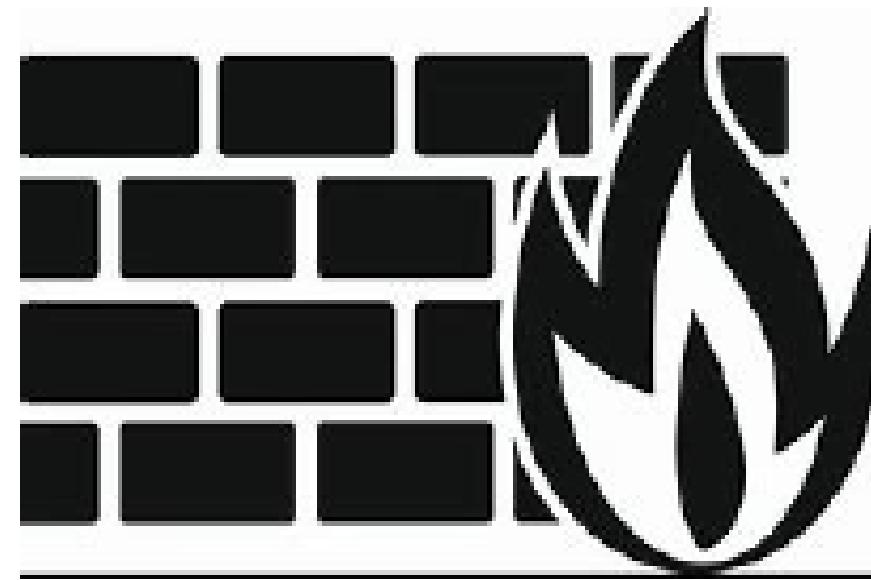


Prof.: José Márcio



Segurança da Informação



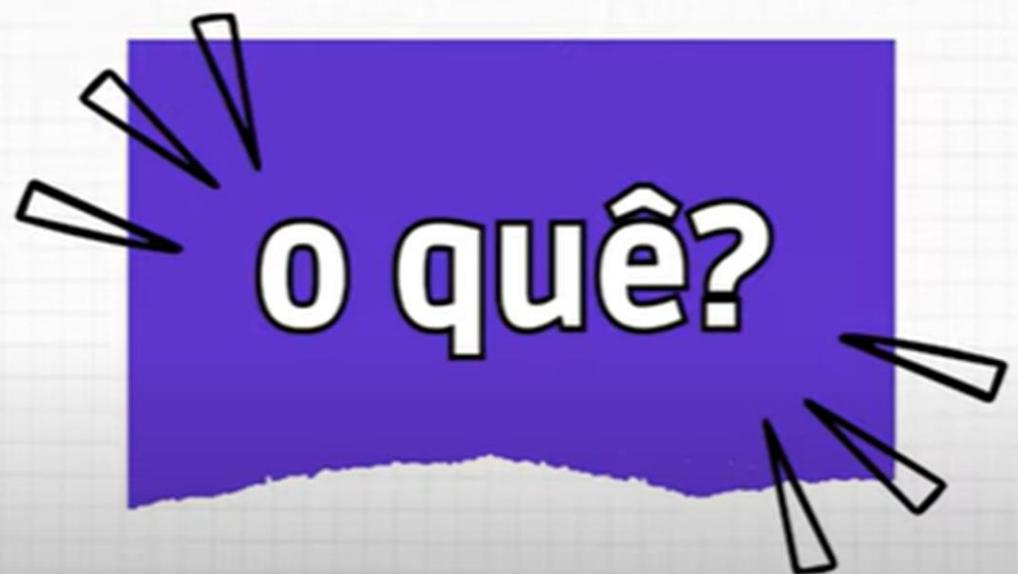
A disciplina tem como objetivo abordar os aspectos inerentes à proteção da informação por meio da **Segurança da Informação**.

Além disso, direcionar as implementações de um conjunto de medidas, ações e métodos para controlar e principalmente evitar ou mitigar potenciais riscos a segurança.

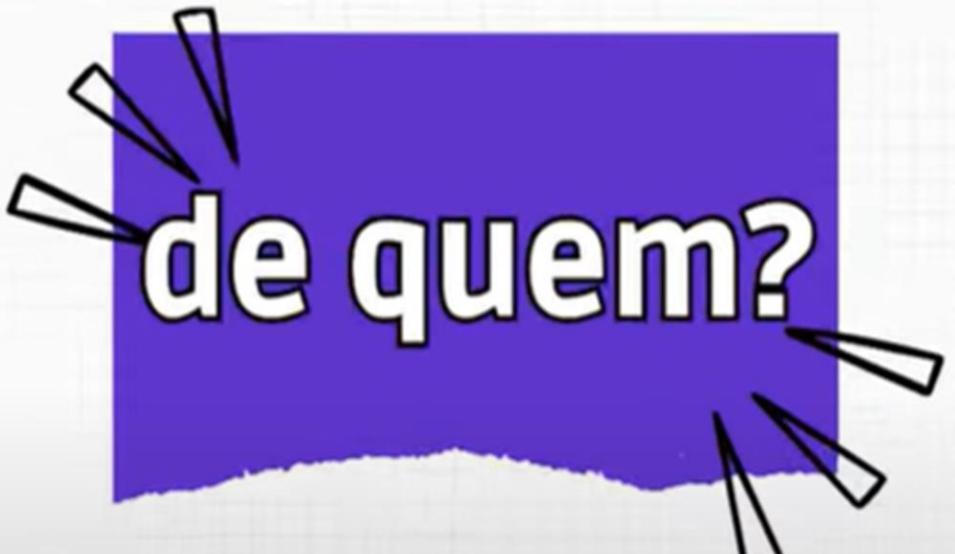
Discutir, elaborar e desenvolver técnicas para uma **Política de Segurança da Informação**.

Visão sobre Segurança da Informação

PROTEGER...



PROTEGER...



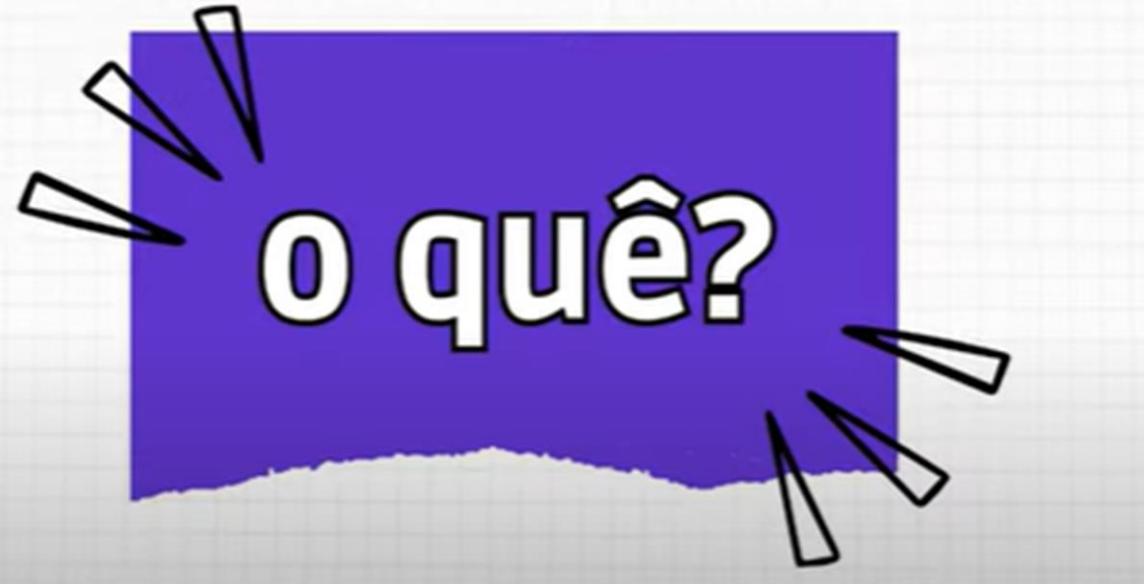
PROTEGER...



PROTEGER...



PROTEGER...



Em um contexto mais amplo, protegemos:

- **Dados sensíveis** (informações pessoais, financeiras, corporativas, etc.).
- **Infraestrutura de TI** (redes, servidores, dispositivos, etc.).
- **Usuários e suas credenciais** (contra phishing, vazamentos, etc.).
- **Continuidade dos negócios** (prevenção contra ataques como ransomware).

Quando falamos de **Segurança da Informação** ou **Cibersegurança**, queremos proteger três pilares fundamentais, conhecidos como **CIA Triad**:

1. **Confidencialidade** – Garantir que apenas pessoas autorizadas tenham acesso à informação. Isso evita vazamento de dados e acessos indevidos.
2. **Integridade** – Assegurar que os dados não sejam alterados de maneira não autorizada, garantindo que as informações sejam confiáveis e precisas.
3. **Disponibilidade** – Garantir que os dados e sistemas estejam acessíveis sempre que necessários, evitando indisponibilidades causadas por ataques ou falhas técnicas.



TRACEABILITY

Além desses pilares, também é comum considerar:

- **Autenticidade** – Garantir que a identidade de usuários e dispositivos seja legítima.
- **Rastreabilidade (Accountability)** – Permitir que ações realizadas no sistema sejam auditáveis, associando atividades a usuários específicos.

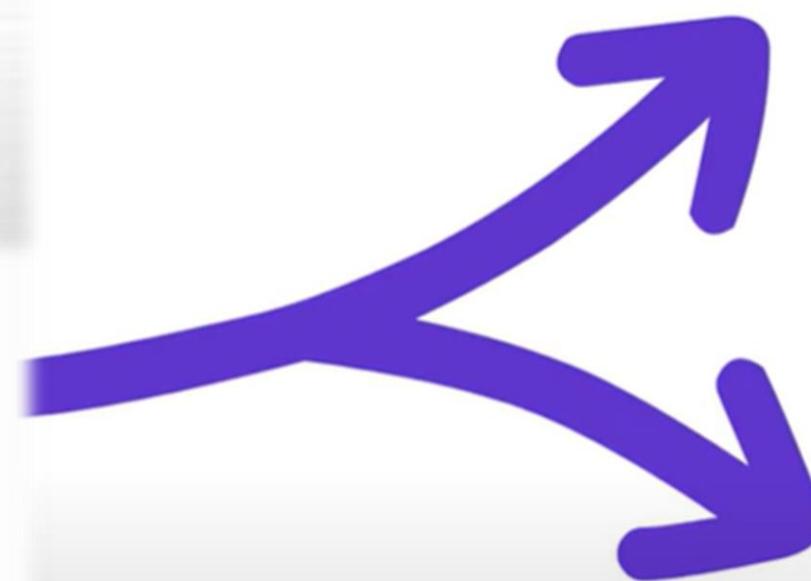
PROTEGER...



Nos protegemos de diversas ameaças, que podem ser divididas em categorias, dependendo da origem e do objetivo do ataque. Algumas das principais ameaças incluem:

1. Ameaças Internas
2. Ameaças Externas

Segurança da informação



A proteção dos sistemas de informação contra acesso, uso, divulgação, interrupção, modificação ou destruição não autorizados, a fim de fornecer confidencialidade, integridade e disponibilidade. (NIST)

Cibersegurança

Práticas para atingir a integridade, confiabilidade e disponibilidade no meio digital.

PROTEGER...



de quem?



Queremos essa segurança...

Nível Lógico
security

Nível Físico
safaty



TRÍADE CIA

- CONFIDENCIALIDADE
- INTEGRIDADE
- DISPONIBILIDADE

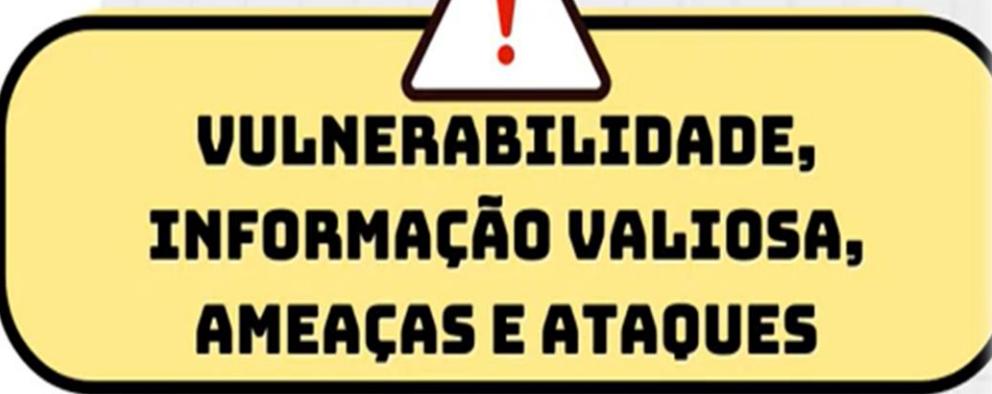
Dica extra: procure o significado de autenticidade e não repúdio no contexto de segurança da informação

PROTEGER...



De quem?

Proteger de qualquer pessoa/organização/código malicioso não autorizado que tente um ATAQUE ou que seja uma AMEAÇA



- **VULNERABILIDADE**
- **INFORMAÇÃO VALIOSA**
- **AMEAÇAS**
- **ATAQUES**



AMEAÇA

Qualquer coisa que possa afetar ou atingir o funcionamento, operação, disponibilidade, integridade da rede ou sistema.

ATAQUE

Técnica específica usada para explorar uma vulnerabilidade

1. Ameaças Internas

São aquelas que vêm de dentro da própria organização, podendo ser intencionais ou acidentais.

- **Funcionários mal-intencionados:** Podem vazar dados, instalar malwares ou prejudicar sistemas.
- **Erro humano:** Uso inadequado de senhas, compartilhamento indevido de informações e descuidos que levam a vazamentos.
- **Engenharia social:** Manipulação psicológica de funcionários para obter informações sensíveis.

2. Ameaças Externas

São ataques realizados por agentes externos, como hackers, grupos criminosos ou até estados-nação.

- **Hackers e cibercriminosos:** Buscam explorar vulnerabilidades para roubar dados, extorquir empresas (ransomware) ou causar danos.
- **Grupos de hackers organizados (APT – Ameaças Persistentes Avançadas):** Grupos patrocinados por governos ou corporações que realizam ataques sofisticados e contínuos.
- **Concorrência desleal:** Empresas rivais podem tentar espionagem industrial para obter vantagens competitivas.

Queremos essa segurança...



3. Softwares Maliciosos (Malwares)

- **Vírus e worms:** Se espalham automaticamente e podem danificar sistemas.
- **Ransomware:** Sequestra arquivos e exige pagamento para liberá-los.
- **Spyware e keyloggers:** Roubam informações sem que o usuário perceba.
- **Botnets:** Redes de computadores infectados que podem ser usadas para ataques em massa.

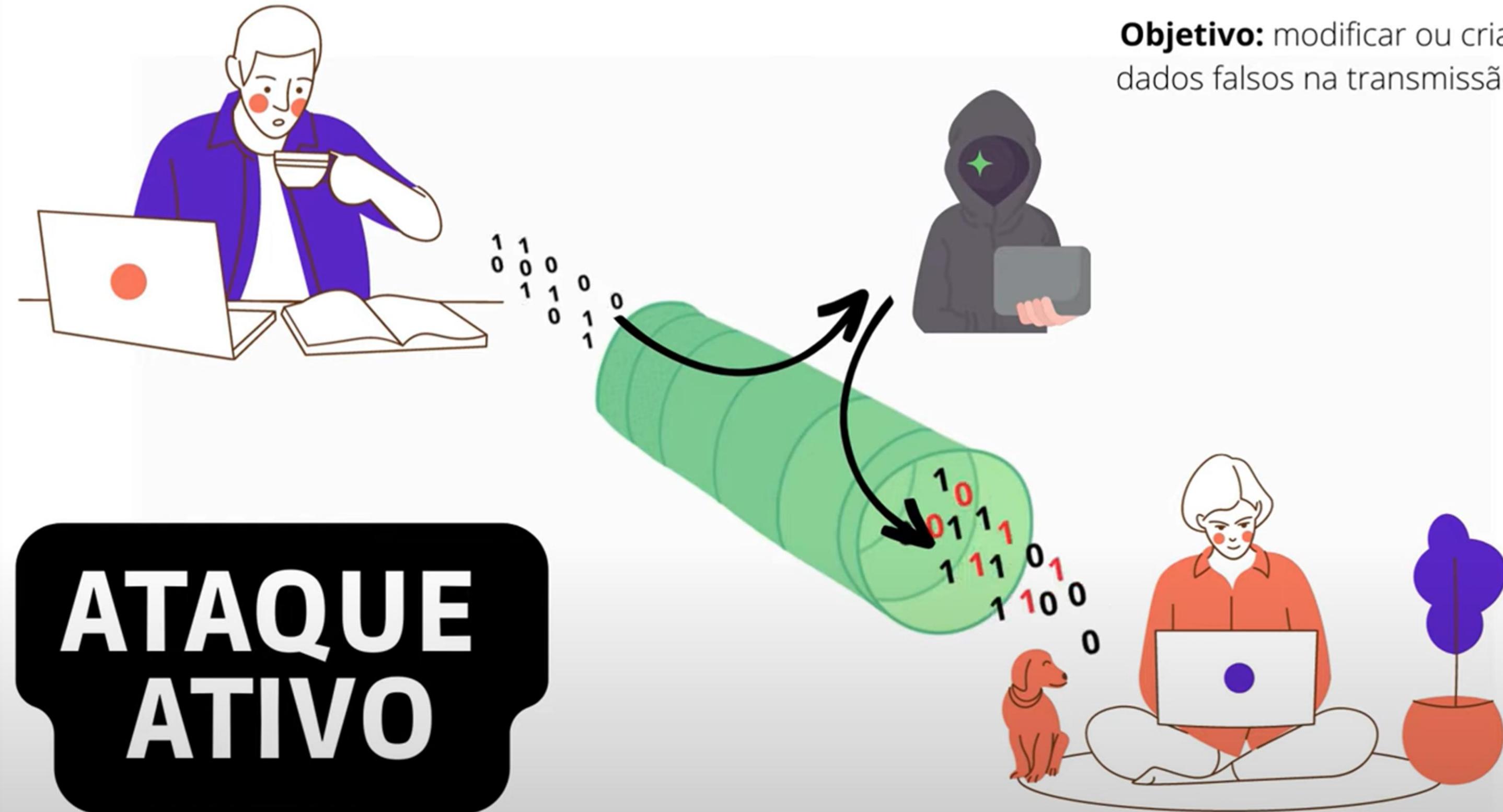
4. Ataques Cibernéticos

- **Phishing:** E-mails ou mensagens falsas tentando enganar usuários para roubar credenciais.
- **DDoS (Ataque de Negação de Serviço Distribuído):** Derruba sistemas ao sobrecarregá-los com tráfego malicioso.
- **Exploits e Zero-Day:** Ataques que exploram vulnerabilidades desconhecidas antes que os fabricantes lancem correções.
- **Man-in-the-Middle (MitM):** Interceptação de comunicações para roubar ou manipular informações.

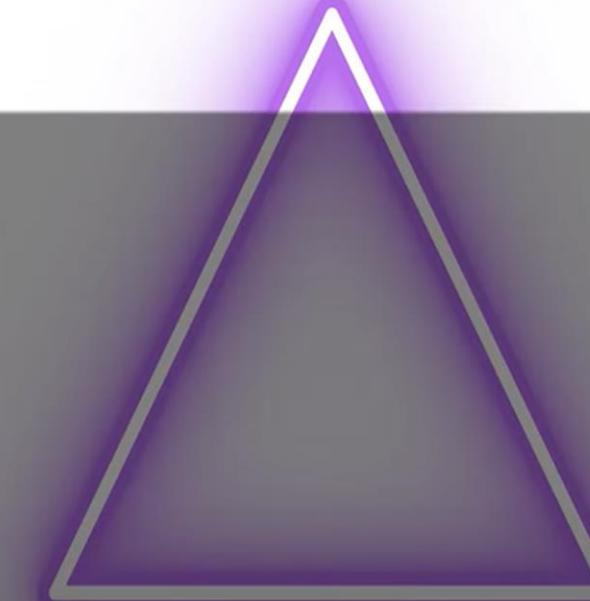
5. Vazamento de Dados

- **Exfiltração de dados:** Roubo de informações sigilosas por insiders ou hackers.
- **Exposição de credenciais:** Uso de credenciais vazadas em ataques de força bruta ou engenharia social.
- **Configurações incorretas:** Falhas na configuração de sistemas na nuvem que deixam informações acessíveis publicamente.





CONFIDENCIALIDADE



DISPONIBILIDADE

INTEGRIDADE



DISPONIBILIDADE

- A **disponibilidade** na segurança da informação garante que sistemas, redes e dados estejam acessíveis **sempre que necessários**, evitando interrupções causadas por falhas, ataques ou desastres.



CONFIDENCIALIDADE

- Apenas pessoas, sistemas ou processos autorizados tenham acesso a informações sensíveis



INTEGRIDADE

- Garante que os dados não sejam alterados de maneira indevida, seja por erro, falha técnica ou ataque malicioso. Isso significa que as informações devem permanecer **precisas, confiáveis e autênticas**, sem modificações não autorizadas.

PROTEGER...



Proteger seus **dados** é essencial porque vivemos em um mundo digital onde informações são ativos valiosos. Sem proteção adequada, seus dados podem ser roubados, manipulados ou usados contra você. Aqui estão algumas razões fundamentais para investir na segurança dos seus dados:

2. Prevenir Perdas Financeiras

- Um ataque de **ransomware** pode sequestrar seus arquivos e exigir pagamento para recuperá-los.
- Golpes como **phishing** podem fazer você transferir dinheiro para criminosos sem perceber.
- Hackers podem invadir **susas contas bancárias** e realizar transações fraudulentas.

A cibersegurança não é só um luxo – é uma necessidade. Com o avanço dos ataques digitais, **quanto mais protegido você estiver, menor a chance de ser vítima de um golpe ou ataque cibernético.**

1. Evitar Roubo de Identidade e Fraudes

- Hackers podem usar **seus dados pessoais** (CPF, endereço, senhas) para cometer fraudes.
- Golpistas podem se passar por você para **fazer compras, abrir contas bancárias ou pedir empréstimos**.
- Dados vazados em sites comprometidos podem ser usados para acessar outras contas suas.

PROTEGER...



COMO garantir
confidencialidade, integridade,
disponibilidade?



Criptografia



Certificados
Digitais



Esteganografia



Serviços de
autenticação

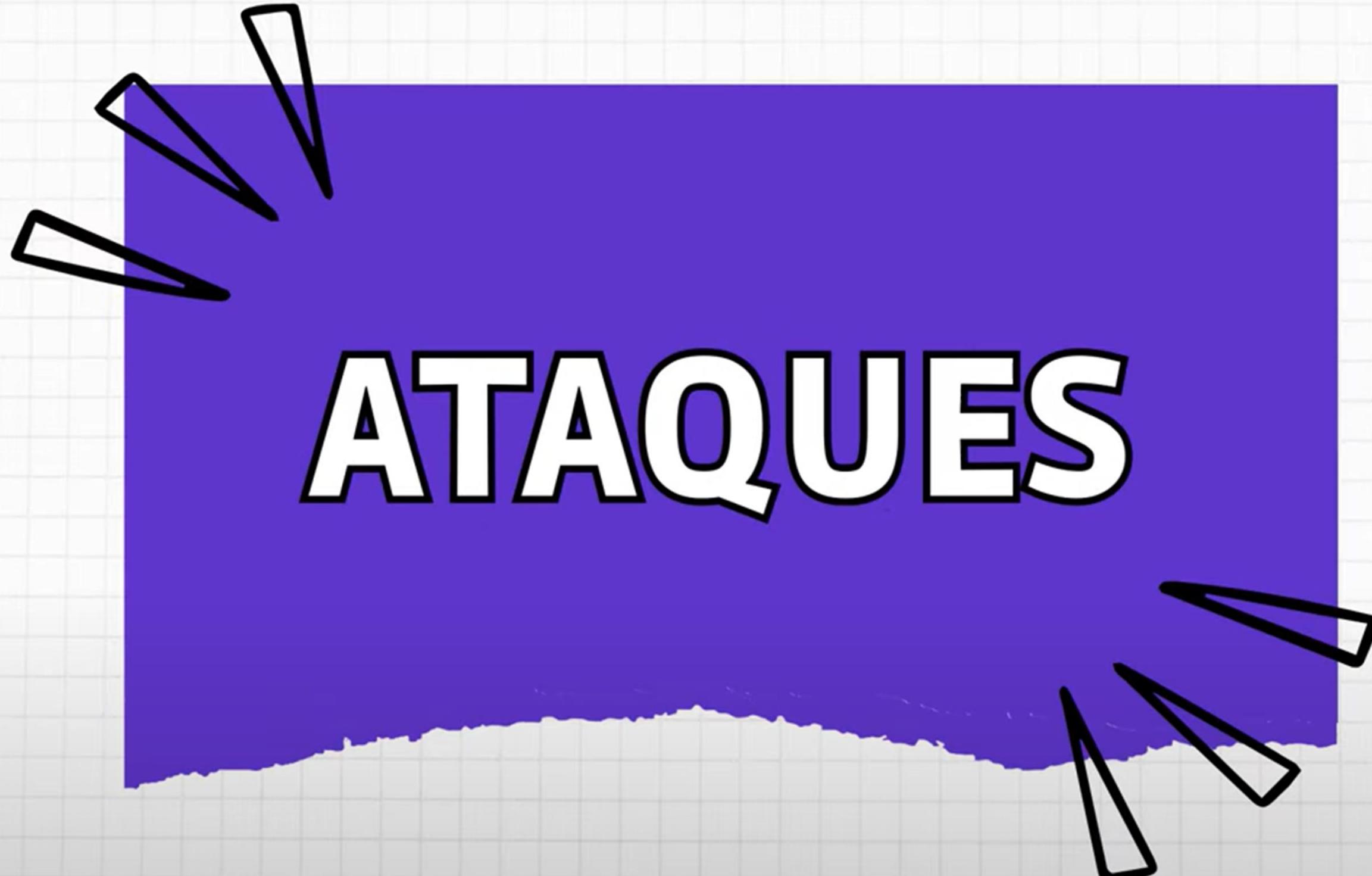


Firewall

- + Políticas de segurança - nível do usuário
- + Segurança de equipamentos

**Protetores precisam estar certos
o tempo todo, atacantes apenas
uma vez.**

**Ninguém gosta de segurança até
que seja necessário.**



Malware

Software malicioso ou Malware é um código escrito com a intenção de causar danos e violar a segurança de um sistema. Existem muitos tipos de Malware: RATs, Keyloggers, Trojans, Rootkits, Backdoors, Adwares

Engenharia social

É o termo usado para uma ampla gama de atividades maliciosas realizadas por meio de interações humanas. A Engenharia Social é utilizada em uma das maiores ameaças da internet: Ataques de Phishing

Phishing

Um ataque de engenharia social que engana o alvo para fornecer informações confidenciais, como nomes de usuário e senhas, sem saber.
Os ataques de phishing são a ameaça número um na Internet e, na maioria dos casos, ocorrem por e-mail, número de telefone ou redes sociais

Ataques força bruta

Tentativas sistemáticas para quebrar senhas por tentativa e erro

DDoS

Um ataque durante o qual o acesso de um determinado sistema é bloqueado geralmente devido a ataques de inundação (ataques contínuos)

Man-in-the-Middle

o invasor secretamente intercepta e retransmite mensagens entre duas partes que acreditam estar se comunicando diretamente uma com a outra.

Injeção de SQL

Inserção de comandos SQL maliciosos para comprometer um banco de dados



- Software usado ou criado para interromper a operação do computador, coletar informações confidenciais ou obter acesso a sistemas de computador privados.
- 'Malware' é um termo geral usado para se referir a uma variedade de formas de software maliciosos.

Vírus de Computador

Um programa malicioso que se replica e se espalha, infectando arquivos e sistemas.

Worm

Malware autônomo que se replica e se espalha por redes e sistemas, explorando vulnerabilidades.

Trojan (Cavalo de Troia)

Um programa que se disfarça como um software legítimo, mas executa ações maliciosas, como roubo de informações ou abertura de uma porta para outros malwares.

Ransomware

Bloqueia o acesso a arquivos ou sistemas e exige um resgate para restaurar o acesso.

Rootkit

Malware projetado para obter acesso privilegiado e ocultar sua presença no sistema, permitindo controle remoto e manipulação não autorizada.

Spyware

coleta informações sobre as atividades do usuário, como senhas, histórico de navegação e dados pessoais, sem o conhecimento do usuário.

Adware

Exibe anúncios indesejados e intrusivos em dispositivos, geralmente acompanhado de rastreamento de atividades do usuário

Botnet

Rede de dispositivos infectados controlados remotamente para realizar ações coordenadas, como ataques DDoS ou envio de spam.

Keylogger

Registra as teclas digitadas pelo usuário, incluindo senhas e informações confidenciais, para fins maliciosos.





White Hat

Um hacker de "chapéu branco" ou hacker ético é um indivíduo que usa habilidades de hacking para identificar vulnerabilidades de segurança em hardware, software ou redes



Gray Hat

Hacker que não é malicioso, nem ético, uma mistura dos dois.



Black Hat

Um hacker que viola a segurança do computador para seu próprio lucro. A invasão feita por um hacker de "chapéu preto" é, em muitos casos, com intenção maliciosa e, em todos os casos, sem permissão.

Ameaça interna

Potencial de que um funcionário ou qualquer pessoa considerada interna possa representar um risco à segurança de uma organização

De quem?

Proteger de qualquer
pessoa/organização/código
malicioso não autorizado que
tente um ATAQUE ou que seja
uma AMEAÇA



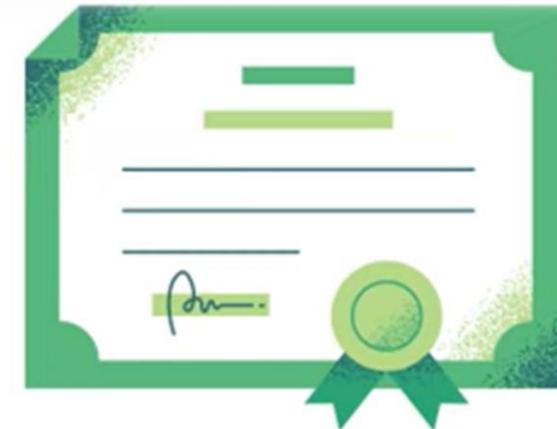


A criptografia é um conjunto de métodos e técnicas para cifrar informações legíveis (texto claro) por meio de um algoritmo e uma chave, convertendo a mensagem para texto cifrado (ilegível). A cifragem dos dados pode ser usada na comunicação, no armazenamento de dados e na autenticação.

- Substituição - Utilizam a substituição de texto claro por texto cifrado (Substituição)
- Transposição - permutação nos caracteres do texto claro
- Uso de apenas chave simétrica
- Uso de chave assimétrica



certificado digital



É um arquivo de dados usados para estabelecer a identidade de usuários (físicos e jurídicos) para proteção de transações online, como o comércio eletrônico e emissão de notas fiscais.

Criptografado com chave assimétrica

Uma Autoridade de Certificação (CA) valida e verifica a identidade de um usuário. A CA gera um certificado digital criptografado com chave assimétrica. A chave privada gera um código exclusivo para cada documento associado ao certificado digital, e a chave pública possibilita a leitura e reconhecimento que o documento é autêntico.





O que podemos autenticar?

Usuários

- Login e senha, certificados digitais, biometria estática e dinâmica, dispositivos portáteis, uso de chaves criptográficas, Kerberos, Active directory, LDAP, RAIDUS

Mensagens

- Verificar a integridade da mensagem e garantir que a identidade afirmada pelo emissor (autenticidade) é válida. Código de verificação de mensagem MAC, função hash criptográfica, assinatura digital

Conexões

Garante que no início da conexão as duas partes da comunicação são autênticas, e garante que não ocorram interferências na transmissão ou na recepção da mensagem. Exemplos de autenticação são: dois módulos TCP em dois sistemas de comunicação com SSL/TSL, uma conexão de VPN por IPSec ou OpenVPN, e os modos de operação CCM,e GCM que fornecem encriptação autenticada (AE), ou seja, sistemas de encriptação que simultaneamente protegem a confidencialidade e a autenticação (integridade) das comunicações



Tech Skills



Básico de
segurança
da
informação



banco de
dados



ferramentas
específicas



engenharia
reversa



análise de
dados



Programação



criptografia



Redes de
Computadores
+Cloud



Sistema
Operacional
+Linux



escrita/
estatística/
gerar
relatórios



Wireshark



Nessus



Metasploit



BurpSuite



Tcpdump



Nmap



Aircrack-ng



Nikto



Kali Linux

