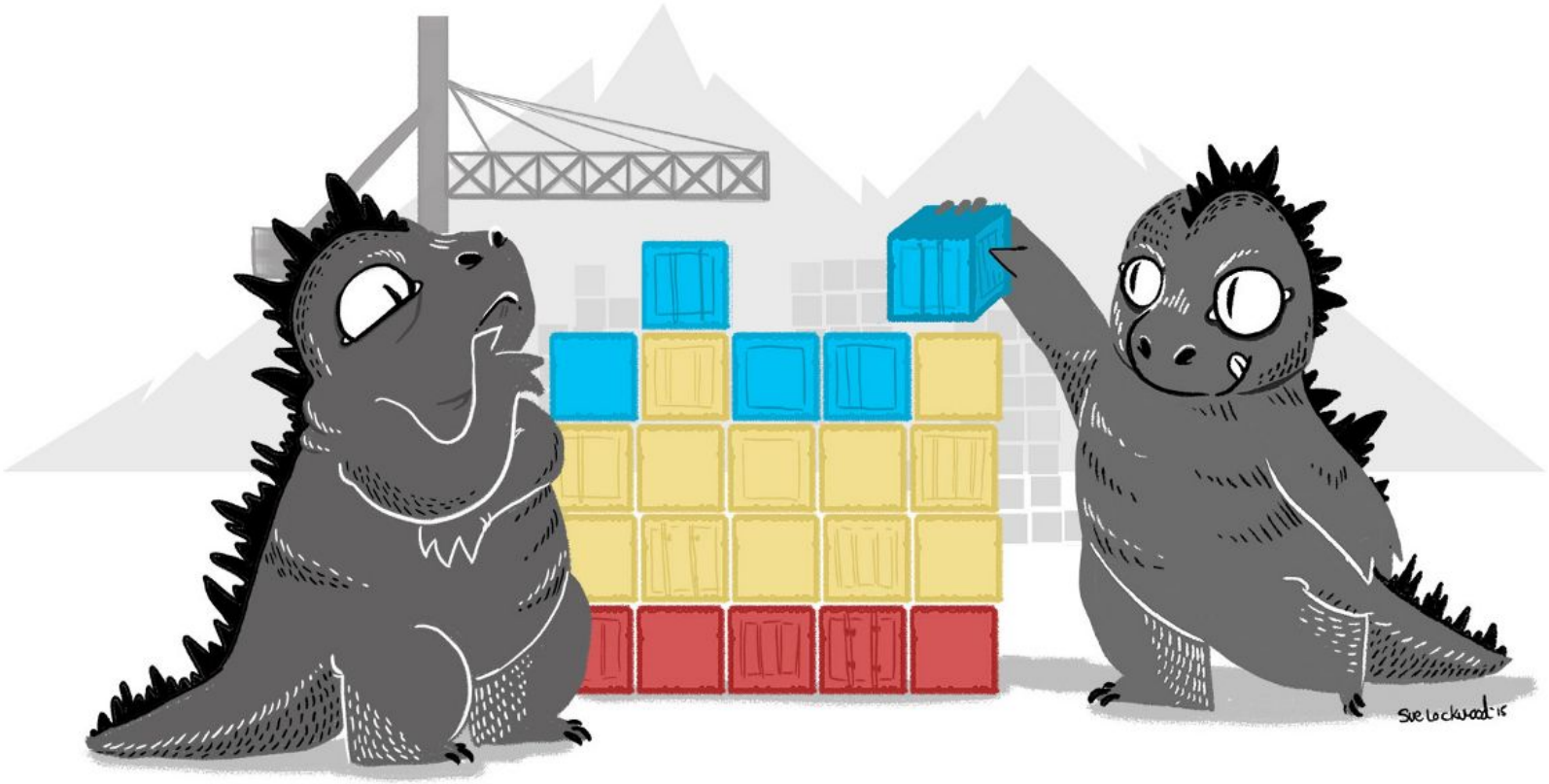


Segurança da Informação em Termos Práticos

Disciplina: Sistemas de Informações Gerenciais

Prof. Bruno Miguel Groth

2º Semestre/2024

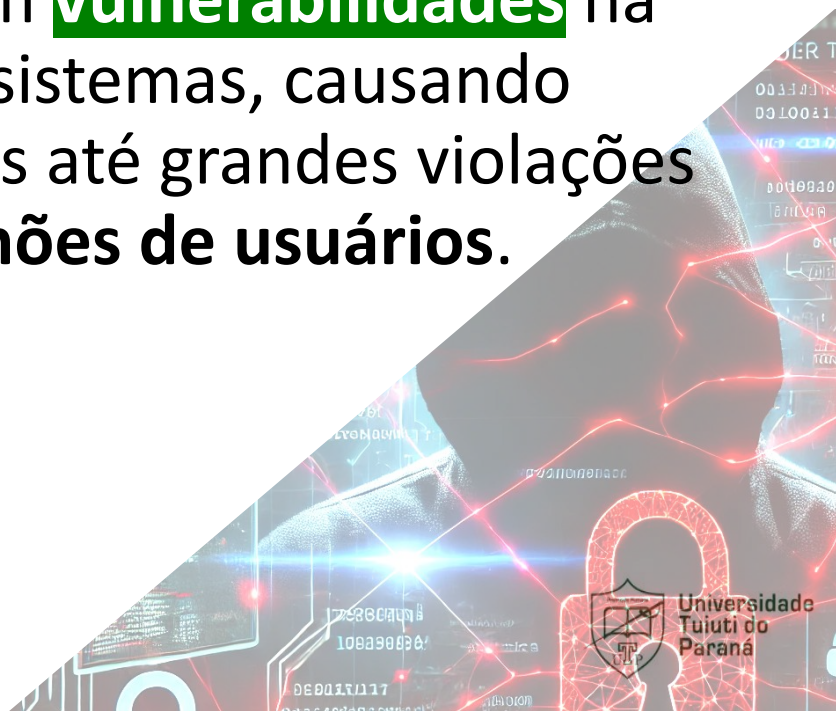
Universidade Tuiuti do Paraná

Objetivos da Aula

- Aprofundar na Tríade da Segurança da Informação.
- Aprender a aplicar medidas de segurança em sistemas na prática.
- Conhecer técnicas e ferramentas práticas para garantia de segurança em ambientes de tecnologia.

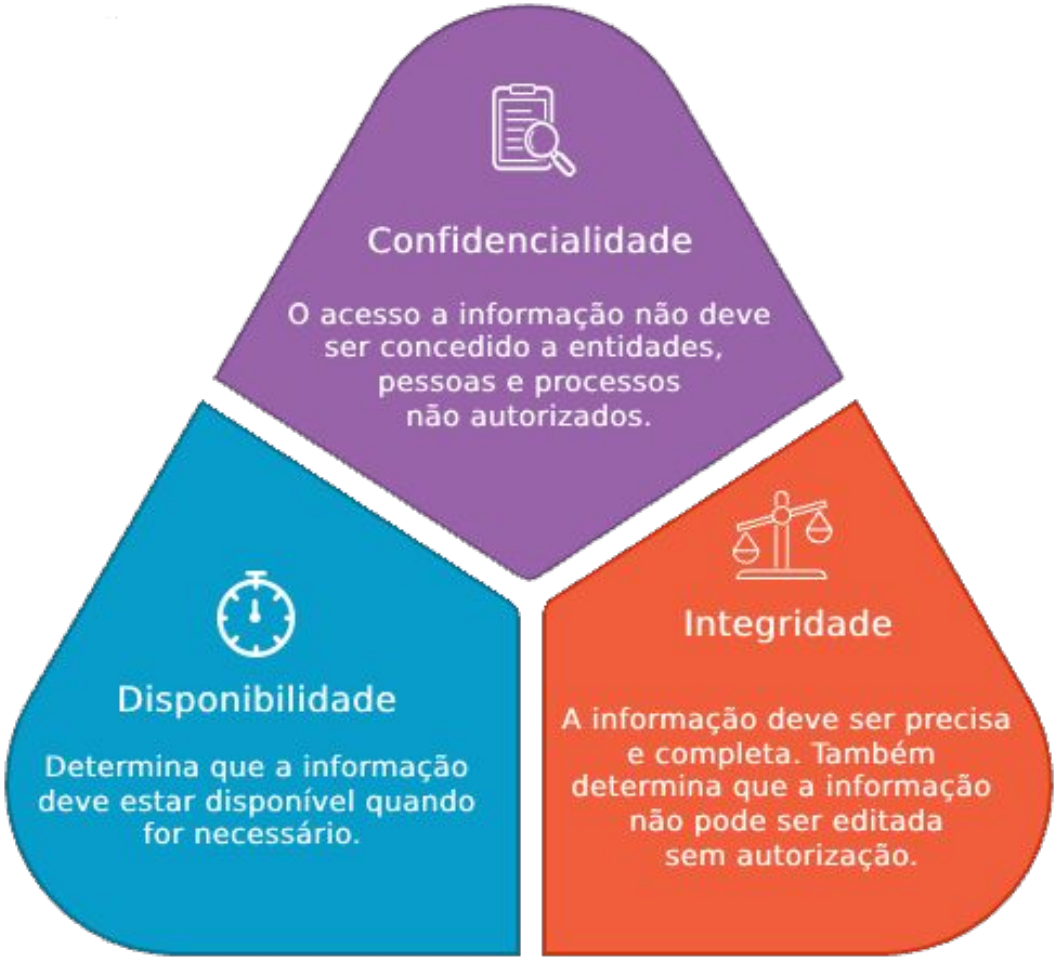
Pudemos observar que...

- Hoje, a informação é um dos ativos mais valiosos para qualquer organização.
- Na última aula, pudemos notar que os ataques cibernéticos estão em **constante evolução** e que diversas **ameaças** exploram **vulnerabilidades** na **infraestrutura** e **rede** dos sistemas, causando desde pequenos incidentes até grandes violações de dados, que afetam **milhões de usuários**.



Assim sendo, vamos aprender a aplicar medidas de segurança eficientes em ambientes de tecnologia.

Tríade da Segurança da Informação *(CIA Triad)*



Universidade Tuiuti do Paraná

É utilizando a Tríade como princípio, que toda a estratégia e solução de segurança é projetada.

Segurança Física e Lógica

Segurança Física

- Envolve a proteção dos ativos **físicos** da organização contra ameaças como roubo, vandalismo, desastres naturais ou falhas de hardware.
- Também garante que o acesso não autorizado aos sistemas críticos seja evitado.
- São exemplos: Cartões de Identificação, Biometria e câmeras de Vigilância e Alarmes.

- A **segurança física** também envolve medidas específicas de manutenção dos ativos, como o **controle de temperatura** (ambientes resfriados, com temperatura monitorada), alarmismo contra incêndios, estabilizadores e **backups de energia** (como geradores e nobreaks) e **sistemas de bloqueio** para impedir acessos físicos não autorizados.

Segurança Lógica

- Se refere às **tecnologias** e **processos** que protegem a integridade e a confidencialidade dos dados em sistemas computacionais.
- Isso inclui o controle de acesso aos dados, as redes e os sistemas de computação.
- Exemplos:
  - **Autenticação:** senhas, tokens e biometria para confirmação de identidade.
  - **Autorização:** Controle de acesso discricionário (**DAC**), Baseado em Função (**RBAC**) e Baseado em Atributos (**ABAC**).
    - Active Directory (AD)

Quais ferramentas podemos utilizar para blindar redes, sistemas e ambientes de tecnologia contra ameaças cibernéticas?

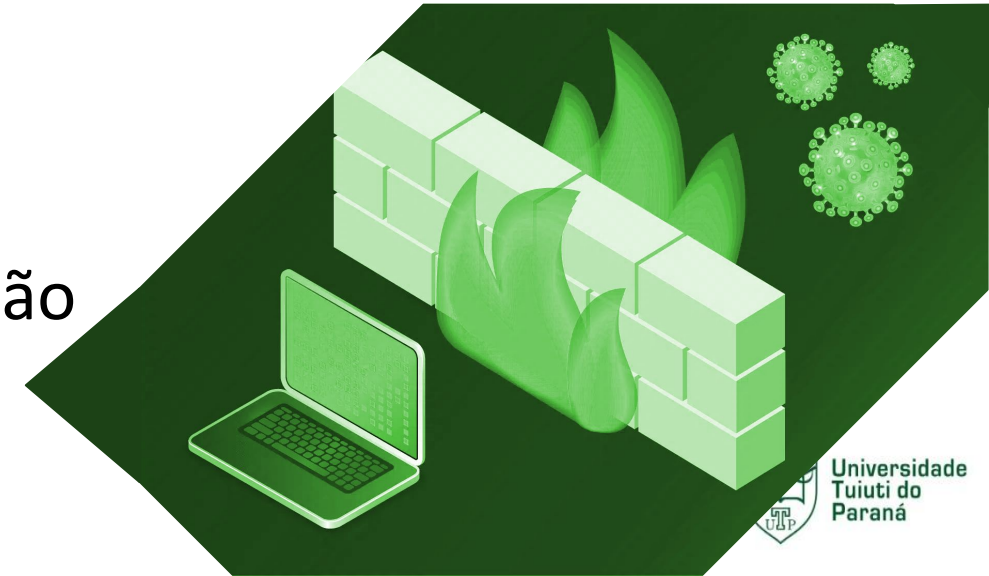
Ferramentas de Segurança

Firewalls

- O **Firewall** é uma ferramenta essencial para proteger **redes** contra **tráfego indesejado ou malicioso**. Ele pode ser implementado como **hardware** (um dispositivo dedicado a essa finalidade) ou **software** (um programa executado no computador ou servidor).

São exemplos:

- Firewall de Rede
- Firewall de Aplicação
- Firewall de Próxima Geração
- Cisco, Palo Alto Networks



IDS/IPS

- **IDS** e **IPS** são ferramentas fundamentais para a detecção e resposta a incidentes de segurança.

- O **IDS** (Sistema de *Detecção* de Intrusão) **monitora** o tráfego de rede e envia **alertas** quando atividades suspeitas são detectadas.

  Ele não interfere diretamente no tráfego - é uma ferramenta passiva.

- Por outro lado, o **IPS** (Sistema de *Prevenção* de Intrusão) vai além e **bloqueia ativamente** as ameaças detectadas, tomando ações para impedir que o ataque cause danos.

Antivírus e Antimalwares

- Os **antivírus** e **antimalwares** são softwares que detectam e removem *vírus*, *worms*, *trojans*, *ransomware*, *spyware* e outros tipos de **malwares** que vimos na última aula.
- São essenciais e usados em larga escala em dispositivos pessoais, profissionais, educacionais, etc.

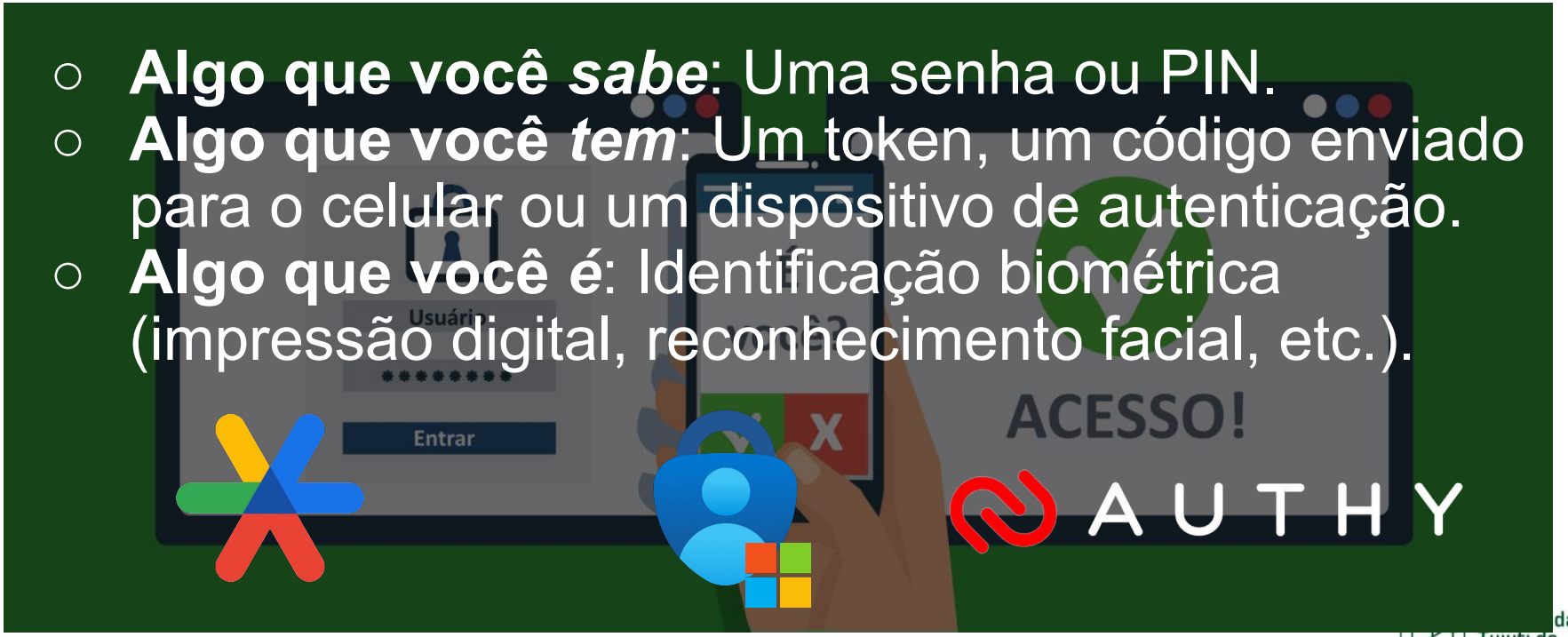
- **Antivírus**: Focam em **vírus** e **worms**, oferecendo escaneamento e limpeza de arquivos e sistemas.
- **Antimalwares**: Além de detectar vírus, podem identificar outras ameaças como *spyware, adware, ransomware e rootkits*, sendo uma solução mais abrangente.

Universidade Tuiuti do Paraná

Autenticação Multifatorial (MFA)

- A **autenticação multifatorial** (MFA) exige que os usuários forneçam **duas ou mais** formas de **verificação de identidade** para acessar sistemas críticos. A **MFA** pode incluir uma combinação de:

  - **Algo que você *sabe***: Uma senha ou PIN.
  - **Algo que você *tem***: Um token, um código enviado para o celular ou um dispositivo de autenticação.
  - **Algo que você *é***: Identificação biométrica (impressão digital, reconhecimento facial, etc.).



Backups

e Recuperação de Desastres

- Mesmo com todas essas medidas de prevenção, problemas **podem** e **irão ocorrer**.
- Sabendo disso, a realização de **backups** e **Planos de Recuperação de Desastres** (*Disaster Recovery Plan*) são medidas cruciais para garantir a continuidade dos negócios e a proteção dos dados em **situações adversas**.
- Esses processos desempenham um papel vital na mitigação de riscos.

Universidade Tuiuti do Paraná

Esses processos garantem que:

- Em caso de falhas, ataques cibernéticos ou desastres naturais, as **informações** essenciais possam ser recuperadas rapidamente, minimizando o impacto.

- Capacidade de Recuperação: ter um **plano de recuperação de desastres bem estruturado** permite restaurar **sistemas** e **operações** com agilidade, reduzindo o tempo de inatividade e minimizando prejuízos financeiros.

Tipos de Backup

- **Backup Completo:** Copia todos os dados, sendo a forma mais simples, mas também a mais demorada.

- **Backup Incremental:** Copia apenas as alterações feitas desde o último backup (completo ou incremental), economizando tempo e espaço.

- **Backup Diferencial:** Copia todas as mudanças feitas desde o último backup completo.

Recuperação de Desastres

- São planos e processos implementados para restaurar a operação normal após uma **interrupção catastrófica**. As métricas chave incluem:

- **RPO (Recovery Point Objective):** Define quanto tempo de dados a organização está disposta a perder após um incidente.
- **RTO (Recovery Time Objective):** Estabelece quanto tempo a organização tem para restaurar seus sistemas e operações.

Estudo de Casos

Caso de Ataque ao Superior Tribunal de Justiça (STJ) – 2020

- Em 2020, o Superior Tribunal de Justiça (STJ) foi alvo de um ataque cibernético ransomware.
- O ataque resultou na **paralisação de seus sistemas por vários dias**.
- O ataque criptografou dados importantes e afetou a operação do tribunal.
- De acordo com as investigações, o ataque foi realizado por hackers que pediram resgates financeiros para liberar os dados.

Caso SolarWinds (2020)

- O incidente **SolarWinds** é considerado um dos **maiores e mais sofisticados ataques cibernéticos da história**, envolvendo hackers **apoiados** por um **governo** e afetando centenas de organizações, incluindo agências governamentais dos Estados Unidos e empresas globais.
- O ataque foi descoberto em dezembro de **2020**, mas acredita-se que tenha começado no meio de 2019.
- O ataque envolveu um **software de gestão de rede**, chamado Orion, que foi comprometido por invasores russos.
- O ataque afetou mais de **18.000 organizações** ao redor do mundo.

Tendências de Segurança

Custo global do crime cibernético

$9.5 trilhões

O crime cibernético está projetado para gerar um impacto financeiro significativo, atingindo a marca de $9.5 trilhões em 2024.

Violações de dados por ransomware

32%

Ransomware é responsável por uma parcela considerável das violações de dados, com 32% das ocorrências relacionadas a esse tipo de ataque.

Desafios éticos emergentes

Adoção de IA generativa

A crescente adoção de IA generativa na segurança da informação traz desafios éticos que precisam ser abordados por profissionais da área.

Universidade Tuiuti do Paraná

Sessão de Q&A:
Dúvidas / colocações?

Universidade Tuiuti do Paraná

Bibliografia

- CRUZ, Tadeu. Sistemas de informações gerenciais: tecnologia da informação e a empresa do século XXI. 2. ed. São Paulo: Atlas, 2000.
- Cavalcante, E. Revolução da informação: algumas reflexões. Caderno de Pesquisas em Administração, São Paulo, v.1, nº1, 2ºSEM, 1995.
- Oliveira, D.P.R. Sistemas, Organização e Métodos: uma abordagem gerencial. 16a ed., São Paulo: Atlas, 2007.


Promoção Humana
UTP
Universidade
Tuiuti do
Paraná