



UDESC - Universidade do Estado de Santa Catarina

# Segurança Aplicada ao Desenvolvimento

Manual de Boas Práticas em Segurança da Informação

---

Autor

**Igor Rismo Coelho**

5º Período - TADS  
Campus Florianópolis

20 de setembro de 2025

## Apresentação

No mundo corporativo de hoje, a informação é um ativo valioso, impactando desde a definição de estratégias até a eficiência operacional. A capacidade de uma empresa de atrair e reter clientes, assim como de otimizar seus processos internos, está diretamente ligada à qualidade e ao uso de seus dados.

Essa importância, no entanto, expõe as informações a riscos constantes, como perdas accidentais ou acessos não autorizados. Incidentes desse tipo podem causar sérios prejuízos, tornando essencial que as organizações invistam em segurança. Para proteger esses dados de forma eficaz, é preciso entender em que etapas eles estão mais vulneráveis e quais tipos de informação demandam maior atenção. Este material abordará os conceitos essenciais de segurança da informação, explorando o valor dos dados para as empresas, o ciclo de vida da informação e os métodos para sua classificação, oferecendo uma base sólida para a proteção de ativos digitais.

Este manual é parte da nossa campanha de conscientização e funciona como a Política de Segurança da Informação para todos os colaboradores. Seu objetivo é orientar sobre o uso responsável dos nossos sistemas e proteger os ativos de informação, que são essenciais para o nosso negócio. A segurança é um esforço contínuo e a responsabilidade é de todos nós.



## 1. O Valor da Informação como Ativo da Empresa

No contexto da segurança, um ativo é qualquer recurso que tenha valor para a organização ou que processe informações. Nossos dados, informações e conhecimento são alguns dos ativos mais importantes, pois seu valor aumenta à medida que são usados e compartilhados. Além disso, a combinação de informações nos dá uma visão sistêmica da empresa.

A informação é um ativo valioso, mas também pode ser perecível, ou seja, perde parte de seu valor à medida que o tempo passa. O uso de dados imprecisos ou o excesso de informação também podem ser prejudiciais.

Para proteger nossos ativos, as informações são classificadas com base em seu nível de sensibilidade, de acordo com a ISO 27001:

- **Pública:** Informações que podem ser de conhecimento geral, dentro e fora da empresa, sem causar prejuízo.
- **Interna:** Informações que precisam de sigilo e restrições de acesso, embora a divulgação não cause danos graves.
- **Confidencial:** Informações que devem ser mantidas nos limites da empresa. O acesso não autorizado pode gerar prejuízos, quebra de confiança com o cliente e vantagem para a concorrência.
- **Secreta:** Informações críticas que exigem o maior esforço de segurança e acesso restrito. Sua manipulação exige extremo cuidado.



## **2. Principais Ameaças aos Nossos Ativos**

As ameaças à segurança da informação podem vir de fontes internas e externas. Segundo Dantas (2011), as principais ameaças incluem:

- Vírus, worm, cavalo de tróia (trojan horse), que se propagam e danificam sistemas.
- Phishing, pharming e spyware, que são usados para roubar dados.
- Acesso não autorizado, má conduta e abuso de privilégios de acesso por funcionários.
- Roubo de hardware e de dados confidenciais.
- Ataques de negação de serviço e invasão de sistemas.

Além dessas ameaças tecnológicas, a principal vulnerabilidade está nas pessoas. A engenharia social é uma técnica que não usa recursos tecnológicos, mas explora a natureza humana para manipular e obter informações. As táticas mais comuns incluem a criação de um senso de urgência, intimidação ou falsa confiança.

Existem outras táticas importantes, como:

- Shoulder surfing: Olhar por cima do ombro para ver senhas ou informações.
- Mergulho no lixo: Procurar documentos descartados em lixeiras.



### 3. Os Pilares e o Ciclo de Vida da Informação

A segurança da informação se baseia em três pilares, que garantem a proteção em diferentes momentos:

- **Confidencialidade:** Evitar que as informações sejam divulgadas para pessoas, recursos ou processos não autorizados. Isso pode ser feito com o uso de criptografia e controles de acesso.
- **Integridade:** Garantir que os dados estejam corretos, consistentes e confiáveis. Métodos como hashing, validação de dados e verificação de consistência são essenciais.
- **Disponibilidade:** Garantir que os dados e informações estejam acessíveis para os usuários autorizados quando necessário. Isso inclui manter sistemas atualizados e monitoramento constante.

A informação também tem um ciclo de vida que, segundo Sêmola (2003), se divide em quatro fases:

- **Manuseio:** O momento de criação e manipulação da informação.
- **Armazenamento:** Onde a informação é guardada em arquivos físicos ou em bancos de dados de sistemas.
- **Transporte:** A transferência da informação (por e-mail, correspondência etc.).
- **Descarte:** O ato de descartar a informação quando ela não é mais relevante.



## **4. Boas Práticas: Nosso Guia de Ação**

A proteção contra ataques e fraudes exige a utilização de diversas ferramentas e a adoção de medidas de segurança. Nossas defesas incluem tecnologia, políticas e práticas e, o mais importante, a conscientização das pessoas.

O que você pode fazer:

### **Gerenciamento de Senhas**

- Use senhas fortes, com variação de letras maiúsculas e minúsculas, números e símbolos.
- Nunca compartilhe suas senhas com ninguém.
- Altere suas senhas periodicamente para manter a segurança.

### **Uso de E-mail e Internet**

- Nunca abra anexos de e-mails de pessoas desconhecidas.
- Seja cauteloso ao abrir anexos, mesmo de pessoas conhecidas, e não preencha cadastros de pesquisas enviados por e-mail.
- Verifique sempre o endereço do link antes de clicar para garantir que não é um site fraudulento.
- Não use e-mails particulares ou acesse contas pessoais em máquinas da empresa se isso for contra a política interna.
- Não divulgue informações da empresa em redes sociais.

## **4. Boas Práticas: Nosso Guia de Ação (continuação)**

A proteção contra ataques e fraudes exige a utilização de diversas ferramentas e a adoção de medidas de segurança. Nossas defesas incluem tecnologia, políticas e práticas e, o mais importante, a conscientização das pessoas.

O que você pode fazer:

### **Proteção do Equipamento e dos Dados**

- Sempre utilize softwares originais e mantenha os sistemas operacionais atualizados para corrigir vulnerabilidades.
- Bloqueie a tela do seu computador quando se afastar da mesa.
- Não utilize hardwares móveis, como pendrives ou HDs externos, em máquinas da empresa se isso for proibido.
- Trate todos os documentos com cuidado, desde o manuseio até o descarte, para evitar que informações confidenciais sejam perdidas. A formatação completa de máquinas antes do descarte é essencial.
- Realize backups periódicos dos dados, conforme a política da empresa, para garantir que as informações não sejam perdidas.



## 5. Conclusão

A segurança da informação não é apenas um trabalho do setor de TI. É um processo contínuo e cíclico que exige a colaboração de todos. Ao seguir estas boas práticas, você ajuda a construir uma cultura de segurança que protege nossos dados, nossa reputação e o futuro do nosso negócio. Se tiver qualquer dúvida, procure o setor de Tecnologia da Informação.

### Referências

- FecomercioSP e Ricupero, Sérgio Roberto. Cartilha de Segurança da Informação para Empresas.
- Dantas, Marcos R. A. Segurança da Informação e Segurança Computacional. Rio de Janeiro: Editora Ciência Moderna, 2011.
- Sêmola, Marcos. Gestão da Segurança da Informação: uma visão prática. Rio de Janeiro: Editora Ciência Moderna, 2003.

