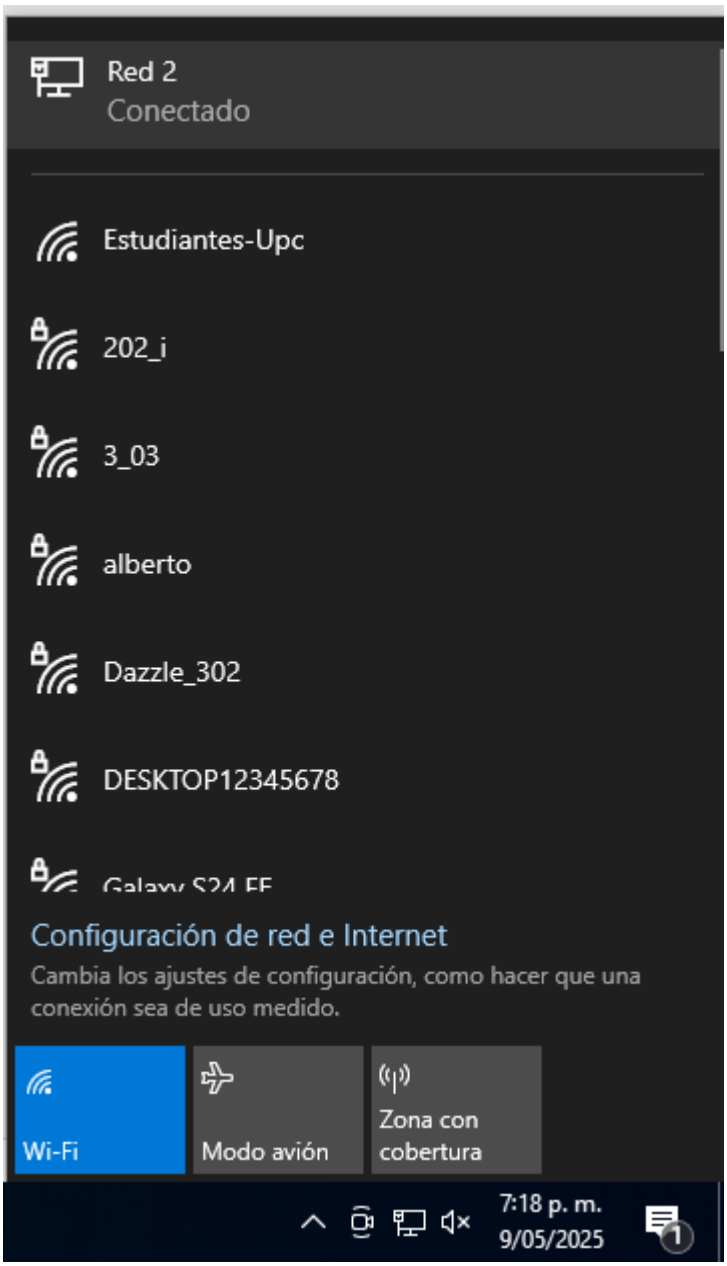
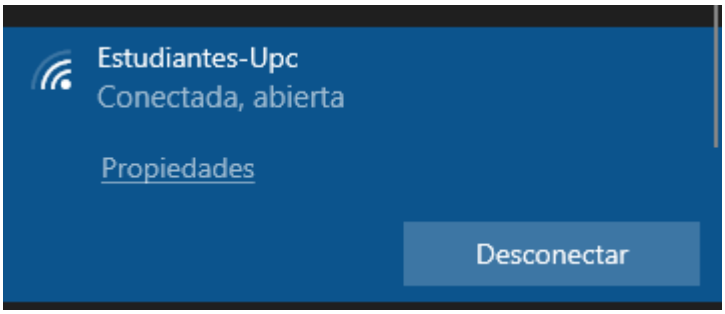
Laboratorio 10 - Uso seguro de redes públicas y privadas

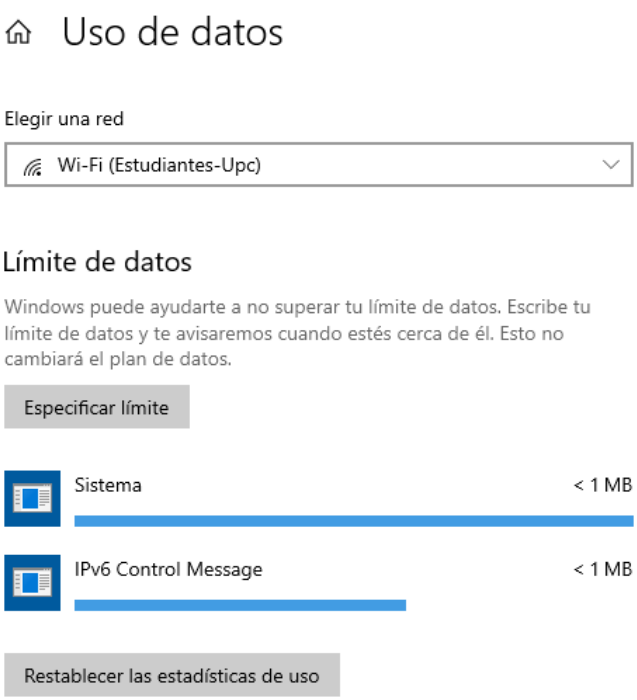
Vamos a ver las redes públicas y privadas que se listan



Nos conectamos a una red pública:

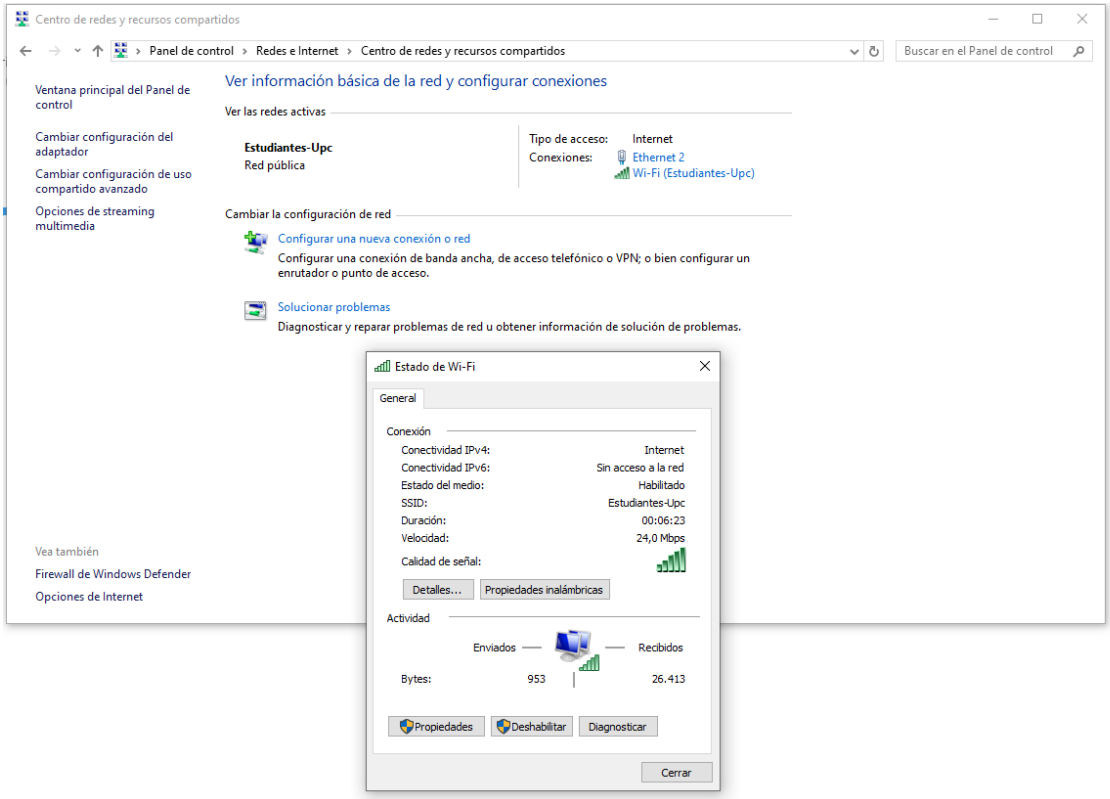


Vemos configuraciones:

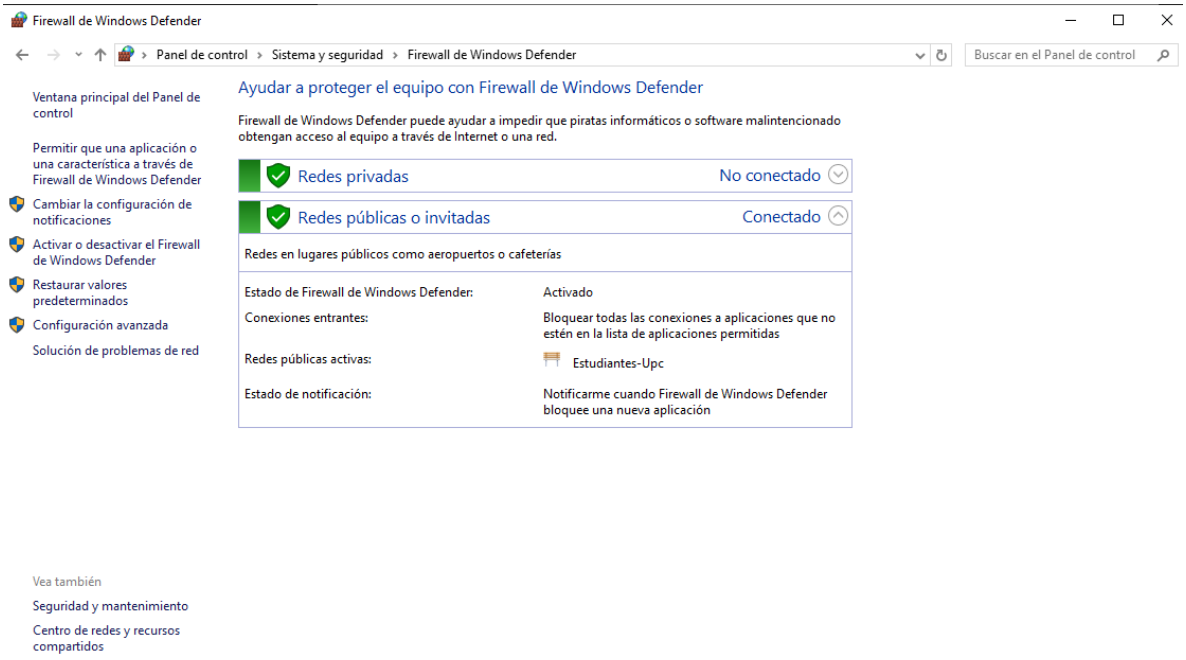


Las redes publicas son vulnerables a ataques man-in-the-middle

Ver más propiedades:


Centro de redes y recursos compartidos
Panel de control › Redes e Internet › Centro de redes y recursos compartidos
Buscar en el Panel de control
Ventana principal del Panel de control
Cambiar configuración del adaptador
Cambiar configuración de uso compartido avanzado
Opciones de streaming multimedia
Ver información básica de la red y configurar conexiones
Ver las redes activas
Estudiantes-Upc
Red pública
Tipo de acceso: Internet
Conexiones: Ethernet 2
Wi-Fi (Estudiantes-Upc)
Cambiar la configuración de red
Configurar una nueva conexión o red
Configurar una conexión de banda ancha, de acceso telefónico o VPN; o bien configurar un enrutador o punto de acceso.
Solucionar problemas
Diagnosticar y reparar problemas de red u obtener información de solución de problemas.
Vea también
Firewall de Windows Defender
Opciones de Internet
Estado de Wi-Fi
General
Conexión
Conectividad IPv4: Internet
Conectividad IPv6: Sin acceso a la red
Estado del medio: Habilitado
SSID: Estudiantes-Upc
Duración: 00:06:23
Velocidad: 24,0 Mbps
Calidad de señal:
Detalles...
Propiedades inalámbricas
Actividad
Enviados
Recibidos
Bytes: 953 26.413
Propiedades
Deshabilitar
Diagnosticar
Cerrar

Firewall:


Firewall de Windows Defender
Panel de control › Sistema y seguridad › Firewall de Windows Defender
Buscar en el Panel de control
Ventana principal del Panel de control
Permitir que una aplicación o una característica a través de Firewall de Windows Defender
Cambiar la configuración de notificaciones
Activar o desactivar el Firewall de Windows Defender
Restaurar valores predeterminados
Configuración avanzada
Solución de problemas de red
Ayudar a proteger el equipo con Firewall de Windows Defender
Firewall de Windows Defender puede ayudar a impedir que piratas informáticos o software malintencionado obtengan acceso al equipo a través de Internet o una red.
Redes privadas
No conectado
Redes públicas o invitadas
Conectado
Redes en lugares públicos como aeropuertos o cafeterías
Estado de Firewall de Windows Defender: Activado
Conexiones entrantes: Bloquear todas las conexiones a aplicaciones que no estén en la lista de aplicaciones permitidas
Redes públicas activas: Estudiantes-Upc
Estado de notificación: Notificarme cuando Firewall de Windows Defender bloquee una nueva aplicación
Vea también
Seguridad y mantenimiento
Centro de redes y recursos compartidos

Desactivación de compartición de archivos:

La desactivación de la compartición de archivos sirve para limitar el acceso a archivos y carpetas entre dispositivos o usuarios en una red. Esto puede ser útil para:

Mayor seguridad:

Previene el acceso no autorizado a información confidencial al impedir que otros usuarios en la red puedan ver o editar tus archivos.

Control de acceso:

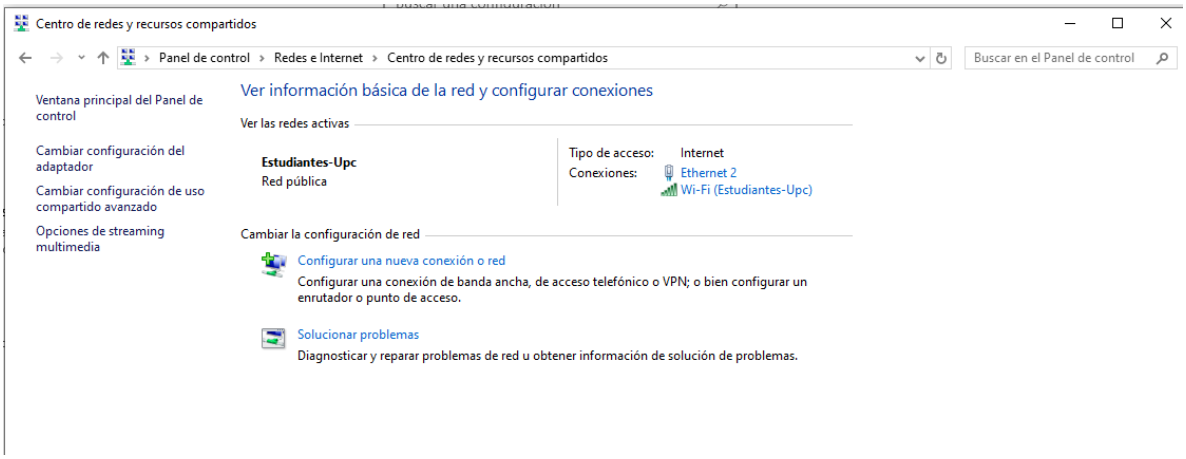
Permite controlar quién puede acceder a qué archivos, limitando la distribución de información a usuarios específicos.

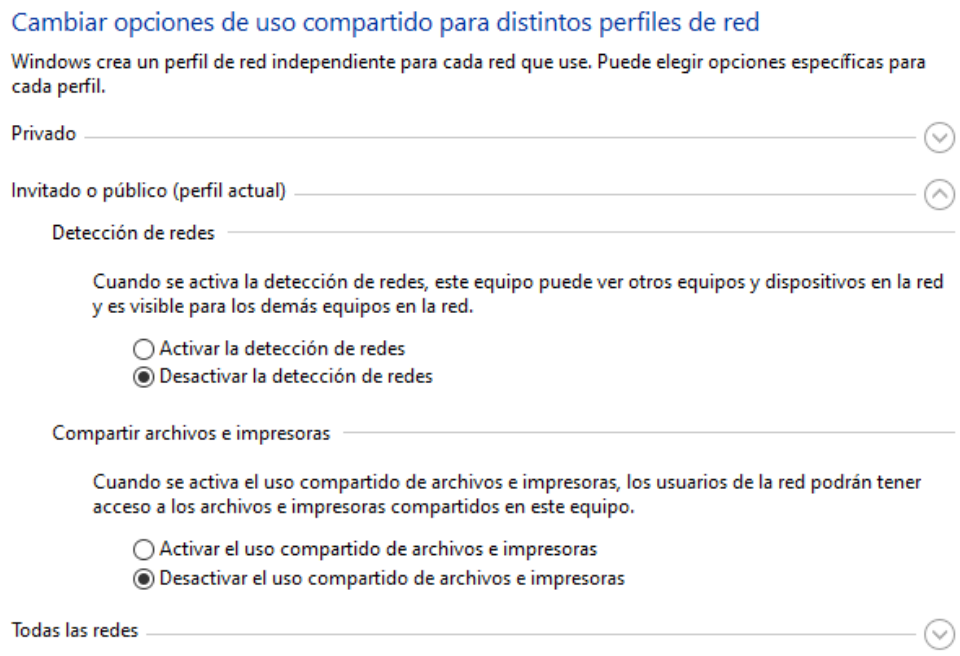
Reducción de riesgos:

Evita la posibilidad de que archivos sean modificados o eliminados accidentalmente por otros usuarios.

Privacidad:

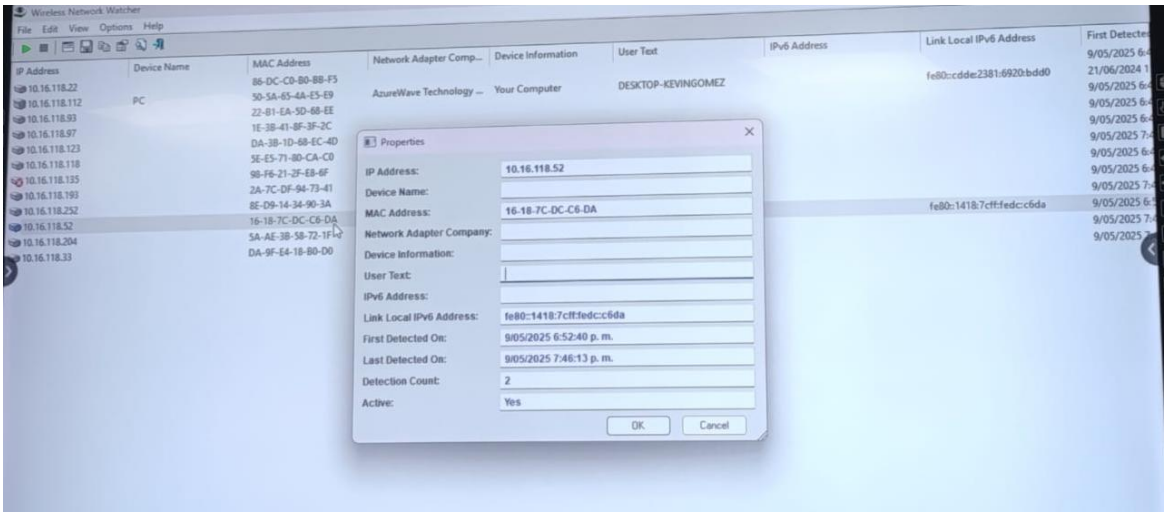
Protege la información personal o sensible que no se quiere compartir con otros.





Wirelles Watcher:

Wireless Watcher es una utilidad que se usa para detectar y mostrar los dispositivos conectados a una red inalámbrica, como una red Wi-Fi. Permite ver información detallada de cada dispositivo conectado, incluyendo su dirección IP, nombre, ubicación y tipo de dispositivo.



Apuntes (ANTES DE HACER EL LABORATORIO):

Redes Públicas
Definición: Son redes de acceso abierto, diseñadas para que cualquier persona con un dispositivo compatible pueda conectarse.
Ejemplos: Wi-Fi gratuito en una cafetería, redes de telefonía móvil, hotspots públicos.

Redes Privadas
Definición: Son redes de acceso restringido, diseñadas para conectar dispositivos dentro de un entorno específico.
Ejemplos: Red Wi-Fi doméstica, red de una empresa, VPN (Red Privada Virtual).

Uso de VPNs para Cifrar la Conexión
Una Red Privada Virtual (VPN) crea un túnel seguro entre tu dispositivo y un servidor remoto, cifrando todos los datos que envías y recibes.

El estándar más seguro: WPA3 es el protocolo de seguridad más reciente y robusto para redes Wi-Fi.

Ocultar el SSID
Invitados: Si necesitas compartir tu red con visitantes, crea una red de invitados separada con restricciones de acceso.

Métodos de detección de antivirus y antispyware

Basados en firmas:

- **¿Qué son las firmas?** Son como huellas digitales únicas de cada tipo de malware. Se crean a partir del código del virus o programa malicioso.
- **¿Cómo funcionan?** El antivirus compara los archivos de tu sistema con una base de datos de firmas conocidas. Si encuentra una coincidencia, identifica el archivo como malicioso y lo elimina o pone en cuarentena.
- **Limitaciones:** Los virus pueden mutar o crear nuevas variantes.

Análisis de comportamiento:

- **¿En qué se basa?** Analiza cómo se comporta un programa en tiempo real. Observa sus acciones y las compara con un modelo de comportamiento normal.

- **¿Cómo funciona?** Detecta programas que intentan autoreplicarse, ocultar su presencia o modificar otros programas.

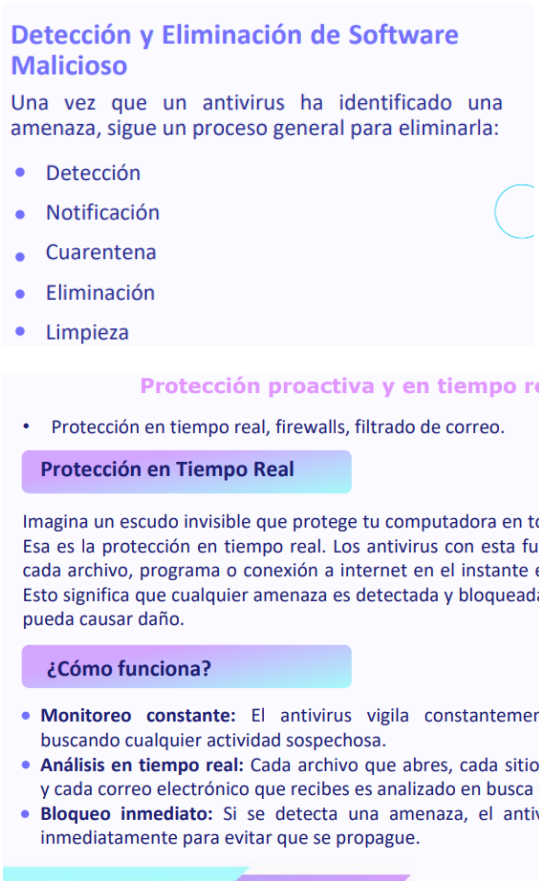
Protección contra software malicioso (antivirus, antispyware)
La mayoría de los antivirus y antispyware combinan estos métodos para ofrecer una protección más completa.
Por ejemplo:

- **Detección inicial con firmas:** Identifica rápidamente las amenazas conocidas.
- **Análisis heurístico y de comportamiento:** Detecta nuevas variantes y malware desconocido.

Método	Ventajas	Desventajas
Basado en firmas	Rápido y preciso para amenazas conocidas	Ineficaz contra malware nuevo o variantes
Heurístico	Detecta malware desconocido	Puede generar falsos positivos
Análisis de comportamiento	Muy eficaz contra malware nuevo	Requiere mayor potencia de procesamiento

Escaneos Completos, Rápidos y Programados

- **Escaneo completo:** Analiza todos los archivos de tu sistema. Es el tipo de escaneo más exhaustivo, pero también el que más tiempo tarda.
- **Escaneo rápido:** Analiza las áreas más vulnerables de tu sistema, como los archivos de inicio y las carpetas temporales. Es más rápido que un escaneo completo, pero menos exhaustivo.
- **Escaneos programados:** Puedes configurar el antivirus para que realice escaneos automáticamente a intervalos regulares, como una vez al día o una vez a la semana.



Firewall

Un firewall es como un guardia de seguridad que controla el tráfico que entra y sale de tu computadora. Actúa como una barrera entre tu dispositivo y la internet, permitiendo solo el tráfico autorizado.

¿Cuál de las siguientes es una característica clave de una red pública?

a. Tiene acceso libre y es común en lugares públicos como cafeterías y aeropuertos. ✓
b. Ofrece una conexión más segura que las redes privadas.
c. Tiene una cobertura limitada a un área específica.
d. Requiere credenciales específicas para acceder.

Respuesta correcta

La respuesta correcta es: Tiene acceso libre y es común en lugares públicos como cafeterías y aeropuertos.

¿Qué medida de seguridad es recomendable al conectarse a una red pública?

a. Desactivar todas las medidas de seguridad del dispositivo.
b. Compartir la red con múltiples dispositivos.
c. Realizar compras en línea sin preocupaciones.
d. Usar una VPN para cifrar la conexión. ✓

Respuesta correcta

La respuesta correcta es: Usar una VPN para cifrar la conexión.

¿Cuál es una diferencia principal entre una red pública y una red privada?

a. Las redes privadas requieren credenciales para acceder, mientras que las públicas tienen acceso libre. ✓
b. Las redes privadas tienen acceso libre, mientras que las públicas requieren contraseñas.
c. Las redes privadas tienen una velocidad de conexión inestable.
d. Las redes públicas ofrecen mayor seguridad que las redes privadas.

Respuesta correcta

La respuesta correcta es: Las redes privadas requieren credenciales para acceder, mientras que las públicas tienen acceso libre.

¿Qué protocolo de seguridad es más recomendable para proteger una red Wi-Fi doméstica?

a. WPA2
b. WEP
c. WPA
d. WPA3 ✓