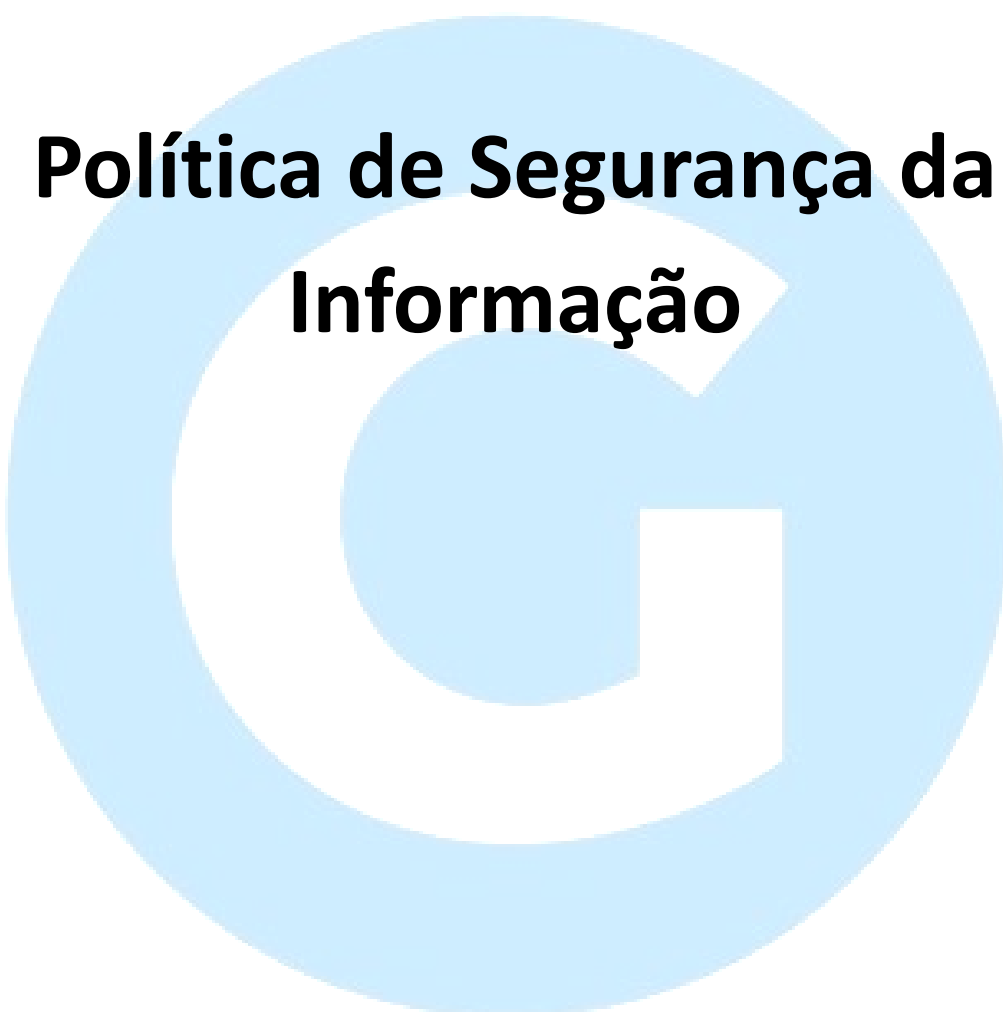




# **Política de Segurança da Informação**

## Versões

| <b>Versão</b> | <b>Data</b> | <b>Responsável</b> | <b>Alteração</b>     |
|---------------|-------------|--------------------|----------------------|
| 01            |             | Rafael Saraiva     | Emissão do documento |

|                                                                  |           |
|------------------------------------------------------------------|-----------|
| <b>Versões.....</b>                                              | <b>2</b>  |
| <b>1. Objetivo.....</b>                                          | <b>4</b>  |
| <b>2. Escopo.....</b>                                            | <b>4</b>  |
| <b>3. Diretrizes e Princípios Gerais.....</b>                    | <b>4</b>  |
| 3.1. Comprometimento da Direção.....                             | 4         |
| 3.2. Confidencialidade, Integridade e Disponibilidade (CID)..... | 5         |
| 3.3. Responsabilidades.....                                      | 5         |
| 3.4. Gestão de Riscos de Segurança da Informação.....            | 5         |
| 3.5. Controle de Acesso.....                                     | 6         |
| 3.6. Proteção de Código-Fonte e Propriedade Intelectual.....     | 6         |
| 3.7. Backup e Continuidade.....                                  | 6         |
| 3.8. Uso Aceitável de Ativos.....                                | 7         |
| 3.9. Conformidade de Fornecedores e Parceiros.....               | 7         |
| 3.10. Desenvolvimento e Serviços em Nuvem.....                   | 7         |
| 3.11. Gestão de Incidentes de Segurança.....                     | 8         |
| 3.12. Treinamento e Conscientização.....                         | 8         |
| 3.13. Encarregado pelo Tratamento de Dados Pessoais (DPO).....   | 8         |
| 3.14. Direitos dos Titulares de Dados Pessoais.....              | 9         |
| 3.15. Conformidade e Sanções.....                                | 9         |
| <b>4. Melhoria Contínua.....</b>                                 | <b>10</b> |
| <b>5. Aprovação e Vigência.....</b>                              | <b>10</b> |

## 1. Objetivo

Estabelecer diretrizes e compromissos que garantam a proteção das informações da Aligera Equipamentos Digitais Ltda, assegurando sua confidencialidade, integridade e disponibilidade, em conformidade com a ISO/IEC 27001 e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), além de estabelecer os fundamentos que garantem o atendimento ao ato 16417/24 da ANATEL.

Esta política define a base para o Sistema de Gestão da Segurança da Informação e Privacidade e orienta todos os colaboradores, parceiros e fornecedores sobre o uso e a proteção dos ativos de informação da empresa.

## 2. Escopo

Esta política aplica-se a:

- Todos os **colaboradores, terceiros e prestadores de serviço** que tenham acesso a informações da empresa;
- Todos os **ativos de informação** da Aligera, incluindo:
  - Código-fonte e repositórios de software;
  - Bancos de dados internos e de clientes;
  - Desenhos técnicos de produtos;
  - Estratégias comerciais e documentos internos;
  - Sistemas corporativos (ERP, suporte técnico, e-mail, etc.);
  - Equipamentos de rede, servidores e ambientes em nuvem;

### 3. Diretrizes e Princípios Gerais

### 3.1. Comprometimento da Direção

A Alta Direção da Aligera:

- Reconhece a segurança da informação como um **valor estratégico** e um diferencial competitivo;
- Assegura os recursos necessários para a implementação e melhoria contínua do SGSIP;
- Compromete-se com o **cumprimento das leis, normas e contratos aplicáveis**;
- Apoia a adoção de **princípios de Security by Design e Privacy by Design** em todos os produtos e serviços, incluindo sistemas em nuvem.

### 3.2. Confidencialidade, Integridade e Disponibilidade (CID)

- **Confidencialidade:** apenas pessoas autorizadas podem acessar as informações.
- **Integridade:** as informações devem ser precisas e protegidas contra alterações indevidas.
- **Disponibilidade:** as informações e sistemas devem estar disponíveis quando necessários para a operação.

### 3.3. Responsabilidades

**Todos os colaboradores** devem proteger as informações da empresa, obedecendo às normas internas.

**Gestores** devem assegurar que suas equipes sigam as práticas de segurança aplicáveis.

**O Gestor de Segurança da Informação (GSI)** é responsável por coordenar o SGSIP e apoiar a direção na tomada de decisões de segurança.

### 3.4. Gestão de Riscos de Segurança da Informação

A Aligera mantém um processo contínuo de avaliação e tratamento de riscos que possam impactar a confidencialidade, integridade e disponibilidade das informações.

Os riscos são identificados, avaliados e tratados considerando:

- A probabilidade de ocorrência e o impacto potencial;
- A importância dos ativos de informação para o negócio;
- Os requisitos legais, regulatórios e contratuais aplicáveis.

O processo de gestão de riscos segue metodologia aprovada pela Direção e é revisto periodicamente para refletir mudanças tecnológicas, organizacionais ou regulatórias. Como parte desse processo a organização deve manter uma avaliação sistemática de identificação e acompanhamento de vulnerabilidades técnicas, incluindo a consulta periódica a bases de dados de CVE (Common Vulnerabilities and Exposures) reconhecidas, tais como:

- Banco Nacional de Datos de Vulnerabilidades (BND)
- MITRE CVE (cve.org)
- National Vulnerability Database (NVD)

As consultas devem ser realizadas com frequência mínima mensal, e as vulnerabilidades identificadas devem ser avaliadas quanto ao seu impacto nos ativos da organização, integrando-se ao processo de gestão de riscos.

As decisões sobre o tratamento de riscos são registradas e acompanhadas pelo Gestor de Segurança da Informação (GSI).

### 3.5. Controle de Acesso

- O acesso às informações e sistemas será concedido com base no **princípio do menor privilégio**.
- Cada usuário é responsável pelo uso seguro de suas credenciais.
- É proibido compartilhar senhas ou deixar sistemas autenticados sem supervisão.
- O acesso administrativo deve ser **registrado e monitorado**.

### 3.6. Proteção de Código-Fonte e Propriedade Intelectual

- O código-fonte dos produtos da Aligera é classificado como **informação confidencial**.
- Deve ser armazenado apenas em **repositórios corporativos autorizados** (com versionamento e controle de acesso).
- É vedada a cópia ou armazenamento local sem autorização formal.

### 3.7. Backup e Continuidade

- Todos os dados críticos devem possuir cópias de segurança diárias, com armazenamento local e em nuvem.
- Backups devem ser criptografados e testados regularmente.
- A empresa manterá planos de continuidade e recuperação para garantir o retorno rápido das operações em caso de falhas.

### 3.8. Uso Aceitável de Ativos

- Recursos corporativos (equipamentos, internet, e-mail, sistemas) devem ser utilizados **exclusivamente para fins profissionais**.
- É proibido instalar software não autorizado, acessar conteúdo indevido ou conectar dispositivos pessoais à rede corporativa sem aprovação.
- A empresa se reserva o direito de **monitorar e auditar o uso de sistemas e redes**.

### 3.9. Conformidade de Fornecedores e Parceiros

A Aligera assegura que **fornecedores, prestadores de serviço e parceiros comerciais** que tenham acesso a informações corporativas ou de clientes **cumpram padrões adequados de segurança da informação e privacidade.**

Os contratos com terceiros devem prever cláusulas sobre:

- Confidencialidade e uso adequado das informações;
- Proteção de dados pessoais, conforme a LGPD;
- Notificação em caso de incidentes de segurança;
- Possibilidade de auditoria ou verificação de conformidade.

Antes da contratação, fornecedores críticos passam por avaliação de risco e conformidade, conduzida pelo GSI em conjunto com as áreas responsáveis.

### 3.10. Desenvolvimento e Serviços em Nuvem

- Todos os produtos e sistemas desenvolvidos devem adotar **práticas de desenvolvimento seguro e testes de vulnerabilidade**.
- Os serviços em nuvem da Aligera devem incluir mecanismos de:
  - **Autenticação segura** (MFA, tokens, certificados);
  - **Criptografia de dados em trânsito e em repouso**;
  - **Registro e rastreabilidade de ações administrativas**;
  - **Isolamento entre clientes (multi-tenancy seguro)**;
  - **Conformidade com a LGPD** quanto ao tratamento de dados pessoais.

### 3.11. Gestão de Incidentes de Segurança

- Todo incidente de segurança (por exemplo, vazamento, acesso indevido, malware, falha de backup) deve ser **reportado imediatamente** ao Gestor de Segurança da Informação.
- A empresa manterá um **procedimento de resposta a incidentes** com etapas de identificação, contenção, análise, correção e aprendizado.

### 3.12. Treinamento e Conscientização

- Todos os colaboradores participarão de treinamentos periódicos sobre segurança e privacidade.
- A conscientização será reforçada por meio de comunicados, campanhas internas e avaliações.

### **3.13. Encarregado pelo Tratamento de Dados Pessoais (DPO)**

Em conformidade com a Lei Geral de Proteção de Dados (LGPD), a Aligera nomeia um Encarregado pelo Tratamento de Dados Pessoais (DPO), responsável por:

- Receber comunicações de titulares e da Autoridade Nacional de Proteção de Dados (ANPD);
- Orientar colaboradores e contratados sobre práticas de proteção de dados;
- Apoiar as áreas da empresa na conformidade com a LGPD;
- Atuar em conjunto com o Gestor de Segurança da Informação na resposta a incidentes de privacidade.

O contato com o DPO estará disponível nos canais oficiais da empresa.

### **3.14. Direitos dos Titulares de Dados Pessoais**

A Aligera assegura aos titulares de dados pessoais todos os direitos previstos na LGPD, incluindo:

- Confirmação da existência de tratamento;
- Acesso aos dados pessoais tratados;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários;
- Portabilidade dos dados a outro fornecedor de serviço;
- Informação sobre compartilhamento com terceiros;

- Revogação do consentimento.

A empresa compromete-se a oferecer canais de comunicação acessíveis para exercício desses direitos, observando prazos legais e registros das solicitações atendidas.

### 3.15. Conformidade e Sanções

- O não cumprimento desta política pode resultar em medidas disciplinares, conforme a legislação e os contratos de trabalho.
- Violações graves podem resultar em sanções legais ou rescisão contratual.

## 4. Melhoria Contínua

A política será **revisada anualmente** ou sempre que houver:

- Mudanças significativas nos sistemas, estrutura ou legislação aplicável;
- Ampliação dos serviços, especialmente com o início das operações em nuvem;
- Resultados de auditorias internas ou externas que recomendem ajustes.

## 5. Aprovação e Vigência

Esta Política de Segurança da Informação foi aprovada pela **Alta Direção da Aligera Equipamentos Digitais Ltda** e entra em vigor na data de sua publicação.

Todos os colaboradores e parceiros devem estar cientes e em conformidade com seu conteúdo.