Laboratorio 10 Cursos Ciberseguridad

Sesión #10 Uso seguro de redes públicas y privadas

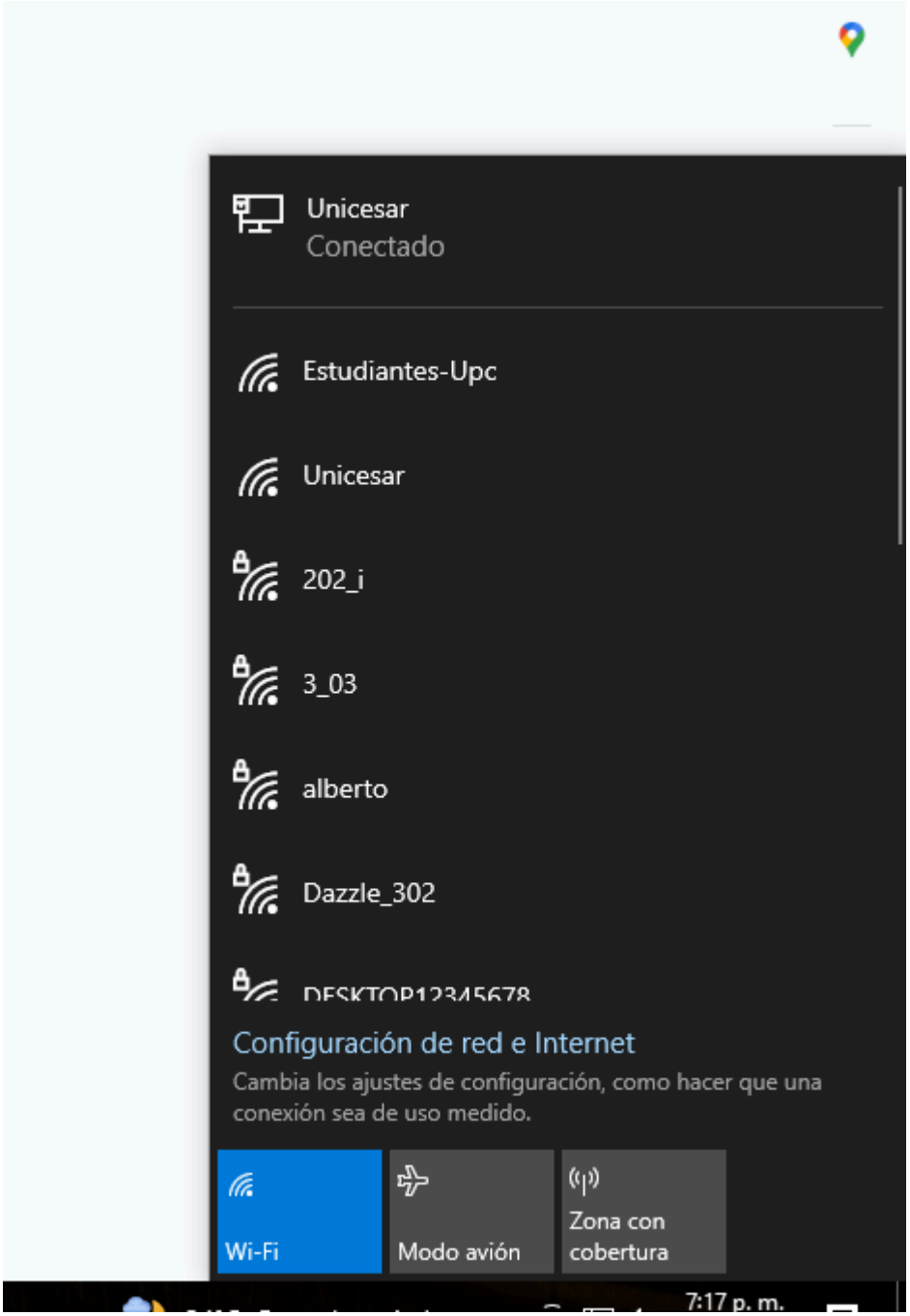
Jesús Rodrigo Toro Navarro

Universidad Popular del Cesar

Uso seguro de redes públicas y privadas

Paso 1 Conexión a una red pública

Comprobamos cuales son las redes públicas y privadas



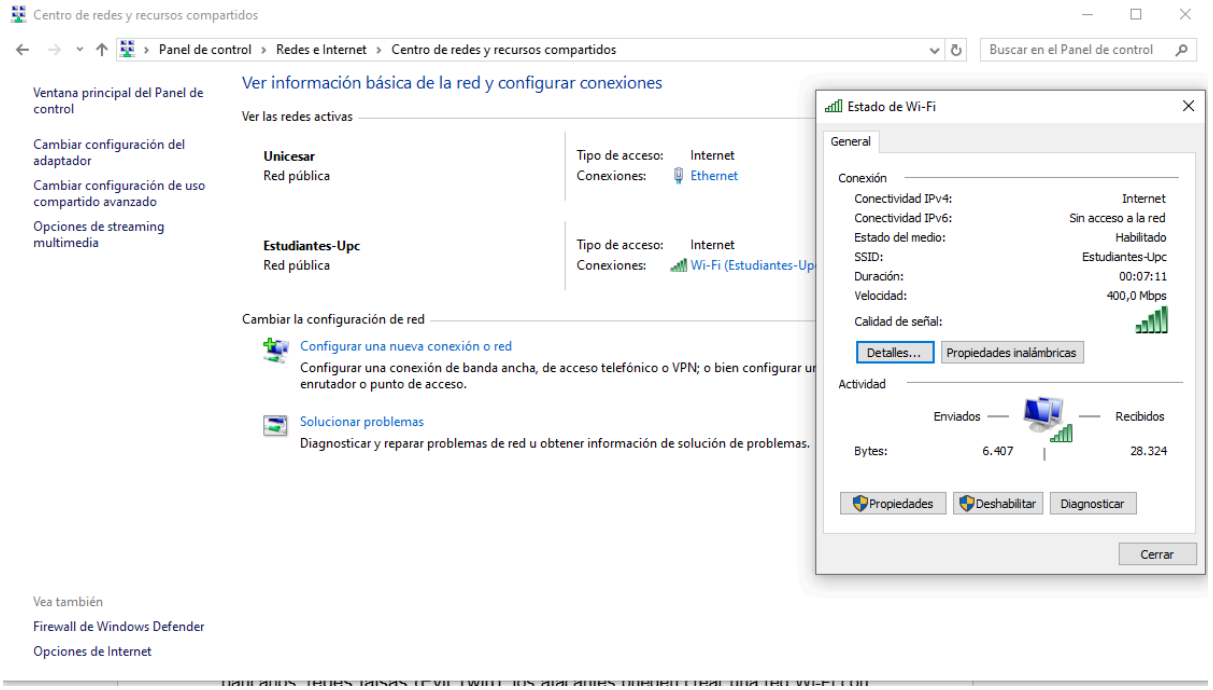
Nos conectamos a una publicas y le damos a propiedades

Comprobamos el uso de datos de la red pública

Conectarse a una red Wi-Fi pública (como en cafeterías, aeropuertos, hoteles o plazas) puede representar varios peligros de seguridad si no se toman precauciones. Por ejemplo, Intercepción de datos (ataque "Man-in-the-Middle"), los ciberdelincuentes pueden interceptar el tráfico entre tu dispositivo y la red para

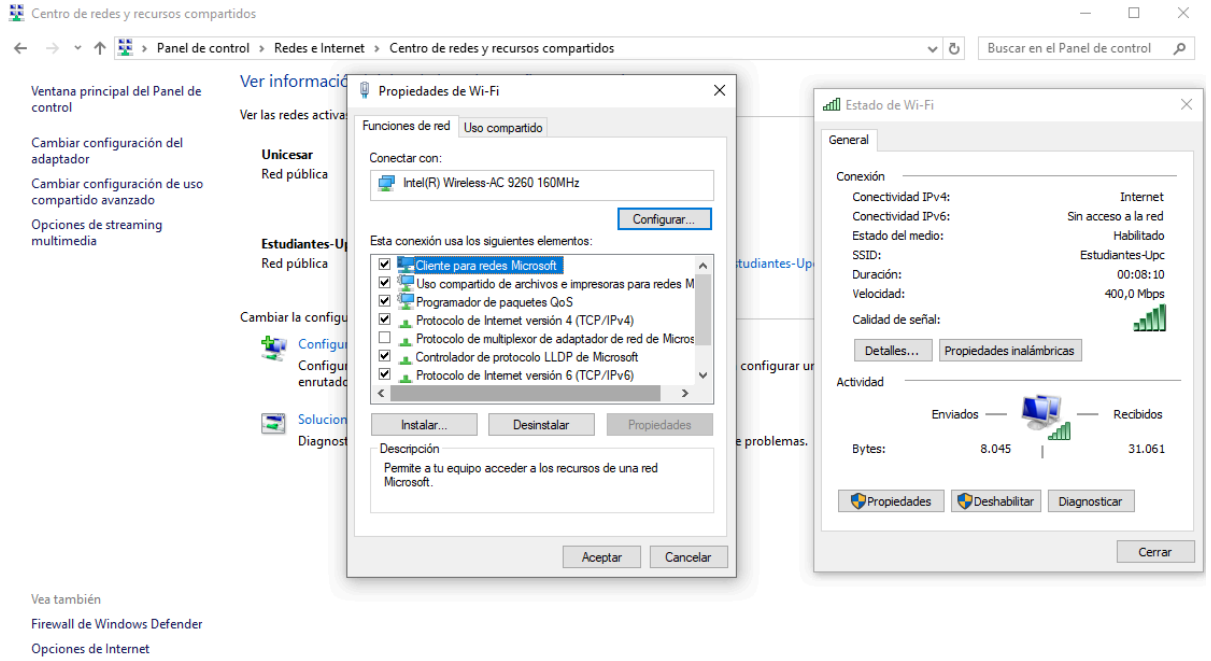
robar información confidencial como contraseñas, correos electrónicos o datos bancarios, redes falsas (Evil Twin), los atacantes pueden crear una red Wi-Fi con un nombre similar (o idéntico) a la legítima para engañar a los usuarios y capturar sus datos cuando se conectan.

Nos vamos a panel de control, redes e internet, centro de redes y recursos compartidos y le damos a nuestra red pública

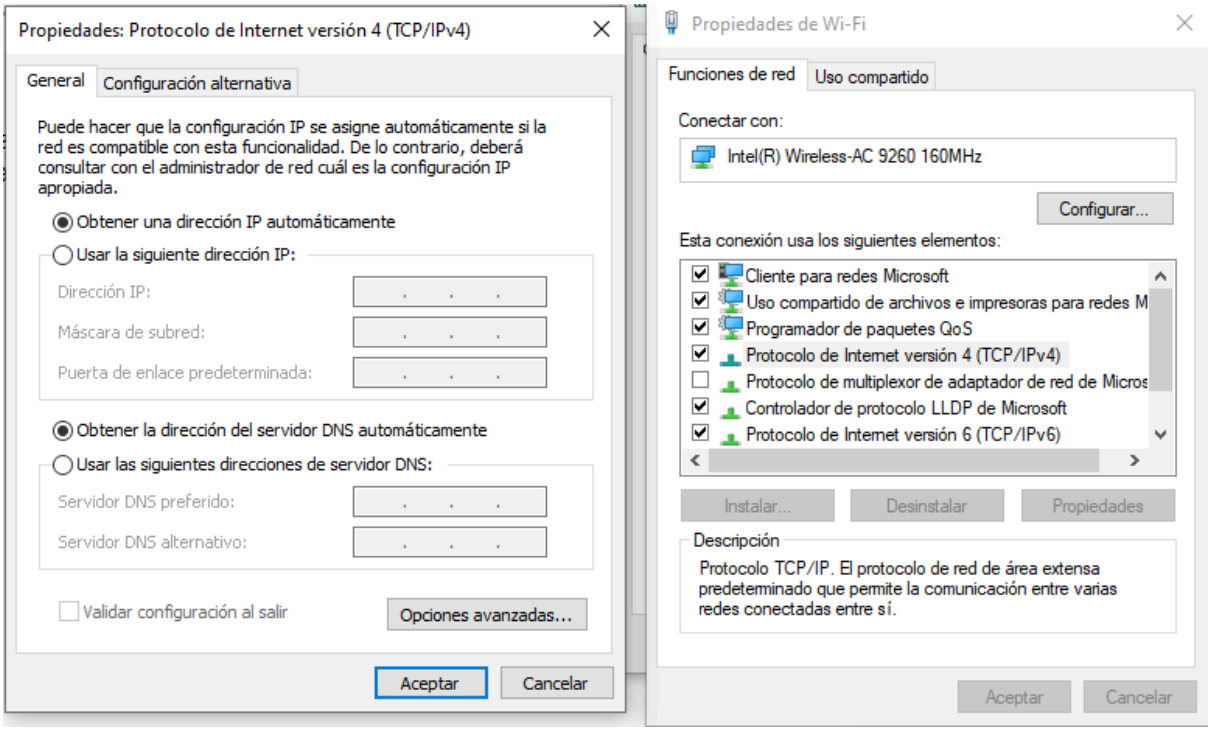


Esta pantalla es útil para diagnosticar conexiones a Internet, verificar si estás conectado correctamente y ver detalles técnicos de tu conexión.

Le damos a propiedades de la red wifi

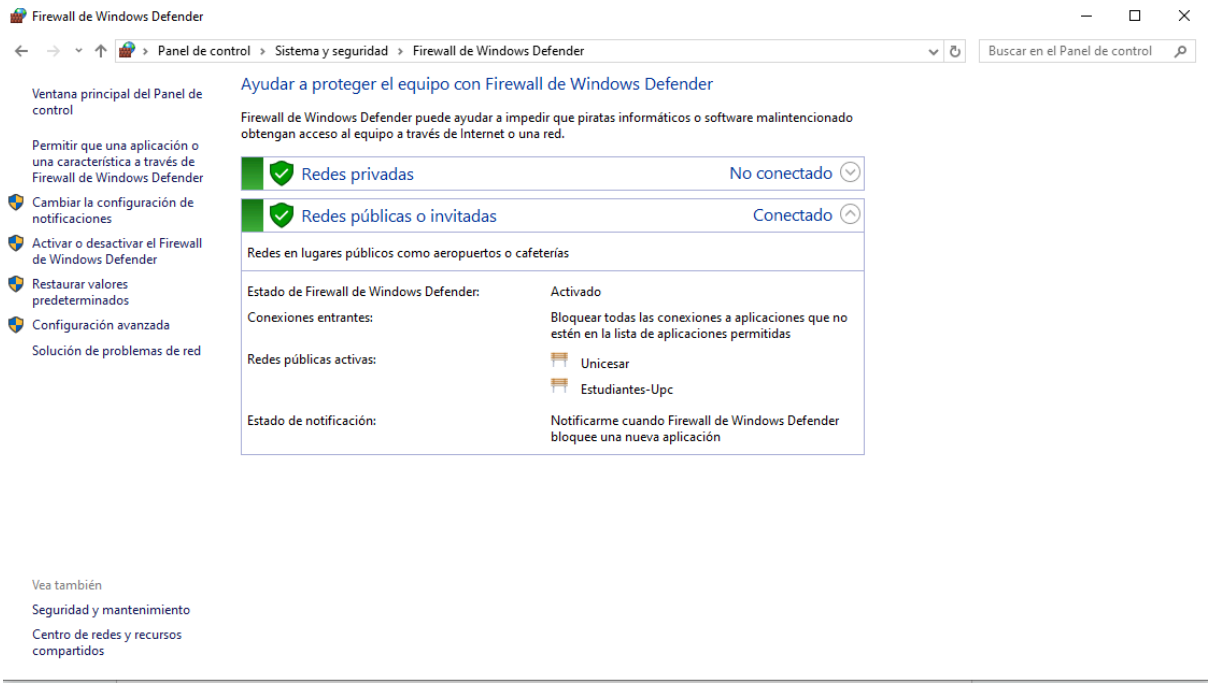


Ahora en protocolo de internet versión 4 (TCP/IPv4) le damos a propiedades

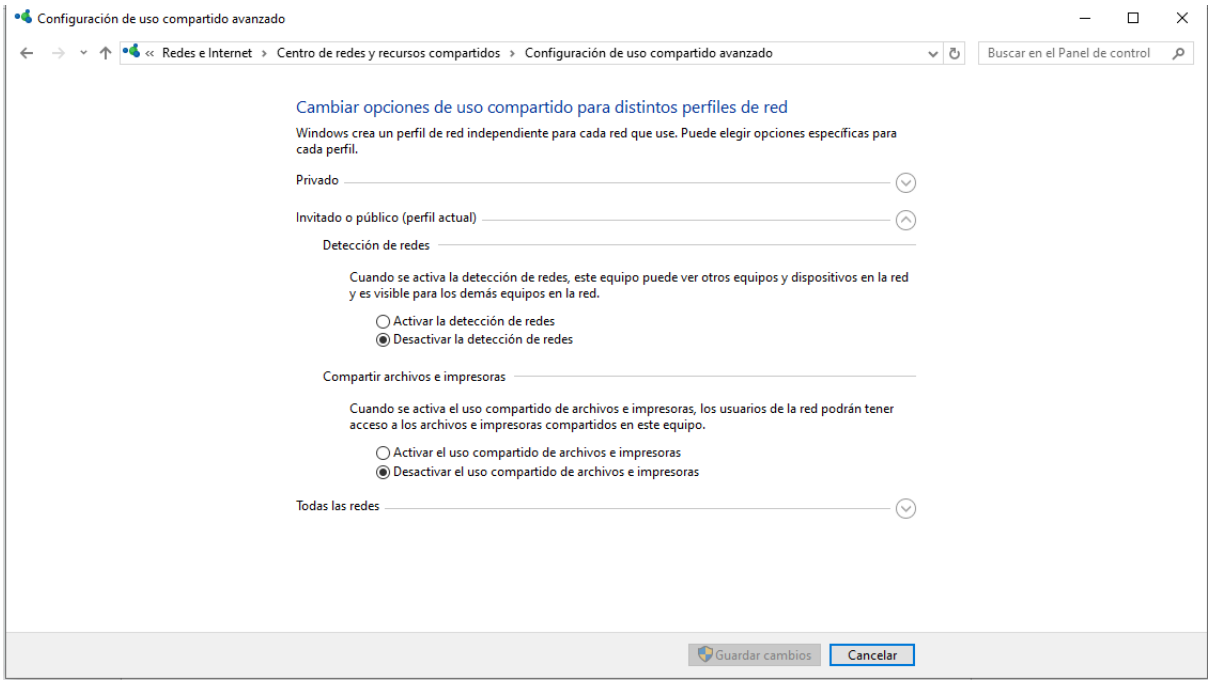


Buenas Prácticas para usar redes públicas y privadas

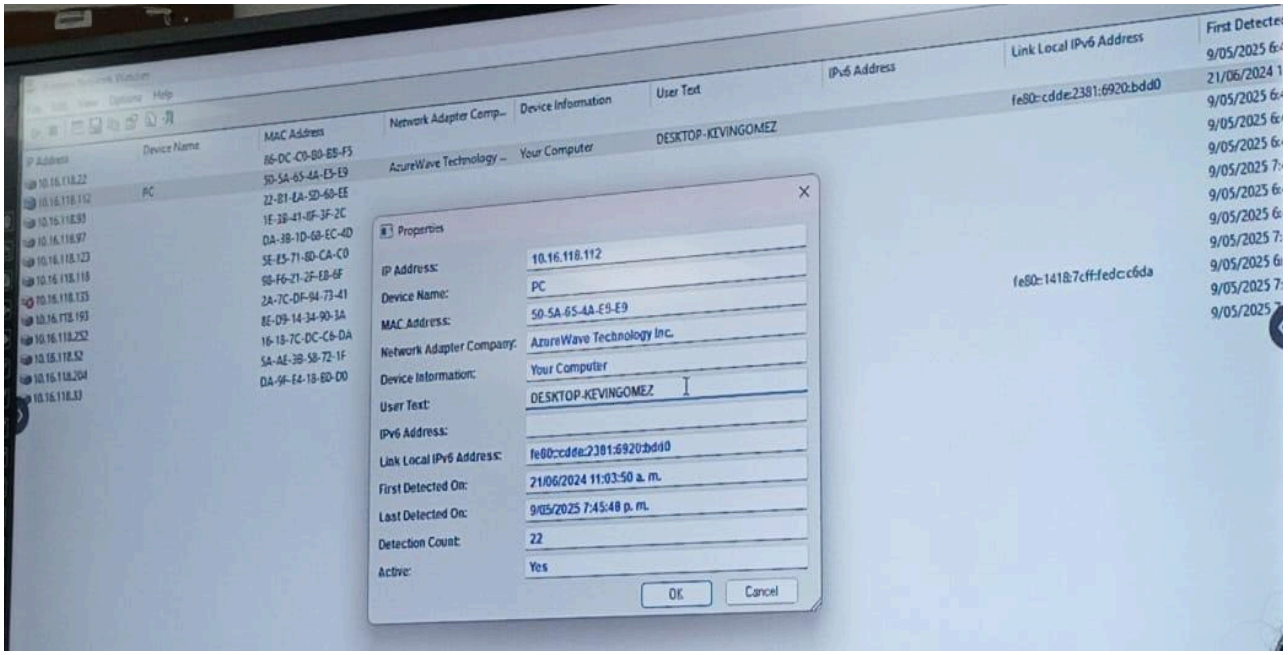
Nos vamos a panel de control, redes e internet, Sistema y seguridad y Firewall de Windows Defender



Ahora nos vamos a panel de control, redes e internet, centro de redes y recursos compartidos y le damos a Configuración de uso compartido avanzado y desactivamos el uso compartido automático



Una última cosa es escanear la red inalámbrica para mostrar una lista de todos los dispositivos conectados a ella. Digitamos en el cuadro de búsqueda de windows WIRELESS NETWORK WATCHER y vemos



REFLEXIÓN

Las redes públicas, como las que se ofrecen en universidades, cafés, centros comerciales o aeropuertos, están diseñadas para ser accesibles a múltiples usuarios. Esto implica que suelen tener una configuración menos restrictiva y más expuesta. Al conectarse a este tipo de redes, los datos que viajan sin cifrar (por ejemplo, si se accede a una página sin HTTPS o se envían contraseñas sin protección) pueden ser interceptados por terceros malintencionados. Asimismo, es común que dispositivos conectados a la misma red puedan verse entre sí, lo que representa un riesgo potencial si no se cuenta con un firewall o antivirus actualizado.

Por otro lado, las redes privadas (como las de nuestros hogares o empresas) permiten mayor control sobre la configuración del router, los permisos de acceso, los dispositivos conectados y el nivel de cifrado utilizado (como WPA3). Estas redes, si están bien configuradas, ofrecen un entorno más seguro para la transferencia de datos confidenciales, como información bancaria, contraseñas o documentos laborales.

La seguridad en la red, sin importar el tipo de conexión, debe ser una prioridad. Usar contraseñas robustas, mantener actualizado el sistema operativo y el software antivirus, evitar ingresar a sitios dudosos y utilizar redes VPN cuando se está en redes públicas, son medidas esenciales para reducir riesgos. Además, comprender el comportamiento de los protocolos de red (como TCP/IP, DNS, etc.) ayuda a entender cómo fluye la información y cómo puede ser protegida.

En conclusión, aunque la conectividad sea inmediata y conveniente, la conciencia sobre los riesgos y las buenas prácticas de seguridad digital es lo que realmente garantiza una experiencia segura en el uso de redes.