

MANUAL DE CONSULTA RÁPIDA: NORMATIVA DE SISTEMAS ANTIINTRUSIÓN Y ALARMAS

Marco Normativo, Grados de Seguridad (UNE-EN 50131), Establecimientos Obligados (Orden INT/317/2011), Verificación Policial (Orden INT/316/2011) y Ley 5/2014 de Seguridad Privada.

1. MARCO LEGAL Y CLASIFICACIÓN POR GRADOS DE SEGURIDAD (UNE-EN 50131-1 / ORDEN INT/316/2011)

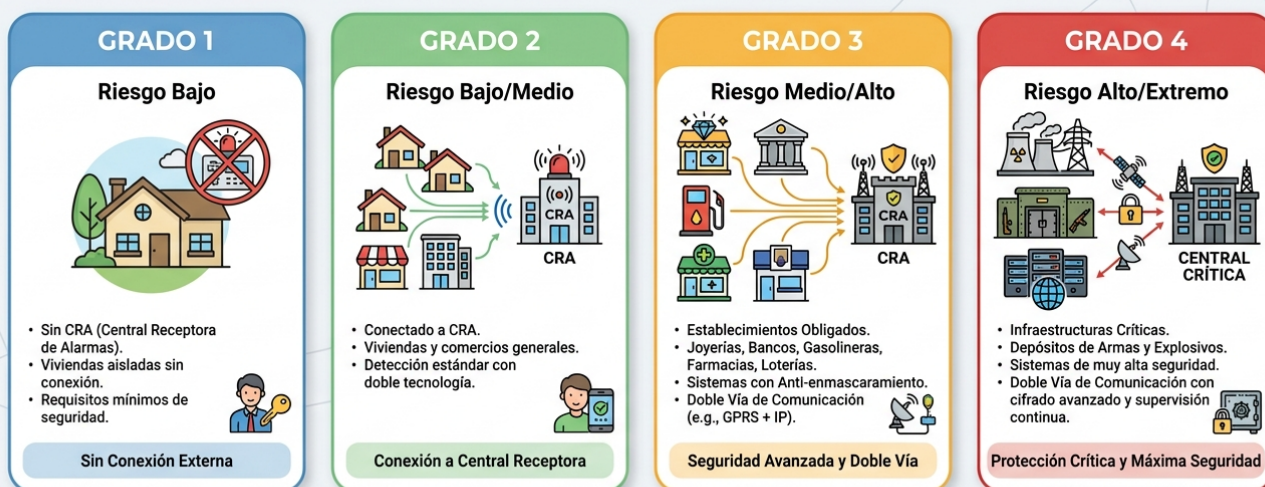
Ámbito de Aplicación y Base Jurídica: La instalación, comercialización, mantenimiento y conexión a Central Receptora de Alarmas (CRA) de los sistemas de seguridad contra robo e intrusión en España se rigen por la **Ley 5/2014, de 4 de abril, de Seguridad Privada**, desarrollada técnicamente por la **Orden INT/316/2011** (sobre funcionamiento de sistemas de alarma) y la **Orden INT/317/2011** (sobre medidas de seguridad privada), así como las normas europeas de la serie **UNE-EN 50131**.

Clasificación de los Sistemas según el Nivel de Riesgo (Grados de Seguridad 1 a 4): La norma UNE-EN 50131-1 establece cuatro grados de seguridad en función del riesgo del espacio a proteger y la vulnerabilidad ante intromisiones no autorizadas:

GRADO DE SEGURIDAD	NIVEL DE RIESGO	ÁMBITO DE APLICACIÓN OBLIGATORIO	REQUISITOS TÉCNICOS CLAVE
GRADO 1	Riesgo Bajo	Sistemas con señalización exclusivamente local. Sin conexión a CRA. Viviendas aisladas o pequeños espacios no conectados.	Instalaciones no conectadas a CRA ni a FCSE. Resistencia frente a intrusos ocasionales.
GRADO 2	Riesgo Bajo / Medio	Viviendas, residencias, pisos, chalets y comercios/negocios generales que pretendan estar conectados a una CRA o centro de control.	Supervisión de línea, resistencia a intromisiones con herramientas básicas. Conexión a CRA obligatoria por empresa habilitada.
GRADO 3	Riesgo Medio / Alto	ESTABLECIMIENTOS OBLIGADOS (Orden INT/317/2011): Joyerías, Bancos/Cajas, Gasolineras, Farmacias, Loterías, Salones de Juego, Armerías, Museos.	Anti-enmascaramiento (anti-masking) obligatorio, doble vía de comunicación redundante (IP + 4G), Proyecto Técnico de Ingeniería.
GRADO 4	Riesgo Alto / Extremo	Infraestructuras Críticas, instalaciones militares, depósitos de explosivos/armas, centros estratégicos de energía y transportes.	Protección contra intrusos expertos. Redundancia total física y lógica, transmisión supervisada continua, máxima protección tamper.

GRADOS DE SEGURIDAD EN ANTIINTRUSIÓN (Norma UNE-EN 50131 / Orden INT/316/2011)

Clasificación técnica de sistemas de alarma según el nivel de riesgo y requisitos normativos en España.



Fuente: Basado en la Norma UNE-EN 50131 y Orden INT/316/2011. Para información detallada, consultar documentación oficial y profesionales homologados.

Figura 1: Clasificación reglamentaria de Grados de Seguridad (Grado 1 a Grado 4) según UNE-EN 50131-1 y Orden INT/316/2011.

2. MEDIDAS DE SEGURIDAD EN ESTABLECIMIENTOS OBLIGADOS (ORDEN INT/317/2011)

Regulación de Establecimientos con Riesgo Especial: La Orden INT/317/2011 impone la instalación de sistemas de seguridad de **GRADO 3** y medidas de protección física específicas para las actividades con elevado riesgo de atraco o intrusión:

TIPO DE ESTABLECIMIENTO	CAJA FUERTE / ALMACENAMIENTO (UNE-EN 1143-1)	CERRAMIENTOS Y ELEMENTOS FÍSICOS	MEDIDAS ELECTRÓNICAS (GRADO 3)
Bancos y Entidades de Crédito	Caja fuerte Grado 4 con retardo de 10 min y temporizador. Cámaras acorazadas Grado VII con pasillo de ronda de 60 cm.	Recinto de caja con blindaje antibala BR2 (UNE-EN 1063). Cristales blindados y esclusa de acceso.	Detectores sísmicos en cámara acorazada, detectores volumétricos con anti-masking, doble vía CRA y pulsadores de atraco.
Joyerías y Platerías	Caja fuerte Grado 4 anclada conforme a UNE 108136 si peso < 2.000 kg. Retardo de 10 min y bloqueo fuera de horario.	Cristales blindados P6B (UNE-EN 356) en escaparates y mostrador. Puertas de acceso Clase 5 (UNE-EN 1627). Cartel visible (18×12 cm).	Detección de intrusión Grado 3 con anti-enmascaramiento, pulsadores de atraco, sistema de niebla de seguridad opcional.
Gasolineras y Estaciones de Servicio	Caja fuerte Grado 4 en zona reservada fuera de la vista del público. Límite de cambio por empleado de 600 €.	Cajas registradoras de cobro automático con límite de 1.200 € en efectivo accesible.	Sistema de alarma Grado 3 conectado a CRA, pulsador de pánico de accionamiento discreto, CCTV de alta resolución.
Farmacias, Loterías y Salones de Juego	Caja fuerte Grado 4 con retardo de 10 min y temporizador de apertura.	Blindaje en mostrador / recinto de caja BR2 o cristal P5A. Dispositivo de dispensación nocturna o bandeja de vaivén.	Sistema de alarma Grado 3, pulsadores fijados en ubicación discreta, supervisión de comunicación por CRA.

MEDIDAS EN ESTABLECIMIENTOS OBLIGADOS (Orden INT/317/2011)

1. Bancos y Entidades Financieras



2. Joyerías y Platerías



3. Gasolineras y Estaciones de Servicio



4. Farmacias, Loterías y Salones de Juego



Ministerio del Interior - España

Figura 2: Exigencias técnicas de seguridad física y electrónica en Establecimientos Obligados conforme a la Orden INT/317/2011.

3. PROTOCOLOS DE VERIFICACIÓN OBLIGATORIA DE ALARMAS ANTE POLICÍA (ORDEN INT/316/2011)

Prohibición Legal de Avisos Directos no Verificados: Conforme al Art. 8 de la Orden INT/316/2011, las Centrales Receptoras de Alarmas (CRA) y los Centros de Control tienen estrictamente prohibido transmitir avisos de alarma a los servicios de emergencia o Fuerzas y Cuerpos de Seguridad del Estado (FCSE) sin haber realizado previamente un protocolo de verificación homologado.

Métodos Oficiales de Verificación de Alarmas: La normativa reconoce cuatro procedimientos válidos para confirmar la presencia real de intrusos:

- 1. **Verificación Secuencial:** Exige la activación consecutiva de **tres o más detectores distintos** en la zona protegida dentro de un intervalo máximo de **30 minutos**. La activación de un solo detector no permite el aviso policial directo.
- 2. **Verificación por Vídeo (CCTV):** La CRA debe recibir y analizar una secuencia de vídeo que confirme la intrusión. La secuencia debe constar obligatoriamente de un mínimo de **2 imágenes Pre-alarma** (anteriores a la activación) y **3 imágenes Post-alarma**.
- 3. **Verificación por Audio:** Escucha directa en tiempo real del área protegida tras la activación de un sensor, mediante la cual el operador de la CRA certifica ruidos de forzamiento, cristales rotos o voces de intrusos.
- 4. **Verificación Personal (Servicio de Acudimiento):** Desplazamiento de un Vigilante de Seguridad habilitado que inspecciona presencialmente el exterior e interior del inmueble (con o sin custodia de llaves).

¡ADVERTENCIA SOBRE FALSAS ALARMAS Y CONSECUENCIAS LEGALES!

La transmisión de falsas alarmas por falta de verificación constituye una **infracción grave** (multas de **3.001 € a 30.000 €**) según la Ley 5/2014. Además, la Autoridad Policial está facultada conforme al **Artículo 55** para ordenar la **DESCONEXIÓN CAUTELAR E INMEDIATA** del sistema de alarma en caso de reiteración de falsas alarmas, quedando el inmueble sin servicio hasta su completa reparación y recertificación.

VERIFICACIÓN OBLIGATORIA DE ALARMAS ANTE POLICÍA (Orden INT/316/2011)

Métodos Legales de Verificación antes de avisar a las Fuerzas de Seguridad



ADVERTENCIA: Sanciones por falsas alarmas y desconexión cautelar.

El incumplimiento puede acarrear multas y la suspensión temporal de la conexión con los servicios policiales.



© 2024 Seguridad

Figura 3: Procedimientos obligatorios de verificación de alarmas por CRA y régimen de sanciones por falsas alarmas (Orden INT/316/2011).

4. TECNOLOGÍA DE DETECCIÓN, ANTI-ENMASCARAMIENTO Y TRANSMISIÓN REDUNDANTE

Tecnologías de Sensores y Detectores (UNE-EN 50131-2): Los elementos de detección deben seleccionarse según el riesgo y el entorno ambiental:

- **Detectores Infrarrojos Pasivos (PIR):** Detectan cambios en la radiación térmica en movimiento. Sensibles a corrientes térmicas brutales.
- **Detectores de Doble Tecnología (PIR + Microondas):** Combinan tecnología térmica e hiperfrecuencia por efecto Doppler. Exigen activación simultánea de ambos canales para generar alarma, eliminando el 99% de falsas alarmas.
- **Contactos Magnéticos (UNE-EN 50131-2-6):** Instalados en puertas y ventanas para supervisar la apertura no autorizada del perímetro.
- **Detectores Sísmicos e Inerciales:** Instalados directamente en estructuras de cajas fuertes, muros acorazados o puertas blindadas para detectar intentos de corte con radial, lanza térmica o impactos.
- **Sistema Anti-enmascaramiento (Anti-Masking):** En instalaciones de Grado 3 y Grado 4, la norma exige de forma obligatoria que todos los detectores cuenten con función Anti-Masking. Esta tecnología detecta de forma inmediata si un intruso intenta tapar o anular el sensor aplicando sprays, pinturas, plásticos, lacas transparentes o cajas a pocos centímetros de la lente, generando de inmediato una señal de sabotaje (Tamper) a la CRA.
- **Supervisión de Comunicaciones y Doble Vía de Transmisión (UNE-EN 50136):** Las centrales de alarma de Grado 3 y 4 deben disponer de doble vía de comunicación independiente y redundante (por ejemplo, Vía 1: IP/Fibra Óptica + Vía 2: Red Celular 4G/5G). La CRA realiza un test periódico de canalización (polling); en caso de corte de fibra o inhibición de la red móvil, la vía secundaria transmite el evento de sabotaje.
- **Sistemas de Niebla de Seguridad (UNE-EN 50131-8):** Generadores de niebla de densidad extrema que, ante una intrusión confirmada, inundan la estancia en menos de **10 segundos**, anulando por completo la visibilidad del delincuente e impidiendo el robo.

TECNOLOGÍA DE DETECCIÓN Y TRANSMISIÓN REDUNDANTE

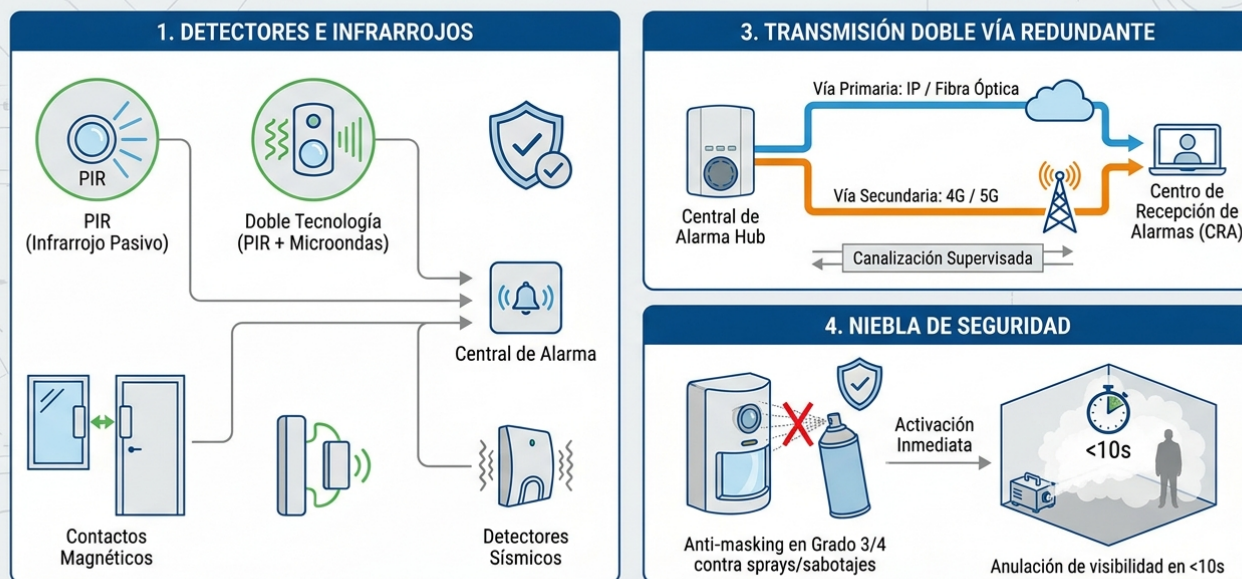


Figura 4: Tecnologías de sensores de seguridad, anti-enmascaramiento y transmisión de comunicaciones de doble vía.

5. EMPRESAS HABILITADAS, PROYECTO TÉCNICO DE INGENIERÍA Y CERTIFICACIÓN (LEY 5/2014)

- **Reserva de Actividad e Inscripción Obligatoria (Art. 5 Ley 5/2014):** Únicamente las Empresas de Seguridad Privada debidamente autorizadas e inscritas en el **Registro Nacional de Seguridad Privada (RNSP)** de la Unidad Central de Seguridad Privada (UCSP) de la Policía Nacional pueden realizar la instalación, mantenimiento y gestión de sistemas de alarma conectados a CRA.
- **Exigencia de Proyecto Técnico de Ingeniería (Art. 46 Ley 5/2014):** Para todas las instalaciones clasificadas en **Grado 3 y Grado 4**, es requisito legal indispensable la elaboración previa de un **Proyecto Técnico de Ingeniería firmado por Ingeniero competente**. El proyecto debe definir el análisis de riesgos, la ubicación de sensores, las especificaciones de blindaje, el plano de canalizaciones y las vías de comunicación redundantes.
- **Homologación de Equipos y Certificación ENAC:** Todo componente (central, teclado, detectores, sirenas) debe disponer del correspondiente Certificado de Evaluación de la Conformidad emitido por una entidad de certificación acreditada por **ENAC (Entidad Nacional de Acreditación)** bajo la norma ISO/IEC 17025.
- **Mantenimiento Preventivo y Libro-Registro:** Las instalaciones de Grado 2, 3 y 4 deben someterse a revisiones de mantenimiento preventivo (presenciales o telemáticas) con la periodicidad establecida. La empresa mantenedora debe expedir el correspondiente Certificado de Mantenimiento y registrar las intervenciones en el **Libro-Registro, que debe conservarse durante mínimo 5 años**.

EMPRESAS HABILITADAS Y PROYECTO TÉCNICO (Ley 5/2014)

ESQUEMA DE REQUISITOS LEGALES PARA SEGURIDAD PRIVADA

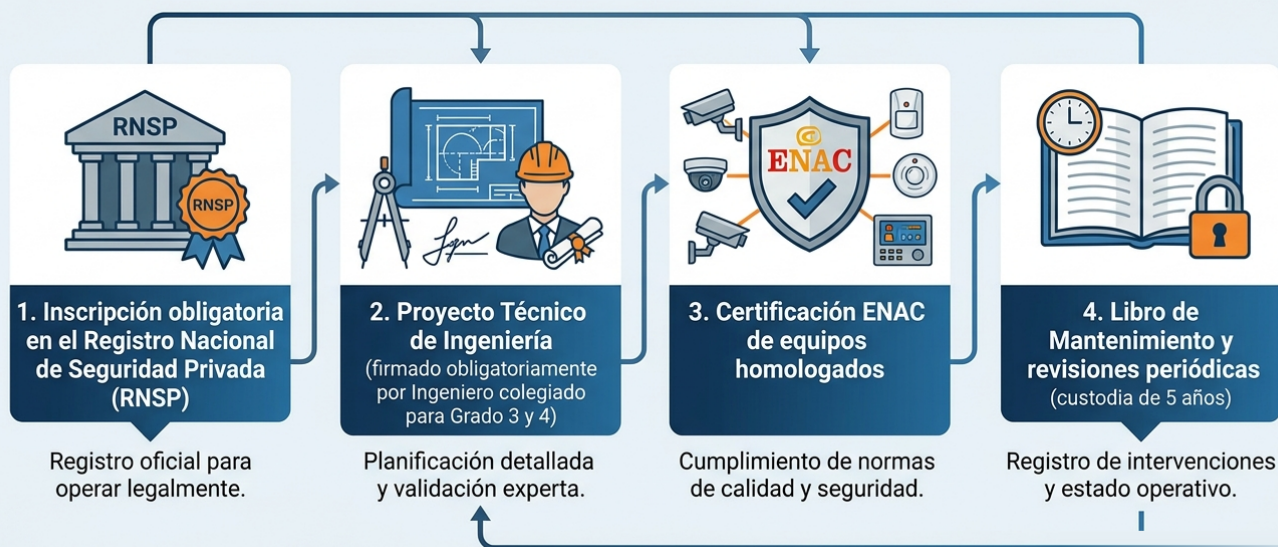


Figura 5: Requisitos de habilitación de empresas de seguridad, Proyectos Técnicos de Ingeniería y certificación ENAC de equipos.

6. RÉGIMEN SANCIONADOR, INTRUSISMO Y MEDIDAS CAUTELARES POLICIALES

Régimen Sancionador en Seguridad Privada (Título VII Ley 5/2014): El incumplimiento de la normativa sobre instalación, mantenimiento y verificación de sistemas de alarma acarrea duras sanciones pecuniarias y administrativas tanto para empresas como para usuarios:

GRAVEDAD DE LA INFRACCIÓN	CONDUCTAS SANCIONABLES TIPO	MULTAS A EMPRESAS DE SEGURIDAD	MULTAS A USUARIOS / TITULARES
INFRACCIONES MUY GRAVES (Art. 57.1 / 59.1)	Prestar servicios sin autorización (intrusismo). Instalación de equipos no homologados que generen vulnerabilidad o riesgo grave.	De 30.001 € a 600.000 € Posible cancelación de la inscripción y cierre de la empresa de 1 a 2 años.	De 20.001 € a 100.000 € Contratar intencionadamente empresas pirata no autorizadas.
INFRACCIONES GRAVES (Art. 57.2 / 59.2)	Transmisión reiterada de falsas alarmas por falta de verificación. Omitir el Proyecto Técnico en Grado 3/4. Falta de revisiones obligatorias.	De 3.001 € a 30.000 € Suspensión temporal de la autorización de 1 a 6 meses.	De 3.001 € a 20.000 € Negarse a reparar deficiencias requeridas por la Policía.
INFRACCIONES LEVES (Art. 57.3 / 59.3)	Irregularidades menores en el Libro-Registro o retrasos en comunicaciones administrativas de trámites secundarias.	De 300 € a 3.000 € Apercibimiento por escrito.	De 100 € a 3.000 € Apercibimiento.

Medidas Cautelares de Intervención Policial (Art. 55 Ley 5/2014): Las Fuerzas y Cuerpos de Seguridad están legalmente facultadas para la **desconexión inmediata del sistema de alarma** en caso de mal funcionamiento recurrente o falsas alarmas que perturben la seguridad ciudadana, así como para la inmovilización cautelar de equipos y precintado en instalaciones realizadas por empresas pirata o no habilitadas.

RÉGIMEN SANCIONADOR Y MEDIDAS CAUTELARES POLICIALES

INFRACCIONES Y SANCIONES		
INFRACCIONES MUY GRAVES	INFRACCIONES GRAVES	INFRACCIONES LEVES
 MULTA HASTA 600.000 € • Cierre por Intrusismo • Falta de Homologación de Equipos/Sistemas	 MULTA 3.001 € a 30.000 € • Falsas Alarmas Recurrentes • Falta de Proyecto Técnico	 MULTA HASTA 3.000 € • Infracciones Menores o Administrativas

**MEDIDAS CAUTELARES POLICIALES**

- **Desconexión del sistema**

- **Inmovilización de empresas no autorizadas**


Intervención policial inmediata para evitar riesgos o daños continuados, aplicando medidas provisionales antes de la resolución final del expediente sancionador

El presente esquema es un resumen informativo y no constituye asesoramiento legal.
Consulte la legislación vigente para detalles completos.

Figura 6: Cuadro del régimen sancionador según la Ley 5/2014 y medidas cautelares policiales de desconexión.