



# **Política de Segurança Cibernética**

**Março 2025**



## I. OBJETIVO

A Política de Segurança Cibernética (“Política”) da Oby Equities Gestora de Recursos Ltda. (“Oby Equities” ou “Gestora”) tem como objetivo assegurar a continuidade das atividades da companhia, com ênfase na proteção das informações confidenciais sob sua responsabilidade, abrangendo tanto os veículos de investimentos sob sua gestão quanto os dados de seus investidores.

Para os fins desta Política, considera-se informações confidenciais todos os dados pertencentes à Gestora, aos veículos de investimentos sob sua gestão, aos investidores, assim como quaisquer informações que ainda não sejam de domínio público ou que a Oby Equities deseje manter restritas.

Assim, é estritamente proibida a divulgação de informações confidenciais fora do ambiente da Gestora ou para terceiros, internos ou externos à Oby Equities, que não necessitem ou não tenham autorização para acessá-las.

A divulgação de qualquer informação confidencial ao público em geral, por qualquer meio, poderá ocorrer apenas se previamente autorizada pela Diretoria.

Todas as informações processadas e armazenadas pela Gestora devem ser mantidas em ambientes seguros e protegidas contra acessos não autorizados.

Os sistemas de informação, a infraestrutura tecnológica, os documentos e as informações internas são considerados ativos da companhia. As medidas de proteção e manutenção descritas nesta Política têm como objetivo garantir a (i) Confidencialidade, (ii) Integridade e (iii) Disponibilidade dos dados e sistemas utilizados, tanto pela Gestora quanto por seus investidores, conforme as definições abaixo:

- i. **CONFIDENCIALIDADE:** Assegurar que as informações tratadas pela Oby Equities sejam acessadas apenas por um grupo restrito de pessoas autorizadas, prevenindo a exposição de dados sensíveis e acessos não autorizados.
- ii. **INTEGRIDADE:** Garantir que as informações permaneçam íntegras, sem alterações não autorizadas por indivíduos não habilitados.
- iii. **DISPONIBILIDADE:** Assegurar que as informações estejam acessíveis para os usuários autorizados sempre que necessário.

## I. IDENTIFICAÇÃO DOS ATIVOS RELEVANTES

No contexto das atividades da Oby Equities, foram identificados os seguintes ativos relevantes, cuja proteção requer especial atenção:

- **Informações Confidenciais:** Dados relacionados aos investidores, colaboradores, à própria gestora e aos veículos sob sua gestão;
- **Softwares e Planilhas:** Ferramentas e planilhas utilizadas pela Oby Equities para a execução de suas atividades empresariais;



- **Arquivos com Evidências dos Monitoramentos, Processos e Controles:** Informações geradas a partir dos processos de controle interno das áreas de Risco, Compliance, Gestão e TI.

Com relação aos riscos cibernéticos, a Oby Equities, conforme o Guia ANBIMA de Cibersegurança, identificou as seguintes ameaças principais para seus negócios:

- **Invasões Externas:** Ataques cibernéticos, geralmente realizados por hackers, que exploram vulnerabilidades no ambiente tecnológico, podendo comprometer a continuidade e operação dos negócios da gestora;
- **Engenharia Social:** Tática que manipula o comportamento dos usuários para obter informações confidenciais da companhia;
- **Malwares:** Programas maliciosos, como vírus, *ransomware*, *spyware*, *phishing*, entre outros, desenvolvidos para comprometer a segurança das redes de computadores.

A lista apresentada não é exaustiva, sendo apenas ilustrativa dos principais riscos aos quais a Oby Equities pode estar exposta no curso normal de suas operações.

Esses riscos serão monitorados continuamente pelas equipes de Risco, Compliance e Controles Internos, com base nas diretrizes de segurança fornecidas pela área de TI da Gestora.

## I. AÇÕES DE PROTEÇÃO E PREVENÇÃO

Com o objetivo de mitigar os riscos identificados, a Oby Equities adota de maneira contínua as seguintes medidas para proteger as informações confidenciais e garantir a continuidade das suas atividades:

### a. Regra Geral de Conduta

É estritamente proibido que os colaboradores façam cópias ou imprimam arquivos utilizados, gerados ou disponibilizados nos escritórios da Oby Equities sem a prévia autorização da Diretoria.

A exceção a essa proibição ocorre quando as cópias ou impressões dos arquivos forem necessárias para a execução e/ou desenvolvimento das atividades da Oby Equities. Nesses casos, o colaborador responsável pelos arquivos será encarregado pela sua adequada conservação, integridade e manutenção da confidencialidade.

O descarte de informações confidenciais, tanto digitais quanto físicas, deve ser realizado de maneira que impossibilite a recuperação dos dados. O descarte de documentos físicos que contenham informações confidenciais deve ser feito imediatamente após o uso, recomendando-se sua destruição total.

### b. Uso dos Sistemas Internos da Gestora

Os colaboradores devem se abster de utilizar dispositivos como pen-drives, disquetes, fitas, nuvem, discos ou qualquer outro meio que não tenha como finalidade a execução exclusiva de suas atividades na Oby Equities.

É proibido conectar equipamentos não autorizados à rede da Oby Equities. Qualquer novo equipamento ou sistema deve ter suas configurações realizadas pela equipe de TI da gestora.



Cada colaborador é responsável pela segurança das informações armazenadas ou disponibilizadas nos equipamentos sob sua responsabilidade. Será obrigatória a alteração periódica da senha de acesso aos equipamentos (login de usuário), conforme as orientações da equipe de TI, utilizando senhas de difícil identificação por potenciais atacantes.

A Oby Equities adotou um sistema de autenticação em duas etapas para aprovação de acesso. Nessa abordagem, o usuário utiliza uma senha pessoal para acessar sistemas ou provedores de informações, enquanto a gestora, por meio dos departamentos de Compliance e/ou Controles Internos, insere uma segunda senha para a autenticação.

É terminantemente proibido o acesso a sites e blogs inadequados ou o envio de e-mails com conteúdo discriminatório, preconceituoso, obsceno, pornográfico, ofensivo, ou com opiniões políticas ou religiosas. Comentários ou mensagens que possam prejudicar a imagem ou reputação da Oby Equities não são permitidos.

Programas instalados nos computadores, especialmente aqueles baixados da internet, devem ser previamente autorizados e avaliados quanto à segurança pela equipe de TI.

Não é permitida a instalação de softwares ilegais ou que possuam direitos autorais protegidos sem a devida autorização da Diretoria.

Todo conteúdo armazenado na rede da Oby Equities, incluindo arquivos pessoais e e-mails, poderá ser monitorado, sendo possível que seu conteúdo seja disponibilizado ou compartilhado com as equipes de Risco, Compliance e Controles Internos para fins de monitoramento e cumprimento das regulamentações e políticas internas. A confidencialidade dessas informações será preservada, conforme necessário.

### **c. Firewall e Softwares Antivírus**

A Oby Equities utiliza serviços de proteção cibernética projetados para detectar e bloquear acessos não autorizados à sua rede interna, como malwares e tentativas de invasão por vírus.

Os dispositivos antivírus são configurados para detectar, prevenir e, sempre que possível, eliminar programas que possam comprometer a segurança dos sistemas da Oby Equities.

As informações internas da Oby Equities também são armazenadas na nuvem para backup. Caso haja indisponibilidade desses dados, os procedimentos descritos na Política de Continuidade de Negócios poderão ser acionados, sob a orientação da Diretoria.

## **II. MECANISMOS DE SUPERVISÃO**

A empresa prestadora de serviços de TI é responsável por monitorar a segurança cibernética da Oby Equities, contando com a supervisão das áreas de Risco, Compliance e Controles Internos. Essas equipes analisarão relatórios periódicos contendo informações sobre vulnerabilidades e sugestões de melhorias, com o objetivo de garantir a continuidade das operações da empresa.

## **III. PLANO DE RESPOSTA**



A definição de um plano de resposta eficaz é fundamental para proteger as atividades da Oby Equities.

Os recursos tecnológicos disponibilizados pela gestora são monitorados por software, que fornece, de forma automatizada, informações atualizadas sobre tentativas de invasão e possível indisponibilidade de serviços.

Por meio da análise dos relatórios gerados, a gestora poderá determinar a necessidade de tomar medidas adicionais.

Colaboradores que identificarem situações de risco iminente devem informar imediatamente à equipe de TI, para que ela inicie a avaliação de um possível ataque cibernético. Após a análise da situação, a equipe de TI orientará a Diretoria sobre as melhores práticas para conduzir as atividades da maneira mais segura possível.

#### **IV. REVISÃO DA POLÍTICA**

Devido à rápida evolução das práticas e soluções em segurança cibernética, que exigem constantes adaptações, esta política será revisada e, se necessário, atualizada pelo departamento de Compliance a cada 24 meses ou sempre que houver alterações na regulamentação que requeiram ajustes.

Durante a revisão, será avaliada a eficácia da política, a identificação de novos riscos e a análise de riscos residuais desde a implementação da política.