



**AES**  
FUNDACIÓN

# **Guía de Desarrollo e Implementación de Proyectos de Instalación de Sistemas Electrónicos de Seguridad**

|                                                                                                                             |           |
|-----------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>1. Introducción</b>                                                                                                      | <b>6</b>  |
| 1.1. Propósito de la guía                                                                                                   | 6         |
| 1.2. Alcance y público objetivo                                                                                             | 7         |
| 1.3. Principios rectores: cumplimiento normativo y buenas prácticas                                                         | 8         |
| <b>2. Contexto y Requisitos del Proyecto</b>                                                                                | <b>10</b> |
| 2.1. Descripción del entorno operativo y riesgos del sector                                                                 | 11        |
| 2.2. Objetivos, restricciones y criterios de éxito                                                                          | 11        |
| 2.3. Partes interesadas y roles (cliente, director/ingeniero de seguridad, instalador, central receptora)                   | 11        |
| <b>3. Marco Normativo Aplicable</b>                                                                                         | <b>12</b> |
| 3.1. Ley de Seguridad Privada, Reglamento y Órdenes Ministeriales                                                           | 12        |
| 3.2. El Proyecto de Instalación según la Norma UNE-CLC/TS 50131-7.                                                          | 14        |
| 3.3. Conexión a Central de Alarmas, Mantenimientos y Revisiones, y Procedimientos de Verificación de Alarmas.               | 17        |
| 3.4. Protección de Datos (RGDP / LOPDGDD) y conservación de imágenes                                                        | 19        |
| <b>4. Ciclo de Vida</b>                                                                                                     | <b>20</b> |
| 4.1. Inicio                                                                                                                 | 20        |
| 4.1.1. Acta de constitución y caso de negocio                                                                               | 20        |
| 4.1.2. Identificación de interesados y estrategia de implementación                                                         | 21        |
| 4.2. Planificación                                                                                                          | 21        |
| 4.2.1. Alcance y EDT (incluyendo paquetes técnicos por subsistema: CCTV, intrusión, control de accesos, interfonía)         | 21        |
| 4.2.2. Diseño técnico y especificaciones (estudio de emplazamiento, selección de recursos, canalizaciones y disponibilidad) | 22        |
| 4.2.3. Cronograma (Gantt), recursos, adquisiciones y presupuesto                                                            | 22        |
| 4.2.4. Planes de gestión: PRL, calidad, comunicaciones, riesgos, seguridad/ciberseguridad y compliance                      | 23        |
| 4.3. Ejecución                                                                                                              | 28        |
| 4.3.1. Replanteo, acopios e instalación física                                                                              | 28        |
| 4.3.2. Configuración, integración y pruebas de comisionado                                                                  | 29        |
| 4.3.3. Formación a usuarios y traspaso operativo inicial                                                                    | 29        |
| 4.4. Monitoreo y Control                                                                                                    | 31        |
| 4.4.1. Seguimiento de cronograma y costes; control de cambios                                                               | 32        |

|                                                                                            |    |
|--------------------------------------------------------------------------------------------|----|
| 4.4.2. Control de calidad, ensayos normativos y auditorías .....                           | 36 |
| 4.4.3. Indicadores (KPI/SLAs) y reporting de cumplimiento .....                            | 38 |
| 4.5. Cierre .....                                                                          | 44 |
| 4.5.1. Verificación final, conexión con Centro de control o CRA y acta de aceptación ..... | 44 |
| 4.5.2. Documentación as-built .....                                                        | 46 |
| 5. Operación y Mantenimiento Post-Implantación .....                                       | 49 |
| 5.1. Plan de mantenimiento normativo y preventivo .....                                    | 49 |
| 5.2. Gestión de incidencias, obsolescencia y mejoras evolutivas .....                      | 53 |
| 5.2.1. Gestión de incidencias y no conformidades .....                                     | 53 |
| 5.2.2. Gestión de la obsolescencia tecnológica .....                                       | 54 |
| 5.2.3. Mejora evolutiva y optimización del sistema .....                                   | 55 |

En la Industria de la Seguridad en España y como asociación decana, AES siempre ha desarrollado un papel vital. Representamos a nuestro país tanto en los Comités Nacionales y Europeos donde se crean las normas como en las dos principales asociaciones europeas como son Eurosafe y Euralarm. Todo ello es posible gracias a la dedicación y conocimiento de nuestros expertos pertenecientes a las diferentes Áreas de Trabajo que disponemos. La información es poder y por supuesto vital para la competitividad de nuestras empresas asociadas. El compromiso social es parte de nuestro ADN y para ello creamos continuamente guías, recomendaciones y publicaciones desde donde transmitimos nuestro conocimiento. En nombre de toda la Junta Directiva de AES esperamos que disfrutes de este trabajo que con tanto cariño hemos realizado.



Iñigo Ugalde Blanco –Presidente de AES.

Después de muchos meses de trabajo y dedicación, el 27 de junio de 2024 quedó registrada AES FUNDACIÓN en el Registro Nacional de Fundaciones. Uno de los objetivos establecidos para la Fundación es la difusión de los documentos elaborados por las áreas de trabajo de AES.

Es por ello por lo que todas las publicaciones de nuestras áreas de trabajo (ya tenemos incorporadas varias guías que puedes consultar sin coste en [Publicaciones AES Fundación](#) así como la Newsletter y el Boletín, han empezado a aparecer con el color naranja distintivo de la Fundación, y en el caso de Newsletter y Boletín, con una nueva numeración de segunda época.

Todo ello forma parte del desarrollo [#UniversoAES](#) y [#HaciendoIndustria](#). Espero que esta nueva publicación que os traemos hoy sirva de ayuda y siga contribuyendo con nuestra propuesta de valor **“dinamizando la seguridad ciudadana”**

Antonio Escamilla Recio –Presidente de AES FUNDACIÓN.



Esta guía es el resultado del trabajo colaborativo desarrollado en el Área de Trabajo de Ingeniería instalación y mantenimiento de AES, fruto del esfuerzo conjunto de profesionales de distintas empresas asociadas que hemos trabajado de forma coordinada con un objetivo común: aportar al sector un documento de referencia práctico, riguroso y alineado con las mejores prácticas.

A lo largo de este documento abordamos el ciclo completo de un proyecto de seguridad electrónica, desde el análisis y la evaluación de riesgos hasta el diseño, la implementación, la operación y la mejora continua de los sistemas, incorporando aspectos clave como la integración tecnológica, la ciberseguridad y el cumplimiento normativo.

Desde AES queremos agradecer la implicación, dedicación y generosidad de todos los compañeros que han participado en la elaboración de esta guía. Confiamos en que este trabajo contribuya a reforzar el conocimiento compartido y sirva de apoyo a los profesionales y organizaciones que afrontan proyectos de seguridad electrónica.

Juan De La Fuente Sánchez

Co-coordinador del área de ingeniería, instalación y mantenimiento de AES





## 1.1. Propósito de la guía

La presente **Guía de Desarrollo e Implementación de Proyectos de Instalación de Sistemas Electrónicos de Seguridad** tiene por objeto proporcionar un marco técnico, metodológico y normativo que permita diseñar, ejecutar y mantener proyectos de seguridad privada con un alto nivel de calidad, trazabilidad y cumplimiento regulatorio.

Su finalidad principal es **homogeneizar criterios y buenas prácticas** en el ámbito de los sistemas electrónicos de seguridad contra intrusión, robo, atraco y protección de personas y bienes, facilitando que los proyectos se desarrollen:

- ➡ De forma **alineada con la Ley 5/2014, de 4 de abril, de Seguridad Privada**, su Reglamento vigente y las Órdenes Ministeriales de desarrollo (especialmente INT/314/2011 e INT/316/2011).
- ➡ Conforme a las **Normas UNE y UNE-EN aplicables** (entre otras, UNE-EN 50130, 50131, 50132, 50133, 50136, UNE CLC/TS 50398 y UNE-CLC/TS 50131-7), en lo relativo al diseño, instalación y funcionamiento de los sistemas de alarma.
- ➡ Integrando las **buenas prácticas de la dirección de proyectos** recogidas en los estándares del Project Management Institute (PMI), con especial énfasis en la gestión del alcance, cronograma, costes, calidad, riesgos y stakeholders.

Esta guía pretende ser una herramienta de referencia para la **planificación, diseño, implantación, operación y mejora continua** de sistemas de seguridad, con un enfoque orientado a la reducción de falsas alarmas, la mejora de la eficacia operativa y la adecuada coordinación entre titulares, empresas de seguridad e instituciones competentes.

## 1.2. Alcance y público objetivo

El alcance de la guía abarca el **ciclo de vida completo** de un proyecto de instalación de sistemas electrónicos de seguridad, desde la conceptualización y el análisis de requisitos hasta la operación y mantenimiento post-implantación, incluyendo:

- 🎯 **Sistemas de intrusión y alarma contra robo/atraco**, con o sin conexión a Central Receptora de Alarmas (CRA) o centro de control.
- 🎯 **Sistemas de videovigilancia (CCTV)** y soluciones de grabación, analítica de vídeo y gestión de imágenes.
- 🎯 **Sistemas de control de accesos**, físicos y lógicos, orientados a la protección de personas, activos e infraestructuras.
- 🎯 Sistemas complementarios de **interfonía, señalización, integración y gestión centralizada** de la seguridad.

La guía se centra en proyectos desarrollados en el marco de la **seguridad privada en España**, particularmente en instalaciones en las que la normativa exige el cumplimiento de determinados grados de seguridad o la conexión a CRA, sin perjuicio de su aplicabilidad a otros entornos y sectores de actividad.

El **público objetivo** de este documento incluye, entre otros:

- 👤 **Directores e Ingenieros de Seguridad**, tanto internos del cliente como pertenecientes a empresas de seguridad.
- 👤 **Gestores de proyecto (Project Managers)** responsables de la planificación y ejecución de soluciones de seguridad.
- 👤 **Responsables técnicos y jefes de obra** de empresas instaladoras y mantenedoras de sistemas electrónicos de seguridad.
- 👤 **Responsables de Centros de Control y Centrales Receptoras de Alarmas (CRA).**
- 👤 **Responsables de Seguridad Corporativa, IT/OT y Cumplimiento Normativo** de organizaciones usuarias de sistemas de seguridad.
- 👤 **Técnicos, auditores y consultores especializados en seguridad física, electrónica, ciberseguridad y protección de datos** vinculados a sistemas de videovigilancia y control de accesos.

La guía no sustituye a la normativa de aplicación, sino que la **complementa y operacionaliza** mediante criterios técnicos, recomendaciones y ejemplos de aplicación práctica, proporcionando una referencia común para todos los actores implicados en el proyecto.

## 1.3. Principios rectores: cumplimiento normativo y buenas prácticas

El diseño y la implementación de proyectos de instalación de sistemas electrónicos de seguridad deben regirse por un conjunto de **principios rectores** que garanticen la coherencia técnica, el cumplimiento legal y la eficacia operativa de las soluciones implementadas. Entre ellos, destacan:

### 1. Cumplimiento normativo integral

- Observancia estricta de la **Ley de Seguridad Privada**, su Reglamento y las Órdenes Ministeriales que regulan el material, la instalación, el funcionamiento de los sistemas de alarma y su conexión a CRA.
- Adecuación de los equipos y sistemas a las **Normas UNE/UNE-EN aplicables**, asegurando que el material esté homologado y certificado por organismos de control acreditados.
- Cumplimiento de la **normativa de protección de datos (RGPD y LOPDGDD)** y de las instrucciones específicas de la AEPD en materia de videovigilancia, especialmente respecto al tratamiento y conservación de imágenes.

### 2. Enfoque basado en el riesgo

- Dimensionamiento de los sistemas en función de los **riesgos y amenazas identificados** en el entorno operativo, evitando tanto el sobredimensionamiento innecesario como la infra-protección de activos.
- Asignación del **grado de seguridad** adecuado de acuerdo con la naturaleza del establecimiento (Grado 2, 3 o 4, según proceda) y las exigencias normativas.

### 3. Gestión profesional del proyecto

- Aplicación de metodologías de **gestión de proyectos estructurada** (inspiradas en los estándares PMI), con una clara definición del alcance, una EDT orientada a subsistemas y actividades, cronograma, presupuesto y planes de gestión (calidad, riesgos, comunicaciones, PRL, etc.).
- Definición de **responsabilidades y roles** (cliente, director de seguridad, ingeniero de seguridad, empresa instaladora, CRA, etc.) y establecimiento de mecanismos de seguimiento y control del proyecto.

#### 4. Calidad técnica, interoperabilidad y mantenibilidad

- Selección de soluciones tecnológicas que garanticen **fiabilidad, disponibilidad y facilidad de mantenimiento**, así como la **interoperabilidad** entre subsistemas (CCTV, intrusión, control de accesos, etc.).
- Documentación completa y actualizada del sistema (planos “s-built” configuraciones, manuales, protocolos de prueba y mantenimiento), facilitando auditorías y futuras ampliaciones o integraciones.

#### 5. Seguridad integral: física, lógica y de la información

- Consideración de la seguridad electrónica como parte de un **modelo de seguridad integral**, coordinado con la seguridad física, la ciberseguridad de redes y dispositivos, y la protección de la información.
- Adopción de medidas técnicas y organizativas que mitiguen riesgos de **ciberataques a sistemas de seguridad**, especialmente en infraestructuras conectadas a redes IP y sistemas remotos.

#### 6. Eficiencia operativa y reducción de falsas alarmas

- Diseño de sistemas y procedimientos que **minimicen la generación de falsas alarmas**, de acuerdo con las recomendaciones técnicas de las normas UNE-CLC/TS aplicables.
- Establecimiento de **protocolos claros de verificación y actuación**, consensuados entre el titular, la empresa de seguridad y la CRA.

#### 7. Mejora continua y ciclo de vida

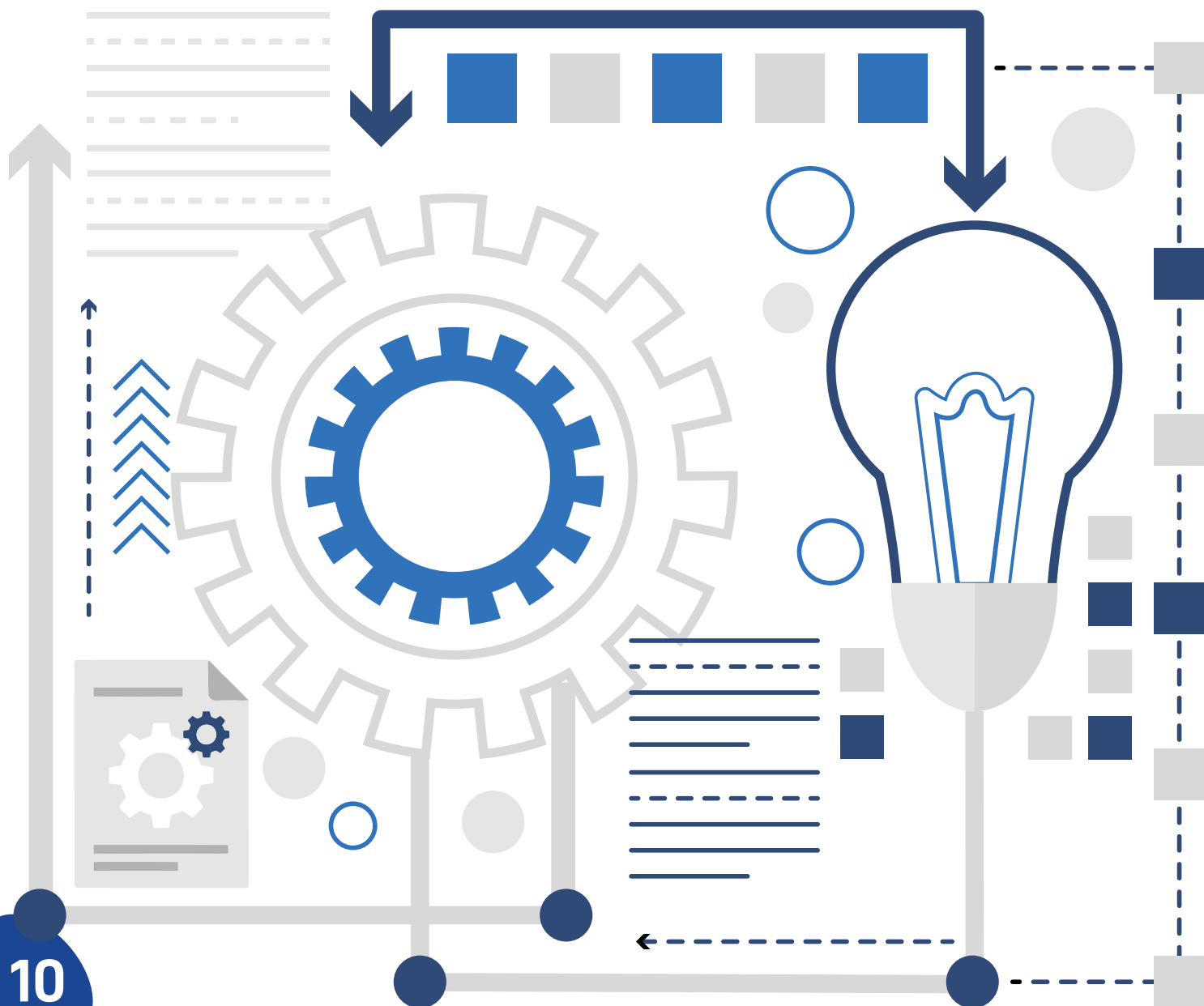
- Consideración del sistema de seguridad como un **activo vivo**, que debe ser revisado, actualizado y mejorado a lo largo de su ciclo de vida para adaptarse a cambios en el riesgo, en la normativa o en la tecnología disponible.
- Definición de **indicadores (KPI/SLAs)** que permitan medir el desempeño del sistema y de los servicios de seguridad, favoreciendo la mejora continua.

La base de cualquier proyecto de seguridad electrónica es la integración de hardware y software bajo estándares que garanticen la operatividad continua.

Contexto: Se sitúa en la necesidad de proteger activos críticos (físicos y digitales) mediante el uso de dispositivos interconectados.

Requisitos Clave:

-  **Control de Accesos:** Gestión de entradas y salidas de personal autorizado.
-  **Integridad y Disponibilidad:** El sistema debe funcionar bajo todas las circunstancias establecidas y proteger la información generada (Triada CIA: Confidencialidad, Integridad y Disponibilidad).
-  **Cumplimiento Normativo:** Adherencia a normas como la UNE EN 50131-1, que regula los grados de seguridad y la calidad de los equipos.



## 2.1. Descripción del entorno operativo y riesgos del sector

El entorno operativo define dónde y cómo se despliegan los sistemas, enfrentando desafíos tanto físicos como cibernéticos.

- ⚙️ **Riesgos Físicos:** Intrusión, sabotaje de sensores, manipulación de fuentes de alimentación o daños por eventos externos.
- ⚙️ **Riesgos del Sector (Ciberseguridad):** Ataques contra la red de comunicaciones, denegación de servicio (DDoS), inyección de comandos en sistemas de control y ransomware.
- ⚙️ **Análisis de Riesgos:** Es el primer paso esencial para identificar activos y amenazas antes del despliegue.

## 2.2. Objetivos, restricciones y criterios de éxito

Un proyecto exitoso debe equilibrar la protección con la viabilidad técnica y económica.

**Objetivos:** Prevenir y proteger contra incidentes, garantizar la vigilancia 24/7 y reducir los tiempos de respuesta ante emergencias.

**Restricciones:**

- ⌚ Presupuesto: Limitaciones financieras para la adquisición de equipos.
- ⌚ Tiempo: Plazos de instalación y configuración.
- ⌚ Técnicas: Alcance de la red y compatibilidad tecnológica.

**Criterios de Éxito:** Se miden a través de la fiabilidad, disponibilidad y mantenibilidad (RAMS) del sistema, además del cumplimiento total de la normativa vigente.

## 2.3. Partes interesadas y roles (cliente, director/ingeniero de seguridad, instalador, central receptora)

La coordinación entre estos actores es vital para la eficacia del sistema.

- 👤 **Cliente:** Define el alcance, aprueba el presupuesto y es el propietario de los riesgos residuales.
- 👤 **Director/Ingeniero de Seguridad:** responsable del diseño técnico, la evaluación de riesgos y la supervisión del cumplimiento de políticas.
- 👤 **Instalador:** Encargado del montaje físico de equipos (sensores, paneles, cámaras) y su configuración inicial bajo estándares de calidad.
- 👤 **Central Receptora de Alarmas (CRA):** Entidad externa que monitorea las señales del sistema 24/7, verifica eventos y gestiona el aviso a las autoridades si es necesario.



### 3.1. Ley de Seguridad Privada, Reglamento y Órdenes Ministeriales.

El actual marco normativo en materia de seguridad privada reserva un apartado expreso a los aspectos que deben tenerse en cuenta a la hora de realizar la instalación de un sistema de seguridad contra atraco e intrusión. Estos aspectos se recogen fundamentalmente en el documento denominado Proyecto de Instalación, mencionado por primera vez en el Reglamento de Seguridad Privada aprobado por el RD 2364/1994 de 9 de diciembre.

Así pues, este Reglamento de Seguridad Privada junto con la actual Ley 5/2014, de 4 de abril, de Seguridad Privada, las Órdenes Ministeriales 314/2011 y 316/2011, y las Normas UNE y UNE\_EN a las que se hacen referencia en la citada regulación, establecen un completo marco normativo aplicable al Proyecto de Instalación.

Por un lado, debemos tener en cuenta que los dispositivos y sistemas empleados deben estar homologados y certificados al objeto de cumplir las normas técnicas aplicables según el artículo 40 del Reglamento de SP en relación con el artículo 22 de la Orden 314/INT/2011, de 1 de febrero, sobre empresas de seguridad privada.

Reglamento de Seguridad Privada:

**“Artículo 40. Aprobación de material**

*1. Los medios materiales y técnicos, aparatos de alarma y dispositivos de seguridad que instalen y utilicen estas empresas, habrán de encontrarse debidamente aprobados con arreglo a las normas que se establezcan, impidiendo que los sistemas de seguridad instalados causen daños o molestias a terceros. [...]”*

Orden INT/314/2011:

**Artículo 22. Material de instalaciones.**

*1. Los elementos que componen los sistemas de seguridad, de acuerdo con el apartado primero del artículo 40 del Reglamento de Seguridad Privada, deberán estar aprobados conforme a las Normas europeas UNE-EN 50130, 50131, 50132, 50133, 50136 y Norma UNE CLC/TS 50398, o aquellas Normas llamadas a reemplazar a las citadas, según sean de aplicación a los diferentes tipos de sistemas*

En este sentido, los artículos 23 y 24 de la citada Orden 314/INT/2011, establecen los requisitos de la normativa sobre la homologación de los sistemas de seguridad y las características que deben reunir.

**“Artículo 23. Homologación de sistemas de seguridad.**

*A los efectos de la normativa reguladora de la seguridad privada, se entenderá por sistema de seguridad el conjunto de aparatos o dispositivos electrónicos contra robo e intrusión o para la protección de personas y bienes, cuya activación sea susceptible de producir la intervención policial, independientemente de que esté o no conectado a una central de alarmas o centros de control.*

*Se considerará que forma parte de la instalación de un sistema de seguridad, todo aquello que complemente a estos dispositivos, automática, material o procedimentalmente, incluyendo controles de acceso y sistemas de video vigilancia. Cuando la instalación se conecte a central de alarmas, deberá ajustarse a lo dispuesto en los artículos 40, 42 y 43 del Reglamento de Seguridad Privada, considerándose homologados si reúnen las características determinadas en los artículos 22 y 24 de la presente Orden.*

**Artículo 24. Características de los sistemas de seguridad.**

*Los sistemas de alarma que se pretendan conectar con una central de alarmas habrán de reunir las siguientes características:*

- a) Disponer del número suficiente de elementos de protección que permitan a la central diferenciar las señales producidas por una intrusión o ataque de las originadas por otras causas.*
- b) Contar con tecnología que permita acceder desde la central de alarmas bidireccionalmente a los sistemas conectados a ella, para posibilitar la identificación y tratamiento singularizado de las señales correspondientes a las distintas zonas o elementos que componen el sistema, así como el conocimiento del estado de alerta o desconexión de cada una de ellas, y la desactivación de las campanas acústicas.”*

Por otro lado, la Orden INT/316/2011, de 1 de febrero, sobre funcionamiento de los sistemas de alarma en el ámbito de la seguridad privada, recoge en su artículo 3 que cualquier elemento o dispositivo que forme parte de un sistema de alarma de los recogidos por la normativa de seguridad privada, deberá cumplir, como mínimo, el grado y características establecidas en las Normas UNE-EN 50130, 50131, 50132, 50133, 50136 y en la Norma UNE CLC/TS 50398, o en aquellas otras llamadas a reemplazar a las citadas Normas, aplicables en cada caso y que estén en vigor.

El citado artículo 3 continúa estableciendo que los productos deberán estar fabricados con arreglo a las Normas UNE o UNE-EN anteriormente mencionadas y contar con la evaluación de la conformidad de Organismos de Control acreditados, por las Entidades de Acreditación autorizadas en cada uno de los países de la Unión Europea, de acuerdo con la Norma EN 45.011.

La Orden INT/316/2011, con el fin de conseguir sistemas de seguridad que generen el mínimo de falsas alarmas, establece que el proyecto de instalación al que se hace referencia en el artículo 42 del Reglamento de Seguridad Privada, deberá elaborarse conforme a lo establecido en la Norma UNE-CLC/TS 50131-7.

Así mismo, el certificado obligatorio de instalación al que hace referencia el citado artículo 42, deberá garantizar que el proyecto está realizado de conformidad con la Norma UNE antes expresada y cumple con las finalidades previstas en el ya mencionado artículo.

Por último, debemos hacer referencia nuevamente a la Orden INT/316/2011, que recoge los Grados de Seguridad de los sistemas de alarma, y ello basándose en la Norma UNE-EN 50131-1. Esta norma establece cuatro grados de seguridad en función del riesgo, quedando en esta Orden asignados, además, en virtud de la naturaleza y características del lugar en el que se va a efectuar la instalación y de la obligación, o no, de estar conectados a una central de alarmas o centro de control.

-  **Grado 1:** sistemas sin conexión a Central de Alarmas.
-  **Grado 2:** viviendas y pequeños comercios.
-  **Grado 3:** establecimientos obligados (bancos, joyerías, salas de juego....
-  **Grado 4:** infraestructuras críticas y alto riesgo.

### 3.2. El Proyecto de Instalación según la Norma UNE-CLC/TS 50131-7.

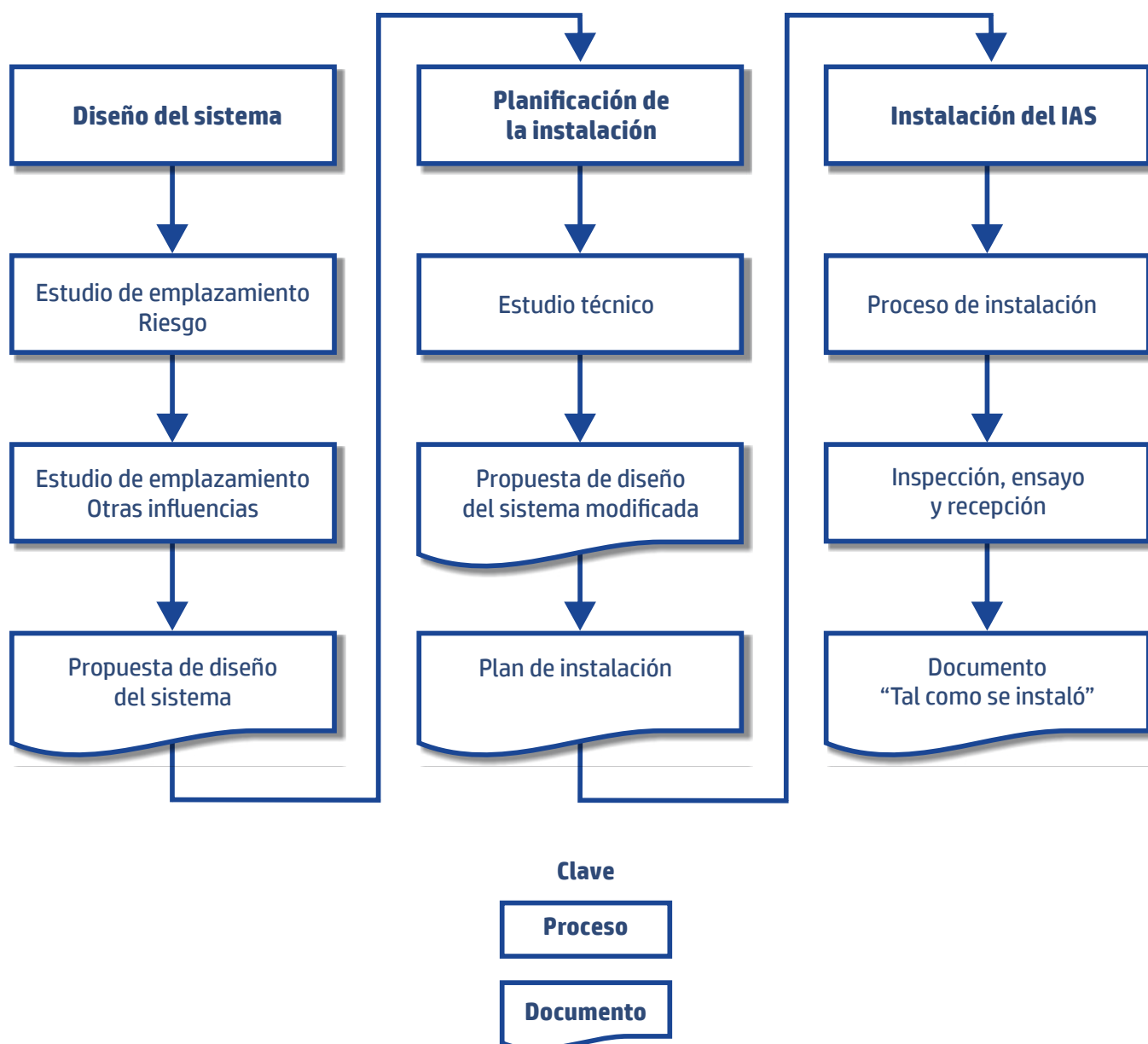
Esta norma establece una guía de aplicación que pretende proporcionar consejos relativos al diseño, instalación, funcionamiento y mantenimiento de los sistemas de alarma de intrusión. La finalidad es garantizar que los sistemas de seguridad generen el menor número posible de alarmas falsas.

Esta guía básicamente describe los procesos a tener en cuenta antes de la instalación, durante la misma y después de ella, estableciendo momentos clave como son:

-  El Diseño del Sistema.
-  La Planificación de la Instalación.
-  La Instalación del Sistema.
-  Comprobación Funcionamiento del sistema instalado.
-  Documentación.

## Diagrama de Flujo de los Procesos establecidos en la Norma UNE-CLC/TS 50131-7.

El diagrama de flujo de debajo describe los principales procesos incluidos en la guía de aplicación. Aunque los procesos se muestran individualmente en el diagrama de flujo, en la práctica se pueden efectuar algunos de los procesos simultáneamente. También se muestra la documentación que surge de cada proceso.





### 3.3. Conexión a Central de Alarmas, Mantenimientos y Revisiones, y Procedimientos de Verificación de Alarmas.

#### Conexión a Central de Alarmas.

Una vez realizada la instalación y las comprobaciones necesarias, se debe tener en cuenta que el proyecto de instalación deberá validarse y firmarse por un Ingeniero acreditado de la Empresa de Seguridad Instaladora, haciéndose entrega de una copia al titular de la instalación.

Así mismo, el certificado de Instalación y el certificado de conexión a Central de Alarmas deberán acreditar que se han realizado las comprobaciones necesarias que justifiquen el correcto funcionamiento del sistema y la correcta conexión con la Central de Alarmas. Este certificado podría elaborarse en un único documento si la empresa instaladora y la prestadora de los servicios de conexión a CRA coinciden.

#### Revisiones y Mantenimientos.

Cuando los sistemas de alarma se conectan a una Central de Alarmas, la regulación establece la obligación, para aquellas empresas de seguridad instaladoras y mantenedoras de dichos sistemas, de realizar revisiones preventivas con la periodicidad requerida, y además, acometer los mantenimientos necesarios para garantizar el correcto funcionamiento del sistema en todo momento.

##### **Artículo 43. Revisiones**

- 1. Los contratos de instalación de aparatos, dispositivos y sistemas de seguridad, en los supuestos en que la instalación sea obligatoria o cuando se conecten con una central de alarmas, comprenderán el mantenimiento de la instalación en estado operativo, con revisiones preventivas cada trimestre, no debiendo, en ningún caso, transcurrir más de cuatro meses entre dos revisiones sucesivas. En el momento de suscribir el contrato de instalación o en otro posterior, la entidad titular de la instalación podrá, sin embargo, asumir por sí misma o contratar el servicio de mantenimiento y la realización de revisiones trimestrales con otra empresa de seguridad.*
- 2. Cuando las instalaciones permitan la comprobación del estado y del funcionamiento de cada uno de los elementos del sistema desde la central de alarmas, las revisiones preventivas tendrán una periodicidad anual, no pudiendo transcurrir más de catorce meses entre dos sucesivas.*
- 3. Las revisiones preventivas podrán ser realizadas directamente por las entidades titulares de las instalaciones, cuando dispongan del personal con la cualificación requerida, y de los medios técnicos necesarios.*
- 4. Las empresas de seguridad dedicadas a esta actividad y las titulares de las instalaciones llevarán libros-registros de revisiones, cuyos modelos se ajusten a las normas que se aprueben por el Ministerio de Justicia e Interior, de forma que sea posible su tratamiento y archivo mecanizado e informatizado.*

5. En el libro de la empresa de seguridad se anotará el número del contrato y fecha de revisión, técnico de la empresa que la realiza, nombre, apellidos o razón social de la empresa cliente, su domicilio, deficiencias observadas y fecha de subsanación. En el libro-catálogo de la empresa cliente deberá constar el nombre de la empresa de seguridad, el número del contrato, las fechas de las revisiones, el técnico que las realiza, las deficiencias observadas, la fecha de subsanación y la firma del técnico, así como los restantes datos que se determinen en el correspondiente modelo.

#### **Artículo 44. Averías**

Para el adecuado cumplimiento de lo dispuesto en el artículo anterior, las empresas de instalación y mantenimiento deberán disponer del servicio técnico adecuado que permita atender debidamente las averías de los sistemas de seguridad de cuyo mantenimiento se hayan responsabilizado, incluso en días festivos, en el plazo de veinticuatro horas siguientes al momento en que hayan sido requeridas al efecto. De las características de este servicio y de sus modificaciones, las empresas informarán oportunamente a la Dirección General de la Policía.

Hay que recordar que las condiciones del mantenimiento y el modo en el que se va a realizar por la empresa de seguridad deberán quedar descritos en el Proyecto de Instalación.

Por último, hay que mencionar que todas las revisiones que se realicen en los sistemas de seguridad conectados a una Central de Alarmas deberán registrarse en los correspondientes Libros Registros que las empresas y usuarios se encuentran obligados a llevar.



## Procesos de Verificación de Señales de Alarma.

Cuando se produzca una alarma, las centrales deberán proceder de inmediato a su verificación, utilizando, para que ésta sea considerada válida, todos o algunos de los procedimientos técnicos o humanos establecidos en la Orden INT/316/2011, comunicando seguidamente, al servicio policial correspondiente, las alarmas reales producidas. (*Artículo 6 de la citada Orden*)

### ● Procedimientos de Verificación:

- |                                                                 |                                                                                    |
|-----------------------------------------------------------------|------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> Verificación Secuencial     | <input checked="" type="checkbox"/> Verificación personal                          |
| <input checked="" type="checkbox"/> Verificación mediante video | <input checked="" type="checkbox"/> Actuaciones complementarias a la verificación. |
| <input checked="" type="checkbox"/> Verificación mediante audio |                                                                                    |

Las alarmas verificadas por uno o varios de los procedimientos anteriormente establecidos tendrán la consideración de alarmas confirmadas, entendiéndose cumplida, en estos casos, la obligación que el apartado segundo del artículo 48 del Reglamento de Seguridad Privada impone a las centrales de alarmas.

Igualmente recordar en este punto, que el documento del Proyecto de Instalación deberá contemplar los procedimientos de verificación acordados con el titular del contrato de servicios de seguridad.

## 3.4. Protección de Datos (RGDP / LOPDGDD) y conservación de imágenes.

La videovigilancia se considera tratamiento de datos personales, ya que las imágenes permiten identificar personas.

### Obligaciones según RGPD y LOPDGDD

La captación y tratamiento de imágenes debe cumplir:

- |                                                                            |                                                      |
|----------------------------------------------------------------------------|------------------------------------------------------|
| ● legitimación adecuada (interés legítimo, obligación legal, art. 6 RGPD), | ● registro de actividades de tratamiento,            |
| ● proporcionalidad en la captación,                                        | ● medidas de seguridad y análisis de riesgos,        |
| ● limitación de finalidad,                                                 | ● evaluación de impacto cuando sea necesario (EIPD). |

También aplica la **Instrucción 1/2006 de la AEPD**, que regula específicamente el tratamiento de imágenes con fines de vigilancia.

### Conservación de imágenes

El límite general de conservación es de 30 días desde su captación, salvo si deben conservarse por una investigación policial o judicial (delito, infracción o incidencia).

Se recomienda la generación de copias de respaldo semanales si hay actualización de datos, conforme al Reglamento de la LOPD.

## 4 Ciclo de vida



El ciclo de vida del proyecto constituye el marco metodológico que permite planificar, ejecutar y controlar de forma ordenada un proyecto de seguridad electrónica, garantizando su alineación con los objetivos del cliente, el cumplimiento normativo y la calidad técnica de la solución implantada.

Este enfoque, alineado con las buenas prácticas de gestión de proyectos y adaptado a la realidad del sector de la seguridad privada en España, facilita la toma de decisiones, la gestión de riesgos y la coordinación entre todos los agentes implicados

### 4.1. Inicio

La fase de inicio tiene como objetivo definir formalmente el proyecto, justificar su necesidad y establecer las bases organizativas y estratégicas para su correcta ejecución.

#### 4.1.1. Acta de constitución y caso de negocio

El Acta de Constitución del Proyecto es el documento que autoriza formalmente el inicio del proyecto y otorga al director del proyecto la autoridad necesaria para planificar y coordinar los trabajos. En el contexto de la seguridad electrónica, este documento debe reflejar de manera clara el propósito del proyecto, su alcance inicial y las condiciones bajo las cuales se desarrollará.

El acta debe incluir, entre otros aspectos, la descripción del problema o necesidad de seguridad detectada, los objetivos generales y específicos del proyecto, los criterios de éxito, las principales restricciones de plazo, coste y normativa, así como los riesgos de alto nivel identificados en esta fase inicial.

El caso de negocio complementa al acta de constitución y analiza la viabilidad del proyecto desde un punto de vista técnico, económico y operativo. Debe justificar la inversión propuesta, evaluar alternativas tecnológicas y considerar los beneficios esperados, tales como la reducción de riesgos, el cumplimiento legal, la mejora operativa o la protección de activos críticos.

### 4.1.2. Identificación de interesados y estrategia de implementación

La identificación y análisis de los interesados resulta especialmente relevante en proyectos de seguridad electrónica, debido a la diversidad de perfiles involucrados. Entre ellos se encuentran el cliente final, los usuarios operativos, los responsables de seguridad, los departamentos de IT, los integradores, instaladores, fabricantes y, en su caso, organismos reguladores o auditores.

Para cada interesado se recomienda evaluar su nivel de influencia, expectativas y necesidades de información, definiendo una estrategia de comunicación adecuada. Una gestión proactiva de los interesados contribuye a minimizar conflictos, facilitar la toma de decisiones y asegurar la aceptación final del sistema.

La estrategia de implementación debe definir el enfoque general del despliegue, contemplando aspectos como la ejecución por fases, la coexistencia con sistemas existentes, la realización de pruebas piloto o la implantación progresiva por áreas o edificios, siempre con el objetivo de minimizar el impacto en la operativa del cliente.

## 4.2. Planificación

La fase de planificación transforma los objetivos definidos en el inicio en un conjunto de planes detallados que servirán de referencia durante la ejecución y el control del proyecto.

### 4.2.1. Alcance y EDT (incluyendo paquetes técnicos por subsistema: CCTV, intrusión, control de accesos, interfonía)

La definición del alcance establece claramente los límites del proyecto, especificando qué sistemas, funcionalidades y servicios están incluidos, así como aquellos que quedan expresamente excluidos. Esta definición resulta clave para evitar desviaciones y conflictos durante la ejecución.

La Estructura de Desglose del Trabajo descompone el proyecto en paquetes de trabajo gestionables. En proyectos de seguridad electrónica se recomienda una descomposición por subsistemas técnicos, incluyendo, al menos, CCTV, sistemas de intrusión, control de accesos e interfonía, así como las actividades transversales de integración, pruebas, documentación y formación.

Cada paquete de trabajo debe contar con un responsable asignado, criterios de aceptación claramente definidos y una identificación de dependencias con otros paquetes.

### 4.2.2. Diseño técnico y especificaciones (estudio de emplazamiento, selección de recursos, canalizaciones y disponibilidad)

El diseño técnico debe basarse en un estudio detallado del emplazamiento, analizando las características físicas del entorno, los riesgos existentes, las condiciones ambientales y la infraestructura disponible. Este análisis permite seleccionar las tecnologías y equipos más adecuados para cada subsistema.

El diseño debe incluir especificaciones técnicas detalladas, esquemas de instalación, necesidades de canalización y requisitos de disponibilidad, redundancia y escalabilidad. Asimismo, debe garantizar el cumplimiento de la normativa vigente y de las recomendaciones de fabricantes y estándares del sector.

### 4.2.3. Cronograma (Gantt), recursos, adquisiciones y presupuesto

El cronograma del proyecto, habitualmente representado mediante un diagrama de Gantt, debe reflejar la secuencia lógica de actividades, los hitos principales y las dependencias entre tareas y subsistemas. Un cronograma realista facilita la coordinación de equipos y la gestión de expectativas del cliente.

La planificación de recursos debe contemplar tanto los recursos humanos como los materiales necesarios, asegurando su disponibilidad en el momento adecuado. El plan de adquisiciones define qué elementos deben ser suministrados por terceros, los plazos de entrega y las condiciones de garantía y soporte.

El presupuesto consolida todos los costes asociados al proyecto, incluyendo suministros, mano de obra, ingeniería, gestión y contingencias, proporcionando una visión clara del coste total del proyecto.



#### 4.2.4. Planes de gestión: PRL, calidad, comunicaciones, riesgos, seguridad/ciberseguridad y compliance

La planificación del proyecto debe complementarse con planes específicos que regulen su gestión. El plan de calidad establece los criterios de aceptación y los procedimientos de verificación. El plan de comunicaciones define los flujos de información entre los interesados. El plan de riesgos identifica y evalúa los riesgos técnicos, operativos y logísticos, estableciendo medidas de mitigación.

Asimismo, resulta imprescindible disponer de un plan de seguridad y ciberseguridad que contemple la protección de los sistemas y la información, especialmente en entornos IP, así como un plan de compliance que garantice el cumplimiento de la normativa legal, sectorial y contractual aplicable.

##### PRL

Durante la ejecución del proyecto se debe llevar a cabo un efectivo Control Preventivo de la prestación de los servicios, con el mayor nivel de Seguridad y protección de la salud de todos los trabajadores involucrados en la actividad

Los mecanismos de control irán encaminados al cumplimiento de la normativa vigente relativa a la Coordinación de Actividades Empresariales y Gestión Preventiva de las Obras, recopilando y haciendo llegar a los trabajadores la información de riesgos, medidas preventivas y medidas de emergencia necesaria para realizar los trabajos en condiciones de Seguridad y Salud.

##### REALIZACIÓN

A la hora de llevar a cabo el control preventivo de la prestación de los servicios nos podemos encontrar con 2 situaciones diferentes:

##### Trabajos que se realizan en instalaciones del CLIENTE

CASO A: No considerados Obra de Construcción.

CASO B: Considerados Obra de Construcción.



## COORDINACIÓN Y GESTIÓN DE OBRAS

### ¿Qué trabajos se consideran Obra de Construcción?

La definición legal de “Obra de Construcción” que recoge el RD 1627/1997. Siempre se deberá consultar con el Cliente si los trabajos contratados se encuentran englobados en una Obra de Construcción.

A continuación, se detalla el procedimiento a seguir para cada uno de los casos de Coordinación identificados.

#### CASO A: Proyectos no considerados “Obra de Construcción” que se realizan en instalaciones de los Clientes

El control preventivo se debería iniciar con la firma del Contrato. Será en el momento de la firma del Contrato cuando se realice el intercambio de información preventiva con el Cliente y se firme la Carta de Coordinación como evidencia de dicho intercambio.

Mediante la Coordinación y el intercambio de información, se informa a los clientes de los riesgos propios de la actividad contratada que introduce en sus instalaciones, y de las medidas preventivas que se deben adoptar para la realización de los trabajos.

A su vez, la información preventiva que haya sido facilitada por el Cliente se pone a disposición de todos aquellos trabajadores, tanto propios como subcontractados, que vayan a realizar trabajos en las instalaciones del Cliente. Con la entrega de dicha documentación se informa a los trabajadores de los riesgos, medidas preventivas y medidas de emergencia propios de las instalaciones del Cliente.

Debe existir un responsable encargado de hacer llegar la información preventiva al personal técnico, ya sea propio o subcontractado, siendo también el responsable de vigilar el cumplimiento de las medidas preventivas, y de dar aviso al Servicio de Prevención de cualquier circunstancia que pudiera suponer un riesgo para los trabajadores.

A parte de la Información de Riesgos y Medidas Preventivas propios de la actividad contratada, se debería aportar al Cliente toda aquella documentación requerida para dar cumplimiento a sus procedimientos internos de Coordinación.

La entrega de documentación siempre estará sujeta al cumplimiento de normativa vigente y, en caso de requerirse, se podrá poner a disposición del Cliente entre otros los siguientes documentos:

- ◆ Certificados de Formación e Información
- ◆ Recibís de Equipos de Protección Individual (EPI)
- ◆ Autorización de Trabajadores para Manejo de Equipos de Trabajo
- ◆ Autorización de Trabajadores para Trabajo con Baja Tensión
- ◆ Formatos de Coordinación propios del Cliente

#### CASO B: Proyectos considerados Obra de Construcción que se realizan en instalaciones de los Clientes

Tal y como se ha comentado anteriormente, para saber si los trabajos contratados se encuentran englobados o no en una Obra de Construcción se deberá consultar con el Cliente. El hecho de que los trabajos sean Obra de Construcción o no puede condicionar en gran medida el cumplimiento de plazos de la Instalación, por lo que cuanto antes se disponga de dicha información mejor será para la marcha del proyecto.

Se recomienda por tanto que dicho aspecto sea tratado en la fase comercial para poder trasladar la información al inicio de la planificación e inicio de los trabajos.

En aquellos Proyectos considerados “Obras de Construcción” se deberá cumplir con los requisitos normativos recogidos en el RD 1627/1997 relativo a Seguridad y Salud en Obras de Construcción.

Las gestiones preventivas en Obras de Construcción se deberán realizar siempre antes del inicio de los trabajos y se llevarán a cabo por el responsable de la Instalación en colaboración con el Servicio de Prevención

En el siguiente apartado se describen los requisitos a cumplir en función de la posición que ocupe la empresa instaladora en la cadena de subcontratación.

#### **Empresa instaladora es Contratista Principal: el Cliente es Promotor de la Obra**

El Promotor (Cliente) designa un Coordinador de Seguridad y Salud (CSS) para la vigilancia de las Condiciones de Seguridad en la Obra

La empresa instaladora solicita el Estudio de Seguridad y Salud (ESS) al Coordinador de Seguridad y Salud.

El Servicio de Prevención de la empresa instaladora elabora Plan de Seguridad y Salud (PSS) a partir del ESS y la información facilitada por responsable de la Instalación.

El CSS aprueba Plan de Seguridad y Salud de la Empresa Instaladora y emite Acta de Aprobación.

Para aquellos casos en los que los trabajos hayan sido considerados por el Cliente “Obra de Construcción” pero no exista un Proyecto, la empresa instaladora elaborará la documentación preventiva que el Coordinador de Seguridad y Salud designado requiera.

Con el Plan de Seguridad y Salud aprobado, la empresa Instaladora tramitará Apertura de Centro de Trabajo, Libro de Visitas y Libro de Subcontratación (en caso de contar con subcontrata).

El Plan de Seguridad, Acta de Aprobación, Apertura de Centro y Libro de Subcontratación deben estar siempre en Obra.

En caso de Subcontrata se deberá entregar copia del Plan de Seguridad y Salud a la Subcontrata para su revisión, adhesión y cumplimiento.

El responsable designado será el encargado de vigilar el cumplimiento de las medidas preventivas en Obra por parte de los trabajadores propios y/o subcontrata. Asimismo, se realizarán inspecciones Periódicas en Obra dirigidas a observar el cumplimiento de las normas de prevención de riesgos.

En función de la peligrosidad de los trabajos, de la concurrencia con otras empresas, o por petición del Cliente, la empresa Instaladora podrá designar Recurso Preventivo propio para vigilar el cumplimiento de los procedimientos de trabajos y medidas preventivas.

La Ley de Subcontratación permite un máximo 3 Niveles de Subcontratación.

**Empresa Instaladora es Subcontrata: el Cliente es Contratista Principal, Subcontrata Nivel 1 o Nivel 2 (No es Promotor)**

Habitualmente nos encontramos en este caso cuando la empresa Instaladora es contratada por una Constructora (Contratista Principal de la Obra)

El Promotor designa un Coordinador de Seguridad y Salud (CSS) para la vigilancia de las Condiciones de Seguridad en la Obra.

La Empresa Instaladora solicita al Cliente el Plan de Seguridad y Salud aprobado por el Coordinador de Seguridad y Salud para su revisión.

En caso de que el Plan de Seguridad tenga el visto bueno del Servicio de Prevención, se firma el Acta de Adhesión al mismo, comprometiéndose e al cumplimiento de todo aquello que nos sea de aplicación en el Plan de Seguridad y Salud.

La empresa Instaladora firma en el Libro de Subcontratación del Contratista Principal.

En caso de existir subcontrata, la subcontrata también deberá Adherirse al Plan de Seguridad y firmar en el Libro de Subcontratación del Contratista Principal.

El responsable designado de los trabajos será el encargado de vigilar el cumplimiento de las medidas preventivas en Obra por parte de los trabajadores propios y/o subcontrata. Asimismo, será el encargado de llevar a cabo Inspecciones Periódicas en Obra dirigidas a observar que los trabajos se realizan con un cumplimiento correcto de las normas de prevención de riesgos

- Con carácter general, en el momento de Homologación de las Subcontratas, se solicitará el Nombramiento de Recurso Preventivo de aquellos trabajadores de la Subcontrata que reúnan las aptitudes de experiencia y formación necesarias.
- La empresa instaladora puede ser Subcontrata de Nivel 1, 2 y 3. En función de la posición que se ocupe se podrá subcontratar o no.
- La Ley de Subcontratación permite un máximo 3 Niveles de Subcontratación.



### 4.3. Ejecución

La fase de ejecución comprende el conjunto de actividades destinadas a materializar el diseño técnico aprobado durante la planificación, llevando a cabo la instalación, configuración e integración de los sistemas electrónicos de seguridad previstos en el proyecto. Durante esta etapa se implementan físicamente los subsistemas (CCTV, intrusión, control de accesos, interfonía u otros), garantizando que su despliegue se realice conforme al diseño técnico, a la normativa aplicable y a los estándares de calidad definidos en el plan del proyecto.

La ejecución debe coordinar adecuadamente los recursos humanos, materiales y técnicos, asegurando el cumplimiento del cronograma, la gestión de riesgos operativos y la correcta comunicación entre las partes interesadas (cliente, director o ingeniero de seguridad, empresa instaladora y, cuando corresponda, la Central Receptora de Alarmas –CRA). Asimismo, se deben aplicar las medidas de prevención de riesgos laborales, seguridad operativa y control de calidad establecidas en los planes de gestión definidos en la fase de planificación.

Durante esta fase se desarrollan las siguientes actividades principales

#### 4.3.1. Replanteo, acopios e instalación física

Antes del inicio de la instalación se realiza el replanteo técnico en campo, que consiste en verificar sobre el terreno las ubicaciones previstas en el proyecto para los diferentes elementos del sistema (cámaras, detectores, lectores de control de accesos, paneles de intrusión, cableado, racks, etc.). Este proceso permite confirmar la viabilidad del diseño, detectar posibles interferencias con otras instalaciones y realizar los ajustes necesarios sin comprometer el cumplimiento del alcance del proyecto.

Una vez validado el replanteo, se procede al acopio y gestión de materiales, asegurando que todos los equipos y componentes cumplen las especificaciones técnicas definidas en el proyecto y las normas aplicables. Es fundamental verificar la integridad, compatibilidad y certificación de los dispositivos antes de su instalación.

La instalación física incluye, entre otras actividades:

- ☀ Tendido y canalización de cableado estructurado y alimentación eléctrica.
- ☀ Montaje de dispositivos de campo (cámaras, detectores, lectores, pulsadores, sirenas, etc.).
- ☀ Instalación de equipos centrales (grabadores, controladores, paneles de alarma, servidores, switches, racks).
- ☀ Integración de sistemas de alimentación ininterrumpida (SAI) y protecciones eléctricas.
- ☀ Etiquetado y ordenación del cableado conforme a buenas prácticas de instalación.

Todas las instalaciones deberán realizarse conforme a las normas UNE/UNE-EN aplicables, garantizando la fiabilidad, seguridad y mantenibilidad de la infraestructura.

### 4.3.2. Configuración, integración y pruebas de comisionado

Una vez completada la instalación física, se procede a la **configuración de los sistemas y dispositivos**, ajustando los parámetros operativos según los requisitos definidos en el diseño técnico.

Entre las principales tareas de configuración se incluyen:

- Parametrización de cámaras, grabadores y software de gestión de vídeo (VMS).
- Programación de zonas, detectores y particiones en sistemas de intrusión.
- Configuración de usuarios, credenciales y políticas de acceso en sistemas de control de accesos.
- Ajuste de comunicaciones, direccionamiento IP y protocolos de red.
- Configuración de alarmas, eventos y notificaciones.

Posteriormente se realiza la **integración de los diferentes subsistemas**, garantizando su interoperabilidad dentro de una plataforma común de gestión de seguridad o mediante interfaces de comunicación estandarizadas.

Las **pruebas de comisionado** tienen como objetivo verificar que el sistema funciona conforme a las especificaciones del proyecto. Estas pruebas pueden incluir:

- Verificación de funcionamiento individual de cada dispositivo.
- Pruebas de detección y generación de alarmas.
- Comprobación de la grabación y visualización de vídeo.
- Validación de la comunicación con la Central Receptora de Alarmas (CRA).
- Ensayos de redundancia, alimentación y recuperación ante fallos.

Los resultados de estas pruebas deben documentarse formalmente como parte del proceso de control de calidad del proyecto.

### 4.3.3. Formación a usuarios y traspaso operativo inicial

Una vez finalizada la instalación y las pruebas de funcionamiento, se procede a la **formación de los usuarios y operadores del sistema**, con el objetivo de garantizar una correcta utilización de las herramientas de seguridad implementadas.

La formación debe incluir, al menos:

- Uso del software de gestión de seguridad (monitorización, visualización de cámaras, gestión de alarmas).
- Procedimientos de actuación ante alarmas o incidencias.
- Gestión de usuarios y credenciales.
- Normas básicas de mantenimiento y buenas prácticas de operación.

Tras la formación, se realiza el **traspaso operativo inicial**, mediante el cual el sistema pasa a ser gestionado por el cliente o por el personal de seguridad designado. Este proceso suele incluir la entrega de manuales de usuario, configuraciones iniciales y documentación técnica necesaria para la operación del sistema.

La correcta ejecución de esta fase garantiza que el sistema instalado no solo funcione adecuadamente desde el punto de vista técnico, sino que también pueda ser operado de forma eficiente y segura por los responsables del servicio de seguridad.



#### 4.4. Monitoreo y Control

El monitoreo y control de proyectos es una fase crítica en la gestión de cualquier proyecto, sea del tipo que sea, por lo tanto, el monitoreo y control también es crítico a la hora de llevar a cabo un proyecto de implantación de un Sistema Electrónico de Seguridad. Un enfoque basado en estándares como puede ser el “ANSI/PMI 99-001-2021 Estándar para la Gestión de Proyectos” nos puede ayudar a que los objetivos del proyecto de instalación se cumplan en cuanto a alcance, tiempo, coste y calidad.

Para llevar a cabo el monitoreo y control de un proyecto es necesario implantar los siguientes procesos:

-  **Monitorear y Controlar el Trabajo del Proyecto:** Implica recopilar, medir y analizar datos de rendimiento para garantizar que el proyecto avance conforme al plan. Se utilizan herramientas como informes de progreso, reuniones de seguimiento y software de gestión de proyectos.
-  **Realizar el Control Integrado de Cambios:** Todo cambio en el alcance, cronograma o presupuesto debe ser evaluado y aprobado por el comité de control de cambios, documentando las razones y el impacto potencial.
-  **Validar el Alcance:** Se verifica que los entregables del sistema de seguridad, como sensores, cámaras y sistemas de control de acceso, cumplen con los requisitos establecidos y son aceptados por el cliente.
-  **Controlar el Alcance, Cronograma y Costes:** Se comparan los avances reales con el plan, identificando desviaciones y aplicando acciones correctivas cuando sea necesario.
-  **Controlar la Calidad:** Se realizan inspecciones y pruebas de funcionamiento de los componentes instalados para asegurarse de que cumplen con los estándares de calidad definidos.
-  **Controlar los Riesgos:** Se monitorizan los riesgos identificados, evaluando la efectividad de las respuestas y actualizando el registro de riesgos según evoluciona el proyecto.

##### Herramientas y Técnicas de Monitoreo y Control

-  **Indicadores de Rendimiento (KPIs):** Por ejemplo, porcentaje de avance en la instalación, número de incidencias reportadas y tiempo de respuesta ante fallos.
-  **Reuniones de Seguimiento:** Sesiones periódicas con el equipo para revisar el estado del proyecto, resolver problemas y coordinar acciones.
-  **Software de Gestión de Proyectos:** Herramientas o aplicaciones específicas que ayudan a registrar y visualizar el avance del proyecto.
-  **Auditorías y Revisiones Técnicas:** Evaluaciones externas o internas para asegurar la conformidad con los estándares y normativas.

Durante la fase de monitoreo y control, es fundamental mantener una documentación rigurosa. Esto incluye:

- Informes de avance semanal o mensual.
- Registro de incidencias y acciones correctivas.
- Actas de reuniones y decisiones tomadas.
- Actualización del plan de proyecto y cronograma

### 4.4.1. Seguimiento de cronograma y costes; control de cambios

El éxito de un proyecto depende en gran medida del seguimiento sistemático y preciso de su cronograma y de sus costes, así como de una gestión eficiente de los cambios. Estos procesos conforman el núcleo de la gestión de proyectos, pues permiten mantener la dirección y el control del mismo ante la complejidad y los retos que puedan surgir. Un seguimiento adecuado facilita la detección temprana de desviaciones, la toma de decisiones informadas y la aplicación de acciones correctivas que preserven los objetivos y recursos definidos en la planificación inicial.

Definiciones:

- 📄 **Cronograma:** Es el plan detallado que establece las actividades, la duración prevista, las dependencias y los hitos del proyecto. Permite visualizar cuándo deben realizarse cada tarea para alcanzar los objetivos del proyecto en el tiempo estipulado.
- 📄 **Costes:** Son los recursos financieros necesarios para ejecutar el proyecto, incluyendo gastos en personal, materiales, tecnología, servicios y cualquier otro elemento que implique desembolso económico.
- 📄 **Acción correctiva:** Es cualquier medida adoptada para ajustar el rumbo del proyecto y alinear la ejecución con los parámetros definidos en la planificación inicial, corrigiendo desviaciones detectadas.
- 📄 **Línea base:** Conjunto de planes originales y aprobados que sirven como referencia para medir y comparar el desempeño real del proyecto.
- 📄 **Desviación:** Diferencia entre lo planificado y lo ejecutado, ya sea en tiempo, coste o alcance.
- 📄 **Control de cambios:** Proceso formal para gestionar cualquier modificación al alcance, cronograma o presupuesto del proyecto, asegurando su documentación, evaluación y aprobación antes de implementarse.

### Seguimiento del Cronograma

El seguimiento del cronograma es el proceso que permite verificar el progreso de las actividades en relación con lo planificado. Este proceso implica la recopilación sistemática de datos sobre el avance real, la comparación con la línea base del cronograma y el análisis de cualquier desviación significativa. Herramientas y técnicas de seguimiento:

- ❑ Diagrama de Gantt: Representa gráficamente las actividades, sus duraciones y relaciones, facilitando la visualización del estado actual del proyecto y la identificación de tareas críticas. Un diagrama de Gantt es una herramienta visual donde cada actividad se muestra en una barra horizontal, indicando su duración y secuencia.
- ❑ Método del Camino Crítico (CPM): Permite identificar la secuencia de actividades que determinan la duración mínima del proyecto. El camino crítico está formado por las tareas cuyos retrasos afectan directamente el plazo final. CPM es fundamental para priorizar recursos y esfuerzos en esas tareas.
- ❑ Método de la Cadena Crítica: Integra los recursos disponibles y las dependencias de actividades, buscando optimizar el uso de recursos y minimizar los retrasos por cuellos de botella. Se diferencia del CPM al considerar restricciones de recursos y no sólo dependencias de tareas.

El seguimiento requiere actualizar regularmente el cronograma, validar el cumplimiento de hitos y coordinar la comunicación entre los miembros del equipo. Es fundamental realizar análisis de variaciones, emplear indicadores como el Índice de Desempeño del Cronograma (SPI), que mide la eficiencia del avance respecto al plan. También es recomendable el uso de técnicas de pronóstico para anticipar retrasos y preparar planes de mitigación. Además, se deben documentar los riesgos identificados, su probabilidad y su impacto, para establecer estrategias de respuesta.

### Seguimiento de Costes

El seguimiento de costes implica controlar y monitorear los gastos incurridos y compararlos constantemente con el presupuesto aprobado del proyecto. Este proceso, permite identificar desviaciones financieras y prevenir sobrecostes que puedan poner en riesgo el alcance del proyecto. Herramientas y técnicas:

- ❑ Técnica del Valor Ganado (Earned Value Management, EVM): Permite correlacionar el coste planificado de las actividades realizadas con el coste real incurrido y el avance físico del proyecto. Consiste en calcular indicadores, como el Cost Performance Index (CPI), que mide la eficiencia del gasto, y el Cost Variance (CV), que refleja la diferencia entre el valor ganado y el coste real. EVM es una metodología integral para monitorear y controlar el rendimiento financiero del proyecto.
- ❑ Gestión de reservas: Consiste en administrar fondos reservados para imprevistos y riesgos. Las reservas pueden ser de contingencia (para riesgos conocidos) o de gestión (para riesgos desconocidos), y permiten absorber sobrecostes sin comprometer el presupuesto total.

- **Actualización de presupuestos:** Implica revisar y ajustar periódicamente los presupuestos asignados a cada actividad, considerando cambios aprobados y fluctuaciones en los precios de los recursos. Mantener los presupuestos actualizados facilita el control y la toma de decisiones.
- **Informes periódicos:** La elaboración de informes sobre el estado financiero permite que las partes interesadas supervisen la evolución de los costes y tomen decisiones basadas en datos objetivos y actualizados. Los informes pueden incluir gráficos, tablas y análisis de tendencias.

El seguimiento de costes requiere analizar las causas de las desviaciones, implementar acciones correctivas oportunas y evaluar el impacto de cada cambio sobre la salud financiera del proyecto. Es fundamental establecer mecanismos de control que aseguren la transparencia, trazabilidad y responsabilidad en la gestión de recursos.

### **Control de Cambios**

El control de cambios es el proceso formal mediante el cual se gestionan todas las modificaciones que afectan el alcance, el cronograma o los costes del proyecto. Este proceso es esencial para mantener el control y la coherencia del proyecto, evitando alteraciones no autorizadas y garantizando que cada cambio sea evaluado y aprobado antes de su implementación. Etapas del control de cambios:

- **Solicitud de cambios:** Toda modificación debe ser documentada y presentada para su evaluación. Esto incluye cambios en los entregables, recursos, plazos o presupuestos. La solicitud debe contener la descripción, justificación y el impacto esperado.
- **Evaluación del impacto:** Antes de aprobar un cambio, se analiza su repercusión en el alcance, cronograma, costes, calidad y riesgos del proyecto. Es fundamental consultar a los equipos técnicos y las partes interesadas para identificar posibles efectos secundarios y asegurar que la decisión sea informada.
- **Aprobación o rechazo:** Las decisiones sobre cambios deben ser tomadas por un comité de control de cambios o por la persona con autoridad designada. Los criterios incluyen la alineación con los objetivos del proyecto, la viabilidad técnica, el impacto financiero y el riesgo.
- **Implementación y seguimiento:** Una vez aprobado un cambio, se actualizan todos los documentos afectados, se comunica a las partes interesadas y se realiza seguimiento para verificar que la modificación se ha implementado correctamente. El registro de los cambios es clave para la trazabilidad y la transparencia.

El control de cambios garantiza que el proyecto se adapte de manera ágil y controlada a nuevas circunstancias, sin perder de vista la trazabilidad. Es clave mantener informadas a todas las partes interesadas y registrar cada decisión para evitar confusiones futuras y facilitar auditorías.

La gestión integral del seguimiento de cronograma y costes, sumada a un control de cambios robusto, proporciona a los equipos de proyecto las herramientas necesarias para gestionar la incertidumbre y cumplir los objetivos establecidos.



### 4.4.2. Control de calidad, ensayos normativos y auditorías

La instalación de un Sistema Electrónico de Seguridad exige una gestión de la calidad estricta. Este tipo de proyecto requiere una integración precisa entre hardware, software y protocolos de operación. Un enfoque estructurado de los procesos de control de calidad, ensayos normativos y auditorías permite garantizar la excelencia desde la planificación hasta la operación del sistema.

El control de calidad en los proyectos de implantación de Sistemas de Seguridad Electrónica se inicia en la fase de planificación, donde se definen los requisitos técnicos, los estándares de aceptación y los criterios de desempeño. El Plan de Gestión de la Calidad incluye especificaciones de equipos (cámaras, sensores, unidades de grabación, etc.), condiciones ambientales, interfaces de usuario, protocolos de comunicación y criterios de redundancia. Principales actividades y herramientas:

- Inspección Visual: Revisión detallada de la instalación física de dispositivos, cableado, soportes y fijaciones para detectar errores, daños o incumplimientos del diseño.
- Prueba de funcionamiento individual: Cada componente (cámara, lector biométrico, central de alarmas, etc.) es activado y monitoreado para confirmar su operatividad.
- Prueba de integración: Se verifica el correcto funcionamiento del sistema como un todo, asegurando la comunicación entre módulos y la interoperabilidad de diferentes tecnologías.
- Verificación de protocolos: Comprobación de configuración de alertas, reglas de acceso, escalado de eventos y respuesta ante incidentes.
- Listas de verificación: Herramientas que permiten evaluar de manera sistemática cada etapa del proyecto, desde la recepción de equipos hasta la puesta en marcha.
- Muestreo estadístico: Selección aleatoria de componentes o procesos para validar la calidad en casos de instalaciones extensas.
- Análisis de datos: Recolección y procesamiento de información sobre fallos, alarmas y desempeño, para identificar patrones y áreas de mejora.
- Gestión de no conformidades: Registro, análisis de causas y aplicación de acciones correctivas y preventivas, como reemplazo de equipos, ajuste de software o capacitación adicional.

En el caso de instalación de Sistemas Electrónicos de Seguridad en entornos con altas necesidades de seguridad se deben realizar pruebas bajo condiciones reales o simuladas, como cortes de energía, intentos de sabotaje, variaciones climáticas y ataques informáticos, para evaluar la resiliencia y la capacidad de respuesta del sistema.

Los ensayos normativos consisten en un conjunto de pruebas y verificaciones técnicas que se realizan sobre los componentes de los Sistemas Electrónicos de Seguridad. El objetivo es comprobar que cumplen con las especificaciones establecidas por la legislación vigente y las normas nacionales e internacionales, entre otras:

- UNE-EN 50131: Sistemas de alarma de intrusión y atraco.
- UNE-EN 60839: Sistemas electrónicos de alarma y de seguridad.
- UNE-EN 62676: Sistemas de videovigilancia para utilización en aplicaciones de seguridad.

Los procedimientos de ensayo varían según el tipo de sistema y la normativa aplicable, pero suelen incluir:

- Verificación de la funcionalidad básica del sistema (detección, señalización, activación de alarmas).
- Pruebas de resistencia frente a interferencias electromagnéticas y condiciones ambientales adversas.
- Simulación de intentos de sabotaje para comprobar la robustez del sistema.
- Evaluación de la integridad y confidencialidad de la transmisión de datos.

La certificación tras superar los ensayos normativos proporciona garantías de calidad y seguridad tanto para los fabricantes como para los usuarios finales. Además, facilita el cumplimiento legal y la interoperabilidad entre equipos de distintos proveedores. La realización de ensayos normativos en Sistemas Electrónicos de Seguridad es esencial para asegurar su correcto funcionamiento y su adecuación a las exigencias legales y técnicas.

Las auditorías de calidad son procesos sistemáticos y documentados para evaluar el cumplimiento de los procesos, estándares y objetivos definidos en el proyecto. Las auditorías pueden ser internas (realizadas por personal propio) o externas (por entidades certificadoras).

Aspectos clave de la auditoría:

- Revisión documental: Inspección de contratos, especificaciones técnicas, registros de pruebas, certificados de calibración y manuales de operación.
- Evaluación del proceso de instalación: Análisis de la secuencia de actividades, cumplimiento de protocolos de seguridad, gestión de riesgos y calidad de la ejecución.
- Verificación de capacitación del personal: Confirmación de la formación técnica, acreditaciones y experiencia de quienes realizan la instalación y operación del sistema.
- Inspección de trazabilidad: Seguimiento de componentes desde la adquisición hasta la puesta en marcha, evitando piezas no certificadas o de origen dudoso.
- Revisión de pruebas realizadas: Análisis de los resultados de ensayos normativos, pruebas de integración, funcionalidad, ciberseguridad y usabilidad.
- Gestión de incidentes y no conformidades: Verificación de los sistemas para registrar, investigar y resolver problemas detectados durante el proyecto.
- Evaluación de riesgos residuales: Identificación de amenazas persistentes, análisis de mitigaciones implementadas y propuestas de mejora.
- Revisión de satisfacción de personas usuarias: Entrevistas, encuestas y pruebas en campo para validar la experiencia y la percepción de seguridad.
- Inspección final y certificación: Auditoría al cierre del proyecto para garantizar que el sistema cumple con todos los requisitos y puede ser oficialmente entregado.

El resultado de las auditorías se plasma en informes técnicos, que incluyen hallazgos, recomendaciones y planes de mejora. Estos documentos son esenciales para la certificación, la operación segura y el mantenimiento futuro del sistema.

La gestión avanzada de la calidad, la realización de ensayos normativos detallados y la ejecución de auditorías exhaustivas son la base para instalar Sistemas Electrónicos de Seguridad confiables y robustos.

## 4.4.3. Indicadores (KPI/SLAs) y reporting de cumplimiento

En la gestión avanzada de proyectos de instalación de Sistemas Electrónicos de Seguridad, la medición del desempeño mediante indicadores estratégicos, operativos y de servicio es esencial para asegurar la calidad, la eficiencia y la satisfacción de todas las partes interesadas. La selección y administración de KGIs (Key Goal Indicators), KPIs (Key Performance Indicators) y SLAs (Service Level Agreements) proporciona un sistema robusto para monitorizar el progreso, anticipar riesgos y evidenciar el cumplimiento de objetivos de alto nivel.

Los KGI (Key Goal Indicators) son métricas que evalúan el grado de consecución de objetivos estratégicos, permitiendo a las personas responsables del proyecto medir el éxito global más allá de los resultados operativos. Los KPI (Key Performance Indicators) cuantifican el rendimiento de actividades clave y procesos que contribuyen al logro de los objetivos definidos por los KGIs. Por su parte, los SLAs (Service Level Agreements) establecen los niveles mínimos de servicio acordados entre proveedor y cliente o entre distintas áreas, especificando parámetros como tiempos de respuesta, calidad y disponibilidad.

### Ejemplos KGI/KPI/SLA

| KGI                                                  | KPI                                           | SLA                                                             |
|------------------------------------------------------|-----------------------------------------------|-----------------------------------------------------------------|
| Porcentaje de cumplimiento del objetivo del proyecto | Porcentaje de avance respecto al cronograma   | Tiempo máximo para resolución de incidencias                    |
| Satisfacción global del cliente                      | Tasa de defectos por unidad instalada         | Porcentaje de cumplimiento en entregas                          |
| Retorno de la inversión (ROI)                        | Tiempo medio de instalación por componente    | Garantía de funcionamiento sin fallos durante un periodo mínimo |
| Alineación con la estrategia                         | Coste acumulado frente al presupuesto inicial | Soporte técnico disponible 24/7                                 |
|                                                      | Número de incidencias críticas reportadas     | Respuesta ante emergencias en menos de 2 horas                  |

La relación entre estos indicadores es jerárquica: los KGIs representan el objetivo estratégico, los KPIs son métricas operativas que impulsan el logro de los KGIs, y los SLAs aseguran que el servicio entregado cumple con los estándares acordados.

Una gestión basada en resultados con una buen diseño e implantación de indicadores es fundamental para mantener el control y la transparencia durante la ejecución del proyecto. Los KGIs, KPIs y SLAs permiten a las personas responsables del proyecto identificar riesgos, optimizar recursos, asegurar la calidad y mejorar continuamente los procesos. Además, facilitan el cumplimiento contractual y la satisfacción de las partes interesadas, evidenciando el avance hacia los objetivos estratégicos y operativos del proyecto, porporcionando información y capacidad de gestión en las distintas actividades del proyecto:

- ▢ Gestión de riesgos: Anticipan desviaciones que pueden poner en peligro la consecución de objetivos, activando planes de mitigación.
- ▢ Control de calidad: Facilitan la supervisión constante de estándares técnicos y la satisfacción de los usuarios.
- ▢ Gestión de las partes interesadas: Proveen información objetiva y transparente para todas las partes interesadas, fortaleciendo la comunicación y confianza.
- ▢ Mejora continua: Los resultados de los indicadores permiten ajustar procesos y estrategias para lograr mayor eficiencia y calidad.

### Identificación y Selección de KGIs, KPIs y SLAs en Proyectos de Instalación

La identificación y la selección de indicadores en un proyecto de instalación de Sistemas Electrónicos de Seguridad debe partir del análisis del alcance, los objetivos estratégicos y operativos, los riesgos y los requisitos específicos del cliente. Involucrar a equipos multidisciplinarios (dirección, gestión, calidad, técnica y personas usuarias) es esencial para definir indicadores relevantes, medibles y alineados con la estrategia organizacional.

- ▢ Revisión de objetivos estratégicos: Identificar las metas críticas del proyecto, como la cobertura total, la satisfacción del cliente o el cumplimiento normativo. Estos serán los KGIs.
- ▢ Mapeo de procesos clave: Detectar actividades cuyo desempeño impacta directamente en los KGIs, definiendo KPIs para su seguimiento.
- ▢ Consulta con las partes interesadas: Recabar expectativas y necesidades, especialmente para definir SLAs que respondan a requerimientos de servicio.
- ▢ Priorización y medición: Elegir indicadores que sean relevantes, alcanzables y que permitan una monitorización eficaz.
- ▢ Definición clara: Establecer valores objetivo, métodos de medición y criterios de cumplimiento para cada indicador.

## 4 Ciclo de vida

El reporte de cumplimiento es el proceso de comunicar el estado real de los indicadores a todas las personas responsables y partes interesadas. Para ser efectivo, debe ser claro, preciso, visual y adaptado a las necesidades de cada público. El reporte se estructura en torno a los KGIs, KPIs y SLAs, permitiendo una visión global, operativa y de servicio. Para ello deben utilizarse herramientas y técnicas como:

- Cuadros de mando: Visualización en tiempo real del avance, cruzando información de KGIs, KPIs y SLAs.
- Informes periódicos: Detalles comparativos con metas estratégicas, operativas y de servicio.
- Sistemas de gestión documental: Almacenamiento y trazabilidad de reportes históricos.
- Sistema de alertas automáticas: Notificaciones ante desviaciones críticas en indicadores.

### KGI/KPI/SLA –Objetivo, Frecuencia y Responsables

| Indicador | Objetivo                                                                       | Frecuencia                                                | Responsable                   |
|-----------|--------------------------------------------------------------------------------|-----------------------------------------------------------|-------------------------------|
| KGI       | Consolidación de datos y reporte estratégico                                   | Mensual o por hitos                                       | Dirección del proyecto        |
| KPI       | Control operativo y reporte de KPIs                                            | Reporte semanal o diario                                  | Jefe de proyecto              |
| SLA       | Verificación de métricas, reporte de SLAs y retroalimentación sobre incidentes | Supervisión mensual y evaluación por entregas de servicio | Equipos de calidad y técnicos |

Es necesario integrar la aplicación de indicadores en todas las fases de un proyecto de instalación de Sistemas Electrónicos, esto garantiza una monitorización continua, permitiendo actuar oportunamente ante desviaciones y fortalecer la gestión de riesgos, calidad y comunicación.

### Integración de indicadores en las fases del proyecto

| Fase                     | Actividad                                                                      |
|--------------------------|--------------------------------------------------------------------------------|
| Planificación            | Definición de KGIs, KPIs y SLAs                                                |
|                          | Asignación de recursos para monitoreo                                          |
|                          | establecimiento de valores objetivos y criterios de éxito                      |
| Ejecución                | Recopilación sistemática de datos                                              |
|                          | Registro de eventos relevantes                                                 |
|                          | Comunicación constante sobre avance y obstáculos                               |
| Monitorización y Control | Verificación de métricas, reporte de SLAs y retroalimentación sobre incidentes |
|                          | Comparación de resultados con objetivos                                        |
|                          | Análisis de causas de desviaciones                                             |
|                          | Implementación de acciones correctivas y preventivas                           |
| Cierre                   | Evaluación final del cumplimiento                                              |
|                          | Documentación de lecciones aprendidas y retroalimentación                      |
|                          | Reporte global de KGIs, KPIs y SLAs.                                           |

La integración debe estar soportada por procedimientos claros de recolección, análisis y comunicación de datos, garantizando la fiabilidad de la información y la capacidad de respuesta ante cualquier situación.

## Ejemplos prácticos de KGIs, KPIs y SLAs en Proyectos de Instalación

| KGI                                                                       | KPI                                   | SLA                                                             | Descripción                                                         | Frecuencia de reporte            | Responsable                                               |
|---------------------------------------------------------------------------|---------------------------------------|-----------------------------------------------------------------|---------------------------------------------------------------------|----------------------------------|-----------------------------------------------------------|
| Cobertura total de instalación                                            | Porcentaje de avance semanal          | Tiempo máximo de respuesta ante fallos                          | Monitoreo del cumplimiento estratégico, operativo y de servicio     | Mensual / semanal                | Dirección de proyecto / Jefe de proyecto / Equipo técnico |
| Satisfacción global del cliente                                           | Número de reclamaciones recibidas     | Garantía de soporte técnico 24/7                                | Evaluación de la experiencia y gestión de incidentes                | Al cierre del proyecto / semanal | Dirección de proyecto / Equipo de calidad                 |
| ROI del proyecto                                                          | Costo acumulado vs presupuesto        | Porcentaje de entregas a tiempo                                 | Control financiero y cumplimiento de plazos                         | Mensual                          | Dirección financiera / Jefe de proyecto                   |
| Alineación estratégica (normas, regulaciones, objetivos organizacionales) | Tasa de defectos por unidad instalada | Garantía de funcionamiento sin fallos durante un periodo mínimo | Supervisión de calidad, cumplimiento normativo y fiabilidad técnica | Mensual / semanal                | Equipo de calidad / Jefe de proyecto                      |

Una gestión avanzada de KGIs, KPIs y SLAs, junto con metodologías de reporte estructuradas, es indispensable para el éxito de los proyectos de instalación de Sistemas Electrónicos de Seguridad. Integrar estos indicadores desde la fase de planificación, involucrar a equipos multidisciplinarios y utilizar tecnología para la visualización y análisis en tiempo real son estrategias que fortalecen el control, la mejora continua y la satisfacción de todas las partes involucradas.



## 4.5. Cierre

### 4.5.1. Verificación final, conexión con Centro de control o CRA y acta de aceptación

La fase de cierre constituye la etapa final del ciclo de vida de un proyecto de seguridad y tiene como finalidad verificar, documentar y formalizar que todos los sistemas instalados cumplen los requisitos técnicos, funcionales, operativos y normativos definidos durante las fases de diseño y ejecución.

Esta fase representa el proceso mediante el cual la instalación pasa de estar en situación de ejecución a convertirse en una infraestructura plenamente operativa, garantizando que los sistemas han sido correctamente instalados, configurados, probados, integrados y entregados al cliente en condiciones adecuadas de funcionamiento.

La fase de cierre debe incluir una revisión completa de los sistemas ejecutados para comprobar que cumplen las especificaciones técnicas definidas en el proyecto y que su funcionamiento es conforme a los requisitos establecidos.

- ✓ **Sistemas de Videovigilancia:** se deberá comprobar la correcta visualización, cobertura y orientación, funcionalidad de analíticas, grabación continua y de eventos.
- ✓ **Sistemas de detección de intrusión:** se deberá verificar la detección y cobertura de cada uno de los sensores instalados, activación de sirenas, supervisión de sabotaje, supervisión de alimentación/baterías y correcta zonificación del área protegida.
- ✓ **Sistemas de control de acceso:** se comprobará el correcto funcionamiento de los lectores, accionamiento de cerraduras/barreras/torniquetes, gestión de usuarios, gestión de horarios y verificación de eventos.
- ✓ **Verificación de integraciones:** se verificará que dentro de las plataformas de gestión unificada usadas se gestione correctamente la operatividad de todos los sistemas y sus módulos de mantenimiento sean capaces de detectar fallos de funcionamiento en alguno de ellos.
- ✓ **Verificación de comunicaciones con la Central Receptora de Alarmas.** Se debe verificar la correcta recepción de señales de cualquier evento en los sistemas de detección de intrusión y analíticas de videovigilancia, plasmándolo después en el documento “Certificado de Conexión” donde se deberá dejar constancia de las señales recibidas en la CRA.

Una vez completadas satisfactoriamente las verificaciones funcionales, deberá impartirse la formación necesaria al personal designado por el cliente, con el fin de garantizar la correcta operación, administración y mantenimiento de los sistemas instalados. La formación deberá cubrir tanto los aspectos operativos habituales como los procedimientos de actuación ante incidencias, alarmas y situaciones de emergencia.

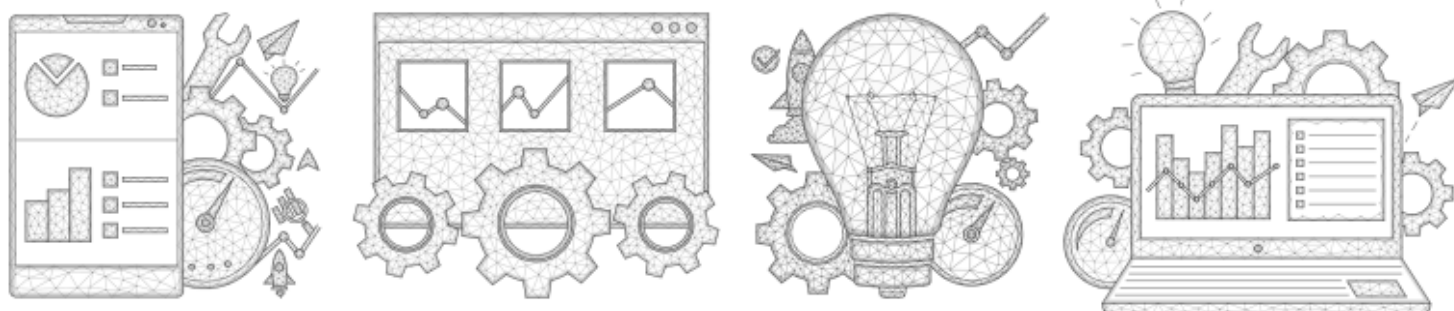
Con una antelación previa de al menos 72h antes de la entrada en explotación de los sistemas instalados se deberá realizar el registro del contrato y los servicios que lo componen, en la página web Segurpri (Policía Nacional).

The screenshot shows the Segurpri web application interface. At the top, there is a header with the Spanish flag, the text 'MINISTERIO DEL INTERIOR', 'Comando General de Seguridad Ciudadana', 'Unidad Central de Seguridad Privada', and the 'Segurpri' logo. Below the header is a navigation bar with links: 'ACTIVIDADES', 'PERSONAL', 'CONTRATOS', 'ESTABLECIMIENTOS', and 'AYUDA'. The main content area is titled 'Contratos >> Contratos de Seguridad >> Contratos >> Añadir...'. It contains a form with two tabs: 'Datos Contrato' (selected) and 'Sujeto'. The 'Datos Contrato' tab has several input fields: 'Empresa' (with sub-fields for 'Denominación' and 'Número Inscripción'), 'Nombre Comercial', 'Código', 'Fecha Inicio', 'Fecha Fin', 'Provincia', and 'Localidad'. There is also a checkbox for 'Alarma Automática' which is checked.

Después de la entrega del sistema de seguridad, se recomienda probarlo durante un periodo de tiempo acordado con el cliente. Durante este proceso, se instruiría a la central de alarmas de que sólo se informe a la empresa instaladora y al cliente en ese caso de que se produjeran alarmas. Para, en el caso de que resultaran ser falsas, se tomaran las acciones correctoras.

Después de la conclusión del periodo de pruebas, el sistema de seguridad ya sería objeto de la recepción definitiva y debe proceder a formalizar el acta de cierre del proyecto.

Acta de cierre: Documento formal que señala la aceptación por parte del cliente o patrocinador, iniciándose a partir de ese momento el periodo de garantía, mantenimiento y explotación de la infraestructura de seguridad.



### 4.5.2. Documentación as-built

La documentación As Built constituye uno de los entregables más importantes dentro del ciclo de vida de un proyecto de seguridad. Su finalidad es reflejar de forma precisa, completa y actualizada cómo ha sido finalmente ejecutada la instalación, incorporando todas aquellas modificaciones, ajustes, ampliaciones o desviaciones que hayan podido producirse respecto al proyecto inicialmente diseñado.

Mientras que la ingeniería de diseño representa la solución prevista durante la fase de proyecto, la documentación As Built describe la realidad física y funcional de los sistemas una vez finalizados, probados y puestos en servicio. Este conjunto documental se convierte en la referencia oficial para las tareas futuras de operación, mantenimiento, ampliación, auditoría, gestión de incidencias y renovación tecnológica.

Índice del documento Documentación as-built

#### 1 Introducción

Debe incluir la descripción detallada de la arquitectura implantada indicando funcionalidades implantadas, modificaciones respecto al proyecto inicial e integraciones entre sistemas.

#### 2 Planos actualizados

Todos los planos deben reflejar exactamente la instalación ejecutada, incluyendo esquema de unifilares, diagramas de red y comunicaciones, diagramas de integración entre subsistemas, así como la arquitectura de servidores y almacenamiento adoptado.

#### 3 Inventario de equipos instalados

Debe elaborarse un inventario completo que incluya los siguientes datos:

- Fabricante.
- Versión de firmware.
- Modelo.
- Ubicación física.
- Número de serie.
- Fecha de instalación.
- Dirección IP.
- Garantía.

#### 4 Configuraciones de sistemas

En este apartado se deben incorporar los parámetros de configuración relevantes de cada sistema, así como a nivel de comunicaciones y ciberseguridad.

## 5 Pruebas realizadas y resultados

Debe incluirse evidencia documental de las:

- pruebas funcionales de los sistemas implantados
- pruebas de transmisión de alarmas
- verificación de integraciones
- comprobación de comunicaciones
- simulaciones de fallo

## 6 Manuales de operación y mantenimiento

Instrucciones de funcionamiento del sistema, con suficiente nivel de detalle para reducir al mínimo la posibilidad de operación incorrecta: cuestiones a tener en cuenta a la hora de conectar el sistema, detalle de los diferentes procesos (conexiones, desconexiones, anulaciones de zona, procedimientos de prueba, .... Así como alguna operativa concreta que especifique el fabricante de los equipos.

## 7 Certificados de los equipos instalados

Dentro de este punto deben quedar claro los siguientes puntos:

- Datos de la empresa instaladora.
- Datos de la empresa encargada de acudir a la atención de las alarmas.
- Datos de la empresa de mantenimiento.
- Detalles sobre todos los procedimientos relativos a la verificación de las alarmas.
- Datos de la central receptora de alarmas.





La fase de **operación y mantenimiento post-implantación** constituye la etapa más prolongada del ciclo de vida de un sistema electrónico de seguridad y resulta crítica para garantizar que la solución implantada continúe cumpliendo, de forma sostenida, los objetivos de seguridad, los requisitos normativos y los parámetros de calidad definidos en el proyecto.

En esta fase, el énfasis se traslada desde la ejecución de obra y la puesta en marcha hacia la **explotación eficiente del sistema**, la **gestión de incidencias** y la **planificación de actuaciones de mantenimiento preventivo y correctivo**, así como la incorporación ordenada de mejoras evolutivas.

## 5.1. Plan de mantenimiento normativo y preventivo

Todo sistema de seguridad sujeto a la normativa de seguridad privada debe disponer de un **Plan de Mantenimiento** formalmente definido, que dé cumplimiento a lo establecido en el Reglamento de Seguridad Privada y en las Órdenes Ministeriales aplicables, y que asegure la operatividad y fiabilidad del sistema durante toda su vida útil.

El Plan de Mantenimiento deberá:

1

### Dar cumplimiento a las exigencias normativas

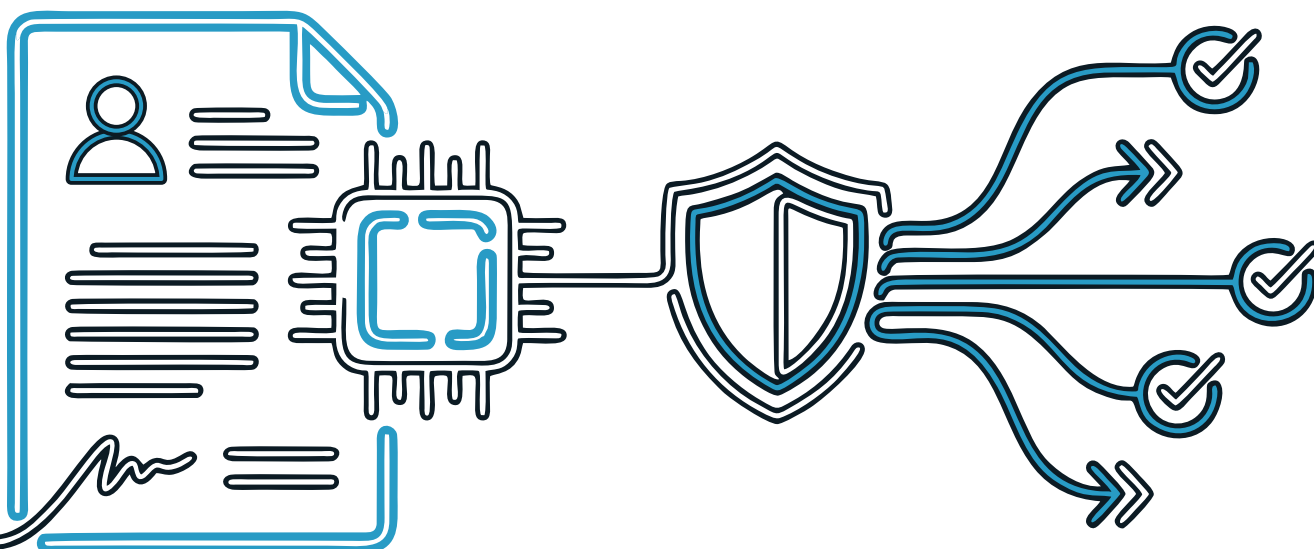
- ☞ Incluir la realización de **revisiones preventivas con la periodicidad establecida** en la normativa aplicable a los sistemas conectados a una CRA o cuya instalación sea obligatoria.
- ☞ Diferenciar las condiciones de mantenimiento en función de la **capacidad de supervisión remota** de los equipos (p.ej., sistemas que permiten comprobación del estado desde la CRA, frente a sistemas que requieren revisión física completa).
- ☞ Contemplar la **obligación de llevar Libros Registros de revisiones**, tanto por parte de la empresa de seguridad como por parte del titular de la instalación, incluyendo:
  - Datos del contrato.
  - Fechas de revisión.
  - Identificación del técnico.
  - Deficiencias observadas.
  - Fecha y forma de subsanación.

## 2

## Establecer el alcance técnico del mantenimiento preventivo

El mantenimiento preventivo deberá, como mínimo, abarcar:

- ❑ **Verificación del funcionamiento de todos los dispositivos** (detectores, cámaras, lectores, pulsadores, sirenas, paneles, grabadores, controladores, etc.).
- ❑ Comprobación de **alimentaciones principales y de respaldo** (SAI, baterías, fuentes de alimentación), incluyendo pruebas de autonomía y tiempos de conmutación.
- ❑ Revisión del **estado físico de cableado, canalizaciones y racks**, verificando ausencia de daños, manipulaciones o condiciones ambientales adversas.
- ❑ Comprobación y, en su caso, ajuste de **parámetros de configuración** (sensibilidades, máscaras de detección, horarios, calendarios de armado/desarmado, perfiles de usuario).
- ❑ Pruebas periódicas de **transmisión de alarmas y eventos**, verificando la correcta comunicación con la CRA o centro de control.
- ❑ Verificación del **registro y conservación de imágenes**, asegurando el cumplimiento de los plazos de retención establecidos y la integridad de los soportes de grabación.



3

## Definir el mantenimiento correctivo y los niveles de servicio (SLAs)

- ❑ Establecer **tiempos máximos de respuesta y resolución** en función de la criticidad del incidente (por ejemplo, indisponibilidad total del sistema, fallo de un subsistema crítico, fallo de un elemento no crítico, etc.).
- ❑ Definir **canales y procedimientos de comunicación de averías** (teléfono, portal web, correo electrónico, herramientas ITSM), con registro automático de tickets e identificación unívoca de cada incidencia.
- ❑ Determinar, cuando proceda, la **disponibilidad de servicio técnico 24x7**, especialmente en instalaciones de alto riesgo o infraestructuras críticas.

4

## Asignar claramente las responsabilidades

- ❑ Establecer una **matriz de responsabilidades** entre el titular de la instalación, la empresa de seguridad instaladora/mantenedora, la CRA y otros proveedores implicados (por ejemplo, operadores de comunicaciones o integradores de sistemas).
- ❑ Especificar qué tareas son responsabilidad del cliente (por ejemplo, cambio de usuarios, gestión de credenciales, custodia de grabaciones) y cuáles competen a la empresa mantenedora.

5

## Integrar el mantenimiento en la gestión de la calidad y el riesgo

- ❑ Relacionar el Plan de Mantenimiento con el **Plan de Gestión de Riesgos** definido en el proyecto, de forma que las revisiones prioricen los elementos más críticos.
- ❑ Establecer **indicadores de desempeño del mantenimiento** (número de averías, tiempo medio de reparación, disponibilidad de sistema, porcentaje de revisiones realizadas en plazo, etc.) que permitan evaluar la eficacia del servicio y la necesidad de mejoras.

El Plan de Mantenimiento deberá formar parte de la **documentación contractual y técnica** del proyecto, y será revisado y actualizado cuando se produzcan cambios sustanciales en el sistema, en la normativa aplicable o en el nivel de riesgo del entorno protegido.



## 5.2. Gestión de incidencias, obsolescencia y mejoras evolutivas

La adecuada explotación de un sistema de seguridad exige disponer de **procesos estructurados** para gestionar incidencias, abordar la obsolescencia tecnológica y planificar mejoras evolutivas que permitan mantener la eficacia del sistema frente a un entorno en constante cambio.

### 5.2.1. Gestión de incidencias y no conformidades

La **gestión de incidencias** debe apoyarse en un procedimiento documentado que contemple, al menos:



#### Registro y clasificación de incidencias

- Registro de todas las incidencias detectadas por los usuarios, la CRA, el servicio técnico o las auditorías internas.
- Clasificación por tipología (fallo de hardware, fallo de software, error de configuración, fallo de comunicaciones, uso indebido, falsa alarma, etc.) y por impacto en la operación.



#### Priorización y escalado

- Definición de niveles de criticidad (crítica, alta, media, baja), en función del impacto sobre la disponibilidad del sistema y el riesgo de desprotección.
- Establecimiento de **rutras de escalado** técnico y jerárquico, tanto dentro de la empresa de seguridad como hacia el cliente y, en su caso, hacia la CRA.



#### Análisis de causa raíz y acciones correctivas

- Aplicación de metodologías estructuradas (por ejemplo, análisis de causa raíz) en incidencias recurrentes o de alto impacto.
- Definición de **acciones correctivas y preventivas (CAPA)** que aborden no solo el síntoma (avería puntual), sino el origen del problema (diseño, configuración, formación, proceso, etc.).



#### Cierre y verificación de eficacia

- Verificación de que la incidencia ha sido realmente resuelta, mediante pruebas de funcionamiento y validación con el usuario o con la CRA.
- Actualización de la **documentación técnica** (planos, configuraciones, inventario) cuando las acciones correctivas supongan cambios en la instalación.

La información obtenida de la gestión de incidencias debe retroalimentar el **Plan de Mantenimiento** y los procesos de mejora continua, permitiendo identificar patrones (por ejemplo, dispositivos o marcas problemáticas, vulnerabilidades de configuración, puntos débiles en el diseño, etc.).

## 5.2.2. Gestión de la obsolescencia tecnológica

Los sistemas electrónicos de seguridad están expuestos a la **obsolescencia tecnológica**, tanto por evolución natural de la tecnología (fin de soporte, discontinuidad de modelos, cambios en protocolos de comunicación) como por cambios en la normativa o en las amenazas (nuevas técnicas de intrusión, ciberataques a dispositivos de seguridad IP, etc.).

La guía recomienda que el titular del sistema y la empresa de seguridad:

- Mantengan un **inventario actualizado** de todos los equipos y versiones de firmware/software.
- Identifiquen los **componentes críticos** cuyo fin de vida (EoL) o fin de soporte (EoS) pueda comprometer la operación o la seguridad.
- Establezcan un **plan plurianual de renovación tecnológica**, priorizado por criticidad, impacto en el riesgo y disponibilidad presupuestaria.
- Consideren, en la planificación de renovaciones, aspectos de **compatibilidad e interoperabilidad**, evitando soluciones que generen dependencias excesivas (vendor lock-in) o problemas de integración.

La gestión de la obsolescencia debe integrarse en la **planificación estratégica de la seguridad** de la organización, coordinándose con otras áreas como IT/OT, ciberseguridad y gestión de activos.



## 5.2.3. Mejora evolutiva y optimización del sistema

Más allá del simple mantenimiento, los sistemas de seguridad deben estar sujetos a un proceso de **mejora evolutiva** que permita:

- Adaptarse a **cambios en el entorno de riesgo** (nuevas amenazas, cambios en la criticidad de activos, ampliaciones de instalaciones, variaciones en los flujos de personas y mercancías, etc.).
- Incorporar **nuevas funcionalidades** (analítica avanzada de vídeo, integración con sistemas de gestión de edificios –MS– sistemas de control de presencia, etc.).
- Alinear el sistema con **cambios normativos o de estándares**, que puedan requerir ajustes en los niveles de protección, en las capacidades de grabación o en los procedimientos de operación y conservación de datos.

Para ello, se recomienda:

- Realizar **revisiones periódicas del diseño de seguridad** (por ejemplo, auditorías anuales o bianuales), evaluando la adecuación del sistema al riesgo actual y a la normativa vigente.
- Definir un **proceso formal de gestión de cambios**, que incluya análisis de impacto, aprobación, planificación, pruebas, puesta en producción y actualización documental.
- Establecer **indicadores de desempeño** (tasa de falsas alarmas, tiempos de respuesta, disponibilidad de sistema, uso de funcionalidades avanzadas, etc.) que permitan identificar oportunidades de optimización.
- Asegurar la **formación continua de los usuarios y operadores**, de forma que las mejoras tecnológicas se traduzcan efectivamente en una mejora real de la seguridad y no solo en capacidades infrautilizadas.

En conjunto, la gestión estructurada de incidencias, la planificación de la renovación tecnológica y la implantación de mejoras evolutivas permiten que los sistemas de seguridad mantengan su **eficacia, cumplimiento normativo y alineamiento con los objetivos de la organización** a lo largo de todo su ciclo de vida.

Guía elaborada por el Área de  
Trabajo de Ingeniería instalación  
y mantenimiento de:



**AES**

ASOCIACIÓN ESPAÑOLA  
EMPRESAS DE SEGURIDAD

C/Alcalá, 99 2ºA - 28009 Madrid

Telf. 915 765 225

[www.aesseguridad.es](http://www.aesseguridad.es) / [aes@aesseguridad.es](mailto:aes@aesseguridad.es)

[www.aesfundacion.es](http://www.aesfundacion.es) / [patronato@aesfundacion.es](mailto:patronato@aesfundacion.es)



@aes\_seguridad



ASOCIACIÓN ESPAÑOLA DE  
EMPRESAS DE SEGURIDAD



aesseguridad2021



@FundacionAES



AES Fundación



aes\_fundacion\_