

Seguridad en Comunicaciones: Códigos y Protocolos para Grupos

Autor: EA4IPV

Fecha: 23/03/2026

Categoría: Electrónica y Energía

Etiquetas: Sin etiquetas

Seguridad en Comunicaciones: Códigos y Protocolos para Grupos

Cuando un grupo de personas coordinadas necesita comunicarse en una situación de crisis, la seguridad de las comunicaciones puede ser tan importante como el propio mensaje. Interceptar una comunicación puede revelar ubicaciones, recursos, planes de movimiento y vulnerabilidades. Este artículo aborda cómo establecer protocolos de comunicación seguros para grupos de preparación, desde sistemas de códigos sencillos hasta el uso correcto de radios y aplicaciones cifradas, siempre dentro de la legalidad española.

Principios Fundamentales de la Comunicación Segura

La seguridad en comunicaciones se basa en tres pilares: confidencialidad (que solo el destinatario entienda el mensaje), integridad (que el mensaje no se altere en tránsito) y autenticación (verificar que el emisor es quien dice ser). En un contexto civil de preparación, la confidencialidad y la autenticación son los aspectos más relevantes.

Todo sistema de comunicación debe diseñarse asumiendo que puede ser interceptado. Esta premisa, conocida como principio de Kerckhoffs, establece que la seguridad debe residir en la clave, nunca en el secreto del sistema.

Necesidad de saber: Solo compartir información con quien la necesita para su función. No transmitir más datos de los estrictamente necesarios en cada comunicación.

Brevedad: Las transmisiones largas son más fáciles de interceptar y localizar (especialmente por radiogoniometría en radio). Mensajes cortos y concisos.

Disciplina de emisión: Establecer horarios de comunicación predefinidos. Las emisiones fuera de horario solo para urgencias reales. Esto reduce la exposición y establece una rutina que facilita la coordinación.

Redundancia de canales: Disponer siempre de al menos dos medios de comunicación alternativos. Si falla el teléfono móvil, usar radio PMR. Si falla la radio, usar mensajeros físicos o señales preacordadas.

Contexto legal: En España, el uso de cifrado en comunicaciones civiles es legal. La Ley 9/2014 General de Telecomunicaciones y la Ley Orgánica 3/2018 de Protección de Datos reconocen el derecho a proteger las comunicaciones. No es necesario justificar el uso de cifrado.

Sistemas de Códigos para Comunicación por Voz

Un sistema de códigos sustituye palabras o frases críticas por términos inocuos, de modo que un oyente casual o interceptor no comprenda el significado real. La clave es la simplicidad: un código demasiado complejo se olvida bajo estrés y genera errores.

Concepto real

Ejemplo de código

Contexto de uso

Punto de encuentro principal

Casa del abuelo

Transmisiones por radio o teléfono

Punto de encuentro alternativo

Casa de la tía

Si el principal está comprometido

Evacuación inmediata

Cumpleaños de María

Activar protocolo de salida

Peligro en la ubicación

Hay visitas en casa

Alerta sin revelar la amenaza

Todo seguro

Buen tiempo hoy

Confirmar que no hay problemas

Necesito ayuda

Me duele la cabeza

Solicitar asistencia sin alarmar

Recursos escasos

La despensa está vacía

Indicar necesidad de suministros

Intruso/amenaza detectada

Perro callejero en la puerta

Alerta de presencia hostil

Tarjeta de códigos: Cada miembro del grupo debe tener una tarjeta plastificada de bolsillo con los códigos. Memorizarlos es ideal, pero bajo estrés la memoria falla. Tamaño tarjeta de crédito, plastificada.

Rotación de códigos: Cambiar los códigos periódicamente (mensual o trimestralmente) o inmediatamente si se sospecha que han sido comprometidos. Identificar cada conjunto de códigos con un color o número:

"Usamos tarjeta azul a partir de ahora".

Código duress (coacción): Establecer una palabra o frase que indique que el emisor está siendo obligado a transmitir bajo coacción. Ejemplo: si la frase de seguridad es "Buenos días" y alguien dice "Buenas tardes", indica que algo no está bien.

Autenticación de identidad: Usar un sistema de pregunta-respuesta para verificar identidad por radio. Ejemplo: "¿De qué color es el coche?" → "El coche es verde". Las respuestas se preacuerdan y no tienen relación lógica con la pregunta.

Comunicaciones por Radio: PMR446 y Radioafición

Las radios son el sistema de comunicación más fiable cuando la infraestructura de telecomunicaciones falla. En España existen opciones legales para uso civil sin licencia y con licencia.

PMR446 (sin licencia): Las radios PMR446 operan en 446 MHz con 0,5 W de potencia. Son legales sin licencia ni registro en toda la UE. Alcance real: 1-5 km en terreno abierto, 200-500 m en zona urbana. Limitaciones: potencia baja, sin repetidores, canales compartidos con otros usuarios.

Radioafición (con licencia): La licencia de radioaficionado (examen en la Jefatura Provincial de Telecomunicaciones) permite usar equipos de mucha mayor potencia (hasta 500 W según categoría) en bandas HF, VHF y UHF. Alcance: local a mundial según banda y condiciones. Es la mejor opción de comunicación en emergencias graves.

Subtonos CTCSS/DCS: Los subtonos no cifran la comunicación (cualquiera puede escuchar), pero filtran el canal para que solo se oigan las radios del grupo. Útil para evitar ruido de otros usuarios en el mismo canal, no como medida de seguridad.

Disciplina de radio: Usar indicativos o nombres en código (nunca nombres reales). Transmitir solo lo necesario. Confirmar recepción con "recibido" y finalizar con "cambio" (mensaje parcial) o "corto" (fin de conversación). Mantener las transmisiones por debajo de 30 segundos.

Sistema
Licencia
Potencia
Alcance típico
Coste equipo

PMR446
No
0,5 W
1-5 km campo, 200-500 m ciudad
25-80 € par

CB 27 MHz

No (desde 2017)
4 W AM / 12 W SSB
5-20 km campo
80-200 €

Radioafición VHF/UHF
Sí (examen)
Hasta 50 W portátil
10-50 km con repetidor
30-300 €

Radioafición HF
Sí (examen)
Hasta 500 W
Nacional a mundial
300-3.000 €

Legalidad: Emitir en frecuencias o con potencias no autorizadas es una infracción administrativa grave tipificada en la Ley 9/2014 General de Telecomunicaciones, con sanciones de hasta 20 millones de euros. En caso de emergencia real (peligro para la vida), la normativa internacional permite el uso de cualquier medio de comunicación disponible, pero esto es una excepción estricta. La obtención de la licencia de radioaficionado es la opción recomendada.

Comunicaciones Digitales Cifradas

Mientras exista infraestructura de datos (internet, redes móviles), las aplicaciones de mensajería cifrada son el medio más seguro y práctico para la coordinación de grupos.

Signal: Aplicación de mensajería con cifrado de extremo a extremo (protocolo Signal). Código abierto y auditado. Permite mensajes autodestructivos, grupos cifrados y llamadas cifradas. Es la opción más recomendada por la comunidad de seguridad informática. Disponible para Android, iOS y escritorio.

Briar: Aplicación que funciona sin internet: puede comunicarse por Bluetooth, Wi-Fi directo o red Tor. Cifrado de extremo a extremo. Ideal para escenarios donde la infraestructura de internet ha caído pero los dispositivos siguen funcionando. Solo Android.

Mensajes autodestructivos: Activar la autodestrucción de mensajes (en Signal: desde 5 segundos hasta 4 semanas). Si un dispositivo es capturado o robado, los mensajes antiguos ya no existirán.

Verificación de identidad: Signal permite verificar la identidad de un contacto comparando números de seguridad. Realizar esta verificación en persona antes de la emergencia para asegurar que se habla con quien se cree.

PIN y bloqueo de app: Proteger la aplicación con PIN independiente del desbloqueo del teléfono. Si el dispositivo se compromete, la app sigue protegida.

Dependencia tecnológica: Todas las comunicaciones digitales dependen de electricidad y, en la mayoría de casos, de infraestructura de red. En una crisis prolongada, estas pueden fallar. Por eso es fundamental tener siempre un plan B analógico: radio PMR, mensajeros físicos o señales visuales/sonoras preacordadas. La tecnología es un complemento, nunca la única opción.

Protocolo de Comunicaciones del Grupo

Un protocolo de comunicaciones es un documento acordado por el grupo que establece reglas claras para cuándo, cómo y a través de qué medio comunicarse. Debe ser sencillo, estar escrito y ser ensayado periódicamente.

Check-in programados: Establecer horarios de contacto obligatorio (ejemplo: 08:00 y 20:00 cada día). Si un miembro no realiza el check-in, se activa un protocolo de verificación escalonado: llamada, mensaje a contacto secundario, visita presencial.

Cascada de contacto: Definir una cadena de contacto: el coordinador contacta a 2-3 líderes de subgrupo, cada uno contacta a 3-4 miembros. Esto evita saturar a una sola persona y acelera la comunicación.

Niveles de alerta: Definir niveles claros. Ejemplo: Verde (normalidad, check-in rutinario), Amarillo (situación de atención, aumentar frecuencia de contacto), Rojo (emergencia activa, activar plan de acción inmediata).

Canal primario y secundario: Canal primario: Signal grupo. Canal secundario: radio PMR canal 8 subtono 12. Canal de emergencia: frecuencia de radio preacordada con hora de escucha. Todos los miembros deben conocer los tres canales.

Ensayos periódicos: Realizar al menos un ejercicio trimestral de comunicaciones: activar la cascada de contacto y verificar que todos reciben el mensaje en un tiempo aceptable (menos de 30 minutos). Registrar los tiempos y corregir los puntos débiles.

Nivel de alerta

Frecuencia de contacto

Canal principal

Acción requerida

Verde

Diaria o semanal

Signal / teléfono

Check-in rutinario

Amarillo

Cada 6-12 horas

Signal + radio PMR

Confirmación de estado, preparar equipo

Rojo

Cada 2-4 horas

Radio PMR + mensajero

Ejecutar plan de acción, reagruparse si procede

⚠ 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.