📢 Seguridad y coexistencia — Vulnerabilidades e interferencias en Bluetooth y Wi-Fi (2.4 GHz)

> ⚠️ **Advertencia legal y ética:** Interferir intencionadamente con señales inalámbricas (jamming) es ilegal en muchas jurisdicciones y puede causar daños a terceros. Este repositorio y documento tienen **fines educativos y de investigación** únicamente. Realiza cualquier prueba **solo** en entornos controlados, con autorización explícita y respetando la legislación local.

> **No me hago responsable del mal uso o de la mala interpretación de la información aquí contenida.**

> **Es totalmente ilegal interferir señales inalámbricas fuera de entornos autorizados.**

📘 Índice

🔎 Resumen

Este documento explica, de forma educativa y técnica, cómo **Bluetooth** y **Wi-Fi** comparten la banda **2.4 GHz**, por qué pueden surgir problemas de **coexistencia** e interferencia, y qué acciones razonables pueden tomarse para mitigar riesgos y reforzar la seguridad en entornos reales.

🎯 Alcance y propósito

- **Alcance:** explicar vulnerabilidades relacionadas con la interacción entre tecnologías que operan en 2.4 GHz (Bluetooth Classic / BLE y Wi-Fi 2.4 GHz) y ofrecer recomendaciones de seguridad y coexistencia.

- **Propósito:** documental / educativo — no se proporcionan ni se permiten instrucciones para ataques reales o dispositivos de jamming en entornos no autorizados.

📡 Frecuencias y canales (2.4 GHz)

- **Bluetooth Classic (BR/EDR):** 79 canales, 2.402–2.480 GHz (FHSS).

- **Bluetooth Low Energy (BLE):** 40 canales, 2.400–2.4835 GHz (2 MHz de separación).

- **Wi-Fi (802.11b/g/n 2.4 GHz):** canales de ~20 MHz dentro de ~2.412–2.472 GHz (numeración y uso varía por región).

Estos sistemas comparten la banda ISM de 2.4 GHz y, por tanto, pueden verse afectados por interferencia mutua, saturación de espectro o implementaciones deficientes de coexistencia.

🧭 Descripción de vectores de vulnerabilidad

>*Nota:* se describen vectores conceptuales **sin** instrucciones operativas.

1. **Interferencia por congestión de espectro**

   - Muchos dispositivos transmitiendo en la misma banda (APs Wi-Fi, dispositivos BLE, microondas, etc.) elevan el nivel de ruido y reducen la calidad de la señal.

2. **Falta de mecanismos de coexistencia en firmware / hardware**

   - Chips o firmwares sin soporte de AFH (Adaptive Frequency Hopping) o sin mecanismos de coordinación Wi-Fi/Bluetooth degradan el rendimiento cuando operan simultáneamente.

3. **Señales espurias o dispositivos defectuosos**

   - Equipos mal configurados o defectuosos pueden generar tráfico que perturba la operación de radios cercanos.

4. **Ataques de denegación locales (teóricos)**

   - Generar ruido intencional o paquetes falsos puede causar DoS a radios en rango; **esto es ilegal fuera de entornos controlados y autorizados**.

⚠️ Impacto potencial

| Afectado | Ejemplo de impacto |

|---|---|

| Usuarios domésticos | Interrupción de audio Bluetooth, pérdida de conexión de periféricos, caída de streaming. |

| Empresas / IoT | Interrupción de sensores, dispositivos críticos y servicios dependientes de 2.4 GHz. |

| Seguridad | Facilita ataques secundarios al forzar reconexiones o cambios a modos menos seguros. |

🛡️ Medidas de mitigación y buenas prácticas

Configuración y arquitectura

- Priorizar uso de **5 GHz** para Wi-Fi cuando sea posible.

- Segmentar redes: separar IoT, invitados y administración.

- Mantener firmware actualizado en APs, routers y dispositivos Bluetooth.

Coexistencia y RF

- Elegir equipos con soporte de **coexistencia Wi-Fi/Bluetooth** y AFH.

- Optimizar selección de canales (evitar solapamientos) y ajustar potencia TX para reducir interferencia.

- Posicionar antenas para minimizar superposiciones indeseadas.

Monitorización

- Usar análisis de espectro y escaneo pasivo para identificar fuentes de interferencia.

- Revisar logs de APs y dispositivos para detectar patrones de degradación.

Políticas

- Prohibir o controlar dispositivos emisores no autorizados.

- Establecer procedimientos para pruebas controladas y divulgación responsable.

🧪 Metodología segura de pruebas (laboratorio controlado)

- **Entorno aislado:** redes y emisiones confinadas dentro de instalaciones autorizadas.

- **Autorización por escrito:** solo equipos propiedad del laboratorio o con permiso expreso del propietario.

- **Registro y reversión:** documentar acciones y restaurar configuraciones tras las pruebas.

- **Medidas de contención:** atenuadores RF, cámaras anecoicas o jaulas Faraday cuando sea necesario para contener emisiones.

- **Ética:** seguir políticas de divulgación responsable; no publicar herramientas que faciliten el abuso.

⚖️ Responsabilidad y legalidad

Interferir señales puede violar leyes de telecomunicaciones y causar daños a terceros. Nunca realices pruebas de interferencia fuera de un entorno controlado y autorizado. Consulta la normativa local antes de cualquier experimento.

📎 Referencias útiles

- Repositorio original que inspiró este documento (proyecto de demostración educativa): **ESP32-BlueJammer** — https://github.com/EmenstaNougat/ESP32-BlueJammer

- Documentación oficial de Bluetooth (especificaciones de canal y coexistencia).

- Guías de fabricantes y artículos técnicos sobre congestión en 2.4 GHz y estrategias de coexistencia.

📒 Nota final

No me hago responsable del mal uso o de la mala interpretación de la información aquí contenida.

Es totalmente ilegal interferir señales inalámbricas fuera de entornos autorizados.

Este README es **educativo** y está orientado a ayudar a técnicos, administradores y estudiantes a comprender problemas reales de coexistencia y seguridad en la banda 2.4 GHz. No incluye instrucciones operativas para la creación o uso de dispositivos que provoquen interferencias en entornos no autorizados.