Cifrado y COMSEC: seguridad en comunicaciones por radio

Autor: EA4IPV
Fecha: 23/03/2026
Categoría: Alimentación
Etiquetas: Sin etiquetas

Cifrado y COMSEC: seguridad en comunicaciones por radio

COMSEC (Communications Security) abarca todas las medidas destinadas a proteger las comunicaciones de la interceptación, el análisis de tráfico y la suplantación de identidad. En radioaficionismo, la legislación prohíbe explícitamente el cifrado de comunicaciones (en España, el artículo 26 de la Orden ITC/332/2010 establece que las emisiones de radioaficionado deben ser en claro). Sin embargo, en otros servicios de radio (PMR profesional, LoRa, Wi-Fi, DMR Tier III) el cifrado es legal y en muchos casos recomendable. Para un grupo preparacionista, comprender los principios de COMSEC permite proteger la información táctica incluso cuando se opera en claro, combinando técnicas de procedimiento con tecnologías de cifrado donde la ley lo permita.

Amenazas a las comunicaciones por radio

Las comunicaciones por radio son intrínsecamente vulnerables porque la señal se propaga en todas direcciones (o en un cono, con antenas directivas) y puede ser captada por cualquier receptor sintonizado en la misma frecuencia. Las amenazas principales son cuatro y deben entenderse para poder mitigarlas.

Amenaza
Descripción
Dificultad para el atacante
Contramedida principal

Interceptación (escucha)
Captar y escuchar las comunicaciones del grupo
Baja: basta un receptor y una antena
Cifrado de la señal o COMSEC procedural

Análisis de tráfico
Sin entender el contenido, deducir información de patrones: quién transmite, cuándo, desde dónde, con qué frecuencia
Media: requiere monitorización prolongada y equipo de radiogoniometría
Disciplina de emisión, saltos de frecuencia, silencio radio

Radiogoniometría (DF)
Localizar físicamente al transmisor mediante triangulación con dos o más receptores direccionales
Media-alta: requiere equipo de DF y personal entrenado
Transmisiones cortas, cambio de ubicación, baja potencia, antenas directivas

Suplantación (spoofing)
Un intruso transmite haciéndose pasar por un miembro del grupo para dar órdenes falsas o desinformación
Baja si no hay autenticación
Autenticación por código, procedimientos de verificación

COMSEC procedural: protección sin tecnología

Incluso operando en frecuencias de radioaficionado donde el cifrado está prohibido, o con equipos PMR446 que no lo soportan, las técnicas procedurales de COMSEC reducen significativamente la información que un adversario puede obtener de las comunicaciones.

Indicativos tácticos: Nunca usar nombres reales al aire. Asignar indicativos tácticos que no revelen la función ni la ubicación: "Base Uno", "Móvil Tres", "Punto Alfa". Rotar los indicativos periódicamente. Un adversario que escuche no debe poder deducir la estructura del grupo.

Brevedad y disciplina: Transmisiones lo más cortas posible. Usar prowords (palabras de procedimiento): "Cambio" (fin de transmisión, espero respuesta), "Corto" (fin de comunicación), "Recibido" (mensaje entendido). No repetir información innecesariamente. Cada segundo de transmisión es una oportunidad para el análisis de tráfico y la radiogoniometría.

Códigos preestablecidos: Crear una tabla de códigos conocida solo por el grupo y memorizada o en tarjeta plastificada. Ejemplo: "Opción Delta" = reagruparse en punto de encuentro secundario; "Tango Cinco" = necesitamos suministros médicos; "Lluvia" = movimiento detectado en el perímetro. No transmitir información operativa en claro.

Ventanas de comunicación programadas: Establecer horarios fijos de comunicación (por ejemplo, cada hora a los 15 minutos) en lugar de transmitir aleatoriamente. Fuera de esas ventanas, silencio radio absoluto salvo emergencia. Esto reduce la exposición al análisis de tráfico y dificulta la interceptación casual.

Saltos de frecuencia manuales: Acordar una secuencia de canales conocida por el grupo (ejemplo: canal 7 a las horas pares, canal 14 a las impares, canal 3 si el primario está ocupado). Un adversario que monitorice un solo canal perderá parte de las comunicaciones. No es tan robusto como FHSS electrónico, pero es mejor que quedarse siempre en el mismo canal.

Cifrado digital: tecnologías disponibles y legales

Cuando la legislación lo permite (fuera del servicio de radioaficionado), existen varias tecnologías de cifrado aplicables a comunicaciones por radio. Su robustez varía enormemente.

Tecnología
Cifrado
Aplicación
Nivel de seguridad

DMR con cifrado básico
XOR con clave de 16/32 bits ("Basic Privacy")
Radios DMR comerciales (Motorola, Hytera, Anytone)
Bajo: la clave de 16/32 bits es trivial de romper con fuerza bruta. Solo disuade escuchas casuales.

DMR con cifrado AES-256
AES-256 (cifrado simétrico estándar militar)
Radios DMR Tier III y equipos profesionales (Motorola DP4800e, Hytera PD785G)
Alto: AES-256 es computacionalmente inviable de romper. Estándar FIPS 197.

LoRa / Meshtastic
AES-256 en capa de aplicación + AES-128 en capa de enlace
Módulos LoRa con firmware Meshtastic
Alto: cifrado de extremo a extremo con intercambio de claves PKI. Canal cifrado incluso sin internet.

Codec2 + FreeDV
Sin cifrado nativo, pero permite añadir AES sobre la capa digital
Software libre para voz digital en HF (freedv.org)
Variable: depende de la implementación del cifrado. Legal solo fuera de bandas de radioaficionado.

Wi-Fi (WPA3)
AES-GCMP-256 con SAE (Simultaneous Authentication of Equals)
Radioenlaces Wi-Fi punto a punto
Alto: WPA3 con clave robusta es seguro contra ataques conocidos.

Legalidad del cifrado en bandas de radioaficionado: En todas las regiones ITU y en la normativa española vigente, las comunicaciones de radioaficionado deben transmitirse en claro (sin cifrado). Usar cifrado en bandas de radioaficionado — incluso en una emergencia — es una infracción administrativa grave. Las técnicas de cifrado descritas aquí son aplicables solo en servicios donde es legal: PMR profesional con licencia, bandas ISM (LoRa 868 MHz), Wi-Fi (2,4/5 GHz) y telefonía móvil.

Implementación práctica de COMSEC para un grupo preparacionista

Un plan de COMSEC realista combina capas de protección: procedural en todas las comunicaciones por radio, cifrado tecnológico donde sea legal, y seguridad física de los equipos y las claves.

Capa 1 — PMR446 con COMSEC procedural: Comunicaciones tácticas de corto alcance. Sin cifrado disponible en equipos legales. Aplicar indicativos tácticos, códigos preestablecidos, saltos de frecuencia manuales y transmisiones breves. Es la capa más vulnerable pero la más accesible e inmediata.

Capa 2 — Meshtastic (LoRa 868 MHz) con cifrado AES-256: Mensajería de texto cifrada de extremo a extremo sin licencia. Alcance de 2–15 km con línea de vista. Cada nodo genera un par de claves y los mensajes se cifran con la clave pública del destinatario. La red mesh permite retransmisión automática. Ideal para coordinar sin exponer información al aire.

Capa 3 — Radioenlace Wi-Fi con WPA3 para datos: Enlace punto a punto de alta capacidad para compartir archivos, mapas, informes y VoIP. WPA3 con clave precompartida de al menos 20 caracteres alfanuméricos. Cambiar la clave periódicamente (cada semana o tras cualquier compromiso sospechado).

Seguridad de las claves: Las claves de cifrado deben distribuirse en persona (nunca por radio). Cada miembro del grupo lleva las claves en una tarjeta plastificada o en un dispositivo offline. Acordar un procedimiento de destrucción de claves si un equipo cae en manos ajenas: borrado remoto en Meshtastic (cambio de clave de canal) o reseteo de fábrica de los equipos.

Seguridad física de los equipos: Un adversario con acceso físico a un radio DMR o un nodo Meshtastic puede extraer las claves de cifrado. Los equipos no deben dejarse desatendidos. Configurar PIN/contraseña de acceso donde el equipo lo permita. En caso de pérdida, cambiar inmediatamente todas las claves del grupo.

 Advertencia: Esta información es orientativa y educativa. En situaciones de emergencia real, consulte a profesionales cualificados siempre que sea posible. No ponga en riesgo su vida ni la de otros sin la formación adecuada.