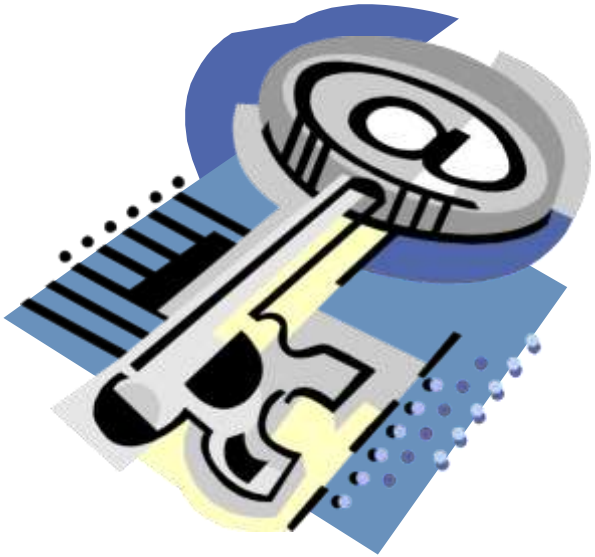
UTN.BA
UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

REDES DE INFORMACIÓN



SEGURIDAD EN REDES DE DATOS

Ingeniero ALEJANDRO ECHAZÚ

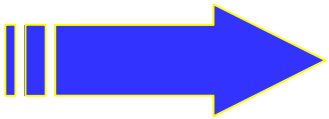
CONCEPTOS GENERALES

CONFIDENCIALIDAD O PRIVACIDAD

AUTENTICIDAD

INTEGRIDAD DE LOS DATOS

ATAQUES INFORMÁTICOS



INTERCEPTACIÓN

FABRICACIÓN

MODIFICACIÓN

DESTRUCCIÓN

ALGUNOS MÉTODOS

CLAVES DE ACCESO: AL SISTEMA O LOS RECURSOS

ENCRIPTADO DE DATOS

SEGURIDAD FÍSICA DE DISPOSITIVOS

FIRMA DIGITAL

FIREWALL

CAPACITACIÓN DE USUARIOS Y ADMINISTRADORES

PROTOCOLOS DE SEGURIDAD (IP SEC POR EJEMPLO)

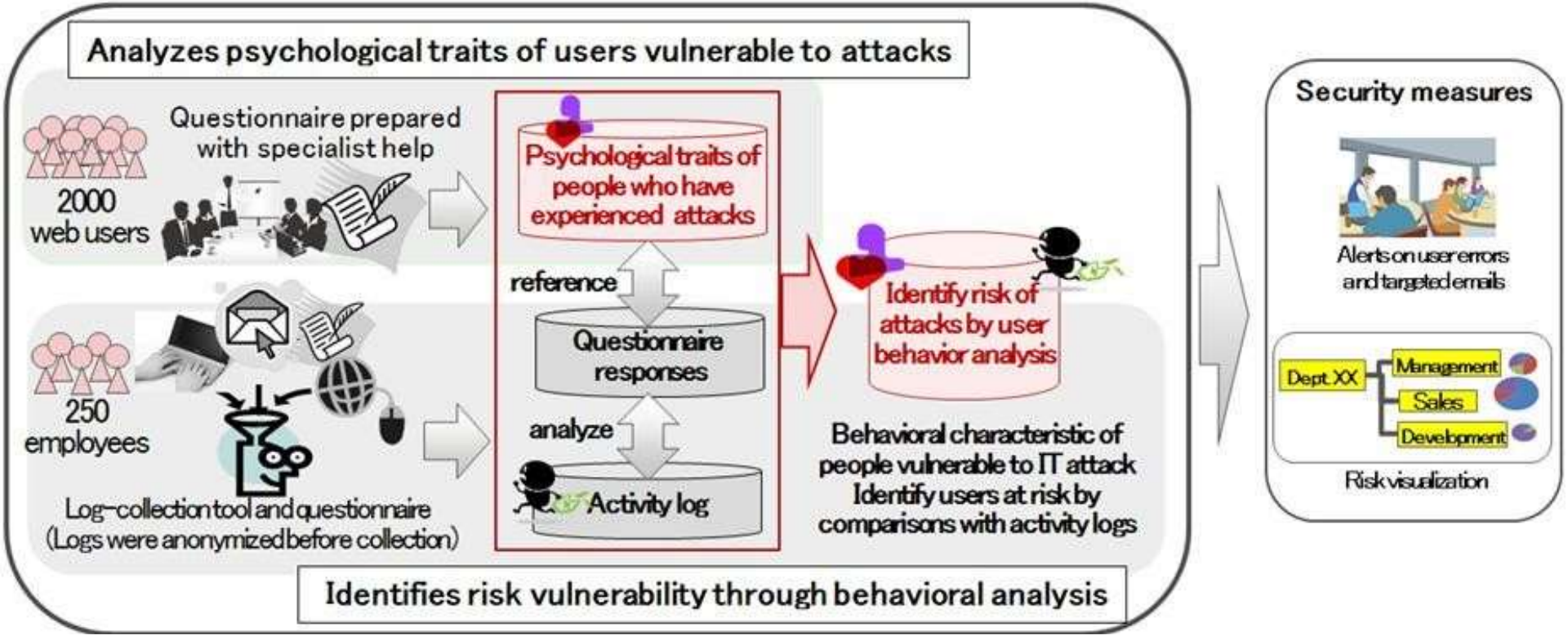
RED PRIVADA VIRTUAL (VPN)

ANÁLISIS DE RIESGOS DE SEGURIDAD

Riesgos en base al comportamiento humano

Fugas de información → **•Errores humanos o acciones accidentales por exceso de confianza**

Ataques de virus → **•Priorizar beneficios sobre los riesgos**



http://www.tendencias21.net/Fujitsu-identifica-a-usuarios-vulnerables-a-ataques-ciberneticos-por-su-comportamiento_a39484.html

SEGURIDAD POR NIVELES

(libro de Alejandro Corletti)

CONSIDERA PROCEDIMIENTOS PARA AUDITAR REDES BASADAS EN 802.3 Y TCP/IP.

MODELO OSI

Último nivel que encapsula a los anteriores.

Uso de analizadores de protocolos para control de direcciones MAC, de configuraciones, análisis de tráfico y de colisiones, evaluación de accesos wifi, etc.

Auditar el canal que se use

Plano de la red

Análisis de la topología

Puntos de acceso físico

Potencias, frecuencias utilizadas

SEGURIDAD POR NIVELES

MODELO OSI

Se audita servidores, accesos remotos, Firewall, correos electrónicos, DNS, etc.

Control de archivos .Log

Se audita el establecimiento de sesiones y los puertos. Operación con conexión (TCP) o sin conexión (UDP).

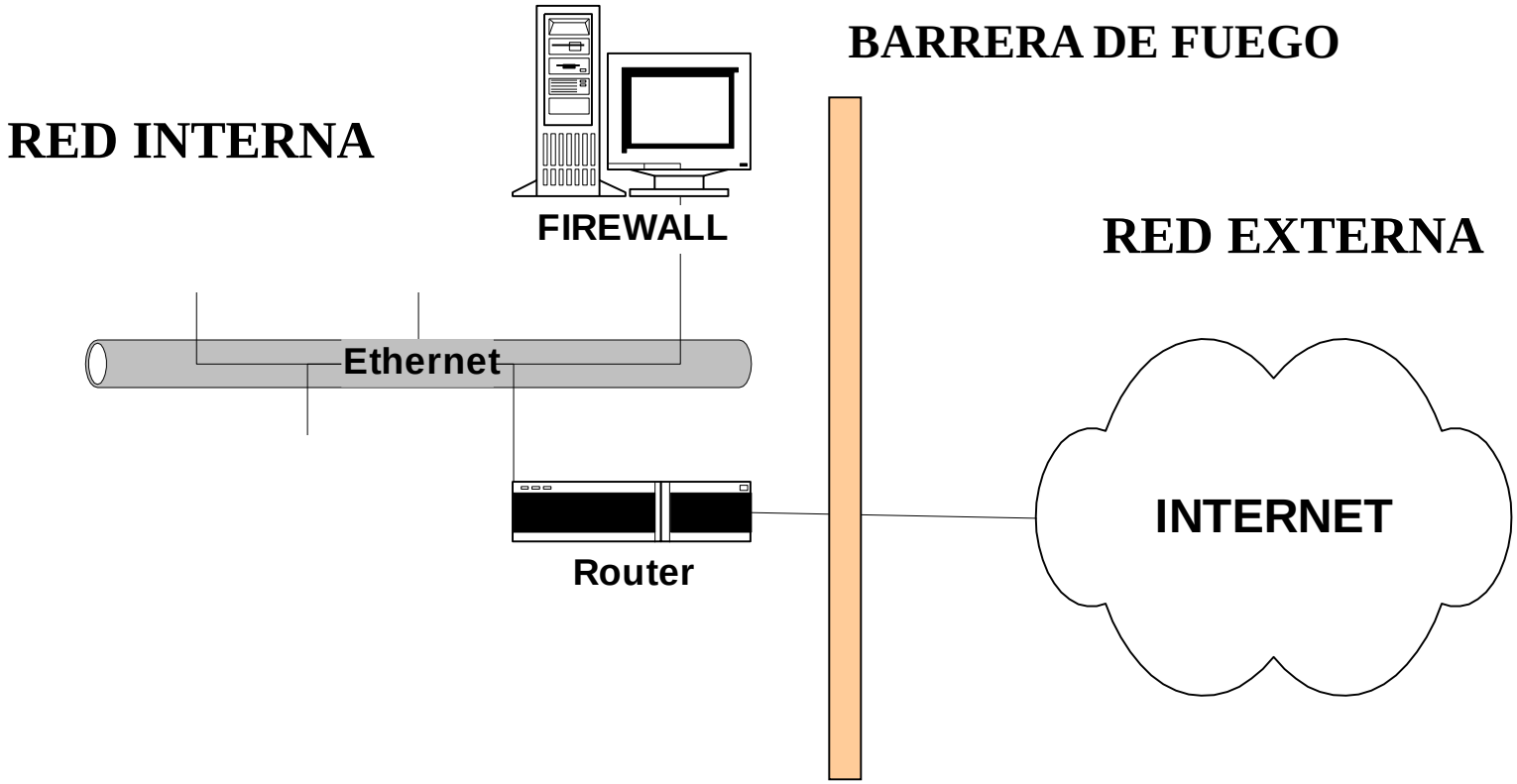
Centro de la auditoría serán las rutas y direcciones.

Trabajo en el Router sobre contraseñas, configuración, protocolo de ruteo, listas de control de acceso, archivos .Log (alarmas), etc.

Auditoría en ARP y direccionamiento IP (estático o dinámico)

FIREWALL

ES UN SISTEMA QUE CREA UNA BARRERA SEGURA ENTRE DOS REDES. SE COMPONE DE HARDWARE Y SOFTWARE.



BENEFICIOS DE UN FIREWALL

- **CONCENTRA SEGURIDAD EN UN ÚNICO PUNTO.**
- **CONTROLA ACCESO.**
- **REGULA EL USO DE LA RED EXTERIOR.**
- **REGISTRA EL EMPLEO DE LA RED INTERNA Y LA EXTERNA.**
- **PROTEGE DE ATAQUES EXTERNOS.**
- **LIMITA EL TRÁFICO DE SERVICIOS VULNERABLES.**
- **MEJORA LA PRIVACIDAD DEL SISTEMA. POR EJEMPLO OCULTAR DIRECCIONES IP INTERNAS O BLOQUEAR SERVICIOS.**

DECISIONES AL IMPLEMENTAR UN FIREWALL

1RO POLÍTICA DE SEGURIDAD DE LA ORGANIZACIÓN.

- **NEGACIÓN DE TODOS LOS SERVICIOS, EXCEPTO ALGUNOS AUTORIZADOS.**
- **PERMITIR LIBRE USO DE TODO, EXCEPTO LO EXPRESAMENTE PROHIBIDO.**
- **MEDIR Y AUDITAR EL USO DE LA RED.**

2DO NIVEL DE SEGURIDAD DESEADO.

- **ANÁLISIS DE NECESIDADES CON NIVELES DE RIESGO ACEPTABLES.**
- **NIVEL DE SEGURIDAD QUE SATISFACE. SOLUCIÓN DE COMPROMISO.**

3RO EVALUACIÓN DE COSTOS.

- **MEJOR RELACIÓN COSTO – BENEFICIO.**

FIREWALL

ES UN COMPONENTE DE LA SEGURIDAD DE UNA RED. HAY QUE COMPLEMENTARLO CON OTRAS ACCIONES.

TIPOS DE FIREWALL

NIVEL DE RED

DIRECCIONES IP Y NÚMEROS DE PUERTO.

EJEMPLO = ROUTER.

NIVEL DE APLICACIÓN

NO PERMITEN TRÁFICO DIRECTO ENTRE LAS REDES.

EJEMPLO = SERVIDOR PROXY.

FIRMA DIGITAL

ES LA TÉCNICA DE SEGURIDAD INFORMÁTICA APLICADA SOBRE LA INFORMACIÓN DIGITAL QUE SE INTERCAMBIA EN UNA RED, BASADA EN:

- **CRIPTOSISTEMA ASIMÉTRICO**

  CLAVE PÚBLICA

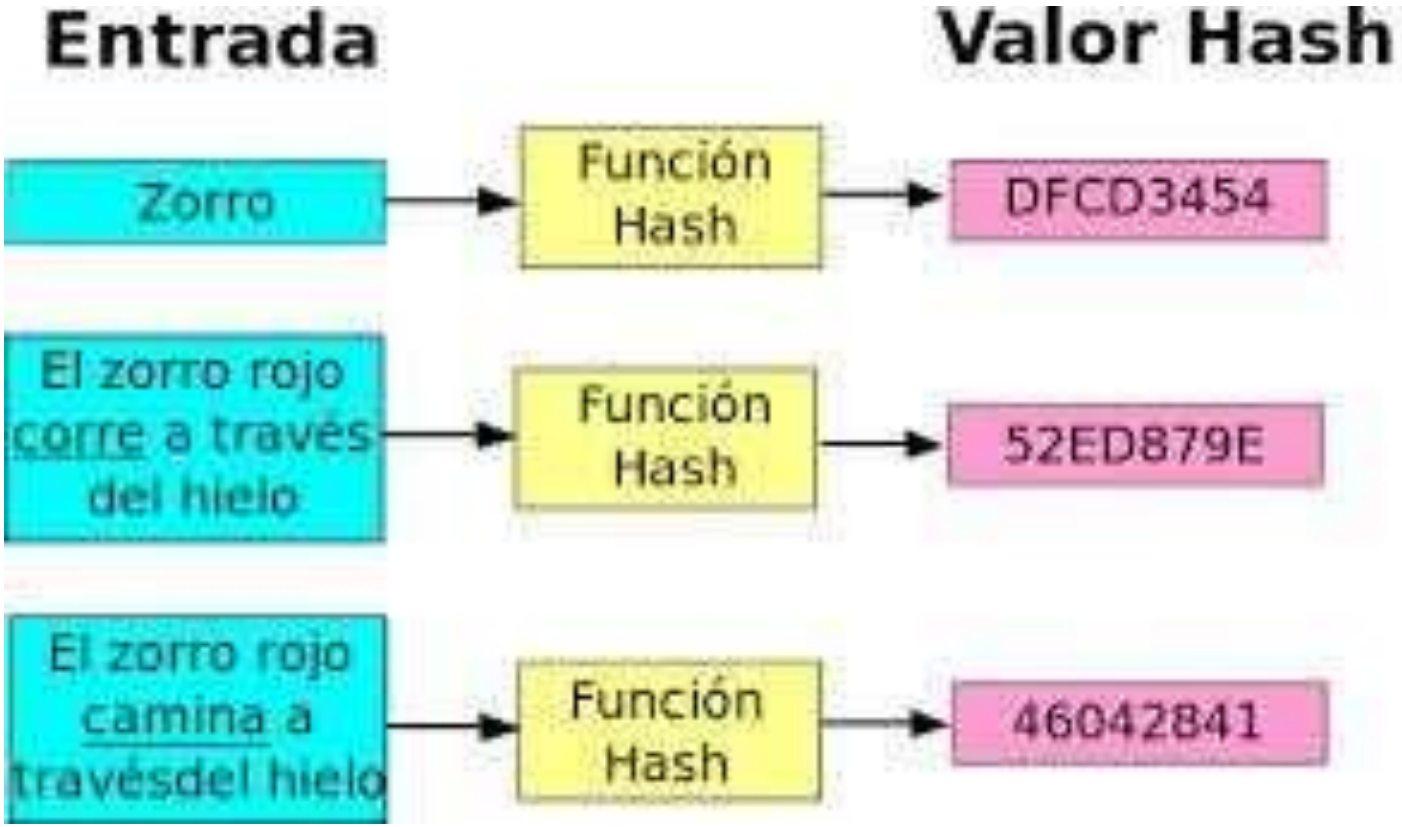
  CLAVE PRIVADA

- **FUNCIÓN MATEMÁTICA (HASH). Salida long fija (DIGEST)**
- **AUTORIDAD CERTIFICANTE**

PROVEE AUTENTICIDAD, INTEGRIDAD Y NO REPUDIO.

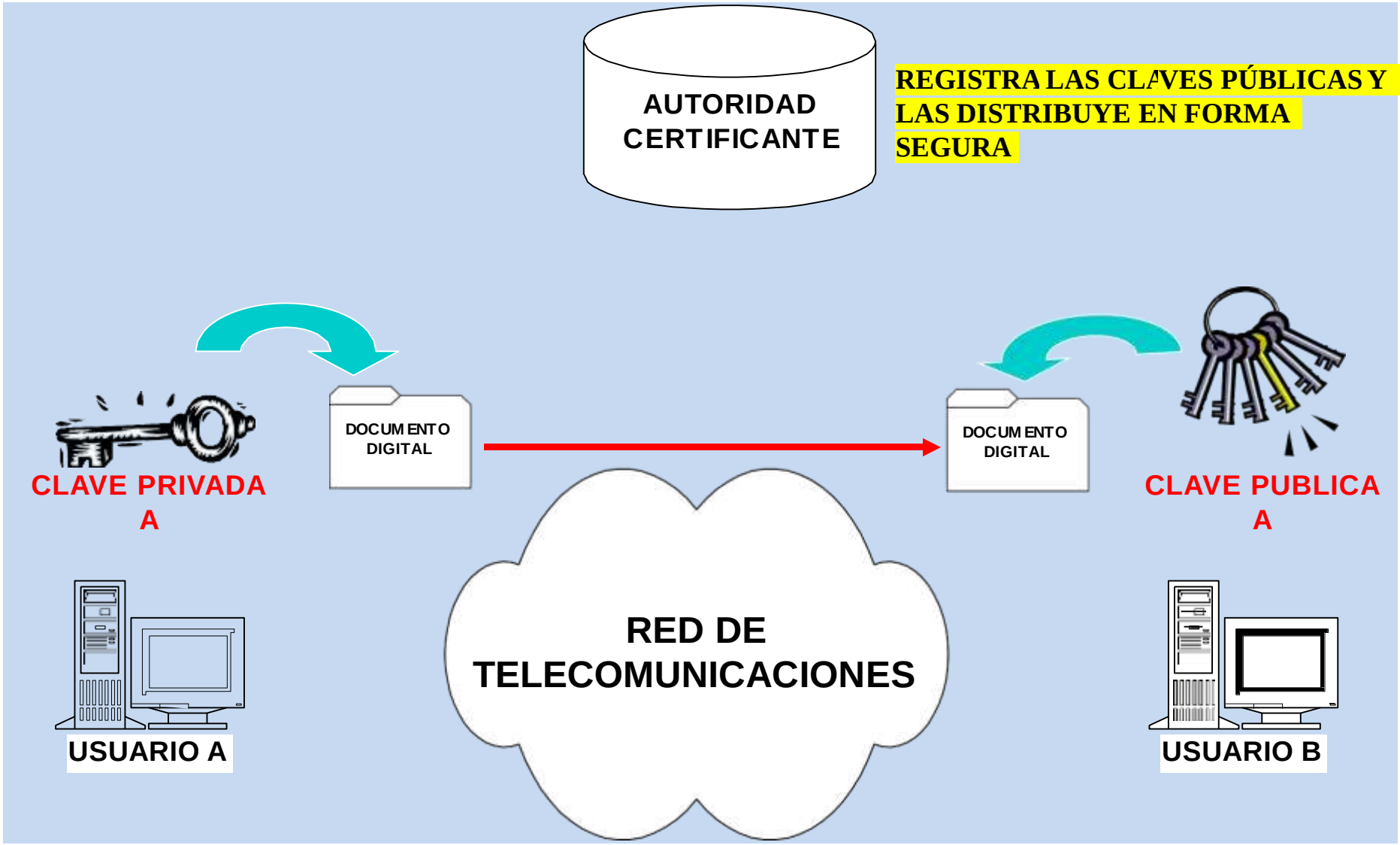
PUEDE ADICIONARSE EL ENCRIPTADO COMPLETO DE UN MENSAJE CON LO QUE SE PROVEE CONFIDENCIALIDAD (PRIVACIDAD)

FUNCIÓN HASH



Firma Digital | Argentina.gob.ar

FIRMA DIGITAL



IP SECURITY

IP SEC

ES UN CONJUNTO DE PROTOCOLOS DE SEGURIDAD QUE PERMITEN AGREGAR ENCRIPTADO Y AUTENTICACIÓN A LA COMUNICACIÓN.

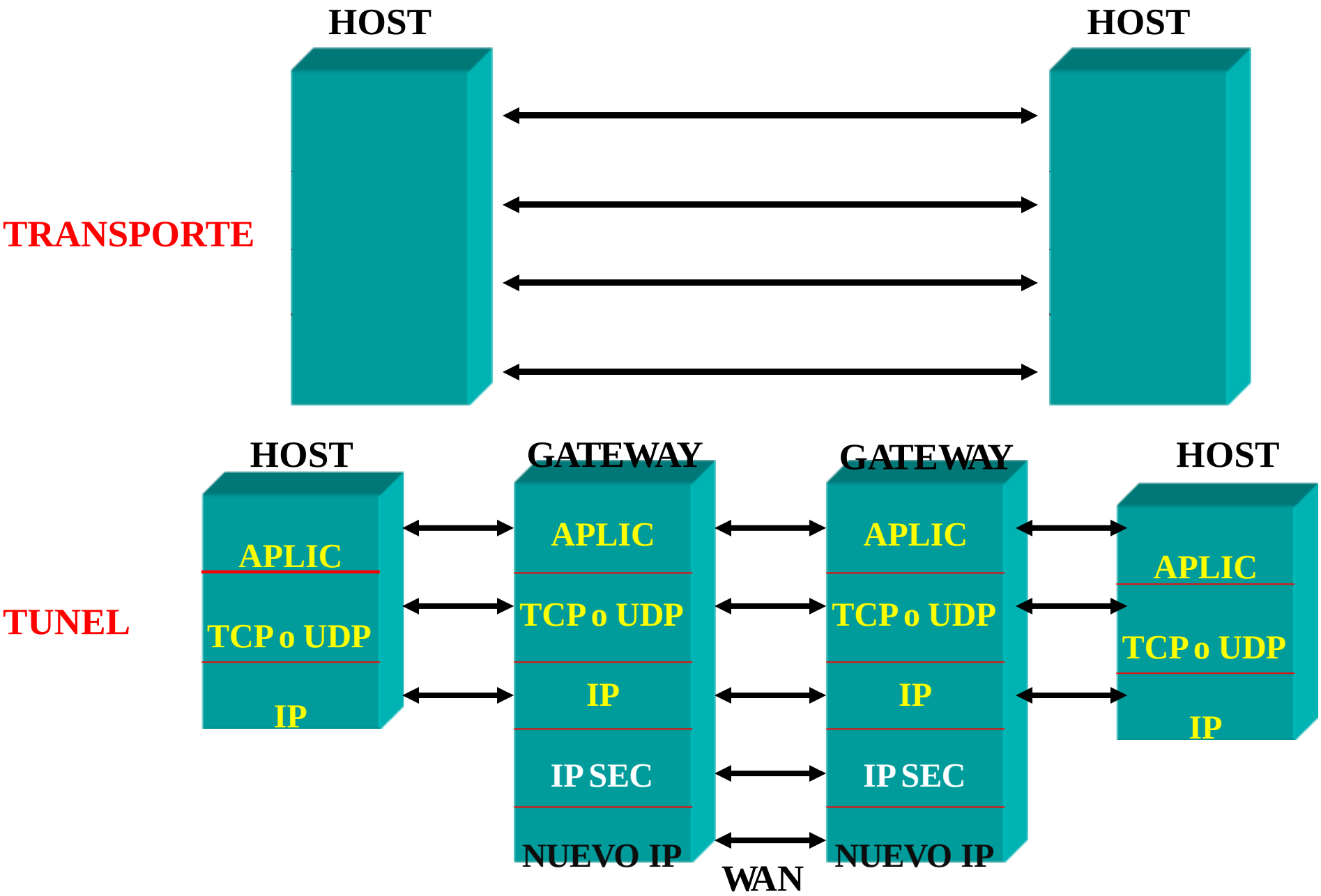
ES DE CAPA 3 RESULTANDO TOTALMENTE TRANSPARENTE PARA LAS APLICACIONES.

USO FRECUENTE EN VPN.

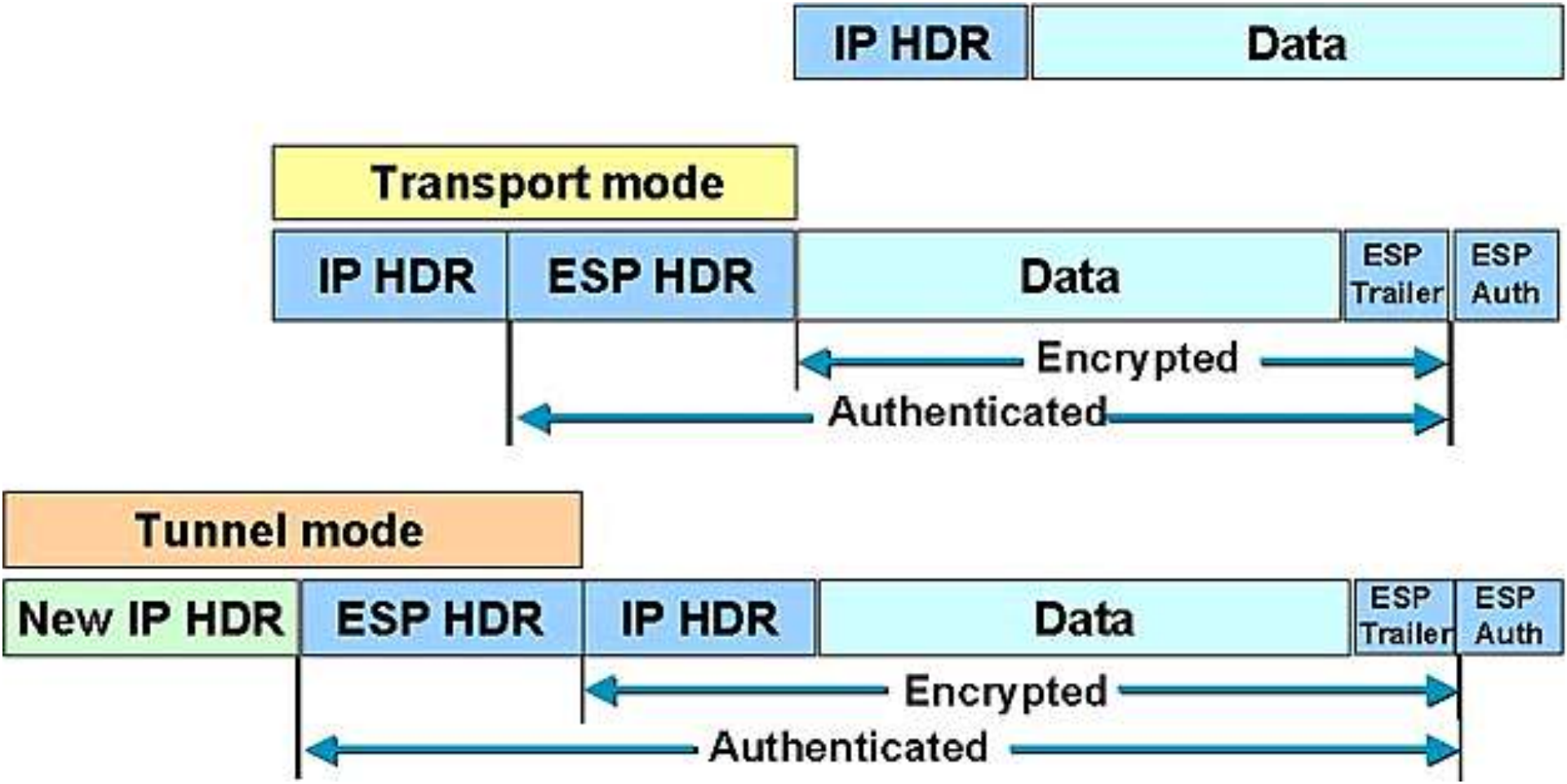
MODOS DE APLICACIÓN:

- **TRANSPORTE**
- **TÚNEL**

IP SEC


HOST
HOST
TRANSPORTE
HOST
GATEWAY
GATEWAY
HOST
TUNEL
APLIC
TCP o UDP
IP
APLIC
TCP o UDP
IP
IP SEC
NUEVO IP
APLIC
TCP o UDP
IP
IP SEC
NUEVO IP
APLIC
TCP o UDP
IP
WAN

MODOS IP SEC



Encapsulating Security Payload (ESP)

SEGURIDAD EN REDES INALÁMBRICAS

- **WPS (WiFi Protected Setup) son mecanismos para facilitar la conexión de dispositivos a una red inalámbrica. El más usado es el intercambio de PIN.**
- **WEP (Wired Equivalent Privacy) ofrece seguridad similar a la red cableada mediante una encriptación.**
- **WPA (Wi-Fi Protected Access) agrega seguridad mediante el uso de claves dinámicas proporcionadas a cada usuario.**
- **WPA2 usa algoritmo de encriptación AES (Advanced Encryption Standard).**
- **WPA2 PSK (Pre-Shared Key) es para uso doméstico o de oficinas pequeñas donde se comparte la clave.**
- **WPA2 TKIP usa un protocolo de integridad de clave temporal que cambia dinámicamente las claves de un sistema a medida que se utiliza.**
- **Otros recursos de seguridad:**
  - **— nombre de la red (SSID)**
  - **— filtrado de direcciones MAC**

SEGURIDAD EN REDES INALÁMBRICAS

WEP vs WPA vs WPA2

	WEP	WPA	WPA2
ENCRYPTION	RC4	RC4	AES
KEY ROTATION	NONE	Dynamic Session Keys	Dynamic Session Keys
KEY DISTRIBUTION	Manually typed into each device	Automatic distribution available	Automatic distribution available
AUTHENTICATION	Uses WEP key as Authentication	Can use 802.1x & EAP	Can use 802.1x & EAP