

MANUAL DE CONSULTA RÁPIDA: NORMATIVA DE CCTV Y PROTECCIÓN DE DATOS

Guía Técnica de Videovigilancia (LOPDGDD / RGPD / Ley 5/2014) para Instaladores e Ingenieros Proyectistas.

PROMUEVE: GUÍA DE REFERENCIA TÉCNICA E INTEGRACIÓN NORMATIVA DE VIDEOVIGILANCIA

Este manual unifica los criterios técnicos de la Ley 5/2014 de Seguridad Privada y la Orden INT/316/2011 con las exigencias legales del RGPD (UE 2016/679) y la LOPDGDD (LO 3/2018). Es de aplicación obligatoria para ingenieros proyectistas, empresas instaladoras, personal de seguridad y responsables del tratamiento.

1. MARCO LEGAL, LEGITIMACIÓN Y ÁMBITO DE CAPTACIÓN DE CÁMARAS

1.1. Base Jurídica del Tratamiento (Art. 6.1 RGPD y Art. 22.1 LOPDGDD): El tratamiento de imágenes mediante sistemas de videovigilancia o CCTV no requiere el consentimiento previo de las personas afectadas. La legitimación legal se fundamenta directamente en el cumplimiento de una misión realizada en **interés público** (Art. 6.1.e RGPD) y en la satisfacción de **intereses legítimos** orientados a la preservación de la seguridad de las personas, bienes e instalaciones (Art. 6.1.f RGPD y Art. 22.1 LOPDGDD). Sin embargo, esta base legal exige el cumplimiento estricto y riguroso del deber de información previa mediante dispositivos informativos (carteles).

1.2. Delimitación del Campo de Visión y Vía Pública (Art. 22.2 LOPDGDD):

- **Regla General de Prohibición:** Las cámaras de videovigilancia instaladas por sujetos privados (particulares, empresas o comunidades) **NO pueden captar imágenes de la vía pública**, terrenos colindantes ni propiedades de terceros. La vigilancia de la vía pública es competencia exclusiva de las Fuerzas y Cuerpos de Seguridad del Estado (FCSE).
- **Excepción por Imprescindibilidad Técnica:** Solo se admite la captación de la **franja mínima e indispensable de la vía pública accedente** cuando resulte estrictamente necesario para garantizar la seguridad de los accesos principales, fachadas, puertas o escaparates (ej. umbral de entrada o puerta de garaje). En ningún caso la toma de la vía pública puede ser desproporcionada ni abarcar el tránsito general de peatones.
- **Excepción para Infraestructuras Críticas:** Se permite una captación más amplia de la vía pública en instalaciones estratégicas o vinculadas a las infraestructuras de transporte (estaciones, puertos, aeropuertos) previa justificación de seguridad.
- **Prohibición Absoluta sobre Viviendas Adyacentes:** Las cámaras no podrán en ningún caso enfocar ni registrar el interior de viviendas, ventanas, jardines o zonas privadas adyacentes pertenecientes a vecinos o terceros.

1.3. Zonas Privadas e Íntimas (Prohibición Absoluta de Grabación): Queda terminantemente prohibida la instalación de cámaras de videovigilancia en espacios donde se presuma un nivel absoluto de privacidad o intimidad: **aseos, servicios higiénicos, vestuarios, probadores, saunas, zonas de descanso de trabajadores, vestuarios de personal y comedores privados**. La colocación de cámaras en estos puntos constituye una infracción muy grave sancionable por la AEPD con **multas de hasta 20.000.000 €**.

1.4. Empresa Habilitada vs. Autoinstalación (Ley 5/2014 de Seguridad Privada):

TIPO DE SISTEMA CCTV	REQUISITO DE INSTALACIÓN	NORMATIVA APLICABLE	CONEXIÓN A CRA
CCTV Conectado a CRA / Grado 2-4	OBLIGATORIO: Empresa de Seguridad Privada habilitada e inscrita en el RII/Seguridad Privada.	Ley 5/2014, Orden INT/317/2011 y LOPDGDD.	SÍ: Verificación de alarmas por CRA
CCTV Aislado ('Offline' / Autoinstalación)	Permitida autoinstalación por titular o instalador de telecomunicaciones (sin CRA).	LOPDGDD (Art. 22) y RGPD.	NO: Solo uso local/interno del titular



Figura 1: Esquema de Legitimación, Delimitación de Campo de Visión y Exigencias de Empresa Habilitada.

2. DEBER DE INFORMACIÓN: CARTELES INFORMATIVOS Y DOBLE CAPA (ART. 22.4 LOPDGDD)

El Reglamento General de Protección de Datos (Art. 12 RGPD) y el Art. 22.4 de la LOPDGDD exigen que el deber de información a los ciudadanos se articule mediante un **sistema de doble capa informativa**:

2.1. Capa 1: Dispositivo Informativo de Primer Nivel (Cartel Normalizado):

- **Ubicación Estratégica Obligatoria:** El cartel de aviso de videovigilancia debe ubicarse en **TODOS los accesos** a la zona videovigilada (puertas de entrada, verjas perimetrales, accesos a garajes, recepción). Debe situarse en un lugar perfectamente visible y **ANTES** de que la persona penetre en el campo de visión o alcance de las cámaras.
- **Contenido Mínimo Obligatorio del Cartel de Primer Nivel:**
 - *Pictograma Normalizado:* Icono identificativo claro de una cámara de videovigilancia.
 - *Identidad del Responsable:* Nombre o Razón Social completa del Responsable del Tratamiento y su NIF/CIF.
 - *Finalidad del Tratamiento:* Explicación concisa (ej. 'Videovigilancia y Seguridad de bienes e instalaciones').
 - *Ejercicio de Derechos ARSOPL:* Referencia explícita a la posibilidad de ejercitar los derechos de Acceso, Supresión, Limitación del tratamiento y Oposición, indicando la dirección postal o correo electrónico ante el cual dirigirse.
 - *Acceso a la Capa 2:* Indicación de dónde obtener la información detallada (ej. 'Información detallada disponible en recepción / www.empresa.com/privacidad' o mediante código QR).

2.2. Capa 2: Información Detallada Completa (Hoja Informativa):

El responsable debe poner a disposición de los usuarios interesados una hoja informativa física (en recepción, conserjería o atención al cliente) o un enlace web directo accesible mediante código QR impreso en el cartel. Esta información de segundo nivel debe detallar: los datos de contacto del Delegado de Protección de Datos (DPO) si existiera, el **plazo de conservación de las imágenes (30 días)**, los posibles destinatarios de las grabaciones (FCSE y Juzgados), la base legal del tratamiento y el derecho a presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD - www.aepd.es).



3. PLAZOS DE CONSERVACIÓN, CUSTODIA Y MEDIDAS DE SEGURIDAD TÉCNICAS

3.1. Regla General de Conservación: Plazo Máximo de 1 Mes (30 Días): Según establece categóricamente el Art. 22.3 de la LOPDGDD, las imágenes grabadas por los sistemas de videovigilancia deberán ser canceladas y suprimidas en el **plazo MÁXIMO DE UN MES (30 días)** desde su captación. Los equipos de grabación (NVR/DVR) deben configurarse para realizar un borrado o sobrescritura cíclica automática transcurrido dicho plazo. Mantener imágenes almacenadas más allá de los 30 días sin una justificación de ilícito constituye una infracción grave sancionable por la AEPD.

3.2. Excepción: Bloqueo y Puesta a Disposición Judicial / Policial (72 Horas):

- **Regla de Conservación para Investigación:** Cuando las cámaras hayan registrado la comisión de un delito, falta, accidente o atentado contra la seguridad de personas o bienes, la obligación de borrado a los 30 días queda suspendida.
- **Procedimiento de Bloqueo:** El responsable debe extraer las imágenes del incidente, proceder a su **bloqueo técnico** (impidiendo su acceso, copia o modificación) y guardarlas únicamente para su entrega a las autoridades.
- **Plazo Obligatorio de Entrega:** Las imágenes deberán ser puestas a disposición de las Fuerzas y Cuerpos de Seguridad del Estado o de la Autoridad Judicial en un plazo **MÁXIMO DE 72 HORAS** desde que se tenga conocimiento de la existencia de la grabación con el suceso.

3.3. Checklist de Medidas de Seguridad del Grabador (Art. 32 RGPD):

ÁREA DE SEGURIDAD	REQUISITO TÉCNICO MÍNIMO OBLIGATORIO	VERIFICACIÓN TÉCNICA
Protección Física	NVR/DVR alojado en armario técnico o rack cerrado bajo llave en recinto restringido.	Verificar cerradura y control de acceso.
Control Lógico	Usuarios individuales con contraseña robusta. PROHIBIDO usar claves por defecto (admin/admin).	Cálculo de complejidad de contraseña.
Registro de Accesos (Logs)	Registro automatizado e inalterable de accesos a visión en directo, grabaciones y descargas.	Comprobar exportación de logs.
Cifrado de Red	Transmisión de vídeo cifrada (RTSPS / HTTPS / VPN). Puertos UPnP desactivados.	Auditoría de puertos del router/NVR.



Figura 3: Cronología de Conservación (30 días), Protocolo de Incidencias (72h) y Medidas de Seguridad NVR/DVR.

4. VIDEOVIGILANCIA EN EL ÁMBITO LABORAL Y CONTROL EMPRESARIAL (ART. 89 LOPDGDD)

El uso de cámaras para el control del cumplimiento de las obligaciones laborales por parte del empresario se rige por el Art. 20.3 del Estatuto de los Trabajadores y el Art. 89 de la LOPDGDD, exigiendo garantías específicas para proteger la dignidad del empleado:

4.1. Información Previa Obligatoria a Trabajadores y RLT: El empleador puede tratar las imágenes obtenidas a través de videovigilancia para el ejercicio de las funciones de control laboral, **SIEMPRE QUE HAYA INFORMADO CON CARÁCTER PREVIO, DE FORMA EXPLÍCITA, CLARA E INEQUÍVOCA** a los trabajadores y, en su caso, a la Representación Legal de los Trabajadores (RLT) sobre la implantación del sistema y su finalidad disciplinaria o de control.

4.2. Excepción por Sospechas Fundadas de Incumplimiento Grave: En el supuesto de que se hayan detectado **sospechas fundadas o indicios de la comisión de actos ilícitos o robos** por parte de los trabajadores, si la empresa no hubiera realizado una notificación previa individualizada, se entenderá cumplido el deber de información siempre que existiera, al menos, el **cartel informativo de primer nivel en lugar perfectamente visible** dentro del centro de trabajo (Criterio AEPD y Doctrina Constitucional).

4.3. Prohibiciones Absolutas: Zonas de Descanso y Grabación de Audio:

- **Lugares Prohibidos:** Se prohíbe de forma tajante la instalación de cámaras en vestuarios, aseos, comedores, salas de descanso y locales sindicales.
- **Prohibición General de Grabación de Sonido (Micrófonos):** La utilización de sistemas de videovigilancia que incorporen **grabación de audio o micrófonos** en los lugares de trabajo está **PROHIBIDA CON CARÁCTER GENERAL** (Art. 89.3 LOPDGDD). Solo se admitirá de forma excepcionalísima cuando existan riesgos graves para la seguridad de las instalaciones derivados de la actividad, previa evaluación de proporcionalidad y estricta necesidad.

'VIDEOVIGILANCIA LABORAL Y CONTROL EMPRESARIAL (ART. 89 LOPDGDD)'



Figura 4: Criterios de Videovigilancia Laboral, Preaviso, Prohibición de Audio y Zonas Protegidas.

5. ESPECIFICACIONES TÉCNICAS, VERIFICACIÓN POR CRA Y SANCIONES AEPD

5.1. Conexión a Central Receptora de Alarmas y Verificación por Vídeo (Orden INT/316/2011): En los sistemas de seguridad de Grado 2, 3 y 4 conectados a Central Receptora de Alarmas (CRA), las imágenes de CCTV son la herramienta técnica fundamental para la verificación de las señales de alarma por intrusión. Secuencia Mínima para Policía: Para confirmar la veracidad de una alarma ante las Fuerzas y Cuerpos de Seguridad, la CRA debe recibir una secuencia de vídeo o ráfaga de imágenes que contenga como mínimo **2 imágenes pre-alarma y 3 imágenes post-alarma** (o vídeo continuo en tiempo real) que permitan identificar claramente la presencia no autorizada.

5.2. Requisitos Técnicos Mínimos de las Cámaras de Seguridad:

- **Iluminación e Infrarrojos (IR):** Las cámaras en exteriores o zonas oscuras deben disponer de visión nocturna mediante LEDs Infrarrojos con alcance adecuado a la distancia de detección o sensores de alta sensibilidad (DarkFighter/ColorVu $\leq 0,001$ lux).
- **Tasa de Cuadros (fps):** Para garantizar la fluidez en la identificación de personas, el grabador debe mantener una tasa mínima de **12 a 25 fps** por canal.
- **Alimentación Ininterrumpida (SAI / UPS):** Es obligatorio dotar al NVR/DVR y switches PoE de un SAI/UPS dimensionado para mantener la grabación continua ante cortes de suministro eléctrico o sabotaje durante el tiempo exigido en el proyecto de seguridad.

5.3. Cumplimiento Administrativo: RAT, EIPD/DPIA y DPO:

- **Registro de Actividades de Tratamiento (RAT):** Todo titular debe crear y mantener actualizado el RAT para la actividad 'Videovigilancia y Seguridad'.
- **Evaluación de Impacto (EIPD / DPIA):** Requerida obligatoriamente en instalaciones masivas (centros comerciales, recintos deportivos, transporte) o cuando se empleen tecnologías avanzadas de analítica de vídeo (reconocimiento facial, biometría, seguimiento de patrones con IA).
- **Delegado de Protección de Datos (DPO):** Obligatorio en entidades públicas, centros sanitarios, empresas de seguridad privada y tratamientos a gran escala.

5.4. Cuadro Sancionador de la AEPD por Infracciones en Videovigilancia:

GRAVEDAD DE INFRACCIÓN	RANGO DE SANCIÓN ECONÓMICA	EJEMPLOS TIPIFICADOS DE INFRACCIÓN (AEPD)
Infracción Leve	Hasta 40.000 €	Cartel informativo incompleto, omisión de datos del responsable o ilegibilidad del cartel.
Infracción Grave	De 40.001 € a 300.000 €	Captación desproporcionada de vía pública sin justificación, conservación > 30 días sin delito, falta de medidas de seguridad en NVR (claves por defecto).
Infracción Muy Grave	De 300.001 € a 20.000.000 € (o 4% facturación)	Cámaras en aseos o vestuarios, cesión/difusión no autorizada de imágenes en redes sociales, uso de reconocimiento facial biométrico sin base legal.

ESPECIFICACIONES TÉCNICAS Y CONEXIÓN A CRA (ORDEN INT/316/2011)

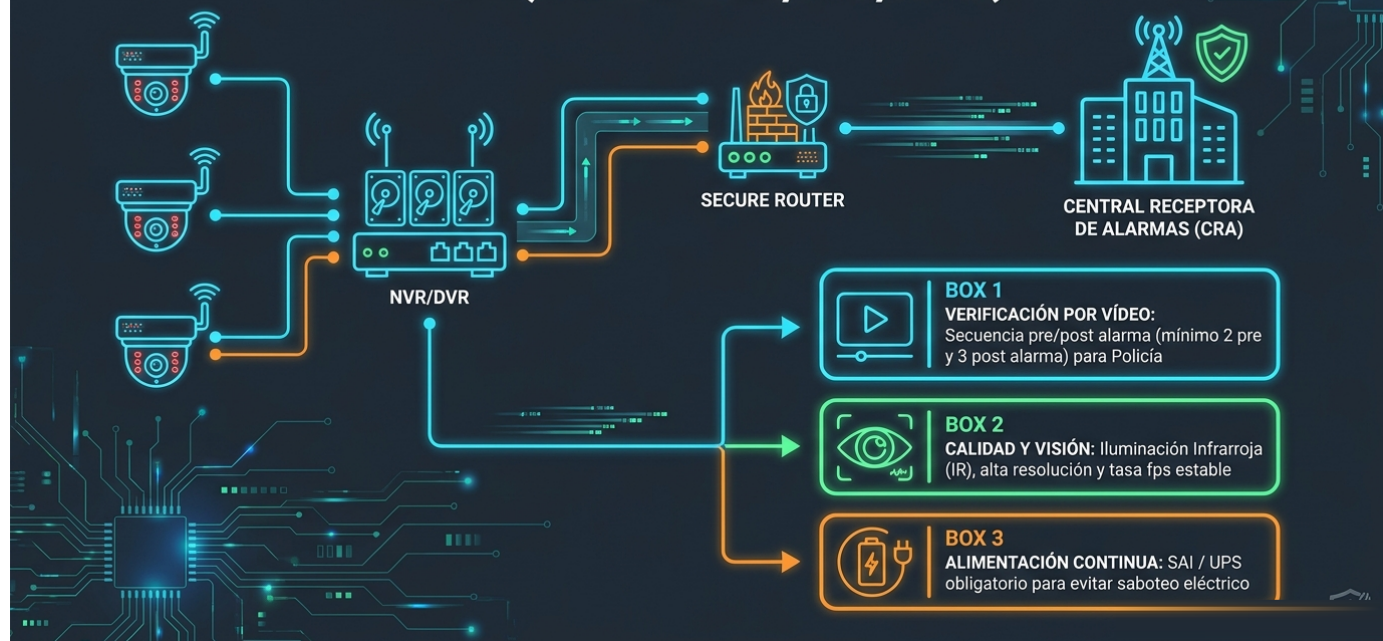


Figura 5: Protocolo de Verificación de Video por CRA (Orden INT/316/2011) y Especificaciones Técnicas.

CUMPLIMIENTO ADMINISTRATIVO Y SANCIONES AEPD



Figura 6: Requisitos Administrativos (RAT, EIPD, DPO) y Escala Sancionadora de la AEPD.