# Política de Segurança da Informação para Terceiros

| CÓDIGO | PUBLICAÇÃO | VIGÊNCIA | VERSÃO |
|---|---|---|---|
| DTI-12 | NOV.2023 | NOV.2025 | v.001 |

| ÁREA RESPONSÁVEL | CLASSIFICAÇÃO DA INFORMAÇÃO |
|---|---|
| Segurança da Informação | Pública |

## 1. VISÃO GERAL

Esta Política estabelece regras e diretrizes de governança adotadas pela Singulare Corretora de Títulos e Valores Mobiliários S/A e Singulare Administração Fiduciária Ltda., em conjunto denominadas ("**Singulare**"), para assegurar que os terceiros que tenham acesso aos seus ativos, garantam o cumprimento dos princípios e disposições estabelecidas na Política de Segurança da Informação e demais Políticas, Normas e Procedimentos que compõem o Sistema de Gestão de Segurança da Informação ("SGSI") da **Singulare**.

---

## 2. PÚBLICO-ALVO

Esta Política e o SGSI se aplicam a todas as áreas, negócios e colaboradores da **Singulare**, bem como terceiros e parceiros, incluindo, mas não se limitando a clientes e parceiros, administradores, gestores, colaboradores, prestadores ou fornecedores de serviços, usuários externos das informações pertencentes/custodiadas pela **Singulare**.

---

## 3. PRINCÍPIOS DE SEGURANÇA CIBERNÉTICA

**Confidencialidade**: Garantir que as informações sejam acessadas somente por aqueles expressamente autorizados e que sejam devidamente protegidas do conhecimento de terceiros não autorizados.

**Integridade**: Garantir que a informação seja mantida em seu estado original, visando protegê-la, no armazenamento ou tramissão, contra alterações indevidas, intencionais ou acidentais.

**Disponibilidade**: Garantir que a informação, se elegível, esteja disponível para ser acessada quando necessário.

---

## 4. DEFINIÇÕES

**Ameaça:** Causa potencial de um incidente indesejado, que pode resultar em dano.

**Aplicativos de Comunicação:** Conjunto de código e instruções compiladas, executados ou interpretados por um Recurso de Tecnologia da Informação e Comunicação, armazenados em um dispositivo ou na nuvem, que são usados para troca rápida de mensagens, conteúdos e informações multimídia.

**Autenticidade:** Garantia de que a informação é procedente e fidedigna, sendo capaz de gerar evidências não repudiáveis da identificação de quem a criou, editou ou emitiu.

**Backup:** Salvaguarda de informações realizada por meio de reprodução e/ou espelhamento de uma base de arquivos com a finalidade de recuperação em caso de incidente ou necessidade de restauração, ou

ainda, constituição de infraestrutura de acionamento imediato em caso de incidente ou necessidade justificada.

**Identidade Digital:** É a identificação em ambientes lógicos, sendo composta por seu nome de usuário (login) e senha ou por outros mecanismos de identificação e autenticação como crachá magnético, certificado digital, token e biometria.

**Incidente de Segurança da Informação e Comunicação**: Ocorrência identificada de um estado de sistema, dados, informações, serviço ou rede, que indica possível violação à Política de Segurança da Informação ou Normas Complementares, falha de controles ou situação previamente desconhecida, que possa ser relevante à segurança da informação.

**Informação:** Conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato.

**Internet:** Rede mundial de computadores interconectada pelo protocolo TCP/IP cuja infraestrutura tem caráter aberto e colaborativo, acessível por meio de dispositivos com conexão e autorizações suficientes e que permite obter informação de qualquer outro dispositivo que também esteja conectado à rede, desde que configurado adequadamente.

**Legalidade:** Garantia de que todas as informações sejam criadas e gerenciadas de acordo com as disposições do Ordenamento Jurídico em vigor.

**Recursos de Tecnologia da Informação e Comunicação (Recursos de TIC**): hardware, software, serviços de conexão e comunicação ou de infraestrutura física necessários para criação, registro, armazenamento, manuseio, transporte, compartilhamento e descarte de informações.

**Risco:** Combinação da probabilidade da concretização de uma ameaça e seus potenciais impactos.

**Segurança da Informação:** é a preservação da confidencialidade, integridade, disponibilidade, legalidade e autenticidade da informação. Visa proteger a informação dos diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios, maximizar o retorno dos investimentos e de novas oportunidades de transação.

**Tentativa de Burla:** A tentativa de burlar as diretrizes e controles estabelecidos, quando constatada, deve ser tratada como uma violação.

**Violação:** Qualquer atividade que desrespeite as regras estabelecidas nos documentos normativos.

## 5. DIRETRIZES GERAIS

A **Singulare** mantém a segurança dos ativos de informação, provendo ferramentas que permitam aplicar as melhores práticas de segurança no ambiente físico ou lógico, a fim de garantir o sigilo, proteção e integridade do ciclo de vida dos dados pessoais e da inofrmação, desde sua recepção, produção, registro,

classificação, controle, acesso, manuseio, reprodução, transmissão, guarda e descarte.

Sendo assim, as diretrizes gerais da Política de Segurança da Informação para Terceiros contempla: **a)** verificação do cumprimento de políticas, procedimentos e controles relacionados a Segurança da Informação, bem como a identificação e correção de eventuais vulnerabilidades identificadas; **b)** critérios para a gestão de fornecedores e terceiros nos temas relativos à segurança da informação; **c)** promoção e capacitação periódica com a criação de cultura organizacional voltada à Segurança da Informação.

---

## 6. PROTEÇÃO DE DADOS E PRIVACIDADE

A informação é um importante ativo da **Singulare** e deve ser preservada e salvaguardada, em conformidade com suas políticas, normas, procedimentos e controles internos, de acordo com as leis e regulamentos vigentes sobre o tema.

---

## 7. SEGURANÇA DA INFORMAÇÃO NO RELACIONAMENTO COM PARCEIROS

Parceiros de negócio da que acessam ativos da **Singulare** devem seguir as diretrizes de Segurança da Informação desta Política. Igualmente, os colaboradores da **Singulare** responsáveis por terceiros, fornecedores, prestadores de serviços e parceiros de negócios, devem:

- Realizar avaliação de conformidade do terceiro, considerando aspectos de segurança da informação, de acordo com relevância e impacto nos processos da **Singulare**, conforme orientações da área de Tecnologia.
- Assegurar a existência de controles voltados à mitigação de riscos à segurança da informação relacionados aos terceiros, bem como identificar eventuais riscos do comparilhamento de informação e dados.
- Assegurar a existência de procedimentos para a prevenção e tratamento de incidentes, conforme relevância e impacto nos processos da **Singulare**.

---

## 8. ACESSO FÍSICO E LÓGICO

Além disso, os gestores de relacionamentos com terceiros, devem assegurar que os acordos contenham os requisitos de Segurança de Informação específicos, bem como conformidade e equilíbrio em função do terceiro envolvido e serviço prestado, especialmente quando a atividade requeira acesso, tratamento, transmissão, gestão da informação, sistemas ou recursos que tratam informações da empresa.

Nenhum acesso físico ou lógico será concedido à rede interna, intranet e a diretórios internos da **Singulare** a terceiros, inclusive consultores em trabalhos internos.

## 9. USO DE ATIVOS

Os gestores de relacionamentos com terceiros devem assegurar que, na eventual disponibilização de ativos a terceiros, a responsabilidade sobre a guarda e segurança e as devidas penalidades no caso de descumprimento destes pontos, estejam claros nos contratos e documentos assinados.

A **Singulare** realiza o monitoramento de seus ambientes físicos e lógicos, visando a eficácia dos controles implantados, a proteção de seu patrimônio e sua reputação, possibilitando ainda a identificação de eventos ou alertas de incidentes ligados à Segurança da Informação.

Desta forma, a **Singulare** poderá auditar ou inspecionar os Recursos Computacionais que estiverem em suas dependências ou que interajam com seus ambientes lógicos sempre que considerar necessário, sempre atendendo aos princípios da proporcionalidade, razoabilidade e privacidade de seus proprietários ou portadores.

## 10. CANAL DE COMUNICAÇÃO

As questões de segurança de informação deverão ser endereçadas ao Diretor responsável pela Política de Segurança da Informação para Terceiros, conforme normas vigentes aplicáveis ao tema.

**Atendimento**:

Telefone: 0800 729 7272

E-mail: atendimento@singulare.com.br

Documento atualizado em novembro de 2023.