



Implicaciones Normativas del ENS en los Sistemas de Videovigilancia

Los sistemas de videovigilancia han evolucionado desde simples herramientas de seguridad física a complejos sistemas de información interconectados. En el contexto regulatorio español, cualquier despliegue de estos sistemas dentro del sector público, o por parte de empresas privadas que le presten servicios, debe alinearse obligatoriamente con el **Esquema Nacional de Seguridad (ENS)**. Esta integración exige que las imágenes y metadatos captados se gestionen bajo rigurosos criterios de ciberseguridad, confidencialidad e integridad técnica.

La Categorización del Sistema: ¿Por qué la videovigilancia es siempre nivel Medio o Alto?

El ENS (regulado por el Real Decreto 311/2022) determina las medidas de protección aplicables a un sistema en función de su categorización (**Básica, Media o Alta**). Este proceso se calcula evaluando el impacto que tendría para la organización un incidente de seguridad que afecte a las dimensiones de Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad (CIDAT) de la información.

En el caso de los sistemas de videovigilancia, la normativa los sitúa de forma casi sistemática en los niveles Medio o Alto, excluyendo prácticamente su consideración como sistemas de nivel Bajo por las siguientes razones técnicas y legales:

1. Tratamiento de datos a gran escala:

Los sistemas en edificios públicos o espacios urbanos monitorizan de forma continua e indiscriminada a un número indeterminado de personas, lo que impide normativamente la clasificación del sistema como Bajo, de acuerdo con el Reglamento General de Protección de Datos (RGPD).



2. **Uso de tecnologías emergentes y analítica:** Las cámaras modernas incluyen lectura de matrículas (LPR) o control de aforos. Si el sistema implementa reconocimiento facial o identificación de patrones de conducta, pasa automáticamente a Nivel Alto, dado que procesa datos de categorías especiales según el RGPD.

3. **Seguridad de las personas e instalaciones críticas:** Un sabotaje lógico al sistema de cámaras facilita intrusiones físicas en sedes gubernamentales o prisiones, lo que eleva el riesgo a un nivel de impacto grave (Medio) o muy grave (Alto).
4. **Vulnerabilidad inherente e interconexión:** Las cámaras IP son dispositivos IoT distribuidos geográficamente (muchas veces en fachadas públicas). Un sistema catalogado como Bajo carecería de la segmentación técnica necesaria para evitar que un atacante manipule una cámara física y salte desde allí a la red corporativa central de la administración.

Consecuencias de la Categorización: Requisitos Técnicos Exigibles

Como consecuencia directa de la clasificación en Nivel Medio o Alto, el ENS activa un catálogo de exigencias estrictas e imperativas recogidas en el **Anexo II del Real Decreto 311/2022** sobre los componentes de la infraestructura:

A. Control de Acceso e Identidad (Medidas [op.acc.1] y [op.acc.2])

- Autenticación Multifactor (MFA) Obligatoria.
- Identificación Unívoca de Componentes (802.1X).
- Principio de Mínimo Privilegio.

B. Protección de los Datos y Canales de Comunicación (Medidas [mp.com.1] y [mp.info.1])

- Cifrado de Extremo a Extremo.
- Cifrado en Reposo de las Grabaciones.
- Segmentación Estricta de Redes.

C. Operación, Gestión y Trazabilidad (Medidas [op.exp.2] y op.exp.3])

- Centralización e Inalterabilidad de Logs.
- Sincronización Temporal Autenticada.
- Gestión Centralizada de Parches.
- Alta Disponibilidad (Obligatoria en Nivel Alto).

El Mandato de la Instrucción [op.pl.5]: Uso Obligatorio del CPSTIC

La instrucción [op.pl.5] (**Componentes Certificados**), perteneciente a la familia de Planificación del Anexo II del Real Decreto, establece de forma tajante que para sistemas de nivel Medio o Alto se utilizará, para la adquisición de productos de seguridad, el **Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC)** del CCN.

Esta directriz transforma por completo la adquisición de hardware y software de videovigilancia:

- **Garantía en las medidas de ciberseguridad:** Los componentes del sistema de videovigilancia deben cumplir con los **Requisitos Fundamentales de Seguridad (RFS)** que establece el CCN, los cuales los habilitan para su cualificación en el catálogo CPSTIC.
- **Vías de cualificación técnica:** Para ingresar en este catálogo del CCN, los fabricantes deben someter sus productos a evaluaciones de laboratorio bajo metodologías como LINCE (comúnmente usada para niveles Medios) o Common Criteria / ISO/IEC 15408 (exigida con frecuencia para niveles Altos).

Evidencia formal: No basta con certificaciones comerciales extranjeras de manera aislada; si un modelo de cámara IP o software VMS concreto no figura en la lista pública del CPSTIC, el sistema incurrirá en una no conformidad de auditoría. Solo se exime su uso si se justifica documentalmente en el Análisis de Riesgos la ausencia absoluta de alternativas en el mercado nacional que estén incluidas en el catálogo.



Diferencia entre Entidad Acreditada, Entidad Certificada y Sistema Conforme

En el ecosistema normativo del ENS coexisten tres términos jurídicos distintos cuya confusión invalida habitualmente los pliegos de prescripciones técnicas (PPT):

- 1 **Entidad Acreditada (El Auditor):** Es la empresa de auditoría externa que ha demostrado su competencia e imparcialidad ante la Entidad Nacional de Acreditación (ENAC). Son las únicas firmas autorizadas legalmente en España para emitir una Certificación de Conformidad con el ENS para niveles Medio o Alto.
- 2 **Entidad Certificada (La Empresa Proveedora):** Es la compañía integradora de seguridad, instaladora o proveedora de servicios de videovigilancia en el Cloud que ha superado la auditoría de una Entidad Acreditada. Certifica que sus procesos de trabajo, la custodia de credenciales y sus sistemas internos cumplen con el ENS. No obstante, que el instalador esté certificado **no significa de forma automática** que la instalación física final sea conforme. Esta certificación no aplica a los componentes del sistema, es decir a los dispositivos. No existe un certificado ENS para los equipos del sistema.
- 3 **Sistema que cumple con los requerimientos (La Infraestructura):** Es el conjunto real de cámaras IP, cableado, switches segmentados y grabadores NVR desplegados en la sede pública que ha sido técnicamente securizado y bastionado bajo las pautas del ENS. Estas pautas exigen medidas técnicas según su categorización, que pueden incluir su cualificación verificable. El fin último de la ley es lograr que esta infraestructura local sea un **Sistema Conforme**.

El Proceso de Auditoría Formal Obligatoria

Los sistemas de videovigilancia categorizados en Nivel Medio o Alto están sujetos a obligaciones de control formal muy estrictas:

- **Auditoría Regular Bienal:** De acuerdo con el Artículo 31 del Real Decreto 311/2022, estos sistemas deben someterse a una **auditoría formal ordinaria al menos cada dos años**. Esta auditoría debe ser ejecutada por una Entidad Acreditada independiente.
- **Auditorías Extraordinarias:** Se debe realizar una auditoría técnica extraordinaria siempre que se produzcan **modificaciones sustanciales** en la infraestructura de videovigilancia (por ejemplo, una migración masiva de almacenamiento local a la nube o la integración de módulos de reconocimiento facial).
- **Dictamen y Plan de Adecuación:** El informe de auditoría analiza la conformidad técnica de cada cámara, switch y grabador con las medidas del ENS. Los hallazgos de vulnerabilidades o incumplimientos técnicos generarán un Dictamen de Auditoría que obliga a la organización a presentar un Plan de Adecuación inmediato para corregir las deficiencias bajo riesgo de perder la Declaración o Certificación de Conformidad.

La convergencia entre el ENS y el RGPD

El cumplimiento del ENS no es independiente de la normativa de privacidad. Mientras que el Reglamento General de Protección de Datos (RGPD) y la Agencia Española de Protección de Datos (AEPD) velan por los derechos de los ciudadanos (proporcionalidad, derecho de información mediante carteles y limitación del plazo de conservación a 30 días), el ENS proporciona el **blindaje técnico** para que esos datos no sufran brechas digitales o ciberataques.



Así se manifiesta textualmente en las directrices de aplicación normativa:

«Para los sistemas de videovigilancia que sean utilizados por entidades públicas, en cuanto que realizan tratamiento de datos personales mediante captación de imágenes, de acuerdo con el artículo 32 del Reglamento (UE) 2016/679 y con la disposición adicional primera de la Ley Orgánica 3/2018 (LOPDGDD), las medidas de seguridad (ciberseguridad) aplicables a dichos tratamientos, cuando son realizados por entidades del sector público, son las previstas en el Esquema Nacional de Seguridad (ENS)»

Por lo tanto, el cumplimiento de la normativa de protección de datos exige también, de forma implícita, el cumplimiento estricto de las medidas de ciberseguridad establecidas por el ENS. En estos niveles Medio o Alto, el marco regulatorio exige realizar de forma conjunta un Análisis de Riesgos formal y una Evaluación de Impacto en la Protección de Datos (EIPD) antes de que la primera cámara comience a grabar.

Implicaciones para la contratación pública y proveedores

Cualquier empresa de seguridad privada o proveedora tecnológica que licite para instalar o mantener sistemas de videovigilancia en la Administración pública debe cumplir con el artículo 2 del Real Decreto 311/2022.

En consecuencia, los pliegos de prescripciones técnicas (PPT) deben exigir explícitamente los siguientes requisitos:

- **Certificación del contratista:** La empresa adjudicataria debe contar con una Certificación de Conformidad con el ENS vigente y adecuada a la categoría del sistema licitado.
- **Cualificación de los componentes:** Los dispositivos y soluciones de la infraestructura (cámaras IP, software VMS, servidores, grabadores, etc.) deben disponer del nivel de cumplimiento y la cualificación técnica en el CPSTIC que corresponda a la categoría del sistema.

Alberto Alonso

Miembro de área de ciberseguridad de AES.