

CURSO SUPERIOR DE ADS

Cibersegurança e Ética Digital: Desafios da Era da Informação



Prof. Fernando Marlon Soares Figueiredo
Disciplina: Introdução à Computação e suas aplicações



Introdução

Vivemos na **era da informação**, um período marcado pela troca constante de dados, pela conectividade global e pela presença da tecnologia em praticamente todos os aspectos da vida.

Com isso, surgem **novos desafios** relacionados à **segurança digital** e à **ética no uso da informação**.

Nesta aula, vamos compreender:

- ❖ O que é **cibersegurança** e sua importância.
- ❖ Os principais **tipos de ameaças digitais**.
- ❖ As boas práticas de **proteção de dados e privacidade**.
- ❖ O papel da **ética digital** e os **impactos sociais e legais** do mau uso da tecnologia.



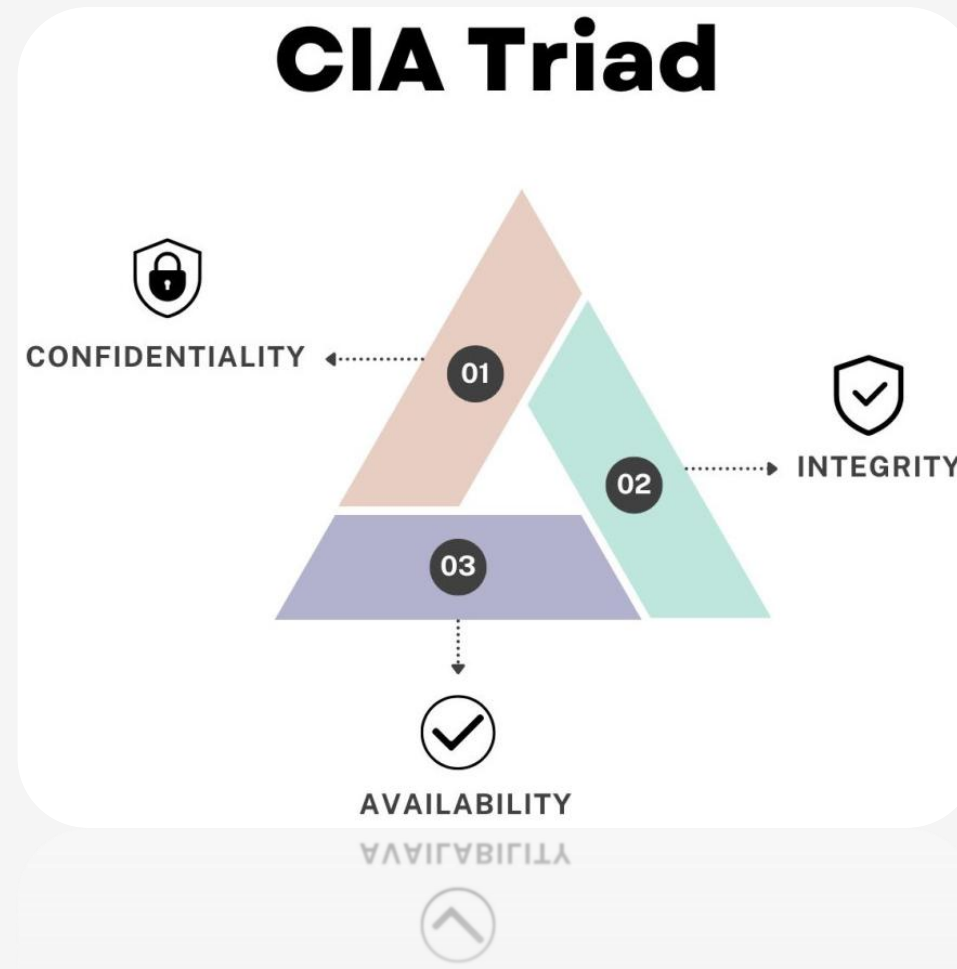
O que é Cibersegurança

Cibersegurança é o conjunto de práticas, tecnologias e políticas voltadas à **proteção de sistemas, redes e dados** contra acessos não autorizados, ataques ou danos.

Ela busca **garantir três princípios fundamentais**, conhecidos como **CIA Triad**:

1. **Confidencialidade:** assegurar que as informações sejam acessadas apenas por pessoas autorizadas.
2. **Integridade:** garantir que os dados não sejam alterados de forma indevida.
3. **Disponibilidade:** assegurar que as informações e sistemas estejam sempre acessíveis quando necessários.

Esses três pilares formam a base de toda a segurança da informação moderna.



Principais Ameaças Digitais

Com a popularização da internet, as ameaças digitais se tornaram cada vez mais sofisticadas. Algumas das mais comuns são:

- ❖ **Vírus e Malwares:** programas maliciosos que podem danificar arquivos, roubar informações ou comprometer o desempenho do sistema.
- ❖ **Phishing:** tentativa de enganar o usuário para que revele senhas, dados bancários ou outras informações sigilosas.
- ❖ **Ransomware:** tipo de malware que sequestra dados e exige pagamento para liberá-los.
- ❖ **Ataques de Engenharia Social:** manipulação psicológica que explora a confiança das pessoas para obter acesso a sistemas ou dados.
- ❖ **Ataques DDoS (Negação de Serviço):** sobrecarregam servidores, tornando sites ou serviços indisponíveis.

Essas ameaças afetam tanto **usuários comuns** quanto **empresas e governos**, podendo causar grandes prejuízos financeiros e reputacionais.



Proteção e Boas Práticas de Segurança

A cibersegurança depende tanto de **tecnologia** quanto de **comportamento humano**.

Entre as principais práticas preventivas estão:

- ❖ Usar **senhas fortes** e diferentes para cada conta.
- ❖ Ativar a **autenticação em dois fatores (2FA)**.
- ❖ Manter **softwares** e antivírus atualizados.
- ❖ Evitar clicar em **links suspeitos** ou **baixar arquivos de origem duvidosa**.
- ❖ Fazer **backup** regular dos dados importantes.
- ❖ Não compartilhar **informações pessoais em redes abertas** ou públicas.

Além disso, as empresas devem investir em **políticas de segurança da informação, treinamentos periódicos** e **monitoramento constante de sistemas**.



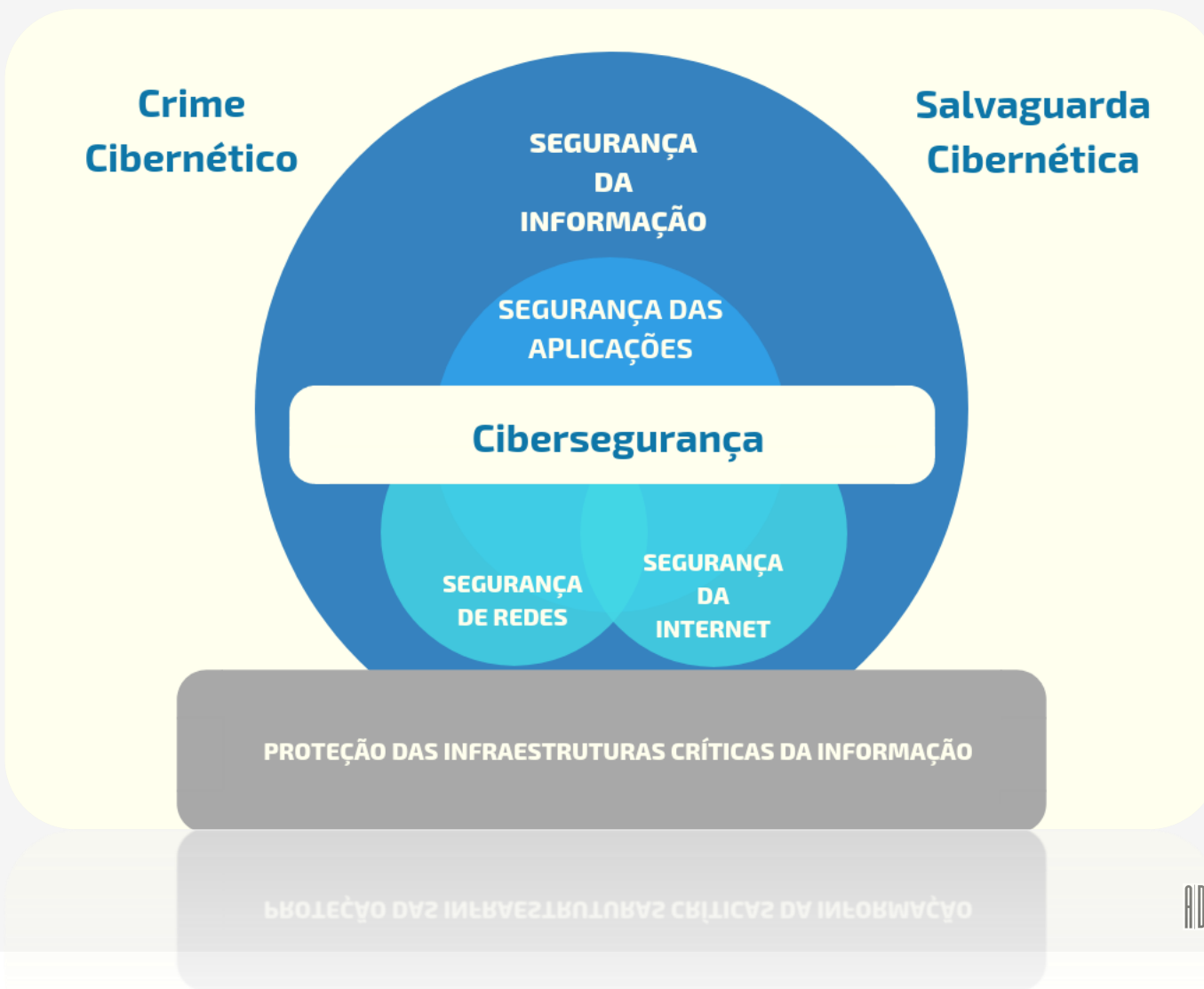
Segurança da Informação x Cibersegurança

Embora estejam relacionadas, **segurança da informação** e **cibersegurança** não são exatamente o mesmo conceito:

Segurança da Informação: proteção de dados em qualquer formato — físico ou digital.

Cibersegurança: proteção do ambiente digital, como redes, sistemas e dispositivos conectados à internet.

Em resumo, toda cibersegurança faz parte da segurança da informação, mas nem toda segurança da informação se limita ao meio digital.



Ética Digital

A **ética digital** trata do **comportamento responsável, consciente e moralmente correto** no uso das tecnologias e da internet.

Ela envolve **respeito à privacidade, autoria de conteúdo, direitos digitais e uso responsável dos dados**.

Com o avanço da tecnologia, surgem dilemas éticos cada vez mais complexos, como:

- ❖ O limite entre **segurança pública** e **privacidade individual**.
- ❖ O uso ético da **inteligência artificial** e **dos dados pessoais**.
- ❖ A responsabilidade sobre **fake news, discurso de ódio e plágio digital**.

Ser ético no ambiente digital significa **agir com integridade**, respeitando leis, direitos e o impacto das nossas ações no mundo virtual e real.



Legislação e Proteção de Dados no Brasil

No Brasil, a **Lei Geral de Proteção de Dados (LGPD)**, criada em 2018, estabelece regras sobre **como empresas e instituições devem coletar, armazenar e usar informações pessoais**.

Principais pontos:

- ❖ **Consentimento:** os dados só podem ser usados com a autorização do titular.
- ❖ **Finalidade:** o uso deve ter um propósito legítimo e claro.
- ❖ **Direito de acesso e exclusão:** o cidadão pode consultar, corrigir ou excluir seus dados de bancos de dados.
- ❖ **Responsabilidade:** quem coleta dados deve protegê-los contra vazamentos.

A LGPD se inspira em leis internacionais, como o **GDPR (General Data Protection Regulation)** da União Europeia, reforçando a importância global da privacidade digital.



Crimes Cibernéticos

Crimes digitais são infrações cometidas por meio de dispositivos eletrônicos, redes ou sistemas informatizados.

Alguns exemplos:

- ❖ **Invasão de sistemas** e roubo de informações sigilosas.
- ❖ **Golpes financeiros e clonagem de cartões.**
- ❖ **Distribuição de conteúdo ilegal** (pornografia infantil, pirataria, etc.).
- ❖ **Difamação e exposição indevida nas redes sociais.**

A legislação brasileira trata desses crimes principalmente na **Lei 12.737/2012 (Lei Carolina Dieckmann)**, que tipifica a invasão de dispositivos, e no **Marco Civil da Internet (Lei 12.965/2014)**, que define direitos e deveres no uso da rede.



Desafios da Era da Informação

Com a transformação digital, enfrentamos um cenário em que **dados se tornaram o principal recurso do mundo moderno**.

Os desafios atuais incluem:

- ❖ O aumento do **cibercrime** e da **espionagem digital**.
- ❖ A manipulação de informações (fake news, deepfakes).
- ❖ A dificuldade em equilibrar **liberdade de expressão e privacidade**.
- ❖ A dependência crescente de tecnologias conectadas, como **IoT e IA**.

Esses desafios exigem **profissionais preparados, educação digital e consciência ética**, para que a tecnologia continue sendo uma ferramenta de progresso e não de risco.



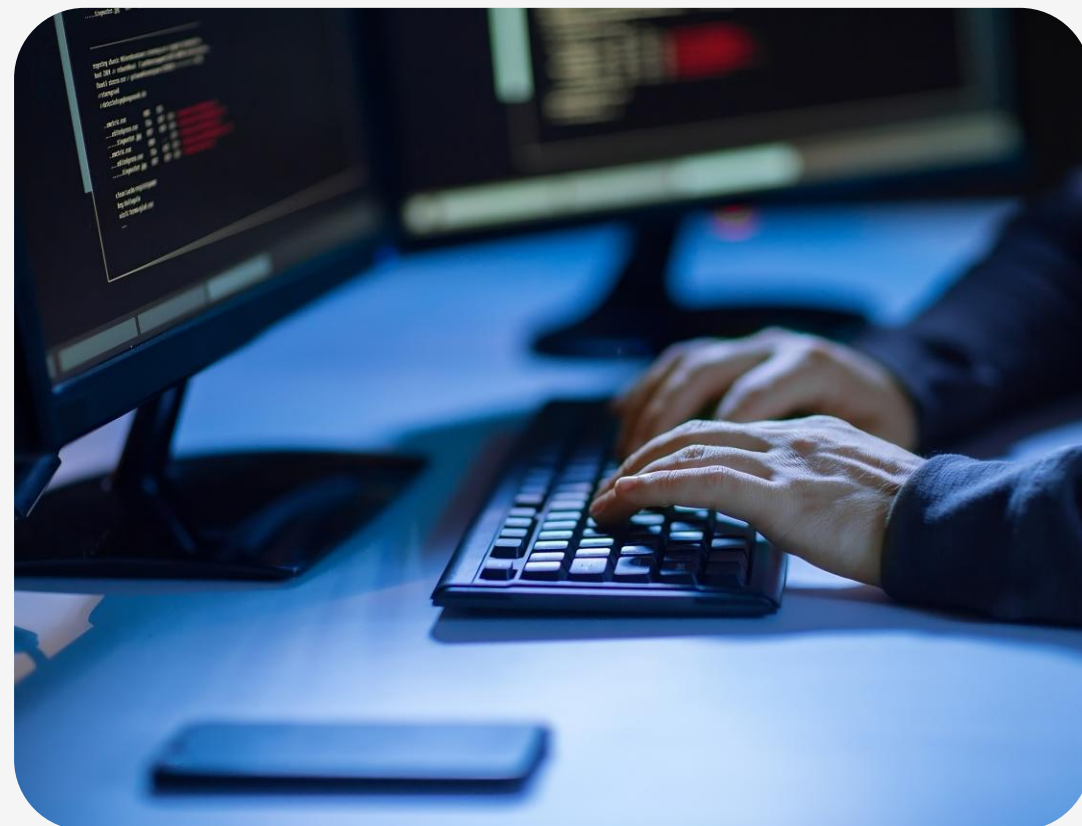
O Papel do Profissional de TI

O profissional de TI deve atuar não apenas como técnico, mas também como **guardião da informação**.

Suas responsabilidades incluem:

- ❖ Implementar práticas seguras em sistemas e aplicações.
- ❖ Garantir conformidade com normas e legislações.
- ❖ Promover o uso ético e transparente da tecnologia.
- ❖ Educar usuários sobre riscos e boas práticas digitais.

Mais do que dominar ferramentas, o profissional moderno precisa compreender o **impacto social da tecnologia** e contribuir para um ambiente digital **seguro e ético**.



Conclusão

A **cibersegurança e a ética digital** são temas centrais na sociedade da informação.

Proteger dados, respeitar a privacidade e agir com responsabilidade digital são atitudes que garantem **confiança, segurança e cidadania tecnológica**.

Em um mundo onde “dados são o novo petróleo”, cabe a cada um de nós profissionais, empresas e cidadãos **agir com consciência e ética** no uso da informação.

