Seguridad en redes inalámbricas.

La seguridad en redes inalámbricas implica proteger una red Wi-Fi del acceso no autorizado y del robo de datos utilizando protocolos de cifrado como WPA3, contraseñas robustas y la segmentación de la red

Vulnerabilidades conocidas y capas de seguridad que se deben implementar para remediar las vulnerabilidades en las siguientes redes de comunicación:

1. Tecnologías NFC (Near Field Communication)

Vulnerabilidades conocidas

- **Skimming**: lectura no autorizada de la comunicación NFC a corta distancia.
- **Eavesdropping**: interceptación de datos debido al bajo nivel de cifrado en el estándar básico.
- **Relay Attack**: extender el alcance de NFC de forma maliciosa para aprobar transacciones sin consentimiento.
- **Data Corruption/Manipulation**: alterar o bloquear la comunicación mediante interferencias.
- **Tag Tampering**: modificar etiquetas NFC para redirigir a sitios maliciosos o ejecutar acciones no deseadas.

Capas de seguridad recomendadas

- **Autenticación fuerte** entre dispositivos antes de realizar transacciones.
- **Cifrado de extremo a extremo (E2E)** para datos sensibles, incluso si NFC no lo incluye por defecto.
- **Secure Element (SE)** para pagos y credenciales.
- **Tokens temporales** en pagos sin contacto.
- **Filtrado y validación de etiquetas NFC** para evitar ataques de etiquetas maliciosas.
- **Requerir autorización del usuario** (tocar, desbloquear pantalla).

2. Bluetooth

Vulnerabilidades conocidas

- **Bluejacking**: envío de mensajes no autorizados.
- **Bluesnarfing**: robo de información de un dispositivo.
- **Bluebugging**: control remoto del dispositivo mediante fallos del protocolo.
- **MITM (Man in the Middle)** en emparejamientos antiguos.

- **Rastreo (Tracking)** por identificadores únicos (MAC address).
- **Ataques de fuerza bruta PIN** en versiones antiguas (Bluetooth Clásico).
- **Vulnerabilidades en BLE** como ataques de repetición y suplantación.

Capas de seguridad recomendadas

- **Usar Bluetooth 4.2 o superior / Bluetooth 5.x** que incluyen LE Secure Connections.
- **Cifrado AES-CCM** habilitado durante la conexión.
- **Métodos de emparejamiento seguros** (Numeric Comparison, Passkey Entry).
- **Desactivar Bluetooth cuando no se use** o hacerlo no visible.
- **Actualizaciones de firmware** constantes.

3. WiFi

Vulnerabilidades conocidas

- **Crackeo de contraseñas débiles** en WPA/WPA2.
- **Ataques KRACK** (Key Reinstallation Attack) en WPA2.
- **Rogue AP / Evil Twin**: puntos de acceso falsos para robar información.
- **Sniffing** de tráfico en redes abiertas.
- **DoS / Deauthentication attacks** que desconectan usuarios de la red.
- **Acceso no autorizado** por mala configuración o filtrado deficiente.
- **Ataques por WPS (PIN)** fácilmente vulnerables.

Capas de seguridad recomendadas

- **Uso obligatorio de WPA3** (SAE) en redes modernas.
- **Contraseñas robustas** y segmentación de red (VLAN invitados / IoT / Admin).
- **Firewall interno + filtrado MAC** (solo como medida auxiliar).
- **VPN** para acceso remoto.

4. WiMAX (Worldwide Interoperability for Microwave Access)

Vulnerabilidades conocidas

- **Ataques de denegación de servicio (DoS/DDoS)** por saturación del canal.
- **Suplantación (Spoofing)** de estaciones base o suscriptores.
- **Ataques de repetición** afectando autenticación de dispositivos.

- **Intercepción de tramas no cifradas** en implementaciones antiguas.
- **Vulnerabilidades en PKM (Privacy Key Management)**, especialmente en PKMv1.
- **Rogue Base Stations**: estaciones falsas que engañan a usuarios.

Capas de seguridad recomendadas

- **Uso de PKMv2** (versión mejorada del sistema de gestión de claves).
- **Certificados digitales X.509** entre estación base y suscriptor.
- **Filtrado de direcciones y control de acceso estrictos**.
- **Detección de intrusiones inalámbricas (WIDS/WIPS)**.
- **Protección contra DoS** mediante limitación de ancho de banda y mecanismos anti-replay.
- **Actualización del firmware del CPE y estación base**.