# **Seguridad en redes:**

## **Problemas**:

* **Confidencialidad o privacidad**: La información solo la pueden ver las personas designadas.
* **Autenticidad**: Acceso o visualización a un usuario que no le corresponde.
  + Control de accesos a la red y a la información.
* **Integridad de los datos**: El dato debe llegar íntegro a destino. (sin modificaciones ni pérdidas).

### **Ataques informáticos:**

* Interceptación.
* Fabricación.
* Modificación.
* Destrucción.

## **Potenciales soluciones:**

* Claves de acceso:
  + Al sistema.
  + A los recursos.
  + Ej: autenticación doble factor.
* Encriptado de datos.
* Seguridad física de dispositivos.
* Firma digital.
* Firewall.
* Capacitación de usuarios y administradores.
* Protocolos de seguridad. (IP SEC)
* VPN.

## **Análisis de riesgos de seguridad:**

* **Riesgos en base al comportamiento humano**:
  + **Fugas de información**: Errores por exceso de confianza.
  + **Ataques de virus**: Priorizar beneficios sobre los riesgos.

## **Seguridad por niveles en OSI:**

* **Físico** (Capa 1):
  + Auditar el canal que se use.
  + Plano de la red.
  + Análisis de la topología.
  + Puntos de acceso físico.
  + Potencias y/o frecuencias utilizadas.
* **Enlace de datos** (Capa 2): Último nivel que encapsula a los anteriores.
  + Uso de analizador de protocolos para control de direcciones MAC.
  + Analizador de configuración.
  + Analizador de tráfico y colisiones.
  + Evaluación de accesos WiFi.
* **Red** (Capa 3): El centro de la auditoría serán las rutas y direcciones.
  + Trabajo en el router sobre las contraseñas, configuraciones, protocolos de ruteo, listas de control de acceso, logs.
  + Auditoría en ARP y direccionamiento IP.
    - Estatico o dinamico.
* **Transporte** (Capa 4): Auditar el establecimiento de sesiones y puertos.
  + Operación con conexión (TCP) o sin conexión (UDP).
* **Aplicación** (Capa 7):
  + Auditar servidores.
  + Auditar accesos remotos.
  + Auditar Firewall y DNS.
  + Auditar Correos electrónicos.
  + Control de logs.

## **Firewall**:

* Sistema que crea una barrera segura entre dos redes. (una interna y otra externa).
* Compuesto por HW y SW.
* **Beneficios**:
  + Concentra la seguridad en un único punto.
  + Controla el acceso.
  + Regula el uso de la red exterior.
  + Registra el empleo de la red interna y externa.
  + Protege de ataques externos.
  + Limita el tráfico de servicios vulnerables.
  + Mejora la privacidad del sistema.
    - Ocultar direcciones IP internas.
    - Bloquear servicios.

### **Tipos**:

* **Nivel de red**: Direcciones IP y números de puerto.
  + Ej: Router.
* **Nivel de aplicación**: No permite tráfico directo entre redes.
  + Ej: Proxy.

### **Decisiones al implementar:**

* **Política de seguridad de la organización:**
  + Negación de todos los servicios salvo los autorizados.
  + Permitir libremente el uso de todo excepto lo prohibido.
  + Medir y auditar el uso de la red.
* **Nivel de seguridad deseado:**
  + Análisis de necesidades con niveles de riesgo aceptables.
  + Nivel de seguridad que satisface.
    - Solución de compromiso.
* **Evaluación de costos:**
  + Mejor relación costo - beneficio

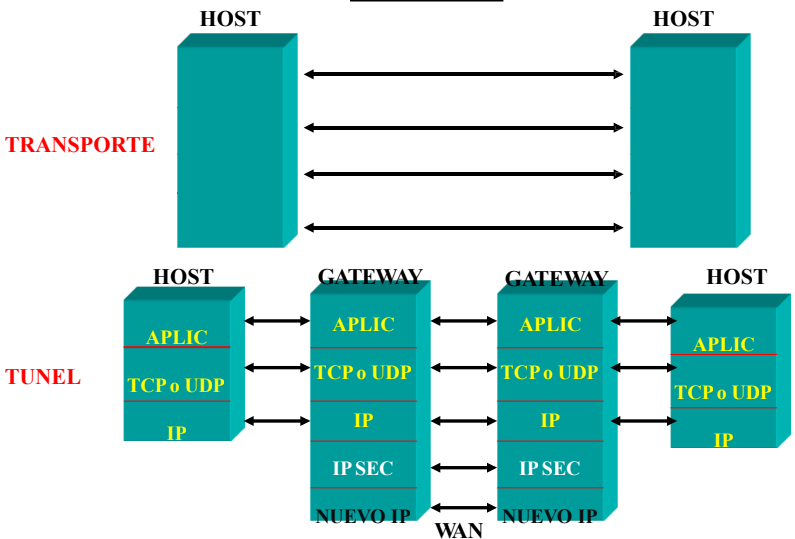
## **Firma digital:**

* Técnica de seguridad informática aplicada sobre la información digital que se intercambia en una red.
* **Se basa en**:
  + **Criptosistema asimétrico**: Dos claves.
    - Clave pública y clave privada.
  + **Función matemática Hash**.
    - Digest: Salida de longitud fija.
  + **Autoridad certificante**: Registra las claves públicas y las distribuye en forma segura.
* **Provee**:
  + **Autenticidad.**
  + **Integridad.**
  + **No repudio.**
* Puede adicionarse el encriptado completo de un mensaje con lo que se provee confidencialidad.

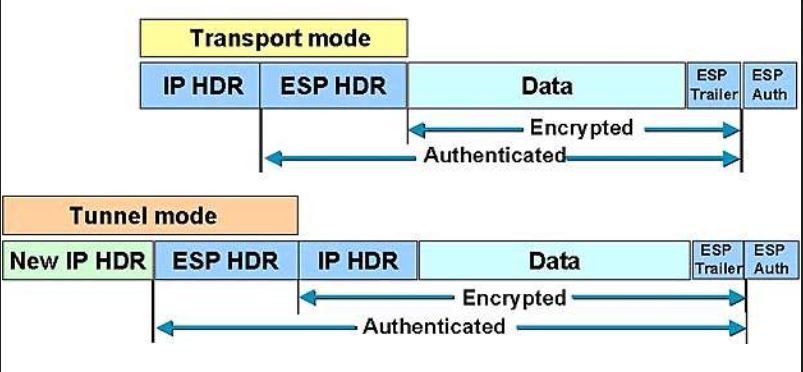
## **IP Security: IP Sec:**

* Conjunto de protocolos de seguridad que permiten agregar encriptado y autenticación a la comunicación.
* **Capa**: 3.
  + Transparente para las aplicaciones.
* Uso frecuente en VPN.

### **Modos de aplicación:**



* **Transporte**: De un host a otro.
  + Izquierda:
    - Capa aplicación.
    - Protocolo TCP o UDP.
    - IPSEC.
    - IP.
  + Derecha:
    - IPSEC.
    - IP.
* **Túnel**:



* **Transporte**: Solo protege la información de transporte. (no protege la info de la capa IP).
* **Túnel**: Protege también la información de capa de red. Protege todo, carga importante de protocolo (el costo que se paga).

## **Seguridad en Wireless:**

* **WPS** (WiFi Protected Setup): Mecanismos para facilitar la conexión de dispositivos a una red inalámbrica.
  + Más usado: Intercambio por PIN.
* **WEP** (Wired Equivalent Privacy): Ofrece seguridad similar a la red cableada mediante una encriptación.
* **WPA** (WiFi protected access): Agrega seguridad mediante el uso de claves dinámicas proporcionadas a cada usuario.
* **WPA 2**: usa algoritmo de encriptación AES.
  + AES: Advanced Encryption Standard.
* **WPA 2 PSK** (Pre Shared Key): Uso doméstico o de oficinas pequeñas.
  + Se comparte la clave.
* **WPA 2 TKIP**: Usa un protocolo de integridad de clave temporal que cambia dinámicamente las claves de un sistema a medida que se utiliza.
* **Otros Recursos:**
  + Nombre de red (SSID).
  + Filtrado de direcciones MAC.

### **Comparativa entre WEP - WPA - WPA 2:**

|  | **WEP** | **WPA** | **WPA 2** |
| --- | --- | --- | --- |
| **Encriptación** | RC4 | RC4 | AES |
| **Rotación de Claves** | No tiene | Claves de sesión dinámicas | Claves de sesión dinámicas |
| **Distribución de claves** | Asignada manualmente a cada dispositivo | Automática | Automática |
| **Autenticación** | WEP Key | 802.1x, EAP | 802.1x, EAP |