Sesión #10

Uso seguro de redes públicas y privadas

Título del Laboratorio: 10 Uso seguro de redes públicas y privadas

Duración: 2 horas

Objetivos del Laboratorio:

El objetivo de este laboratorio es enseñar a los participantes a identificar y utilizar de manera segura tanto redes públicas como privadas, minimizando los riesgos asociados a la conexión a internet en diferentes entornos. Los participantes aprenderán a configurar conexiones seguras, utilizar herramientas de protección, y aplicar buenas prácticas al conectarse a redes.

Materiales Necesarios:

- 1. Un computador portátil con conexión a internet.
- 2. Acceso a una red Wi-Fi pública (simulada o real, como en una cafetería o punto de acceso móvil).
- 3. Acceso a una red Wi-Fi privada (como una red doméstica o de oficina).
- 4. Software de VPN (puede ser gratuito, como ProtonVPN o Windscribe).
- 5. Un teléfono móvil (opcional) para demostrar la conexión a redes Wi-Fi públicas y privadas.

Estructura del Laboratorio:

Paso 1: Conexión a una Red Pública y Evaluación de Seguridad (30 minutos)

- Identificación de Redes Públicas:
- Conexión a la Red Pública:
- Evaluación de Seguridad:

Paso 2: Uso de una VPN en Redes Públicas (30 minutos)

- Instalación de VPN:
- Conexión a la VPN:
- Verificación de Protección:
- Navegación Segura:

Paso 3: Conexión Segura a una Red Privada (20 minutos)

- Identificación de Redes Privadas:
- Conexión a la Red Privada:
- Configuración de Seguridad:

Paso 4: Buenas Prácticas para Usar Redes Públicas y Privadas (20 minutos)

- Evitar Transacciones Sensibles:

- Desactivación de Conexiones Automáticas:
- Uso de Configuraciones de Firewall:
- Desactivación de Compartición de Archivos:

Paso 5: Conclusión y Reflexión (20 minutos)

- Revisión de lo Aprendido:
- Reflexión:
- Cierre: