uniesp
Centro Universitário

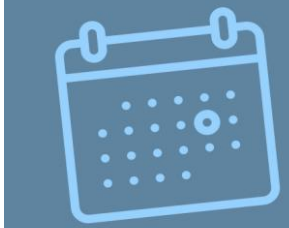
SISTEMAS PARA INTERNET

REDES DE COMPUTADORES

PROFª PRISCILLA DE ALMEIDA

REDES DE COMPUTADORES

AULA 08



Segurança em Rede Básica

- Noções de criptografia
- Boas práticas para proteger dados
- Lidando com ameaças simples

SEGURANÇA EM REDE: POR QUE? PARA QUE?

A segurança em uma rede básica é fundamental por diversas razões, e seu propósito principal é proteger os ativos digitais e a comunicação de uma organização ou indivíduo.

Algumas razões essenciais para a segurança em rede:
Confidencialidade
Integridade
Autenticidade
Disponibilidade
Privacidade
Proteção contra Ameaças
Cumprimento de Normas e Regulamentações
Manutenção da Reputação
Proteção de Recursos Críticos

ALGUMAS RAZÕES ESSENCIAIS

1. Confidencialidade:
Por que: Proteger informações sensíveis contra acesso não autorizado.
Para que: Evitar o vazamento de dados confidenciais, como informações pessoais, dados financeiros ou propriedade intelectual.

2. Integridade:
Por que: Garantir que os dados não sejam modificados ou corrompidos durante a transmissão ou armazenamento.
Para que: Assegurar que as informações mantêm sua precisão e confiabilidade ao longo do tempo.

3. Autenticidade:
Por que: Verificar a identidade de usuários, sistemas e dispositivos.
Para que: Prevenir a falsificação de identidades e garantir que apenas usuários autorizados acessem recursos.

ALGUMAS RAZÕES ESSENCIAIS

4. Disponibilidade:

Por que: Garantir que os serviços e recursos estejam disponíveis quando necessários.
Para que: Evitar interrupções no funcionamento normal de sistemas, prevenindo ataques de negação de serviço (DoS) e falhas não autorizadas.

5. Privacidade:

Por que: Proteger a privacidade das informações pessoais.
Para que: Cumprir regulamentações de privacidade e construir a confiança dos usuários na gestão de seus dados.

6. Proteção contra Ameaças:

Por que: Prevenir e mitigar ameaças como malware, phishing e outras formas de ataques.
Para que: Evitar danos aos sistemas, roubo de informações e interrupções nas operações normais.

ALGUMAS RAZÕES ESSENCIAIS

7. Cumprimento de Normas e Regulamentações:

Por que: Atender requisitos legais e regulatórios específicos do setor.
Para que: Evitar penalidades legais e manter a reputação da organização.

8. Manutenção da Reputação:

Por que: Construir confiança entre clientes, parceiros e stakeholders.
Para que: Preservar a reputação da organização diante de incidentes de segurança e demonstrar responsabilidade na proteção de informações.

9. Proteção de Recursos Críticos:

Por que: Salvaguardar ativos digitais essenciais para o funcionamento da organização.
Para que: Evitar perdas financeiras, interrupções nos negócios e danos à reputação.

NOÇÕES DE CRIPTOGRAFIA

Criptografia é o processo de transformar informações legíveis em um formato ilegível (cifrado) e, posteriormente, reverter esse processo (decifrar) para tornar as informações legíveis novamente. Isso é fundamental para garantir a confidencialidade, integridade e autenticidade dos dados transmitidos em uma rede.

NOÇÕES DE CRIPTOGRAFIA

Tipos:

- **Criptografia Simétrica:** Utiliza a mesma chave para cifrar e decifrar a informação. Exemplos incluem o AES (Advanced Encryption Standard) e o DES (Data Encryption Standard).

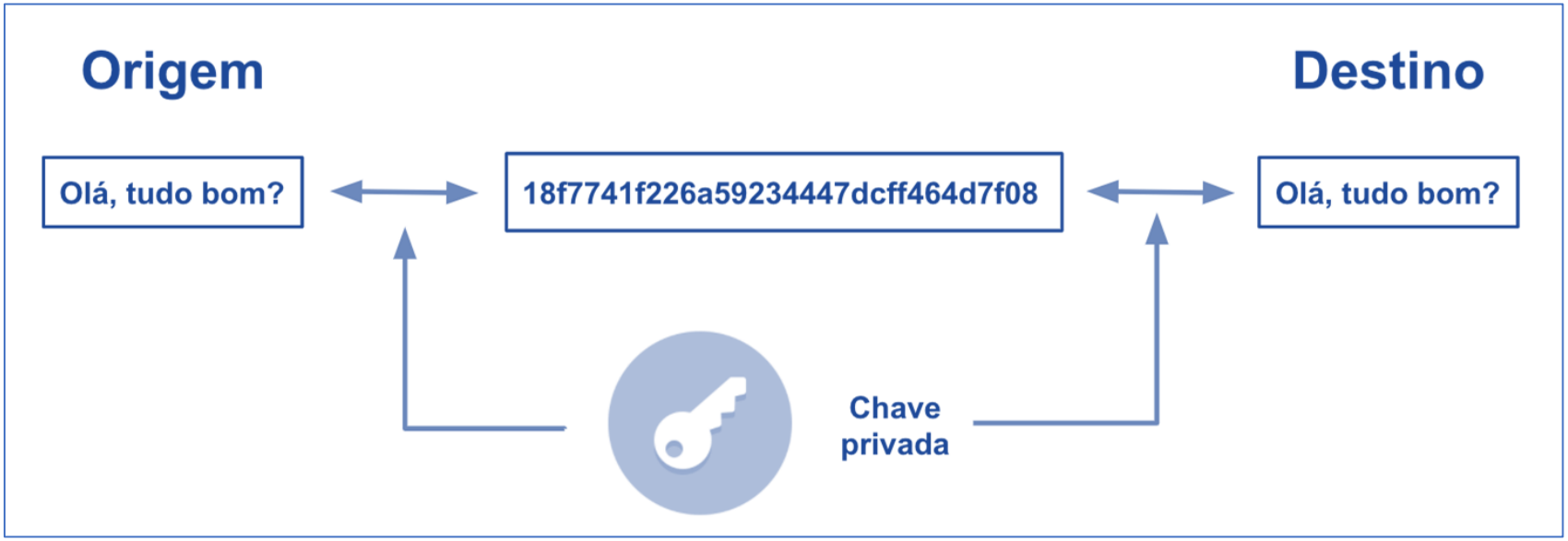
- **Criptografia Assimétrica:** Usa pares de chaves (pública e privada) para cifrar e decifrar informações. Exemplos incluem RSA e ECC (Elliptic Curve Cryptography).

- **Hashing:** Não é exatamente criptografia, mas é usado para verificar a integridade dos dados. Funções hash como SHA-256 geram uma sequência fixa de caracteres (hash) a partir de dados de entrada, e qualquer alteração nos dados resulta em um hash completamente diferente.

NOÇÕES DE CRIPTOGRAFIA

CRIPTOGRAFIA SIMÉTRICA

Na criptografia simétrica, a mesma chave é usada para cifrar (criptografar) e decifrar (descriptografar) os dados. Ambas as partes envolvidas na comunicação precisam compartilhar a mesma chave secreta.



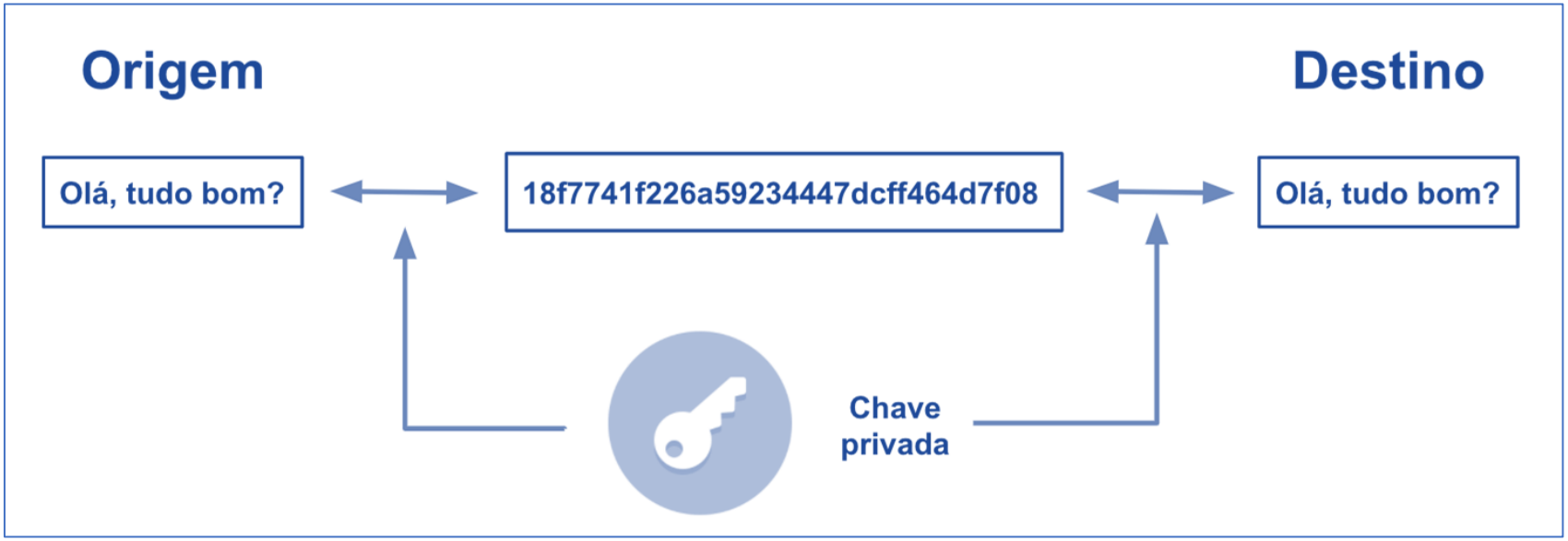
CRIPTOGRAFIA SIMÉTRICA

Exemplo Prático

Algoritmo: AES (Advanced Encryption Standard)

Funcionamento:

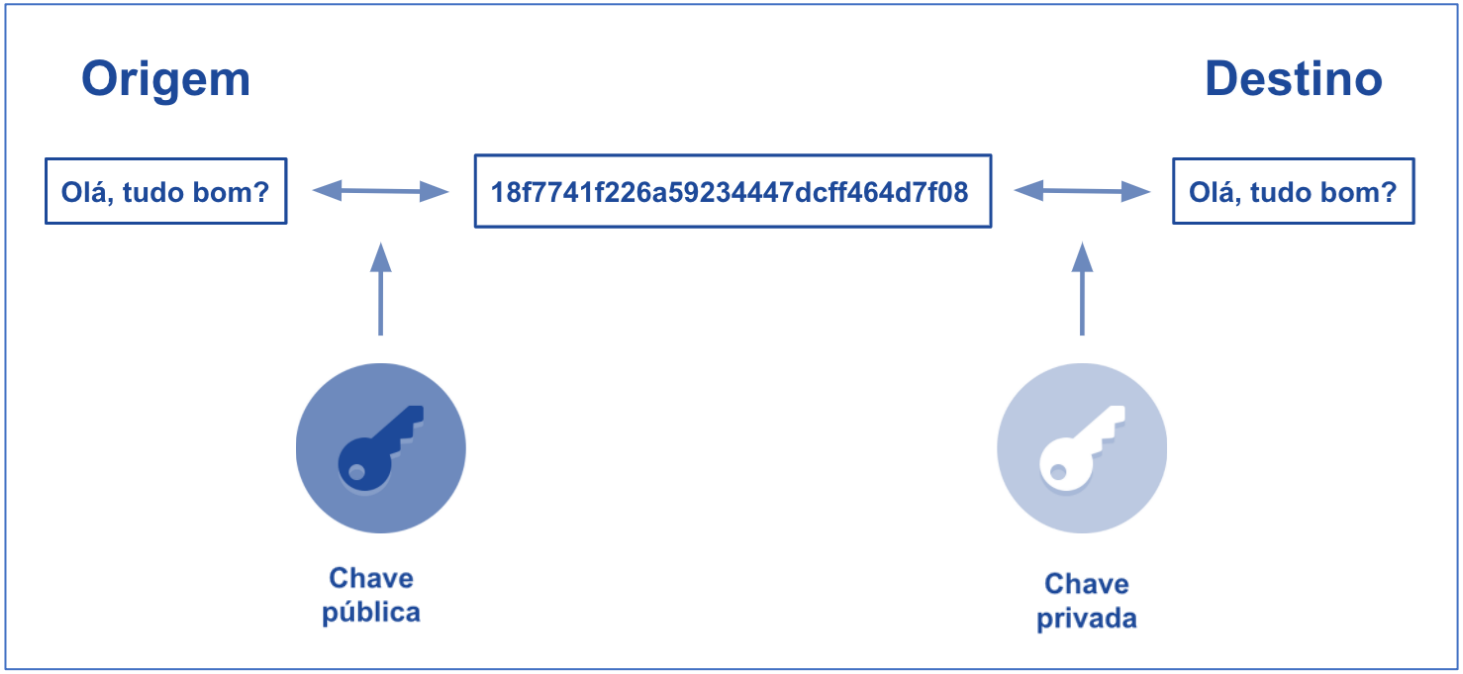
1. **Cifragem: O remetente e o destinatário compartilham a mesma chave secreta.**
2. **O remetente cifra a mensagem usando a chave e envia a mensagem cifrada.**
3. **O destinatário usa a mesma chave para decifrar a mensagem.**



NOÇÕES DE CRIPTOGRAFIA

CRIPTOGRAFIA ASSIMÉTRICA

Na criptografia assimétrica, um par de chaves é usado: uma chave pública para cifrar e uma chave privada correspondente para decifrar. A chave pública pode ser compartilhada abertamente, enquanto a chave privada deve ser mantida em segredo.



NOÇÕES DE CRIPTOGRAFIA

CRIPTOGRAFIA ASSIMÉTRICA

Exemplo Prático

Algoritmo: RSA (Rivest-Shamir-Adleman)

Funcionamento:

1. **Geração de Chaves: O destinatário gera um par de chaves (pública e privada).**
2. **Distribuição: O destinatário compartilha a chave pública, e a chave privada é mantida em segredo.**
3. **Cifragem: O remetente cifra a mensagem usando a chave pública do destinatário.**
4. **Decifragem: O destinatário usa sua chave privada para decifrar a mensagem.**

Chave Pública:
Pode ser compartilhada abertamente.
Usada para cifrar dados ou verificar assinaturas digitais.
Chave Privada:
Deve ser mantida em segredo.
Usada para decifrar dados cifrados pela chave pública ou para assinar digitalmente dados.

NOÇÕES DE CRIPTOGRAFIA

CRIPTOGRAFIA
SIMÉTRICA *vs.* ASSIMÉTRICA

Simétrica: Eficiente para grandes volumes de dados, mas requer compartilhamento seguro de chaves.

X

Assimétrica: Resolve o problema de compartilhamento de chaves, mas é computacionalmente mais intensiva.

UTILIZAÇÃO CONJUNTA

Prática Comum: Criptografia simétrica para a transferência eficiente de dados e criptografia assimétrica para estabelecer chaves de sessão seguras.

NOÇÕES DE CRIPTOGRAFIA

CRIPTOGRAFIA SIMÉTRICA *vs.* ASSIMÉTRICA

USO COMBINADO:

Cenário Típico:
Criptografia assimétrica é frequentemente usada para estabelecer uma chave de sessão segura.
Criptografia simétrica é usada para cifrar os dados usando a chave de sessão.

Vantagens:
Combina a eficiência da criptografia simétrica com a capacidade da criptografia assimétrica de resolver o problema de compartilhamento de chaves.

NOÇÕES DE CRIPTOGRAFIA

CRIPTOGRAFIA
SIMÉTRICA *vs.* ASSIMÉTRICA

TRADE-OFFS

Simétrica:

- **Vantagens: Eficiência computacional.**
- **Desvantagens: Necessidade de compartilhamento seguro de chaves.**

Assimétrica:

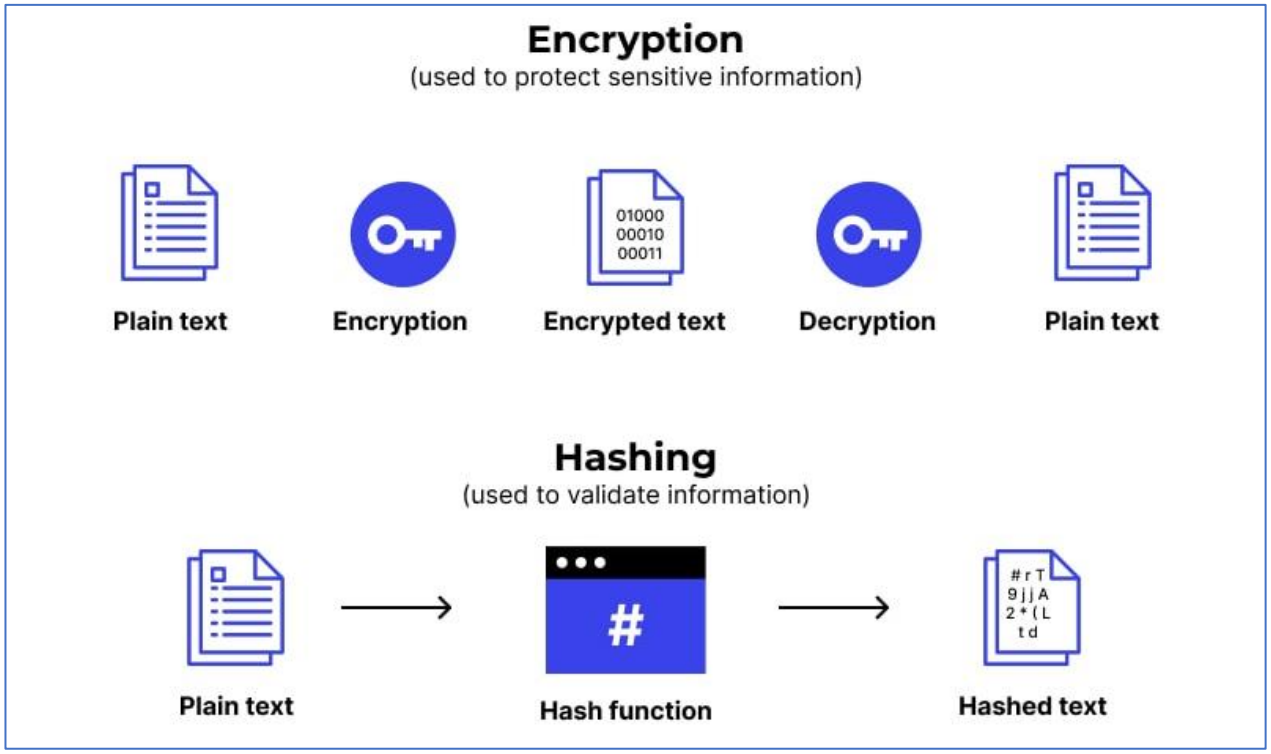
- **Vantagens: Elimina a necessidade de compartilhamento seguro de chaves.**
- **Desvantagens: Maior carga computacional.**

A combinação de ambos os tipos de criptografia é frequentemente chamada de "criptografia híbrida" e é amplamente utilizada para obter os benefícios de ambas as abordagens.

NOÇÕES DE CRIPTOGRAFIA

HASHING

Hashing não é exatamente criptografia, mas é fundamental para garantir a integridade dos dados. Uma função hash gera uma sequência fixa de caracteres (hash) a partir de dados de entrada.



HASHING

Exemplo Prático

SHA-256 (Secure Hash Algorithm 256-bit)

Funcionamento:

1. Criação de Hash:

- Um algoritmo de hash, como o SHA-256 (Secure Hash Algorithm 256-bit), é uma função matemática que aceita um conjunto de dados de entrada (mensagem) e produz uma sequência fixa de caracteres, o hash.
- O algoritmo de hash gera um valor único e "irreversível" para cada conjunto de dados exclusivo.

HASHING

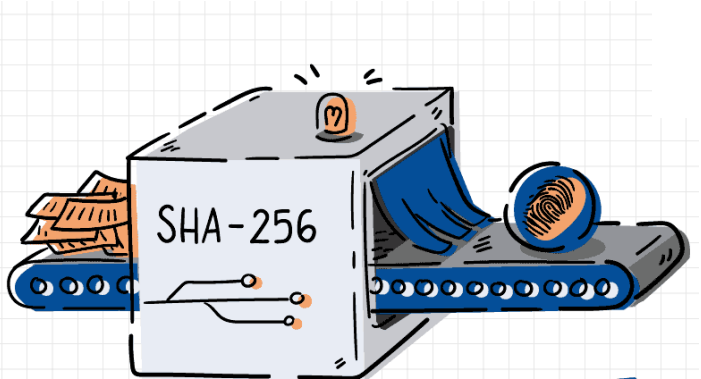
Exemplo Prático

SHA-256 (Secure Hash Algorithm 256-bit)

Funcionamento:

2. Integridade:

- **A propriedade fundamental dos algoritmos de hash é que qualquer alteração nos dados de entrada resulta em um hash completamente diferente.**
- **Mesmo uma pequena modificação em um único bit dos dados de entrada produzirá um hash drasticamente diferente.**
- **Isso é chamado de propriedade de avalanche, indicando que uma pequena mudança nos dados deve causar uma grande mudança no hash.**



NOÇÕES DE CRIPTOGRAFIA

HASHING

Exemplo Prático

SHA-256 (Secure Hash Algorithm 256-bit)

Funcionamento:

3. Verificação de Integridade:

- **O remetente gera um hash da mensagem original antes de enviá-la e anexa o hash à mensagem.**
- **O destinatário recebe a mensagem e recalcula o hash usando a mesma função de hash.**
- **O destinatário compara o hash recalculado com o hash recebido.**
- **Se os hashes coincidirem, isso indica que os dados não foram modificados durante a transmissão.**

Hashing e Integridade

Hashing: Garante a integridade dos dados, mas não fornece confidencialidade.

NOÇÕES DE CRIPTOGRAFIA

HASHING

Exemplo Prático em Python

```python
import hashlib

def criar_hash(dados):
    # Cria um objeto hash SHA-256
    sha256 = hashlib.sha256()

    # Atualiza o hash com os dados
    sha256.update(dados)

    # Retorna o hash como uma sequência hexadecimal
    return sha256.hexdigest()

# Exemplo de Uso
mensagem_original = b"Esta é uma mensagem original"
hash_original = criar_hash(mensagem_original)

# Simulação de Transmissão
mensagem_transmitida = mensagem_original  # Neste exemplo, assumimos que a m

# Verificação de Integridade
hash_recalculado = criar_hash(mensagem_transmitida)

if hash_original == hash_recalculado:
    print("Os dados não foram modificados durante a transmissão.")
else:
    print("Os dados foram modificados durante a transmissão.")
```

Este exemplo simplificado ilustra como criar um hash (SHA-256) para uma mensagem e como verificar a integridade da mensagem recalculando o hash e comparando-o com o hash original. Essa técnica é frequentemente usada para garantir que os dados não foram alterados ao longo de sua jornada pela rede.

BOAS PRÁTICAS PARA PROTEGER DADOS

Para proteger dados em uma rede, é essencial adotar boas práticas de segurança.

BOAS PRÁTICAS PARA PROTEGER DADOS

Para proteger dados em uma rede, é essencial adotar boas práticas de segurança.

Práticas Comuns
Atualização Regular dos sistemas
Firewalls
Controle de Acesso
Backup Regular
Conscientização do Usuário

BOAS PRÁTICAS PARA PROTEGER DADOS

Atualização Regular:

Descrição:

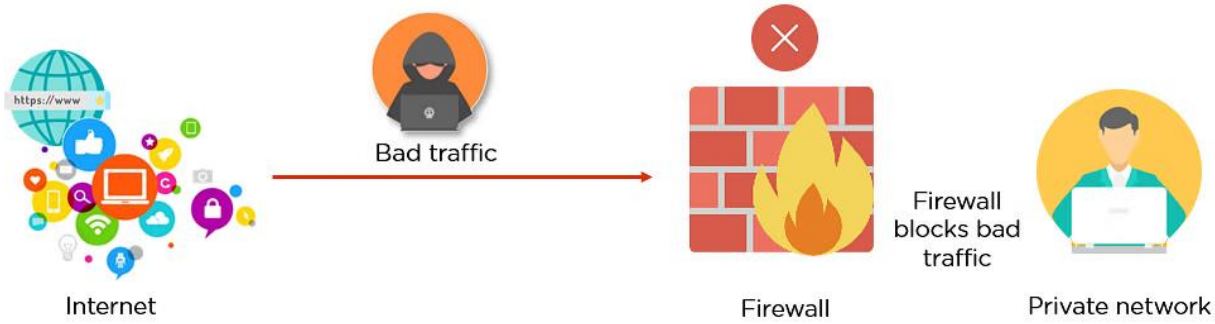
- **Manter sistemas operacionais, aplicativos e software atualizados é crucial para garantir que as últimas correções de segurança estejam implementadas.**
- **Fornecedores lançam atualizações para corrigir vulnerabilidades descobertas após o lançamento do software.**

•Implementação:

- **Configurar atualizações automáticas quando possível.**
- **Estabeleça procedimentos para monitorar e aplicar regularmente as atualizações manualmente, se necessário.**

BOAS PRÁTICAS PARA PROTEGER DADOS

Firewalls:



Descrição:

- Firewalls são barreiras de segurança que monitoram e controlam o tráfego de dados entre redes.
- Podem ser implementados em nível de software ou hardware para filtrar pacotes de dados com base em regras predefinidas.

Implementação:

- Configurar firewalls para bloquear tráfego não autorizado.
- Definir regras específicas para permitir ou negar determinados tipos de tráfego.

BOAS PRÁTICAS PARA PROTEGER DADOS

Firewalls de Hardware:

Firewall de Dispositivo de Rede:

Dispositivos físicos dedicados que filtram o tráfego de rede com base em regras de segurança.
Exemplo: Cisco ASA (Adaptive Security Appliance), Fortinet FortiGate.

Roteador com Firewall Integrado:

Roteadores que incluem funcionalidades de firewall para controlar o tráfego de entrada e saída.
Exemplo: Ubiquiti EdgeRouter, TP-Link Archer C5400X.

Firewalls de Software:

Firewall de Sistema Operacional:

Software incorporado em sistemas operacionais para monitorar e controlar o tráfego de rede.
Exemplo: Firewall do Windows Defender (integrado ao Windows), iptables (Linux).

Firewall de Aplicativo:

Software especializado que monitora e controla o tráfego de aplicativos específicos.
Exemplo: Little Snitch (macOS), ZoneAlarm.

BOAS PRÁTICAS PARA PROTEGER DADOS

Firewall Virtual:

Firewall de Máquina Virtual:

Firewalls implementados como máquinas virtuais, oferecendo flexibilidade em ambientes virtualizados.
Ex: Palo Alto Networks VM-Series, Check Point CloudGuard.

Firewalls Pessoais:

Firewall Pessoal:

Software de firewall projetado para uso em computadores pessoais.
Ex: ZoneAlarm, Norton Internet Security.

Firewalls de Aplicativos Web (WAF):

Firewall de Aplicativos Web:

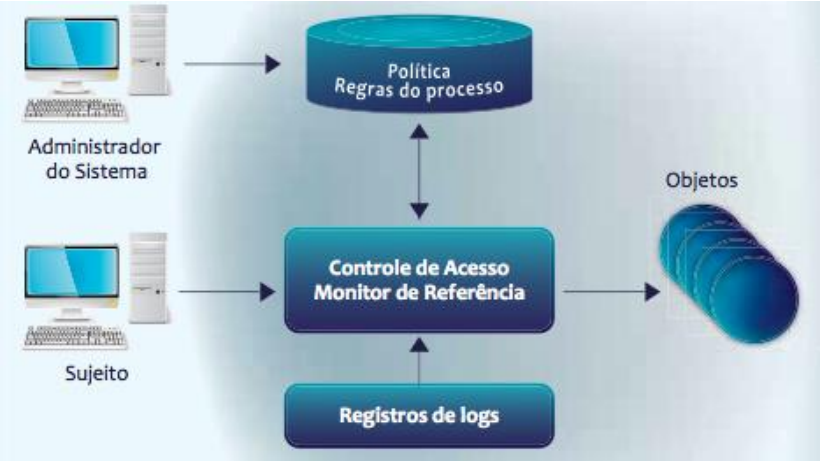
Especializado em proteger aplicativos web, identificando e bloqueando ataques específicos.
Ex: ModSecurity, Imperva Web Application Firewall.

Firewalls de Próxima Geração (NGFW):

Firewalls que vão além do simples controle de portas e protocolos, incorporando inspeção profunda de pacotes e funcionalidades avançadas de segurança.
Ex: Palo Alto Networks PA-Series, Fortinet FortiGate (NGFW).

BOAS PRÁTICAS PARA PROTEGER DADOS

Controle de acesso:



Descrição:

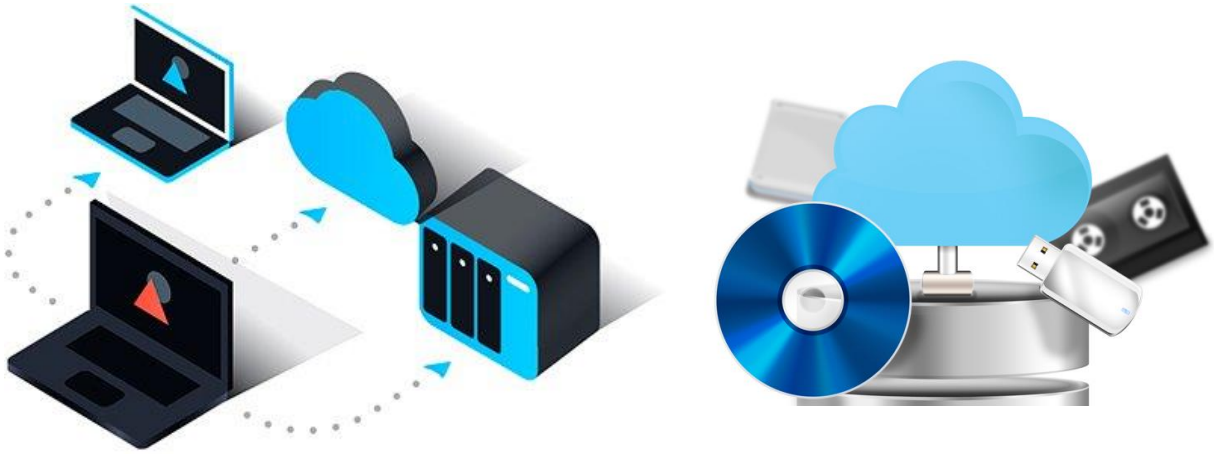
- Controle de acesso refere-se à prática de limitar o acesso a recursos da rede com base em políticas de segurança.
- Garante que apenas usuários autorizados tenham permissão para acessar determinados sistemas, dados ou áreas da rede.

Implementação:

- Adote autenticação forte, como senhas robustas ou autenticação de dois fatores.
- Atribua permissões de acesso de acordo com a função e necessidade do usuário.

BOAS PRÁTICAS PARA PROTEGER DADOS

Backup regular:



Descrição:

- **Realizar backups regularmente é essencial para evitar perda irreversível de dados em caso de falhas, ataques de ransomware ou outros incidentes.**

Implementação:

- **Estabeleça uma política de backup regular, considerando a frequência e os tipos de dados a serem salvos.**
- **Armazene os backups em locais seguros, preferencialmente fora da rede principal.**

BOAS PRÁTICAS PARA PROTEGER DADOS

Conscientização do usuário:

Descrição:

- **A conscientização do usuário é uma medida preventiva crucial, pois muitos incidentes de segurança resultam de ações inadvertidas dos próprios usuários.**

Implementação:

- **Fornecer treinamento de segurança regular aos usuários, destacando práticas seguras online e offline.**
- **Educar sobre a identificação de phishing, não clicar em links desconhecidos e relatar comportamentos suspeitos.**

BOAS PRÁTICAS PARA PROTEGER DADOS

Estas práticas formam uma base sólida para a segurança de dados em uma rede.

Ao implementar essas medidas de forma consistente, as organizações podem reduzir significativamente o risco de violações de segurança e proteger a integridade, confidencialidade e disponibilidade de seus dados.

LIDANDO COM AMEAÇAS SIMPLES

PRÓXIMA AULA...

REVISÃO

REVISÃO

Em resumo, a segurança em rede é essencial para preservar a confiança, garantir a integridade dos dados, proteger contra ameaças e manter a disponibilidade de recursos críticos. Além disso, é um elemento-chave para o cumprimento de regulamentações e a preservação da reputação da organização.

A Criptografia é fundamental para garantir a confidencialidade, integridade e autenticidade dos dados transmitidos em uma rede.

- **Criptografia Simétrica: Utiliza a mesma chave para cifrar e decifrar a informação.**
- **Criptografia Assimétrica: Usa pares de chaves (pública e privada) para cifrar e decifrar informações.**
- **Hashing: Não é exatamente criptografia, mas é usado para verificar a integridade dos dados.**

Para proteger dados em uma rede, é essencial adotar boas práticas de segurança. Que são:

REVISÃO

- **Atualização Regular:** Manter sistemas operacionais e software atualizados para corrigir vulnerabilidades.
- **Firewalls:** Utilizar firewalls para controlar o tráfego de entrada e saída na rede.
- **Controle de Acesso:** Implementação de políticas de controle de acesso para garantir que apenas usuários autorizados tenham acesso aos recursos.
- **Backup Regular:** Fazer backups regulares dos dados para evitar perda irreversível em caso de incidente.
- **Conscientização do Usuário:** Educar os usuários sobre práticas seguras, como não clicar em links suspeitos ou divulgar informações sensíveis.

Ao incorporar essas práticas e entender os princípios básicos de criptografia, você pode construir uma rede mais segura e resistente contra ameaças comuns. Esses são passos fundamentais na construção de uma postura de segurança robusta em ambientes de rede.

... ATÉ A PRÓXIMA!