Colaborador, este permanecerá obrigado a observar as restrições ora tratadas, sujeito à responsabilização nas esferas civil e criminal.

3. INFORMAÇÃO PRIVILEGIADA E INSIDER TRADING

É considerada como informação privilegiada qualquer Informação Relevante (conforme definido abaixo) a respeito de alguma empresa, que não tenha sido publicada e que seja conseguida de maneira privilegiada, em consequência da ligação profissional ou pessoal mantida com um Cliente, com colaboradores de empresas estudadas ou investidas ou com terceiros, ou em razão da condição de Colaborador.

Considera-se Informação Relevante, para os efeitos deste Manual de *Compliance*, qualquer informação (completa ou parcial), decisão, deliberação, ou qualquer outro ato ou fato de caráter político-administrativo, técnico, negocial ou econômico-financeiro ocorrido ou relacionado aos seus negócios da Gestora que possa influir de modo ponderável: *(a)* na rentabilidade dos valores mobiliários administrados pela Gestora; *(b)* na decisão de Clientes de comprar, vender ou manter cotas de fundos de investimento administrados pela Gestora; e *(c)* na decisão dos Clientes de exercer quaisquer direitos inerentes à condição de titular de cotas de fundos de investimento administrados pela Gestora.

As informações privilegiadas precisam ser mantidas em sigilo por todos que a acessarem, seja em função da prática da atividade profissional ou do relacionamento pessoal.

Em caso de o Colaborador ter acesso a uma informação privilegiada que não deveria ter, deverá transmiti-la rapidamente à Diretoria de *Compliance*, não podendo comunicá-la a ninguém, nem mesmo a outros membros da Gestora, profissionais de mercado, amigos e parentes, e nem usá-la, seja em seu próprio benefício ou de terceiros. Se não houver certeza quanto ao caráter privilegiado da informação, deve-se, igualmente, relatar o ocorrido à Diretoria de *Compliance*.

3.1. *Insider Trading e "Dicas"*

Insider trading baseia-se na compra e venda de títulos ou valores mobiliários com base no uso de informação privilegiada, com o objetivo de conseguir benefício próprio ou para terceiros (compreendendo a própria Gestora e seus Colaboradores).

"Dica" é a transmissão, a qualquer terceiro, de informação privilegiada que possa ser usada como benefício para a compra e venda de títulos ou valores mobiliários.

É proibida a prática dos atos mencionados anteriormente por qualquer membro da empresa, seja agindo em benefício próprio, da Gestora ou de terceiros.

A prática de qualquer ato em violação deste Manual de Compliance pode sujeitar o infrator à responsabilidade civil e criminal, por força de lei. O artigo 27-D da Lei nº 6.385, de 07 de dezembro de 1976 tipifica como crime a utilização de informação relevante ainda não divulgada ao mercado, da qual o agente tenha conhecimento e da qual deva manter sigilo, capaz de propiciar, para si ou para outrem, vantagem indevida, mediante negociação, em nome próprio ou de terceiro, com valores mobiliários. As penalidades previstas para esse crime são tanto a pena de reclusão, de 1 (um) a 5 (cinco) anos, bem como multa de 3 (três) vezes o montante da vantagem ilícita obtida em decorrência do crime. Além de sanções de natureza criminal, qualquer violação da legislação vigente e, portanto, deste Manual de Compliance, poderá, ainda, sujeitar o infrator a processos de cunho civil e administrativo, bem como à imposição de penalidades nesse âmbito, em conformidade com a Lei nº 6.404, de 15 de dezembro de 1976 e a Resolução CVM nº 44, de 23 de agosto de 2021 ("Resolução CVM 44").

É de responsabilidade da Diretoria de Compliance verificar e processar periodicamente as notificações recebidas a respeito do uso pelos Colaboradores de informações privilegiadas, insider trading e "dicas". Casos envolvendo o uso de

informação privilegiada, *insider trading* e "dicas" devem ser analisados não só durante a vigência do relacionamento profissional do Colaborador com a Gestora, mas mesmo após o término do vínculo, com a comunicação do ocorrido às autoridades competentes, conforme o caso.

3.2. *Vazamento de Informações Confidenciais, Reservadas ou Privilegiadas*

Considera-se como vazamento de informações confidenciais, reservadas ou privilegiadas qualquer divulgação não autorizada, intencional ou involuntária, de dados sensíveis relacionados às atividades da Gestora, seus clientes ou parceiros de negócios, que possam influenciar de maneira significativa:

a) a tomada de decisão por parte de investidores ou clientes da Gestora em relação aos fundos geridos;

b) a rentabilidade dos ativos administrados pela Gestora; ou

c) a reputação e a integridade das operações financeiras conduzidas pela empresa.

Para mitigar esses potenciais riscos de vazamentos, serão adotadas pela Gestora as seguintes condutas:

(i) Acesso a informações confidenciais será permitido apenas a colaboradores autorizados, com rígido controle de entradas e saídas de dados. No caso de mudanças de função ou desligamento de colaboradores, o acesso será imediatamente revisto e, se necessário, bloqueado.

(ii) Sistemas de informação serão protegidos por meio de mecanismos de segurança atualizados e monitorados regularmente para prevenir o vazamento de dados, com especial atenção aos meios eletrônicos e dispositivos móveis.

(iii) Na ocorrência de vazamento de informações, o colaborador que tomar conhecimento deverá comunicar o fato imediatamente à Diretoria de Compliance, que investigará o incidente e adotará as medidas corretivas

necessárias. Isso inclui a identificação da origem do vazamento, notificação das partes afetadas e implementação de ações de contenção e prevenção de novos incidentes.

(iv) Todos os colaboradores da Gestora receberão treinamentos regulares sobre a importância da proteção de informações confidenciais, bem como as medidas a serem adotadas em caso de incidente. Esse treinamento será obrigatório e abrangente, reforçando as políticas internas de segurança da informação e as penalidades em casos de violação.

A Diretoria de Compliance será responsável por monitorar o cumprimento dessas diretrizes e conduzir auditorias internas para garantir que todos os processos estejam alinhados às melhores práticas de mercado.

4. PLANO DE CONTINUIDADE DO NEGÓCIO

Na execução de suas atividades, a Gestora está sujeita a riscos relacionados à ocorrência de eventos que possam comprometer, dificultar ou mesmo impedir a continuidade das operações da Gestora, tais como catástrofes naturais, ataques cibernéticos, sabotagens, roubos, vandalismos e problemas estruturais.

Este plano de continuidade do negócio busca descrever os procedimentos, estratégias, ações e infraestrutura empregados pela Gestora para garantir a continuidade das suas atividades em situações de contingência.

O responsável pelo cumprimento do plano de continuidade do negócio e pela ativação do plano de contingência é a Diretoria de *Compliance*.

4.1. Estrutura e procedimentos de contingência

A Gestora garantirá a continuidade de suas operações no caso de um desastre ou qualquer outra interrupção drástica dos negócios.

Os servidores da Gestora podem ser acessados de forma virtual via *cloud*, de forma que todas as informações podem ser acessadas remotamente de qualquer lugar com acesso à internet.

Em caso de emergência na sede da Gestora que impossibilite o seu uso, os Colaboradores trabalharão remotamente, a partir de seu ambiente residencial ou lugar a ser definido na oportunidade pelo Diretor de *Compliance* e de Gestão.

Além disso, a Diretoria de *Compliance* estabelecerá um controle das atividades de maior criticidade para o negócio, de modo a proporcionar meios substitutivos, caso aplicável, em situações de interrupção total ou crítica.

4.2. Plano de contingência

O plano de contingência será acionado toda vez que, por qualquer motivo, o acesso às dependências da Gestora fique inviabilizado.

Nesses casos, os Diretores de *Compliance* e de Gestão, de comum acordo, devem determinar a aplicação dos procedimentos de contingência, autorizando os Colaboradores a trabalharem remotamente, no ambiente residencial do Colaborador, ou em lugar a ser definido na oportunidade pelos Diretores de *Compliance* e de Gestão, o qual possua conexão própria e segura. Os Colaboradores utilizarão os notebooks da Gestora e terão acesso a todos os dados e informações necessárias por meio do servidor na nuvem, de modo a manterem o regular exercício de suas atividades.

Após a normalização do acesso à Gestora, os Colaboradores deverão apresentar à Diretoria de *Compliance* relatório de atividades executadas durante o período de contingência, expondo, ao menos: quais atividades foram executadas; o tempo de duração das medidas de continuidade dos negócios; os prejuízos identificados; e as visões de melhoria aplicáveis.

4.3. Atualização do plano de continuidade do negócio

Os procedimentos, estratégias e ações constantes do plano de continuidade do negócio serão testados e validados, no mínimo, a cada 12 (doze) meses, ou em prazo inferior, se exigido pela regulamentação em vigor.

5. SEGURANÇA CIBERNÉTICA

A Gestora adota mecanismos de segurança cibernética com a finalidade de assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

O responsável pelo cumprimento das regras e procedimentos de segurança cibernética é a Diretoria de *Compliance*.

5.1. Avaliação dos riscos

No exercício das suas atividades, a Gestora poderá estar sujeita a riscos cibernéticos que ameacem a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados. Entre os riscos mais comuns, estão:

i) *Malwares*: softwares desenvolvidos para corromper computadores e redes:
   a. Vírus: software que causa danos à máquina, rede, outros softwares e bancos de dados;
   b. Cavalo de Tróia: aparece dentro de outro software e cria uma porta para a invasão do computador;
   c. *Spyware*: software malicioso para coletar e monitorar o uso de informações; e
   d. *Ransomware*: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

ii) Engenharia social: métodos de manipulação para obter informações confidenciais, como senhas, dados pessoas e número de cartão de crédito:
   a. *Pharming*: direciona o usuário para um site fraudulento, sem o seu conhecimento;

b. *Phishing*: links transmitidos por e-mails, simulando se ruma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
c. *Vishing*: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
d. *Smishing*: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais; e
e. Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

iii) Ataques de DDoS (distributed denial of services) e botnets: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos botnets, o ataque vem de um grande número de computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços; e

iv) Invasões (*advanced persistent threats*): ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

5.2. Ações de prevenção e proteção

Com a finalidade de mitigar os riscos cibernéticos e proteger seus sistemas, informações, base de dados, equipamentos e o andamento dos seus negócios, a Gestora adota as seguintes medidas de prevenção e proteção:

i) Controle de acesso adequado aos ativos da Gestora, por meio de procedimentos de identificação, autenticação, hierarquização e autorização dos usuários, ou sistemas, aos ativos da Gestora;

ii) Estabelecimento de regras mínimas (complexidade, periodicidade e autenticação de múltiplos fatores) na definição de senhas de acesso a dispositivos corporativos, sistemas e rede em função da relevância do ativo acessado. Além disso, os eventos de login e alteração de senha são auditáveis e rastreáveis;

iii) Limitação do acesso de cada Colaborador a apenas recursos relevantes para o desempenho das suas atividades e restrição do acesso físico às áreas com informações críticas/sensíveis;

iv) Rotinas de backup;

v) Criação de logs e trilhas de auditoria sempre que permitido pelos sistemas;

vi) Realização de diligência na contratação de serviços de terceiros, prezando, sempre que necessário, pela celebração de acordo de confidencialidade e exigência de controles de segurança na própria estrutura dos Terceiros;

vii) Implementação de recursos *anti-malware* em estações e servidores de rede, como antivírus e firewalls pessoais; e

viii) Restrição à instalação e execução de softwares e aplicações não autorizadas por meio de controles de execução de processos (por exemplo, aplicação de *whitelisting*);

ix) Identificação dos dados de maior criticidade, com mapeamento do seu ciclo de vida e adoção de suas medidas protetivas respectivas.

5.3. Monitoramento

A Gestora possui mecanismos de monitoramento das ações de proteção implementadas, para garantir seu bom funcionamento e efetividade.

Nesse sentido, a Gestora mantém inventários atualizados de hardware e software, bem como realiza verificações periódicas, no intuito de identificar elementos estranhos à Gestora, como computadores não autorizados ou softwares não licenciados.

Além disso, a Gestora mantém os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas. As rotinas de backup são monitoradas diariamente, com a execução de testes regulares de restauração dos dados.

São realizados, periodicamente e de forma documentada, testes de invasão externa e *phishing*, bem como análises de vulnerabilidades na estrutura tecnológica, sempre que houver mudança significativa em tal estrutura.

Ainda, a Gestora analisa regularmente os logs e as trilhas de auditoria criados, de forma a permitir a rápida identificação de ataques, sejam internos ou externos.

5.4. Plano de resposta

Caso seja identificado um potencial incidente relacionado à segurança cibernética, a Diretoria de *Compliance* deverá ser imediatamente comunicada.

Num primeiro momento, a Diretoria de *Compliance* se reunirá com os colaboradores diretamente envolvidos para compreender o evento ocorrido, os motivos e consequências imediatas, bem como a gravidade da situação. Neste mesmo momento, deverá ser estruturada a Equipe de Resposta a incidentes, que contará com colaboradores com as expertises necessárias para o combate, erradicação e recuperação do incidente.

Caso os diretores avaliem que o incidente ocorrido pode gerar danos iminentes à Gestora, serão tomadas, em conjunto com os assessores de tecnologia da informação da Gestora, as medidas imediatas de cibersegurança cabíveis, que podem incluir a redundância de TI, redirecionamento das linhas de telefone para os celulares, instrução do provedor de telefonia para que desvie linhas de dados e e-mails, entre outros.

Na hipótese de o incidente comprometer, dificultar ou mesmo impedir a continuidade das operações da Gestora, serão observados os procedimentos previstos no plano de continuidade do negócio, descrito no item 12 acima.

Além disso, os diretores avaliarão a pertinência da adoção de medidas como (i) registro de boletim de ocorrência ou queixa crime; (ii) comunicação do incidente aos órgãos regulatórios e autorregulatórios; (ii) consulta com jurídico interno ou externo para avaliação dos riscos legais e medidas judiciais cabíveis para assegurar os direitos da Gestora.

5.5. Reciclagem e revisão

A Gestora manterá o programa de segurança cibernética continuamente atualizado, identificando novos riscos, ativos e processos e reavaliando os riscos residuais.

A Diretoria de *Compliance*, responsável pela implementação dos procedimentos de segurança cibernética, realizará a revisão e atualização deste plano de segurança cibernética a cada 24 (vinte e quatro) meses, ou em prazo inferior sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão da Diretoria de *Compliance*.