

**UNIVERSIDADE TIRADENTES**  
**ANÁLISE E DESENVOLVIMENTO DE SISTEMAS**  
**AUDITORIA EM SISTEMAS DE INFORMAÇÃO**

**ALISSON ANDRADE NUNES**

**OBJETIVO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS**

**Aracaju**

**2024**

## **FICHAMENTO**

### **Objetivo da Política de Segurança da Informação nas Empresas**

#### **Referências:**

- Alura. "Política de segurança da informação para empresas de tecnologia."
- Infnet. "Política de Segurança da Informação: guia completo."
- Siteware. "O que é e como fazer uma política de segurança da informação?"
- HLTI. "Política De Segurança Da Informação: O Que É E Como Criá-la."

#### **Resumo:**

A política de segurança da informação nas empresas tem como principal objetivo proteger os ativos de informação contra acessos não autorizados, alterações indevidas e interrupções nos serviços, assegurando a confidencialidade, integridade e disponibilidade das informações. Essa política é crucial para prevenir prejuízos financeiros, legais e de reputação, bem como para cumprir com regulamentações como a Lei Geral de Proteção de Dados Pessoais (LGPD). **Palavras-chave:**

- Segurança da Informação
- Confidencialidade
- Integridade
- Disponibilidade
- LGPD
- Proteção de dados
- TI

#### **Conteúdo:**

- **Política de Segurança da Informação (PSI):** Conjunto de diretrizes e regras para gerenciar e proteger os ativos de informação.
- **Confidencialidade, Integridade e Disponibilidade (CID):** Pilares fundamentais da segurança da informação.

#### **Citações:**

"A política de segurança da informação é fundamental para reduzir os riscos de ataques cibernéticos e, por consequência, evitar as perdas financeiras e os prejuízos à reputação de imagem da empresa"

"As políticas de segurança da informação são essenciais para proteger os ativos digitais de uma empresa e evitar prejuízos financeiros e de reputação"

### **Discussão:**

- A implementação de uma política de segurança da informação eficaz requer a participação de todas as áreas da empresa. É necessário um diagnóstico inicial para identificar ameaças e vulnerabilidades e, em seguida, definir normas claras sobre o uso e proteção dos dados.
- A conformidade com a LGPD é um aspecto crucial, pois além de proteger os dados, evita multas e sanções legais.

### **Conclusões:**

A auditoria de TI é uma ferramenta essencial para a gestão de riscos e para a governança de TI. O auditor de TI tem um papel fundamental na garantia da segurança e confiabilidade dos sistemas de informação.

### **Recomendações:**

- **Treinamento e Conscientização:** Treinar regularmente os colaboradores sobre as políticas e práticas de segurança da informação.
- **Monitoramento Contínuo:** Revisar e atualizar a política periodicamente para refletir mudanças tecnológicas e organizacionais.

### **Observações:**

- A política de segurança da informação não é um documento estático; ela deve evoluir conforme a empresa cresce e novas ameaças surgem.
- O comprometimento da alta administração é essencial para o sucesso da implementação da política