UNIVERSIDAD SERGIO ARBOLEDA | Colsubsidio

Diplomado de Ciberseguridad y Gestión de Seguridad de la Información

Módulo 5:

Gestión de Identidades y Seguridad en Dispositivos y Redes

Sesión 2:

Seguridad en dispositivos y redes

OBJETIVO DE LA SESIÓN:

Al finalizar la sesión, el estudiante estará en capacidad de comprender los fundamentos de la gestión de identidades digitales, diferenciar los conceptos de autenticación y autorización, identificar los métodos de autenticación más comunes, y aplicar buenas prácticas básicas para proteger su identidad en entornos digitales personales y organizacionales.

Tipos de dispositivos y sus riesgos

¿Qué es un dispositivo digital?

Todo equipo que almacena, procesa o transmite información. Ejemplos:

- Computadores de escritorio y portátiles
- Teléfonos móviles y tablets
- Dispositivos de Internet de las Cosas (IoT): impresoras Wi-Fi, cámaras de seguridad, asistentes virtuales, relojes inteligentes

Tipo de Dispositivo	Riesgos comunes
Computador	Malware, robo de archivos, keyloggers, ataques remotos
Celular	Robo físico, spyware, acceso a redes sociales, apps maliciosas
IoT (casa inteligente)	Uso de contraseñas por defecto, falta de actualizaciones, red abierta

Ejemplo:

Un televisor inteligente sin contraseña y sin actualizaciones puede ser vulnerado y usado como punto de entrada a tu red doméstica.

Buenas prácticas de seguridad en dispositivos

a) Actualizaciones automáticas

- Mantener el sistema operativo y aplicaciones actualizadas reduce la posibilidad de que los atacantes aprovechen vulnerabilidades conocidas.
- Muchos ataques ocurren semanas después de que una empresa publica un parche... porque la gente no lo instala.

Recomendación:

Activa las actualizaciones automáticas en tu celular, computador y router.

b) Uso de bloqueo de pantalla y contraseñas seguras

- Usa PINs, patrones o biometría (huella, rostro) para bloquear tus dispositivos.
- Configura el tiempo de bloqueo automático a 30 segundos – 1 minuto.

Ejemplo:

Si tu celular se pierde o te lo roban, el bloqueo de pantalla evita que accedan fácilmente a tus cuentas, fotos, y banca.

Buenas prácticas de seguridad en dispositivos

c) Desinstalar apps innecesarias

- Muchas aplicaciones piden más permisos de los necesarios.
- Elimina aquellas que ya no usas.

d) Antivirus y protección contra malware

- Especialmente en computadores, es necesario tener un antivirus actualizado.
- En celulares, evita instalar apps fuera de las tiendas oficiales.

Herramientas gratuitas recomendadas:

- **PC:** Windows Defender (incluido en Windows 10/11)
- **Android:** Avast Mobile Security, Bitdefender Free

e) Copias de seguridad (backups)

- Haz copias periódicas de tus documentos, fotos y archivos importantes.
- Puedes usar la nube (Google Drive, OneDrive) o discos externos cifrados.

Recomendación:

Haz al menos una copia mensual en un lugar diferente al dispositivo principal.

Ejercicio 1: Auditoría personal del dispositivo

Completar una lista de chequeo para evaluar cuán seguro está su dispositivo (actualizaciones, contraseñas, backup, etc.).

Seguridad en redes

¿Qué es una red?
Es el conjunto de dispositivos conectados entre sí para compartir datos e internet. Puede ser cableada o inalámbrica (Wi-Fi).

Tipo de red	Ejemplo	Nivel de riesgo
Red doméstica privada	Tu red de casa	Medio
Red corporativa segura	Oficina, universidad	Bajo (si está bien gestionada)
Red Wi-Fi pública	Café, centro comercial, aeropuerto	Alto

Riesgos en redes públicas:

- Intercepción de datos (sniffing)
- Ataques de intermediario (man-in-the-middle)
- Falsas redes Wi-Fi con nombres engañosos (“WiFi-Libre”, “Starbucks_Free”)

Ejemplo

Un atacante puede crear una red llamada “WiFi Gratis” y, si te conectas, interceptar tu tráfico y robar credenciales.

¿Qué es Sniffing/man in the middle (MITM)?

Sniffing: es una técnica para interceptar y analizar paquetes de datos que se transmiten a través de una red

MITM: el atacante se interpone entre víctima y servidor, interceptando y hasta modificando mensajes.

¿Cómo funciona?

- Captura de paquetes: Se capturan los paquetes de datos que viajan por la red.
- Análisis: Luego, el atacante analiza estos paquetes para extraer información valiosa.
- Uso malicioso: La información recopilada puede usarse para cometer fraude, robo de identidad u otras actividades ilícitas.

Ejemplo

Escenario:

Carlos se conecta a “WiFi_CaféGratis”.

Tráfico sin cifrar:

Atacante ve: usuario=carlos, clave=12345.

¿Cómo protegerse?

- Utiliza redes VPN y conexiones HTTP (cifradas) siempre que sea posible.
- Descarga software de fuentes confiables y mantén tus programas actualizados.
- Evita conectarte a redes Wi-Fi públicas o desconocidas.

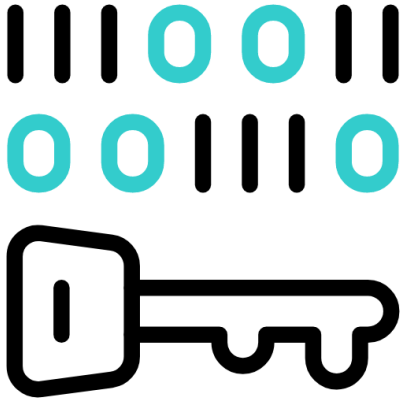
Tráfico cifrado (HTTPS o VPN):

Atacante solo ve: f93hd93hd8s3dh....

Resultado: Con HTTPS o VPN, el ataque se vuelve inútil

¿Qué es la encriptación?

Proceso de transformar datos legibles (texto plano) en datos ilegibles (texto cifrado) usando un algoritmo y una clave.



Solo quien tenga la clave correcta puede recuperar la información.

Ejemplos de uso diario:

- VPN → cifra todo tu tráfico de internet en un túnel seguro.
- HTTPS → cifra la comunicación entre navegador y servidor web.
- WhatsApp/Telegram → cifrado extremo a extremo en mensajes.

Beneficio clave:
Confidencialidad: aunque un atacante intercepte el tráfico, no podrá leerlo.

Tipos de cifrado

Los principales tipos de cifrado son simétrico y asimétrico. El cifrado simétrico usa una única clave secreta para cifrar y descifrar, mientras que el asimétrico (o clave pública) usa un par de claves: una pública para cifrar y una privada para descifrar.

Cifrado Simétrico

- Una misma clave secreta se usa para cifrar y descifrar.
- Ejemplo: AES (Advanced Encryption Standard).
- Rápido, ideal para cifrar grandes volúmenes de datos.

Cifrado Asimétrico

- Usa un par de claves: pública (cifrar) y privada (descifrar).
- Ejemplo: RSA (Rivest–Shamir–Adleman).
- Más seguro para compartir claves, pero más lento.

Cifrado Asimétrico

El cifrado asimétrico, o de clave pública, usa un par de claves vinculadas matemáticamente: una pública para cifrar y una privada para descifrar. La clave pública se distribuye ampliamente, permitiendo que cualquiera cifre un mensaje para el destinatario. Sin embargo, solo la clave privada correspondiente, que el destinatario mantiene en secreto, puede descifrar ese mensaje. Este sistema es crucial para la confidencialidad y la autenticación a través de firmas digitales.

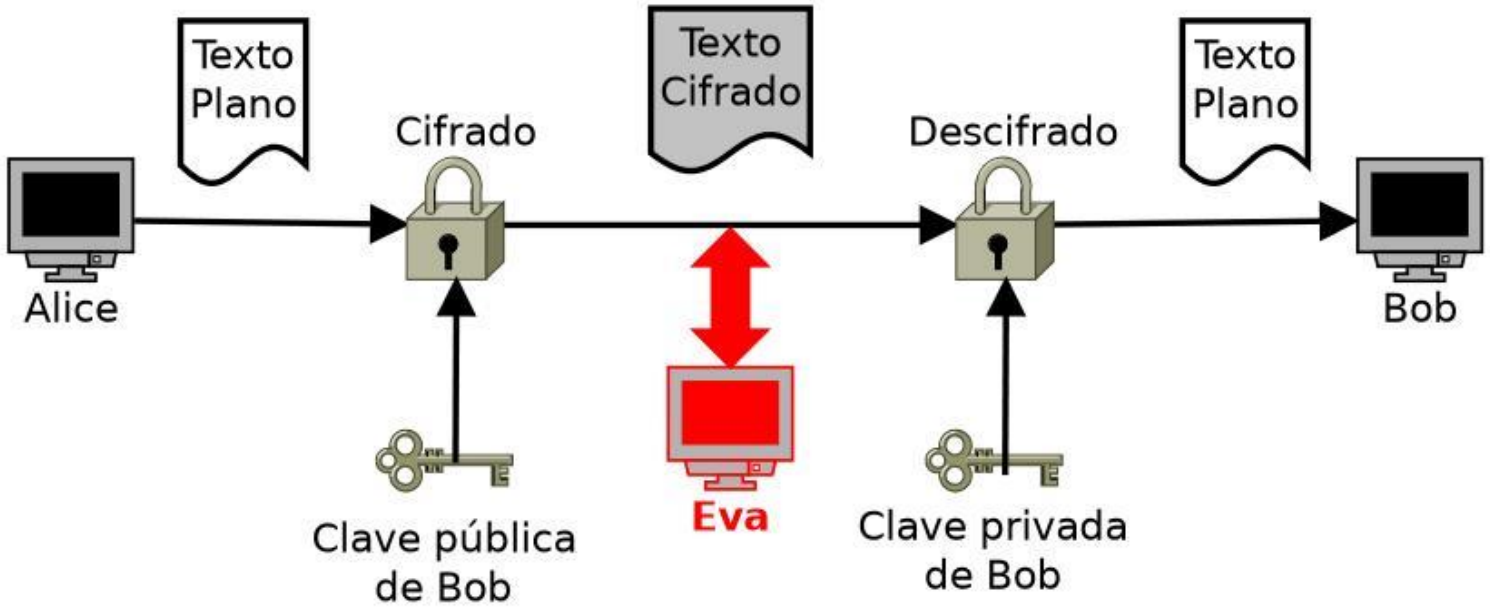
Cómo funciona

1. Generación de claves:
Cada usuario genera un par de claves, una pública y una privada.

2. Distribución de la clave pública:
El usuario comparte su clave pública con quien quiera que se comunique con él.

3. Cifrado:
Una persona toma la clave pública del destinatario y la usa para cifrar un mensaje.

4. Envío y descifrado:
El mensaje cifrado es enviado al destinatario, quien utiliza su clave privada (que solo él conoce) para descifrarlo y leerlo.



Tomada de 15

RSA (Rivest, Shamir y Adleman):
Se basa en la dificultad de factorizar grandes números primos, y se utiliza para cifrar y autenticar con firmas digitales en aplicaciones web y transacciones.

DSA (Algoritmo de Firma Digital):
Permite a un emisor firmar digitalmente un mensaje, que luego puede ser verificado por un receptor usando la clave pública del emisor.

ECC (Criptografía de Curva Elíptica):
Ofrece un nivel de seguridad equivalente al de RSA pero con claves más cortas, lo que lo hace más eficiente y popular en sistemas con recursos limitados, como las redes IoT.

RSA (Rivest, Shamir y Adleman)

El algoritmo RSA es un sistema de cifrado asimétrico que utiliza un par de claves, una pública y otra privada, para asegurar la comunicación y la autenticación. Se basa en la dificultad de factorizar grandes números primos. La clave pública, compartida abiertamente, se usa para cifrar datos, mientras que la clave privada, que se mantiene en secreto, se utiliza para descifrarlos. RSA es fundamental en la seguridad de internet, autenticando la identidad mediante firmas digitales y protegiendo las transferencias de datos sensibles en protocolos como TLS/SSL.

Generación de claves:
Se crean dos claves criptográficamente vinculadas: una pública y una privada.

Descifrado (con clave privada):
Solo el poseedor de la clave privada puede descifrar el mensaje cifrado con la clave pública correspondiente.

Cifrado (con clave pública):
Cualquier persona puede usar la clave pública para cifrar un mensaje.

Ejemplo

Escenario:
Se quiere enviar un mensaje seguro a Ana.
Ana genera dos claves:
Clave pública → se comparte con todos.
Clave privada → solo ella la tiene.

Cifrado: Se usa la clave pública de Ana para cifrar: "Hola Ana" → 8d93jf83...

Descifrado: Ana recibe el texto cifrado y usa su clave privada → recupera "Hola Ana".

Cifrado Simétrico

Los tipos principales de cifrado simétrico son los cifrados de bloque y los cifrados de flujo, donde los cifrados de bloque procesan datos en bloques de tamaño fijo (como AES), mientras que los de flujo los procesan de forma continua, bit a bit o byte a byte (como RC4).

Son ideales para cifrar grandes volúmenes de datos, como sistemas de archivos, bases de datos o copias de seguridad.

Son muy útiles para la transmisión en tiempo real de datos, como video o audio.

Casos de uso para el cifrado simétrico

- Seguridad de datos (especialmente para grandes cantidades de datos)
- Comunicación y navegación web seguras
- Seguridad en la nube
- Cifrado de bases de datos
- Integridad de los datos
- Cifrado de archivos, carpetas y discos
- Cifrado basado en hardware
- Gestión del cumplimiento

Tipos

- Data Encryption Standard (DES) y Triple DES (3DES)
- Advanced Encryption Standard (AES)
- Twofish
- Blowfish
- RC4

Advanced Encryption Standard (AES)

Es un algoritmo de cifrado simétrico de bloque que protege datos sensibles transformando información legible en un formato seguro e ilegible, utilizando la misma clave para cifrar y descifrar.

Muy rápido y seguro: usado en VPN, HTTPS, WiFi (WPA2/WPA3), WhatsApp.

Cómo funciona:

Se divide el mensaje en bloques de 128 bits (16 caracteres)

Cada bloque pasa por varias rondas de sustitución, permutación y mezcla

El resultado es un texto cifrado irreconocible

Con la misma clave se aplica el proceso inverso para descifrar.

A finales de agosto de 2023, Microsoft Purview Information Protection comenzó a utilizar el Estándar de cifrado avanzado (AES) con una longitud de clave de 256 bits en modo de encadenamiento de bloques de cifrado (AES256-CBC)

Ejemplo de Cifrado Simétrico (AES)

Escenario:
Mensaje original: "Hola Luis“
Clave secreta: "ABC12345“

Cifrado (con AES):Texto plano → Algoritmo AES + clave → h93j8fs8dhf9...

Descifrado: Texto cifrado + misma clave → Algoritmo AES → "Hola Luis"

Cómo cifran VPN y HTTPS

VPN

- Antes de salir a internet, todos los datos pasan por un algoritmo de cifrado (AES-256).
- El tráfico viaja dentro de un **túnel seguro** → nadie puede leerlo en redes públicas.

HTTPS

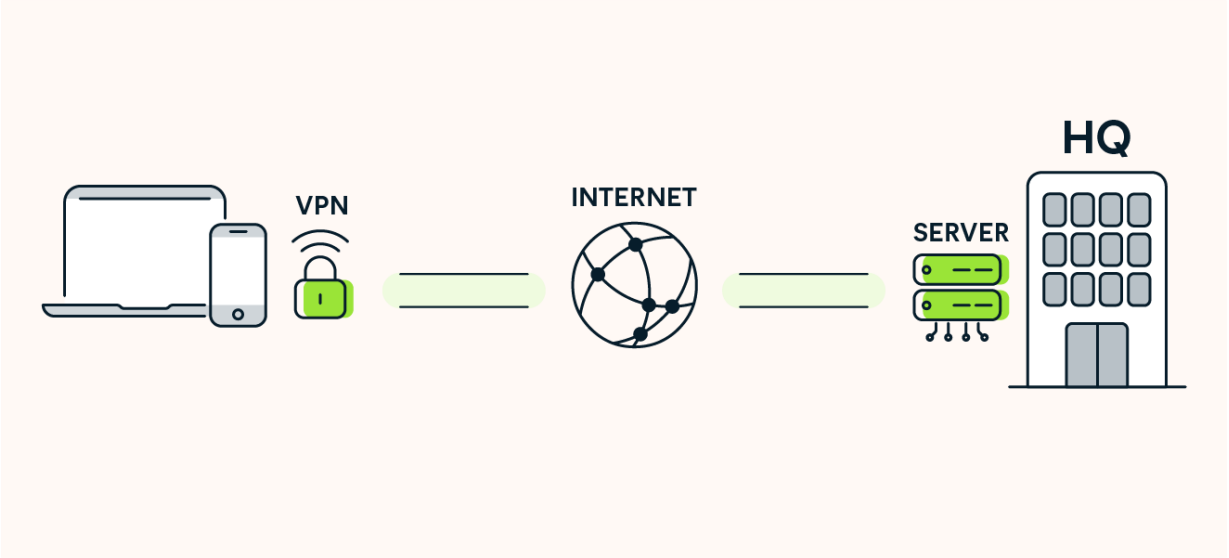
- Navegador ↔ Servidor usan **asimétrico (RSA)** para intercambiar una clave secreta.
- Luego usan **simétrico (AES)** para cifrar toda la sesión (más rápido).
- Resultado: si un atacante captura el tráfico, verá solo datos cifrados.

¿Qué es una Red Privada Virtual (VPN)?

Crea un túnel cifrado entre tu dispositivo e internet.
Actúa como si estuvieras conectado directamente a la red de confianza (empresa, casa).

Beneficios:

- Evita que atacantes lean tu tráfico en WiFi públicas.
- Oculta tu dirección IP real.
- Permite acceso seguro a sistemas corporativos.

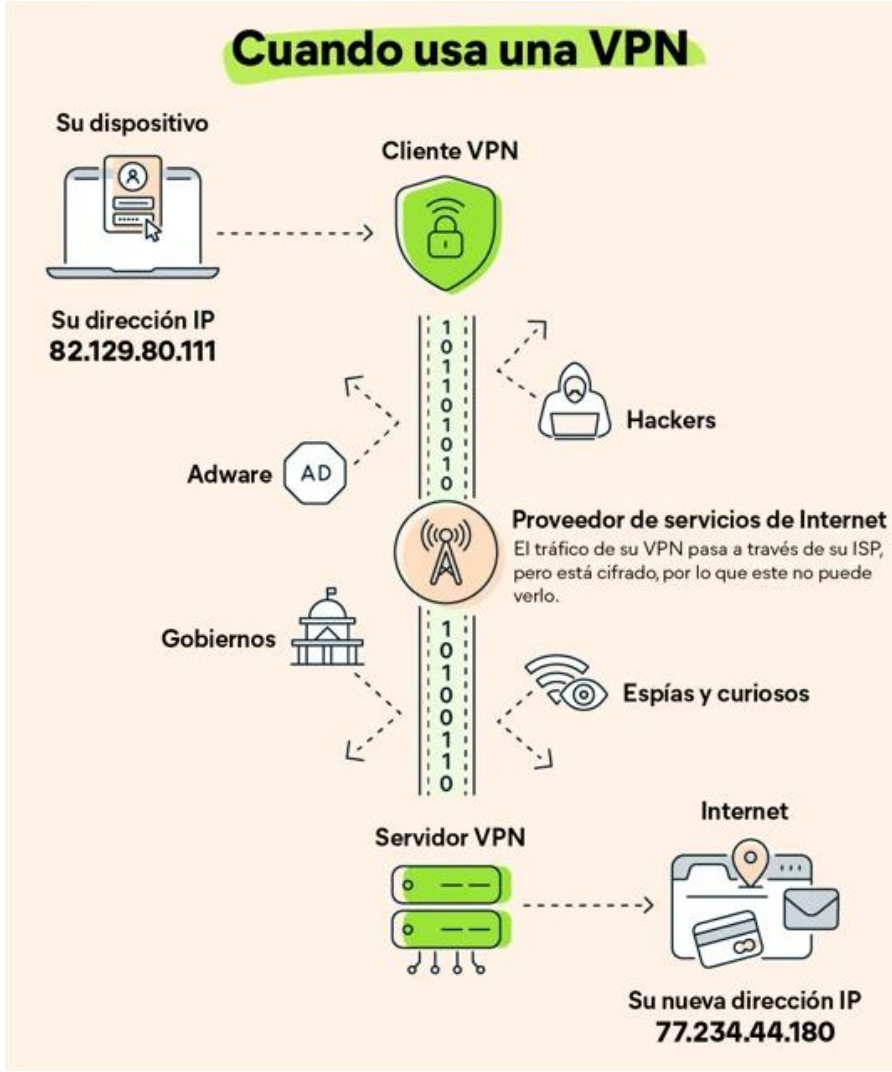


Tomado de [14]

Al utilizar una VPN, se oculta la información siguiente:

- Ubicación y dirección IP
- Búsquedas recientes (ocultas a tu proveedor de servicios de internet)
- Sitios web que has visitado (ocultos a tu proveedor de servicios de internet)
- Los datos que envías y recibes
- Los archivos que descargas

Tomado de [14]



Tomado de [14]

Ejemplo

Escenario:
Laura está en un aeropuerto y necesita entrar al sistema contable de su empresa.

Sin VPN:
El atacante en la WiFi pública captura tráfico en texto plano → ve credenciales de Laura.
Con VPN:
Todo su tráfico viaja cifrado dentro de un túnel.El atacante solo ve “basura cifrada” como: 8fj39sd9fhs82....

Resultado:
La VPN convierte una red insegura en un canal protegido.

¿Qué es un Firewall?

Un firewall es como un guardia de seguridad que decide qué tráfico de red entra y sale.

Funciona mediante reglas de filtrado.

Puede ser software (en tu PC) o hardware (en routers/servidores).

Puertos

Un puerto es como una "puerta" en un edificio por donde entra un tipo de tráfico.
Ejemplos:

- 80 → HTTP (web sin cifrar)
- 443 → HTTPS (web segura)
- 25 → SMTP (correo)
- 21 → FTP (transferencia de archivos)

Un firewall permite cerrar puertas innecesarias para reducir riesgos.

Escenario:
Una empresa quiere proteger su servidor web.

Requisitos:
- Solo debe responder a clientes en la web segura (HTTPS, puerto 443).
- Se prohíben accesos a Telnet (23) y FTP (21), usados por atacantes.

Reglas del Firewall
- Permitir entrada TCP puerto 443.
- Bloquear entrada TCP puerto 23 (Telnet).
- Bloquear entrada TCP puerto 21 (FTP).

Un escaneo con Nmap mostraría “puerto cerrado”.

Resultado:
Los clientes acceden a la web segura, pero un atacante que intente conectarse por Telnet no puede pasar.

Segmentación de redes

Dividir una red en subredes o segmentos independientes.

Cada segmento tiene accesos limitados → si uno es atacado, el resto se mantiene seguro.

En un hospital:
•**Red 1:** médicos y enfermeras → acceso a historias clínicas.
•**Red 2:** administrativos → acceso a nómina y finanzas.
•**Red 3:** IoT (monitores, cámaras, impresoras).

Un atacante vulnera una cámara de seguridad.
•Con segmentación: solo afecta la red de IoT.
•Sin segmentación: podría moverse hacia la base de datos de pacientes.

La segmentación limita el alcance del ataque y protege los datos sensibles.

Zero Trust Architecture

Modelo de seguridad basado en el lema: “Nunca confíes, siempre verifica”.

Nadie es confiable por defecto, ni siquiera los usuarios dentro de la red.

Principios:

- Autenticación en cada acceso.
- Autorización granular (solo lo que necesitas).
- Monitoreo continuo.

Escenario:
Pedro quiere entrar al servidor de nómina.

Modelo tradicional:
Al estar en la red corporativa, accede sin restricción.

Zero Trust:
Debe autenticarse con usuario + contraseña + MFA (token SMS).
Además, su acceso se limita a su rol: solo puede ver su propia nómina, no la de otros.

Resultado:
Incluso si un atacante roba las credenciales de Pedro, sin MFA ni permisos no puede hacer nada.

Buenas prácticas para proteger redes y conexiones

a) Cambiar nombre y contraseña del router doméstico

- Evita usar nombres como “Red de Juan” o el que viene por defecto (ej. “TP-LINK_1234”).
- Usa claves largas y difíciles de adivinar.

b) Usar cifrado WPA2 o WPA3

- Estos protocolos protegen la comunicación entre tu dispositivo y el router.
- No uses WEP (inseguro desde hace más de 10 años).

c) Desactivar la conexión automática a redes Wi-Fi

- Muchos celulares se conectan automáticamente a redes conocidas (y a redes que imitan sus nombres).
- Revisa esta configuración y desactívala.

d) No acceder a datos sensibles en redes públicas

- Evita abrir tu correo institucional, banca en línea o subir documentos importantes desde Wi-Fi públicas.
- Si es necesario, usa una VPN (red privada virtual) para cifrar tu conexión.

Ejercicio 2: Simulación de ataque por red Wi-Fi pública

Imagina que te conectas a una red abierta en un café y sufres interceptación de datos.

Cómo puedes evitarlo y que medidas preventivas tomarías.

FORO 5 ¿Y si tu teléfono fuera la puerta de entrada?

Pregunta detonante

“¿Crees que tu teléfono móvil o red de casa podrían ser un punto de entrada para un ciberdelito? ¿Qué puedes hacer hoy para reducir ese riesgo?”

Instrucciones

1. Responde con una reflexión personal (mínimo 150 palabras) en la que:

- Analices si tus dispositivos y red doméstica presentan riesgos.
- Describas al menos dos acciones concretas que podrías tomar para protegerlos mejor.

2. Comenta la publicación de al menos dos compañeros, aportando ideas, experiencias o recomendaciones complementarias de forma respetuosa y constructiva.

Referencias

1. Bishop, M. (2003). *Computer Security.*
2. Briceño, E. (2021). *Seguridad De La Información*
3. Kremer, E. Et al. (2019). *Ciberseguridad*
4. Ozkaya, E. (2019). *Cybersecurity: The Beginner's Guide: A comprehensive guide to getting started in cybersecurity*
5. *Bhatt, H. (2024, marzo 4). What is RSA? How does an RSA work? Encryption Consulting. https://www.encryptionconsulting.com/education-center/what-is-rsa/*
6. BrendaCarter. *(s/f). What is Zero Trust? Microsoft.com. Recuperado el 2 de septiembre de 2025, de https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview*
7. Farrier, E. (2023, agosto 12). *¿Qué es el sniffing de paquetes? Definición, tipos y protección. ¿Qué es el sniffing de paquetes? Definición, tipos y protección; Avast. https://www.avast.com/es-es/c-packet-sniffing*
8. Panda Security. *(2023, julio 27). ¿Qué es el cifrado AES? Una guía sobre el Advanced Encryption Standard. Panda Security Mediacenter. https://www.pandasecurity.com/es/mediacenter/cifrado-aes-guia/*
9. *¿Qué es el cifrado simétrico? (2024, octubre 11).* Ibm.com. *https://www.ibm.com/es-es/think/topics/symmetric-encryption*
10. *¿Qué es la encriptación y cómo funciona? (s/f). Google Cloud. Recuperado el 2 de septiembre de 2025, de https://cloud.google.com/learn/what-is-encryption?hl=es-419*
11. *¿Qué es la segmentación de la red? (s/f).* Palo Alto Networks. *Recuperado el 2 de septiembre de 2025, de https://www.paloaltonetworks.es/cyberpedia/what-is-network-segmentation*
12. *¿Qué es un firewall? Funcionamiento de los firewalls y tipos de firewalls. (2019, mayo 13). /. https://latam.kaspersky.com/resource-center/definitions/firewall?srsltid=AfmBOorZ3yBQKh5A9FOkQ1RIGROT3BiqV4TEYs3Qvp-z-Y1gEoGPR8QM*
13. *¿Qué es una red privada virtual o VPN? (s/f).* Microsoft.com. *Recuperado el 2 de septiembre de 2025, de https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-vpn*
14. Latto, N. (2020, abril 8). *¿Qué es una VPN y cómo funciona? ¿Qué es una VPN y cómo funciona?; Avast. https://www.avast.com/es-es/c-what-is-a-vpn*
15. Córdoba, D. (2022, octubre 5). *Criptografía asimétrica - Conceptos clave. Junco TIC. https://juncotic.com/criptografia-asimetrica-conceptos-clave/*