

# Seguridad de Redes

Manuel Hidalgo Carmona  
Fernando de la Hoz Moreno  
Nikita Stetskiy



# Introducción a la seguridad

**Confidencialidad:** cualidad de la información para no ser divulgada a personas o sistemas no autorizados.



# Introducción a la seguridad de redes TCP/IP

Actualmente hacemos un uso intensivo de las redes para transmitir todo tipo de información

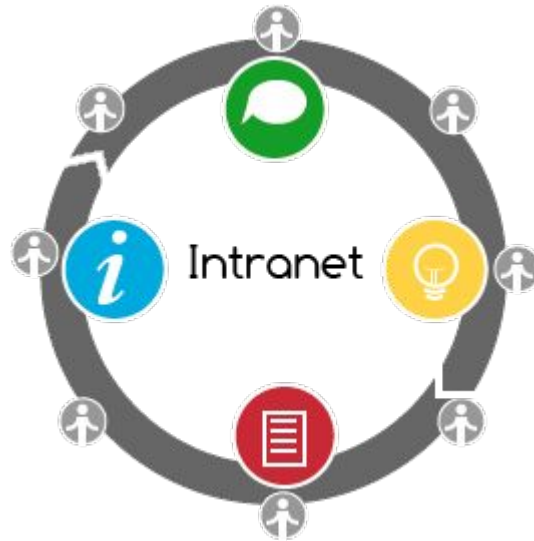
Tipos de redes:

Según área:

- LAN
- WLAN
- WAN
- VPN

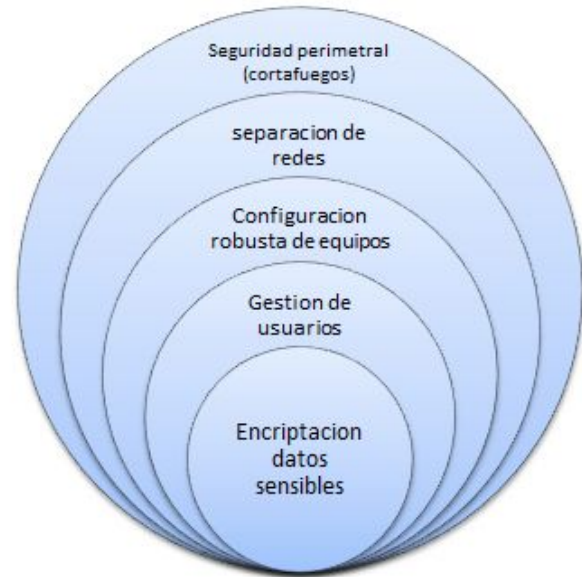
Según su propiedad:

- Pública
- Privada

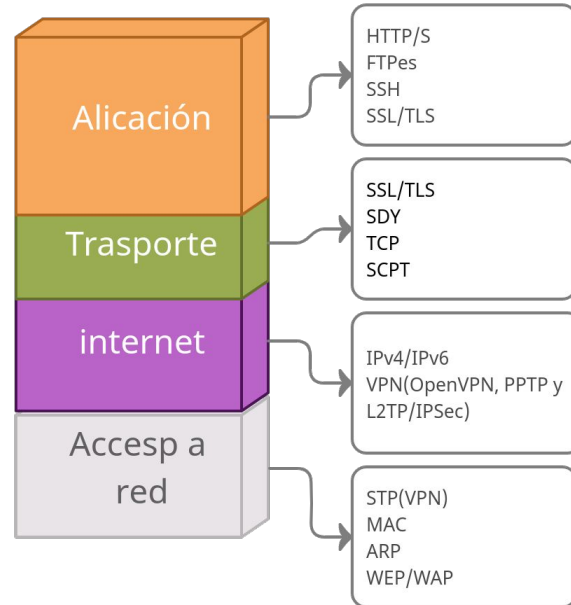


# Aspectos de una red segura

- Concepto de capas
- Autenticación
- Políticas de acceso
- Control de acceso
- Arquitectura de red
- Seguridad física de dispositivos finales
- Encriptación
- Redes inalámbricas



# Modelo de capas TCP/IP



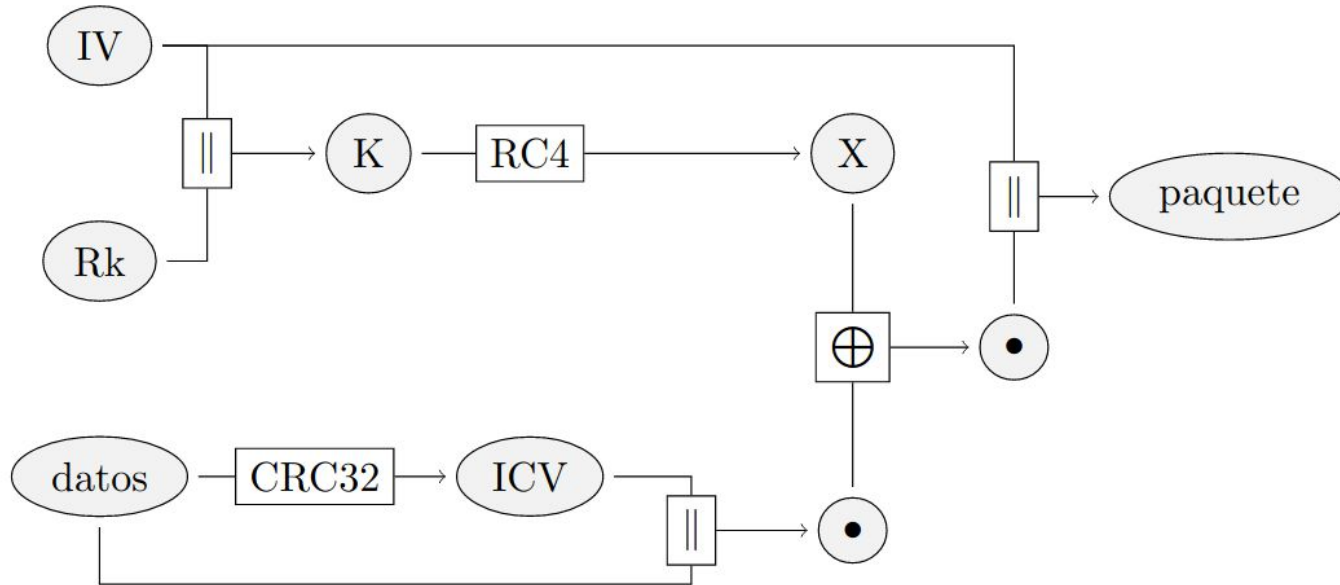
# Seguridad de redes WLAN



# Wired Equivalent Privacy



# WEP





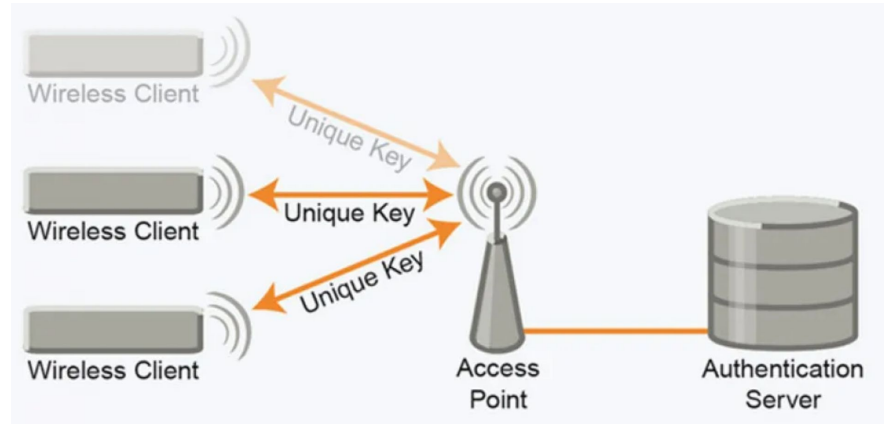


# WEP

## Vulnerabilidades:

- Se puede realizar un ataque por fuerza bruta si la clave es corta.
- Es posible hallar la clave teniendo un texto cifrado y el original.
- Usando vectores de inicio débiles se puede revelar la clave.
- Últimos ataques han conseguido recolectar 40.000 paquetes en 60 segundos para alcanzar un 50% de eficacia rompiendo el cifrado.
- Es posible alterar los datos y actualizar el ICV sin conocer la clave.

# Wi-fi Protected Access



# Wi-fi Protected Setup





**SSL / TLS**



**TLS**





# SSL / TLS

- Confidencialidad: oculta el contenido de los mensajes, es decir, es la capacidad de garantizar que la información será protegida y solamente podrá acceder a ella la persona a quien va dirigida
- Integridad: detecta cuando los mensajes han sido manipulados, es decir, es la capacidad de garantizar que los datos no se modifican desde su envío hasta su recepción.
- Autenticación: es la capacidad de garantizar que el interlocutor es quien realmente dice ser.

# TLS - Handshake Protocol

## Secure Sockets Layer

- ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
  - Content Type: Handshake (22)
  - Version: TLS 1.0 (0x0301)
  - Length: 186
- ▼ Handshake Protocol: Client Hello
  - Handshake Type: Client Hello (1)
  - Length: 182
  - Version: TLS 1.2 (0x0303)  Versión SSL/TLS soportadas por el cliente
  - ▶ Random
  - Session ID Length: 0
  - Cipher Suites Length: 22  Cipher Suites soportadas por el cliente
  - ▼ Cipher Suites (11 suites)
    - Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02b)
    - Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02f)
    - Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA (0xc00a)
    - Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA (0xc009)
    - Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0xc013)
    - Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0xc014)
    - Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x0033)
    - Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0039)
    - Cipher Suite: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x002f)
    - Cipher Suite: TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0035)
    - Cipher Suite: TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (0x000a)
  - Compression Methods Length: 1



# TLS - Funcionamiento y fases

TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384\_P384

Protocolo

Intercambio de claves

Firma digital

Cifrado  
simétrico

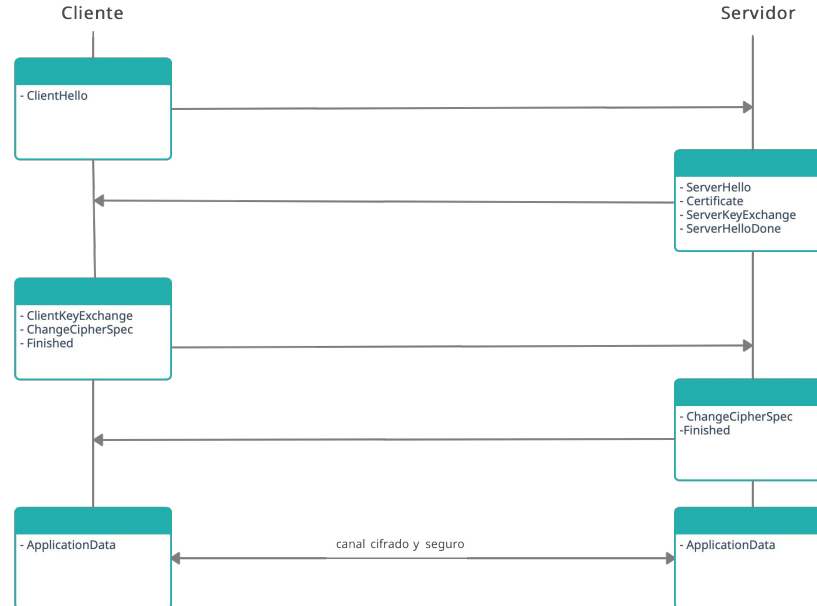
Longitud de  
clave

Modo de  
encriptación

Hash

Curva

# TLS - Handshake Protocol

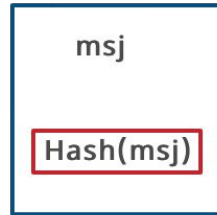




# TLS - Primera posible solución

Alice

$\text{Enc}(\text{Priv}, \text{Hash}(\text{msj}))$



Mallory

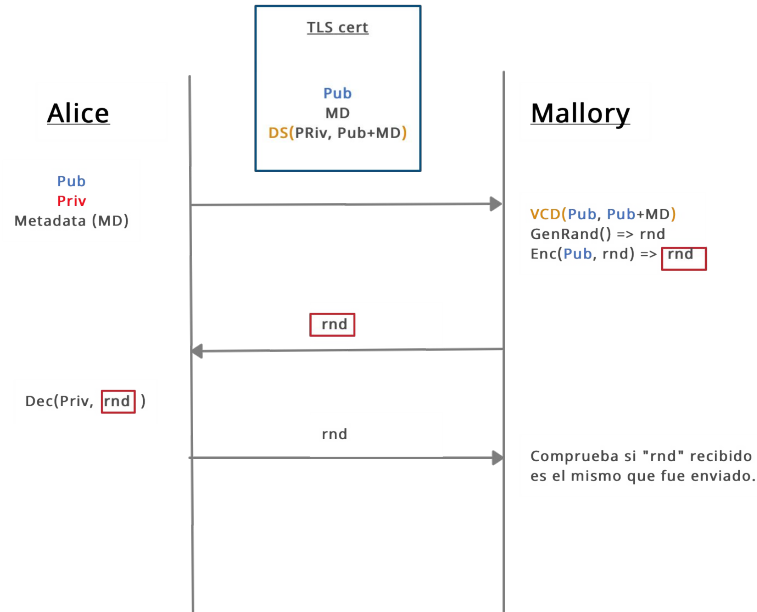
$\text{Hash}(\text{msj}) == \text{Dec}(\text{Pub}, \text{Hash}(\text{msj}))$

Asegura que "msj" no se haya modificado en el tránsito.

Certificado Digital:  $\text{CD}(\text{Priv}, \text{msj}) = \text{Enc}(\text{Priv}, \text{Hash}(\text{msj})) = \text{Hash}(\text{msj})$

Verificación de Certificado Digital:  $\text{VCD}(\text{Pub}, \text{msj}) = \text{Dec}(\text{Pub}, \text{Hash}(\text{msj})) = \text{Hash}(\text{msj})$

# TLS - Primera posible solución



# TLS - Segunda posible solución

