Asociación Española de empresas de Seguridad

Dinamizando la Industria de la Seguridad

Guía de interpretación instalaciones grado 3 y 4

CONTENIDO

1 Prólogo

En un contexto de transformación empresarial y avance tecnológico acelerado con una exposición cada vez mayor de las empresas a nuevas amenazas se hace necesaria la actualización y adecuación de los servicios de seguridad sobre las instalaciones grado 3 y 4.

Desde las distintas Áreas de Trabajo de AES se considera prioritario el presente estudio para la correcta evolución del sector, la identificación de medidas que faciliten el incremento en la calidad de los servicios y soluciones de seguridad sobre las infraestructuras esenciales y críticas (grado 4) así como para los negocios que por su actividad y exposición al riesgo requieren de un alto grado seguridad (grado 3).

2 Introducción

La base tecnológica para la prestación de los servicios de seguridad con la calidad y eficiencia adecuada depende del diseño y combinación e integración de diferentes soluciones o tecnologías, que por un lado hacen más eficiente la gestión de incidentes y por otro complementan la intervención de las diferentes partes interesadas o concurrentes en los procesos de seguridad.

La continua evolución tecnológica y su aplicación al sector de la seguridad ha provocado la tendencia hacia la "hibridación" de soluciones de seguridad, que requieren la interoperación y/o integración de diferentes sistemas, en especial sistemas de detección de intrusión, control de accesos y videovigilancia.

No cabe discusión en lo referente a las mejoras introducidas a través de esta vía, permitiendo una mayor eficiencia en la intervención de los diferentes actores de este segmento y en concreto en los procesos de detección y verificación de alarmas, minimizando las falsas alarmas lo que a su vez redunda en un uso eficiente de las comunicaciones a FCS, así como mayores tiempos de reacción por parte del personal de vigilancia.

Sin embargo, el diseño de este tipo de soluciones de seguridad, resultado de la combinación de diferentes tecnologías, plantea dudas en el aspecto normativo, al confluir diferentes normas y estándares.

La presente **"Guía de interpretación"** o de mejores prácticas sobre la norma y su aplicabilidad en instalaciones Grado 3 y 4 tiene un carácter eminentemente de "guía y recomendaciones", por lo que lo indicado no sería de obligado cumplimiento, quedando del lado de las propias empresas de seguridad y clientes la decisión sobre su implantación y cumplimiento.

Reseñar como aspecto muy relevante la figura del **Ingeniero de Seguridad** responsable del **diseño y certificación** de nuevas soluciones de seguridad siguiendo los preceptos de cumplimiento, ciclo de vida y calidad en la implantación de sistemas de seguridad de grado 3 y 4, que evidencia y hace imprescindible la intervención y reconocimiento de forma explícita por parte de la Administración y del Sector de Seguridad.

3 Alcance

El alcance del presente documento es el de promover una serie de actuaciones que tiene por objetivo la evolución y adecuación en materia de diseño, certificación y cumplimiento normativo de los sistemas combinados e integrados de seguridad electrónica para instalaciones Grado 3 y 4.

Así mismo, los criterios y tecnologías descritos en la presente guía pueden ser de aplicación a zonas sensibles dentro del edificio o instalación, como el centro de control o de videovigilancia, centros de procesos de datos (CPD), etc., cuyo diseño específico será objeto de posteriores guías el diseño, atendiendo a su regulación, normativa, marco de trabajo (framework) y recomendaciones específicas.

La presente guía desarrolla en los siguientes capítulos la información y análisis de los aspectos más relevantes y permiten establecer una serie de criterios que deberán ser considerados en las diferentes etapas del ciclo de vida de este tipo de instalaciones:

- Beneficios de la implantación de la Guía
- Marco Normativo
- Relación UNE 50398 con 50131-7
- Características de la norma UNE 50398 en instalaciones grado 3 y 4
- Responsabilidad contractual y roles
- Requisitos del sistema en instalaciones
- Ciclo de instalación (Etapas de trabajo)
- Certificación de la instalación

Quedan fuera del alcance de esta guía de aplicación otros aspectos relevantes, que también deben ser considerados en el diseño, implantación, gestión y mantenimiento de sistemas de seguridad, como los relacionados con la ciberseguridad y ciber-resiliencia de los sistemas de seguridad o la gestión de datos de carácter personal sujetos al Reglamento General de Protección de Datos (RGPD) como consecuencia de la implantación de sistemas de videovigilancia, biometría, etc.

En lo referente a la aplicación de medidas y controles de ciberseguridad sobre sistemas de seguridad se recomienda seguir las pautas pendientes de publicación desde el Grupo de Trabajo de Ciber de AES y a lo establecido en las siguientes guías:

- "Guía Sobre Controles De Seguridad En Sistemas OT" del Ministerio del Interior."
- "AEINSE 10/21. Guía de buenas prácticas de ciberseguridad en proyectos de seguridad física" del Grupo de Trabajo de AEINSE, "ciberseguridad aplicada a los Sistemas de Seguridad Física"

4 Beneficios de la implantación de la Guía

En el presente capítulo se describen los principales beneficios a partir de la implantación de la Guía de Interpretación.

- **Cumplimiento** en los requisitos relacionados con la **normativa y mejores prácticas** asociadas a la propuesta de diseño de sistemas de seguridad adecuados para instalaciones sujetas a obligado cumplimiento de medidas de seguridad (grado 3) o cuyo uso es la prestación de servicios esenciales y protección de infraestructuras críticas (grado 4).
- Presentación de un esquema de **roles y responsabilidades** que facilite a los responsables y profesionales de seguridad, dentro de organizaciones complejas y considerando el ciclo de vida de este tipo de soluciones, identificar a los diferentes interlocutores, así como establecer y actualizar los mecanismos de control para un adecuado diseño y posterior operación de la seguridad.
- **Seguridad en el diseño y por defecto** de los propios sistemas de seguridad electrónica e información que integran la solución de seguridad combinada en su conjunto a partir de las consideraciones de **ciberseguridad** para este tipo de entornos.
- **Fiabilidad y excelencia** en la implantación de soluciones, alineadas con el diseño validado en la fase inicial, a partir de la recomendación de un **modelo de certificación**, compatible con la certificación actual.

5 Marco Normativo

El presente capítulo describe el marco normativo de aplicación a los sistemas de seguridad electrónica grado 3 y 4 desde la perspectiva de los organismos reguladores nacionales adscritos al Ministerio del Interior (UCSP y CNPIC) con competencias en la aprobación y certificación de instalaciones en grado, así como las normas técnicas de aplicación españolas (UNE) con base en el estándar europeo (EN).

5.1 Regulación Española

Grado 3

La Orden INT/316/2011 define **Grado 3** *como de riesgo medio/alto, destinado a establecimientos obligados a disponer de medidas de seguridad, así como otras instalaciones comerciales o industriales a las que por su actividad u otras circunstancias se les exija disponer de conexión a central de alarmas o, en su caso, a un centro de control.*

Grado 4

La Orden INT/316/2011 define **Grado 4**, *considerado de alto riesgo, reservado a las denominadas infraestructuras críticas, instalaciones militares, establecimientos que almacenen material explosivo reglamentado, y empresas de seguridad de depósito de efectivo, valores, metales preciosos, materias peligrosas o explosivos, requeridas, o no, de conexión con central de alarmas o, en su caso, a centros de control.*

Se deberán considerar los siguientes:

Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada y sus modificaciones, con posterioridad se publicaron las Órdenes Ministeriales que introducían y desarrollaban el concepto de Grado de Seguridad.

Orden INT/316/2011, de 1 de febrero, sobre funcionamiento de los sistemas de alarma en el ámbito de la seguridad privada.

- Artículo 2. Grados de seguridad de los sistemas.
- Artículo 3. Aprobación de material.
- Artículo 12.2. Alarma confirmada.
- Disposición Transitoria Segunda.
- ANEXOS II y III

Orden INT/314/2011, de 1 de febrero, sobre empresas de seguridad privada.

- Artículo 6. Armeros.
- Artículo 7. Sistema de seguridad de las empresas de depósito.
- Artículo 8. Cámaras acorazadas.
- Artículo 9. Depósitos de explosivos.
- Artículo 12. Locales de centrales de alarmas.
- Artículo 22. Material de instalaciones.

Orden INT/317/2011, de 1 de febrero, sobre medidas de seguridad privada.

- Artículo 1.4.a). Transporte de monedas, billetes, títulos-valores y objetos preciosos.
- Artículo 5. Dispositivos electrónicos de seguridad.
- Artículo 8. Cámaras acorazadas.
- Artículo 9. Cajas fuertes.
- Artículo 10. Cajas y compartimentos de alquiler.

Orden INT/1504/2013, de 30 de julio, por la que se modifica la Orden INT/314/2011, de 1 de febrero, sobre empresas de seguridad privada, la Orden INT/316/2011, de 1 de febrero, sobre funcionamiento de los sistemas de alarma en el ámbito de la seguridad privada, la Orden INT/317/2011, de 1 de febrero, sobre medidas de seguridad privada, y por la que se establecen las reglas de exigibilidad de Normas UNE o UNE-EN en el ámbito de la seguridad privada.

Ley 5/2014, de 4 de abril, de Seguridad Privada.

- Artículo 52.2. Tipos de medidas.

*Orden INT/826/2020, de 3 de septiembre, por la que se modifican en lo relativo a plazos de adecuación de medidas de seguridad electrónica.

Regulación correspondiente a Infraestructuras Críticas

- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
- Resolución de 15 de noviembre de 2011, de la Secretaría de Estado de Seguridad, por la que se establecen los contenidos mínimos de los planes de seguridad del operador y planes de protección específicos conforme a lo dispuesto en el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de infraestructuras críticas. Modificada por Resolución de fecha 29 de noviembre de 2011.
- Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos.
- Guía de Buenas Prácticas del PSO y PPE publicada por CNPIC
- Guía de contenidos mínimos del PSO y PPE publicada por CNPIC.

5.2 Normativa UNE-EN relativa a sistemas electrónicos de seguridad

Seguridad electrónica	
UNE-EN 50131-1	Sistemas de alarma. Sistemas de alarma contra intrusión y atraco. Ver ampliación de la serie UNE 51131 en Anexo I
UNE-EN 60839-11-2:2015/AC:2016	Sistemas electrónicos de alarma y de seguridad. Parte 11-2: Sistemas electrónicos de control de acceso. Guía de aplicación.
UNE-EN 62676-1-1:2015	Sistemas de videovigilancia para utilización en aplicaciones de seguridad. Parte 1-1: Requisitos del sistema. Generalidades
UNE-EN 62820-1-1:2016	Sistemas de intercomunicación de edificios. Parte 1-1: Requisitos generales
UNE-EN 50398	Sistemas de alarma combinados e integrados
UNE-EN 50518	Centro de supervisión y recepción de alarmas

6 Responsabilidad contractual y roles

En el presente capítulo se describen los actores relevantes presentes en la contratación de soluciones de seguridad combinadas e integradas para instalaciones sujetas a cumplimiento grado 3 y 4, en línea con los requisitos que establece la norma UNE-EN 50398.

De forma muy resumida el contrato es el documento que establece las condiciones en la prestación de un servicio entre las partes: cliente y proveedor.

A continuación, se describen los perfiles más relevantes que participan en el esquema de contratación en cada una de las partes:

- Usuario de Seguridad
- Director de Seguridad
- Ingeniero de Seguridad

6.1 Usuario de Seguridad

En este punto se debe recordar que la actividad de planificación de seguridad es competencia del **director de seguridad**, pero también se debe considerar que en el caso de instalaciones de clasificadas **grado 3 o incluso como grado 4,** no todas las empresas sujetas a cumplimiento de medidas están obligadas a disponer de un director de seguridad o departamento de seguridad.

Según establece el artículo 36 2) de la Ley 5/2014, de 4 de abril, de Seguridad Privada "*Los usuarios de seguridad privada situarán al frente de la seguridad integral de la entidad, empresa o grupo empresarial a un director de seguridad cuando así lo exija la normativa de desarrollo de esta ley por la dimensión de su servicio de seguridad; cuando se acuerde por decisión gubernativa, en atención a las medidas de seguridad y al grado de concentración de riesgo, o cuando lo prevea una disposición especial.*

Lo dispuesto en este apartado es igualmente aplicable a las empresas de seguridad privada."

Tenemos, por tanto la problemática asociada al cumplimiento de la normativa asociada a grado de seguridad en instalaciones que requieren de la combinación e integración de diferentes sistemas y tecnologías (fraude, ocupación, ascensores, etc.) o eficiencia energética, sistemas BMS (Building Management System), por parte de una tipología de diferentes usuarios, el correspondiente a grandes empresas y entidades, que por su naturaleza disponen de Departamento de seguridad y/o director de seguridad, y el caso de medianas o pequeñas empresas sujetas al obligado cumplimiento de medidas de seguridad electrónica.

A continuación, se indican la tipología de usuarios sujetos al cumplimiento en grado 3 y 4 más habituales:

- Operadores Críticos (Grado 3 y 4)
- Sujetos de obligado cumplimiento (Grado 3)
- Otros

6.1.1 Operadores Críticos

En la mayor parte de los casos la norma se refiere a instalaciones gestionadas por operadores críticos encargados de gestionar la seguridad de un parque más o menos amplio de instalaciones, o reducido como pudiera ser el caso de los operadores 112 de emergencias o del sector sanitario u otros, donde no todas las instalaciones del catálogo están clasificadas como críticas, pero es recomendable que exista una homogeneidad en los criterios de diseño, instalación, operación y mantenimiento del parque completo.

Cuando hablamos de Infraestructuras Críticas el grado aplicable a las instalaciones de seguridad será el 4, siendo bastante habitual que el resto de las instalaciones consideradas esenciales de un Operador Crítico sean clasificadas como grado 3.

Corresponde a los operadores críticos, según el artículo 13 del Real Decreto 704/2011 entre otras las siguientes:

c) *Elaborar el Plan de Seguridad del Operador y proceder a su actualización periódicamente o cuando las circunstancias así lo exijan, conforme a lo que establece el Capítulo III, Título III del presente reglamento.*

d) *Elaborar un Plan de Protección Específico por cada una de las infraestructuras consideradas como críticas en el Catálogo así como proceder a su actualización periódicamente o cuando las circunstancias así lo exijan, conforme a lo establecido en el Capítulo IV, Título III del presente reglamento.*

e) *Designar a un Responsable de Seguridad y Enlace, en virtud de lo dispuesto en el artículo 34 del reglamento.*

La Ley PIC prevé que los operadores críticos designen a un Responsable de Seguridad y Enlace (y su sustituto) a quien se exige la habilitación de director de seguridad que concede el Ministerio del Interior al personal de seguridad de las empresas de Seguridad Privada en virtud de lo dispuesto en el Real Decreto 2364/1994, o habilitación equivalente, según su normativa específica. Igualmente, se contempla la designación de un Delegado de Seguridad por cada una de las infraestructuras críticas identificadas.

Queda claro que es responsabilidad del Responsable de Seguridad y Enlace del operador crítico la elaboración del correspondiente Plan de Protección Específico (PPE), incluyendo la propuesta de diseño de seguridad o proyecto que incluya los controles de seguridad electrónica.

Es común y cobra todo el sentido que la elaboración de en este tipo de propuestas técnicas más complejas, que incluyen soluciones combinadas de diferentes sistemas, el director de seguridad asuma el rol de cliente y realice el encargo de servicios profesionales a una empresa de ingeniería o profesional de seguridad especializado.

6.1.2 Sujetos de obligado cumplimiento

En el caso de instalaciones Grado 3, no correspondientes a operadores críticos, lo habitual es que se trate de empresas que por su ámbito de actividad estén sujetas al obligado cumplimiento de determinadas medidas de seguridad activas y pasivas de acuerdo a la legislación de seguridad privada vigente. El listado de entidades sujetas a su cumplimiento se establece la Orden INT/317/2011, de 1 de febrero, sobre medidas de seguridad privada.

A diferencia del punto anterior, solamente en casos muy concretos (entidades financieras de crédito, juegos de azar, organización de grandes eventos, centros comerciales, etc.) existe la obligatoriedad de que la empresa disponga de un director o departamento de seguridad integrado en su plantilla, por lo que en el caso pequeños negocios lo más habitual es que la función de seguridad sea asumida por el propietario del negocio o el gerente o responsable de la tienda o local.

En estos casos, donde no existe personal de seguridad habilitado integrado en la plantilla o no se dispone de un conocimiento experto de soluciones de seguridad integradas, es recomendable que la empresa solicite o encargue los servicios profesionales de una empresa, preferentemente de seguridad, especializada en la ingeniería y diseño de soluciones integradas de seguridad para ese tipo de instalaciones.

En estos supuestos el papel del Ingeniero de Seguridad, cobra una especial relevancia pues será el que defina, diseñe y ratifique las medidas de seguridad a implantar y su operatividad y funcionalidad, y quien finalmente certifique que la instalación cumple con las obligaciones contractuales legalmente establecidas frente al propietario y/o usuario de la instalaciones y frente a las correspondientes Unidades de Seguridad Privada encargadas de la inspección, supervisión y control de estas instalaciones.

6.1.3 Otros

Para el resto de los supuestos en los que legislativamente no sea exigible, pero que el nivel de riesgo de la instalación aconseje la implantación de medidas de grado 3, el usuario precisará igualmente de una empresa de seguridad que diseñe, instale y mantenga la instalación correspondiente bajo la supervisión y certificación del Ingeniero de Seguridad de su estructura.

6.2 Director de Seguridad

Según establece el artículo 36 de la Ley 5/2014, de 4 de abril, sobre los directores de seguridad:

1. En relación con la empresa o entidad en la que presten sus servicios, corresponde a los directores de seguridad el ejercicio de las siguientes funciones:

a) La organización, dirección, inspección y administración de los servicios y recursos de seguridad privada disponibles.

b) La identificación, análisis y evaluación de situaciones de riesgo que puedan afectar a la vida e integridad de las personas y al patrimonio.

c) La planificación, organización y control de las actuaciones precisas para la implantación de las medidas conducentes a prevenir, proteger y reducir la manifestación de riesgos de cualquier naturaleza con medios y medidas precisas, mediante la elaboración y desarrollo de los planes de seguridad aplicables.

d) El control del funcionamiento y mantenimiento de los sistemas de seguridad privada.

e) La validación provisional, hasta la comprobación, en su caso, por parte de la Administración, de las medidas de seguridad en lo referente a su adecuación a la normativa de seguridad privada.

f) La comprobación de que los sistemas de seguridad privada instalados y las empresas de seguridad privada contratadas, cumplen con las exigencias de homologación de los organismos competentes.

h) La interlocución y enlace con la Administración, especialmente con las Fuerzas y Cuerpos de Seguridad, respecto de la función de seguridad integral de la entidad, empresa o grupo empresarial que les tenga contratados, en relación con el cumplimiento normativo sobre gestión de todo tipo de riesgos.

Se puede establecer con certeza que el director de seguridad de la empresa o entidad usuaria, debería ser el interlocutor a todos los efectos, encargado de la verificación del cumplimiento del contrato dentro de la empresa o entidad cliente.

En el caso de operadores críticos, como se indica en el punto anterior, el puesto de Responsable de Seguridad y Enlace (RSE) y su sustituto, deben disponer de la preceptiva habilitación de seguridad como director de seguridad y como mejor práctica se recomienda que también disponga de dicha habilitación el Delegado de Seguridad de cada una de las infraestructuras críticas (DSI).

Aunque no es objeto de la presente guía, en el caso particular de los departamentos de seguridad, en los supuestos previstos en el artículo 96.2 del Reglamento (RD 2364/1994) y los servicios y sistemas de seguridad tal y como se describe en los artículos 112 a 117, al frente del departamento habrá un director de seguridad designado por la entidad, empresa o grupo empresarial, que ejercerá las funciones determinadas en los artículos 95, 97 y 98, excepto las previstas en los párrafos d) y h) del artículo 95.

6.3 Ingeniero de Seguridad

Si bien su rol principal es del lado del proveedor, como se describe más adelante, se trata de un perfil polivalente y de alto valor que en el seno de una empresa de seguridad, también puede intervenir a instancia del cliente, asesorando y apoyando en el diseño, implantación y traspaso del proyecto.

En primer lugar la norma UNE-EN 50398 establece en el punto *"4.3 Responsabilidad contractual"* la necesidad de "entregar del sistema integrado completo al cliente y de proporcionar una declaración de funcionamiento frente a la especificación del sistema".

Por lo que en relación con la responsabilidad contractual que establece la norma UNE-EN 50398, el **ingeniero de seguridad** debe asumir la responsabilidad global del diseño de la solución con el objetivo de la entrega completa al cliente y de proporcionar una declaración de funcionamiento frente a las especificaciones del sistema, así como de las desviaciones, si estas existieran.

En segundo lugar tras la entrada en vigor de la Ley 5 2014 de Seguridad Privada se liberalizó la actividad de planificación, consultoría y asesoramiento en materia de actividades de seguridad privada, consistente en la elaboración de estudios e informes de seguridad, análisis de riesgos y planes de seguridad referidos a la protección frente a todo tipo de riesgos, así como en auditorías sobre la prestación de los servicios de seguridad, pasando a ser una actividad compatible, no reservada a las empresas de seguridad privada.

Reseñar el papel fundamental del **ingeniero de seguridad** integrado en la empresa de seguridad responsable del diseño e implantación de la solución como "garante" del anterior requisito a través del **liderazgo técnico del sistema integrado y durante todo el ciclo de vida de la solución**, desde la etapa de Planificación hasta la de Mantenimiento, asumiendo las siguientes responsabilidades *("4.4 Etapas del trabajo")*:

- Planificación: Estudio y especificación de requisitos funcionales adaptados a la estrategia y priorización de riesgos y casos de uso así como selección de tecnologías adecuadas.
- Diseño: Documento de especificaciones funcionales del sistema integrado.
- Implantación: Aclaración de cuestiones relativas a la funcionalidad requerida y justificación de desviaciones y/o ampliaciones consensuadas con cliente.
- Puesta en Marcha: Elaboración del protocolo de pruebas del sistema integrado.
- Verificación del sistema: Control de calidad de la solución integrada.
- Traspaso: Elaboración de la documentación que describa el proceso de transferencia al cliente del sistema integrado.
- Mantenimiento y soporte post-instalación.

Regresando al esquema de contratación, el ingeniero de seguridad debería ser el responsable de la empresa prestadora del servicio (proveedor) con los siguientes condicionantes:

- Ingeniero de seguridad integrado en empresa de seguridad privada en todo el ciclo de vida de la solución, desde la etapa de Planificación hasta la de Mantenimiento.
- Ingeniero de seguridad integrado en empresa cuya actividad sea la planificación y consultoría, en las etapas de planificación y diseño.

En el caso de empresas cuya actividad sea la planificación y consultoría, el ingeniero de seguridad, además de la planificación y diseño, puede prestar al cliente el servicio de dirección facultativa del proyecto de implantación, verificación y traspaso, actuando en nombre del cliente con la limitación de que no puede extender el preceptivo certificado de grado de seguridad, competencia del ingeniero de seguridad integrado en la empresa instaladora de seguridad.

En este punto, tras la etapa de diseño y de cara a la implantación de la solución, se debe considerar la casuística adicional de que el responsable del diseño sea un profesional diferente, no teniendo que ser expresamente el ingeniero de la empresa integradora de seguridad.

Se recomienda como mejor práctica que en el caso de que la empresa instaladora de seguridad no sea la encargada de la redacción del proyecto de diseño, la empresa instaladora tendrá la potestad, a través del ingeniero acreditado, de emitir un **informe de viabilidad y cumplimiento** respecto a las especificaciones solicitadas por cliente, normativa y legislación que incluya la identificación de desviaciones y si procede de la modificación del proyecto de diseño que cumpla con especificaciones solicitadas por cliente, normativa y legislación, dado que de él y de su criterio dependerá la correspondiente certificación final del sistema instalado

En cualquier caso previo a la contratación del servicio es recomendable que el cliente solicite la acreditación de la experiencia y formación del ingeniero de seguridad en el diseño de soluciones combinadas e integradas de seguridad electrónica según el tipo y complejidad de las instalaciones objeto del contrato.

7 Guía de aplicación UNE 50131-7 y criterios generales sistemas de alarma integrados 50398:1

El presente capítulo trata de ser una ayuda que permita avanzar en la problemática asociada a la certificación de soluciones de sistemas integrados de seguridad (G3 y G4) mediante el esquema establecido por la guía de aplicación de la norma UNE 50131-7, que considera los aspectos básicos (estudio de emplazamiento, estudio técnico, etc.) y las fases que pueden ser complementados con los requisitos de aplicación establecidos por la norma UNE 50398.

7.1 Contexto

Tras la publicación de la Orden INT/316/2011, de 1 de febrero, sobre funcionamiento de los sistemas de alarma en el ámbito de la seguridad privada, donde se establecían los denominados "Grados de seguridad de los sistemas" (Art. 2) según Norma UNE-EN 50131-1 y considerando lo indicado en el Art. 3, sobre la "Aprobación de material" sobre el cumplimiento con Normas UNE-EN (sistemas de alarma) o en aquellas otras llamadas a reemplazar a las citadas Normas, aplicables en cada caso y que estén en vigor en su punto 4) y el Anexo I Relación de Normas UNE o UNE-EN que resultan de aplicación en los sistemas de alarma.

La aplicación de la citada norma genera una serie de cuestiones que condicionan la selección de equipos en la fase de diseño para la correcta implantación y certificación de la instalación según establece el Art. 42 del Reglamento (RD 2364/1994).

En el caso de los sistemas de detección de intrusión (IAS) la Orden INT/316/2011 establece un criterio claro, indicando la obligatoriedad de cumplimiento en sus partes o componentes certificables con la preceptiva certificación UNE-EN serie 50131.

Consultadas las correspondientes normas UNE-EN relacionadas con el resto de sistemas complementarios de seguridad no existe la misma unanimidad que en el caso de los sistemas de intrusión y en muchas ocasiones tampoco existe un criterio o guía formal para el diseño de soluciones que combinen diferentes tecnologías, lo que dificulta la "certificabilidad" integral de este tipo de soluciones.

Se indican a continuación los sistemas de seguridad electrónica más habituales, así como la normativa UNE (serie) asociada:

- CCTV- Sistemas de videovigilancia para utilización en aplicaciones de seguridad (UNE-EN 62676)
- Control de accesos (UNE-EN 60839)
- Sistemas de intercomunicación de edificios (UNE-EN 62820)
- Centro de supervisión y recepción de alarmas (UNE-EN 50518)

Adicionalmente también se debe considerar la aplicación de la Ley PIC 8/2011 complementada por el Real Decreto 704/2011, en lo referente a la organización, gestión y toma de decisiones en materia de seguridad en Operadores Críticos.

7.2 UNE-EN 50398-1:2018 Sistemas de alarma. Sistemas de alarma combinados e integrados.

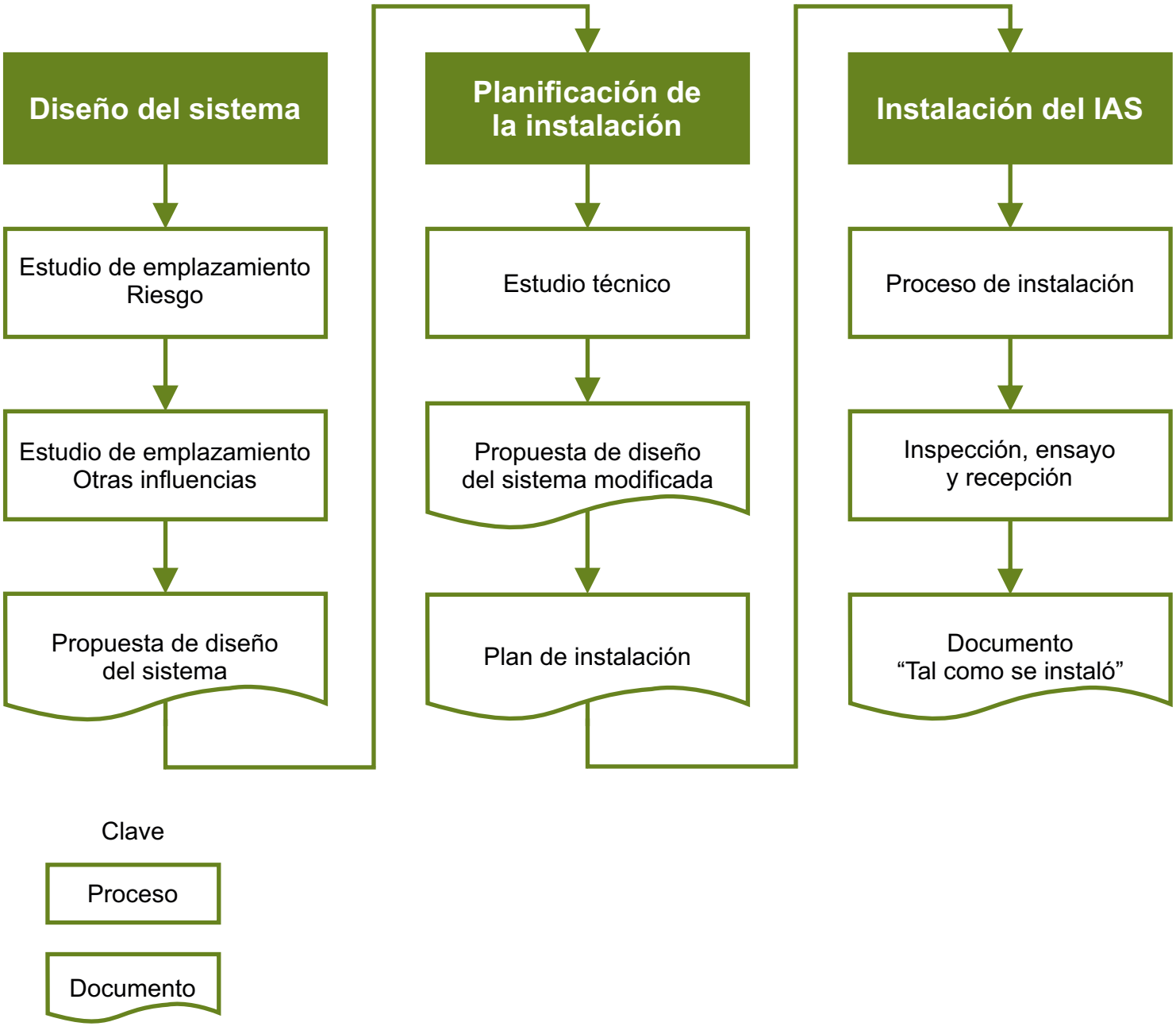
De forma complementaria a la existencia de normas UNE específicas de los sistemas de seguridad anteriormente mencionados o complementarios, la norma UNE-EN 50398 habilita la implantación de sistemas de alarma combinados e integrados mediante la consideración de una serie de requisitos generales y tipos de configuración cuando las aplicaciones que se están integrando son una aplicación de alarma.

En la definición de la norma, se establece que la aplicación de las normas de sistemas específicos (UNE 50131, 62676, etc.) tienen precedencia sobre los requisitos establecidos por la UNE-EN 50398, circunstancia que deberá ser considerada para la "certificabilidad" de la solución integrada. La aplicación de las normas específicas de los diferentes sistemas complementarios de seguridad está fuera del alcance del presente documento.

7.3 Guía de aplicación UNE-CLC(TS_50131-7)

Para el presente documento se parte de la base normativa establecida en la Guía de aplicación UNE-CLC(TS_50131-7), referida a los sistemas de alarma de intrusión, y las normas UNE complementarias en lo referente al cumplimiento de equipamiento e instalación de este tipo de sistemas (5013x-x) que permiten la certificación de las instalaciones conforme a grado y a lo establecido por la Orden INT/316/2011.

En la citada norma se identifican los principales procesos (ver diagrama de flujo a continuación).



Fuente UNE-CLC(TS_50131-7)

Sin entrar en el contenido específico de cada una de las fases, convenientemente descrito en la citada norma UNE-CLC(TS_50131-7), en el presente capítulo nos referiremos a lo indicado en el capítulo 7 **"Diseño del Sistema"** y más en concreto a las siguientes actividades:

- Estudio del emplazamiento
- Propuesta de diseño del sistema (7.5) (Anexo F)

7.4 Estudio del emplazamiento (infraestructuras críticas)

En el caso particular de IICC y de forma complementaria a lo establecido en la norma UNE relativas al *Contenido, Edificio, niveles de supervisión mínimos y otras influencias,* el operador crítico debe contar con una **metodología de análisis de riesgos** que permita identificar y gestionar los principales riesgos a los que se encuentran expuestos los servicios esenciales o IICCs, de forma que las métricas que se utilizan y las estimaciones de los diferentes parámetros (vulnerabilidad, impacto…) sean repetibles y sigan un mismo criterio a lo largo del tiempo para poder obtener valores comparables.

La metodología debería incluir al menos las siguientes fases:

- Identificación y valoración de los activos que soportan los servicios esenciales
- Identificación y evaluación de amenazas
- Valoración y gestión de riesgos

La valoración de los activos estriba, principalmente, en la estimación de las consecuencias derivadas de la interrupción del servicio.

Desde el punto de vista de los criterios para realizar esta valoración se deberá tener en consideración lo establecido por la ley 8/2011 en lo relativo a "criterios horizontales de criticidad".

7.5 Propuesta de diseño del sistema ANEXO F (UNE-CLC TS_50131-7)

El Anexo F relativo a la **"Información a incluir en la propuesta de diseño"** como referencia en la identificación de los puntos en común o que deberían ser considerados cuando se plantean soluciones integradas de seguridad con el objetivo de facilitar la certificación bajo un esquema similar y compatible con el actualmente en vigor relativo a los sistemas de detección de intrusión.

Sobre los puntos del Anexo F se indica a continuación la información complementaria relativa a sistemas integrados de alarma

F3. Grado de seguridad

Identificar el grado de seguridad requerido según Orden INT/316/2011, en este sentido se considerará el asociado al sistema de detección de intrusión.

De forma complementaria, este apartado debería presentar el listado de sistemas de seguridad (o subsistemas) que conforman el sistema de seguridad integrado así como el grado de seguridad asociado, siguiendo el criterio establecido por la preceptiva norma UNE de aplicación (si procede*).

Sirva como referencia que en el caso de CCTV la norma UNE 62676 establece una categorización en grado diferente a la establecida en el caso de intrusión (serie 50131), que deberá ser considerada en las etapas de planificación y diseño de la solución.

*De forma análoga, los sistemas de seguridad no sujetos a norma UNE o categorización en grado no deben impactar en la clasificación global en grado de instalación.

F4. Clase ambiental

Incluir la clase ambiental de los sistemas y sus partes que componen en sistema integrado.

F5. Programa del equipo: Descripción equipos, ubicaciones y coberturas

Referido al listado de equipos que forman parte de la solución integrada.

Se deberá considerar si la propuesta de diseño parte de una especificación inicial del sistema, previamente aprobado por parte del cliente, donde se homologa la combinación de los sistemas que forman parte de la solución integral. (V*er etapa de Planificación y Diseño, especificación inicial del sistema)*

Al tratarse de varios sistemas, este apartado debería incluir información de la arquitectura básica de funcionamiento de cada sistema y de las partes que lo componen.

Este apartado se debería complementar con la información básica de interconexión e interoperación de los sistemas a través de la **especificación funcional de integración**, tal y como se indica en el apartado 4.4.2 de la norma UNE 50398-1:2018,

La propuesta de diseño incluirá la siguiente documentación técnica cada sistema de seguridad (Intrusión, CCTV, CCAA y Centralización):

- Distribución por planta de elementos de campo (detectores, lectores, cámaras, etc.) y cálculo de cobertura y ubicación (CCTV, intrusión).
- Equipos de centralización de sistemas.
- Elementos de red de datos necesarios.
- Detalle de cableado necesario y cálculo de cuadros eléctricos.
- Planos de detalle de los puntos anteriores y unifilar de sistemas de seguridad.

F6. Configuración del sistema

Se debería indicar la correspondencia **de las medidas o controles de seguridad electrónica** incluidas en la solución integrada con los riesgos identificados en la fase de planificación.

Descripción de "interdependencias" entre los sistemas que componen el sistema integrado de seguridad (ver especificación de requisitos funcionales).

Adicionalmente este campo debería incluir el particionado, agrupación o la asociación de dispositivos y zonas de la instalación de cada sistema en la instalación, identificando las condiciones de disparo y activación, el elemento del sistema donde se procesa y/o debe ser centralizada, así como el comportamiento esperado cuando ésta se encuentra activa.

F7. Notificación

Detalles del tipo/s de transmisión de alarmas propuesto y el nombre de la Central de alarmas (si se ha establecido) y/o centro de control donde se enviarán las señales.

Se debería indicar el listado de señales que desencadenan los procesos de verificación por parte del centro de control o central receptora de alarmas. En este sentido se debe especificar el medio de transmisión y protocolo asociado para la transmisión de señales, todo lo anterior sin perjuicio en el cumplimiento de lo establecido para los sistemas de intrusión y la norma técnica correspondiente UNE-EN 50136-x.

En el caso de que la instalación disponga de un centro de control o de videovigilancia se deberá especificar cual es el centro de control externo encargado de su supervisión y las señales y condiciones que provocan la intervención de este último.

F8. Legislación

Ver Marco Normativo (NJ) de la presente guía.

Considerar normativa de seguridad de ámbito local y autonómico.

F9. Normas

Referencia a normas técnicas nacionales (UNE) e internacionales que se han utilizado para el cumplimiento y como mejores prácticas recomendadas.

F11. Certificación

Incluir los certificados de aceptación y conformidad de los sistemas que componen la solución integrada de seguridad.

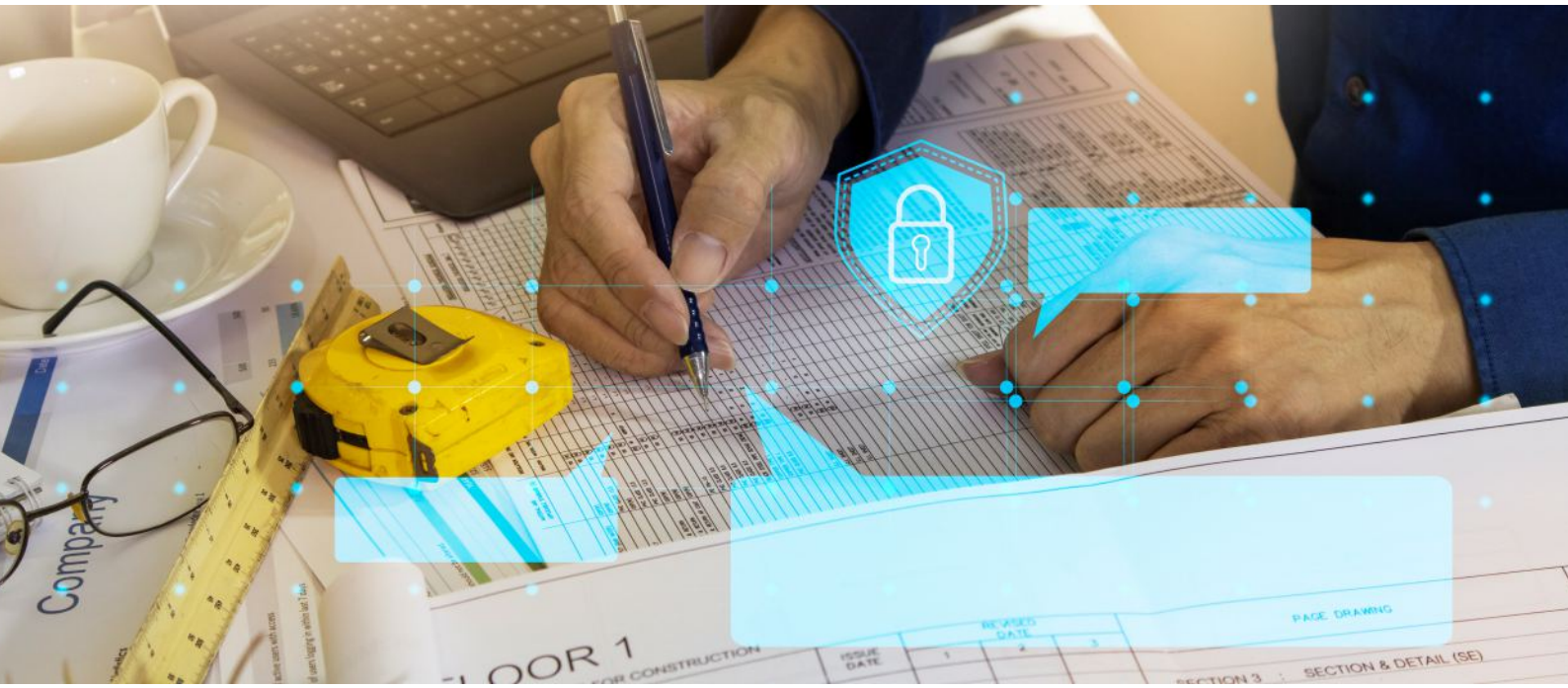
F12. Intervención

Se debe considerar que sobre este tipo de instalaciones (G3 y G4) disponen de una política y marco normativo por lo que se deberán tomar como referencia los procedimientos de operación de seguridad establecidos por el Departamento de Seguridad o responsable de seguridad del cliente (director de seguridad y otros).

En el caso de IICC se deberá consultar y tener en consideración lo establecido en el Plan de Protección Específico y/o Planes de Emergencia y Evacuación, autoprotección de la instalación según la administración normativa vigente en cada ámbito territorial.

En este último caso se deberá considerar los mecanismos de respuesta establecidos en los Planes de Apoyo Operativo, desarrollado por las Fuerzas y Cuerpos de Seguridad competentes en la jurisdicción donde se ubiquen las infraestructuras críticas. El operador crítico deberá tener acceso de forma limitada al contenido de dichos planes para armonizarlos con los PPEs de sus propias instalaciones.

8 Características de la norma UNE 50398 en instalaciones grado 3 y 4



El objetivo del presente capítulo incluye la interpretación de la norma UNE 50398 en lo referente a los aspectos susceptibles de ser considerados sobre el tipo de soluciones requeridas para la protección de instalaciones Grado 3 y 4.

La interpretación trata de ser abierta y flexible de forma que habilite el diseño y certificación de este tipo de soluciones, cuya principal característica es la combinación de sistemas heterogéneos y complementarios de seguridad, en el que no todos suelen estar sujetos a normas específicas de cumplimiento.

Sobre la citada norma según establece el punto *"4.3 Responsabilidad contractual"* reseñar el papel fundamental del **ingeniero de seguridad** integrado en la empresa de seguridad responsable de la implantación como responsable de "entregar el sistema integrado completo al cliente y de proporcionar una declaración de funcionamiento frente a la especificación del sistema".

El **ingeniero de seguridad** ostenta el liderazgo técnico del sistema integrado y su papel es fundamental en todo el ciclo de vida de la solución, desde la etapa de Planificación hasta la de Mantenimiento, asumiendo las siguientes responsabilidades *("4.4 Etapas del trabajo")*:

- Planificación: Especificación inicial del sistema.
- Diseño: Documento de especificaciones funcionales del sistema integrado.
- Implantación: Aclaración de cuestiones relativas a la funcionalidad requerida y justificación de desviaciones y/o ampliaciones consensuadas con cliente.
- Puesta en Marcha: Elaboración del protocolo de pruebas del sistema integrado.
- Verificación del sistema: Control de calidad
- Traspaso: Elaboración de la documentación que describa el proceso de transferencia al cliente del sistema integrado.
- Mantenimiento y soporte post-instalación

Con el objetivo de concretar el papel y actividades del ingeniero de seguridad en las diferentes etapas del ciclo de vida de la solución en los siguientes apartados se describen los aspectos más relevantes:

8.1 Planificación y Diseño

En las etapas de planificación y diseño (apartado 4.4 Etapas de trabajo) se desarrolla la especificación inicial del sistema y especificación de requisitos funcionales.

La especificación inicial del sistema se debe entender como una primera versión del esquema de la solución integrada de seguridad y cuyo objetivo fundamental es la identificación de las medidas técnicas, tecnologías y controles que permiten la consecución de los objetivos específicos sobre la instalación a proteger y responder a la estrategia de gestión de riesgos establecida en la **etapa de planificación** tras conocer el resultado del análisis de riesgos y el estudio del emplazamiento.

La norma UNE-50398 en el apartado 4.4.2 propone una serie de aspectos que debería contener la especificación inicial del sistema como los siguientes:

- Listado de sistemas de seguridad y complementarios ("aplicaciones" según la terminología del documento) y sus requisitos funcionales.
- Objetivos a conseguir mediante la integración de los sistemas
- Características de la ubicación donde se instalará el sistema integrado.
- Tipo de integridad para cada instalación común.
- Clasificación del CCF (Central Control Facility). Este aspecto está con la clasificación del software o aplicativo utilizado por el personal de operación para la gestión sobre los sistemas que componen el sistema integrado de seguridad, lo que comúnmente se denomina PSIM (Physical Security Information Management). La clasificación se deberá corresponder con alguna de las 4 indicadas en el apartado 5.13 de la norma.
- Determinar si son precisas pruebas de ensayo en fábrica o "in situ", comúnmente denominadas pruebas FAT* y SAT**.

Sobre este último aspecto comentar que el objetivo principal de las pruebas FAT y SAT es el de asegurar que el sistema integrado cumple con los requisitos establecidos con el cliente.

En el caso concreto de IICCs, la integridad en la planificación y diseño de las medidas y controles cobra una especial relevancia ya que, según el tipo de integración requerida y dada la complejidad de determinadas instalaciones, es probable que se deban integrar sistemas o equipos "legacy" o nuevos sistemas sobre los que no existe un módulo de integración o "driver" aún disponible, o no está claro si el mismo incluye la funcionalidad deseada, en estos casos es habitual la necesidad de recurrir de forma genérica al API, SDK o protocolo de integración del fabricante.

***FAT** (Factory Acceptance Test) es el proceso de aceptación de un equipo en fábrica. Consiste en un conjunto de **pruebas** ordenadas, protocolizadas y registradas que realiza el fabricante de un equipo, una vez terminada la fabricación y antes de su envío a las instalaciones del cliente.

****SAT** (Site Acceptance Test) Las Pruebas de aceptación del sitio (SAT) son el conjunto de pruebas que se realizarán en el sitio del cliente, es decir, la nueva ubicación del equipo.

Documento de especificación de requisitos funcionales

Tras la validación con cliente de la especificación inicial del sistema desarrollado en la etapa de planificación se debe proceder con la documentación de la **especificación de requisitos funcionales,** tal y como establece el apartado 4.4.3 de la norma en la etapa de diseño, donde se concrete con mayor detalle la información previamente indicada.

Se recomienda que el documento incluya los requisitos del sistema recogido en el apartado 5 de la norma en lo referente al diseño que garantice la correcta operación del conjunto y la integridad con respecto a los objetivos establecidos, en concreto:

- Diseño general, limitando la transmisión de fallos entre los sistemas que componen la solución.
- Niveles de acceso consistentes entre los sistemas que componen la solución.
- Instalación común para control y señalización, considerando la identificación manual de control de alguno de los sistemas y las prioridades en la señalización de la información.
- Integridad de los elementos de tratamiento de alarmas normalizados.
- Interconexión y conexión al sistema de transmisión de alarmas.
- Fuentes de alimentación
- Requisitos de tiempo de respuesta y ocurrencia simultánea de eventos
- Requisitos sobre la supervisión y libro de registro del sistema en las etapas de operación y mantenimiento.

El documento debería incluir el análisis del impacto del fallo de una instalación común sobre el sistema integrado de seguridad y la integridad de los elementos de tratamiento de alarmas normalizados, según lo indicado en el apartado 5.5 de la norma.

Se debe indicar el medio o medios de transmisión de datos que se utilizarán para el envío de información de la instalación, considerando lo establecido por la norma técnica de aplicación a cada una de las instalaciones, diferenciando entre la transmisión de señales de alarma y señales de sistemas complementarios mediante las **prioridades** establecidas en el apartado 5.4.3 de la norma.

Finalmente se debería indicar si para la verificación de la integridad de la solución es precisa la realización de pruebas FAT y/o SAT, o es suficiente con la acreditación de cumplimiento por parte del fabricante o desarrollador de los módulos de integración.

Estudio Técnico

Considerar lo indicado en el Anexo G-50131-7

8.2 Soporte a la implantación, puesta en marcha y verificación de la solución

El papel del ingeniero de seguridad en la etapa de implantación incluye la aclaración de cuestiones relativas a la funcionalidad requerida y justificación de desviaciones y/o ampliaciones consensuadas con cliente.

Así mismo, como responsable de la integridad del funcionamiento lidera la interlocución con el equipo o empresa de desarrollo responsable de la integración de los diferentes sistemas, identificando la aplicabilidad en base al documento de especificaciones técnicas, determinando si existen desviaciones respecto al mismo.

Dentro de la etapa de puesta en marcha se incluye la elaboración del protocolo de pruebas del sistema integrado, necesario para el control de calidad, verificación y entrega de la solución.

La elaboración del protocolo de pruebas deberá tener en consideración el documento de especificaciones funcionales y los cambios o desviaciones consensuados con cliente en las anteriores etapas.

8.3 Traspaso

El ingeniero de seguridad se encarga de la elaboración de la documentación que describa el proceso de transferencia al cliente del sistema integrado.

En función de la complejidad de la instalación y contexto de la organización el proceso de transferencia puede ser abordado en diferentes fases, este aspecto debería haber sido tratado en la contratación por el impacto en la dedicación de recursos involucrados y el tiempo necesario hasta que el sistema pueda ser puesto en producción.

También es posible que el traspaso se realice de forma progresiva a partir de las etapas anteriores de puesta en marcha y verificación del sistema integrado.

El documento de traspaso o entrega a cliente debería contener al menos la siguiente información:

- Verificación de los componentes instalados y de su funcionalidad.
- Verificación del sistema integrado y funcionalidad (según especificación funcional).
- Pruebas FAT y/o SAT, o documentación de fabricante que garantice la funcionalidad.
- Pruebas de alta disponibilidad y redundancia (si son requeridas).
- Manual de operación y mantenimiento.
- Registro de formación de personal de operación y administración de sistemas (si procede).
- Documentación de cumplimiento respecto a normas de aplicación.
- Libro de registro

8.4 Mantenimiento

Para la etapa de "Mantenimiento", si bien cabe la posibilidad de que el cliente se encargue del mantenimiento de los sistemas, incluido el sistema integrado de alarma, se debe considerar que lo habitual es que este servicio sea prestado por una empresa especializada registrada en la actividad de mantenimiento de sistemas de seguridad, según establece el Reglamento (RD 2364/1994).

En este sentido cobra especial relevancia, por parte de las empresas licitantes, de la disponibilidad de un **ingeniero de seguridad** que se responsabilice de la actualización, *modificación y reparación del sistema integrado de seguridad*, tal como indica el punto 4.4.8 de la norma y que esta circunstancia sea tenida en consideración por parte del cliente en el momento de la licitación del servicio.

9 Requisitos del sistema en instalaciones

Tal y como se plantea en el objeto del presente documento, la pretensión es contribuir en la estandarización de requisitos y a una mejor interpretación en lo referente al alcance que debe ser considerado en fase de diseño de sistemas en grado 3 y 4 para que no existan dudas en la fase de instalación y en consecuencia en la expedición del preceptivo certificado en grado 3 y 4 por parte de la empresa instaladora de seguridad.

Sin embargo, el diseño de este tipo de soluciones de seguridad, resultado de la combinación de diferentes tecnologías, plantea dudas en el aspecto normativo, al confluir diferentes normas y estándares.

Abordar el diseño e instalación de un sistema de seguridad de una infraestructura crítica, esencial o estratégica, instalaciones todas ellas calificadas de Grado 3 o incluso Grado 4, plantea importantes retos en las distintas fases del proyecto de instalación de un sistema de seguridad.

En cualquier caso debemos partir de:

- que el análisis de riesgos previo ya ha sido realizado
- que las posibles vulnerabilidades de nuestra instalación han sido analizadas
- y que las correspondientes amenazas han sido debidamente valoradas en el correspondiente Plan de Protección.

De esta manera podemos asegurar que tenemos claro lo que vamos a proteger y de qué o de quién vamos a protegernos, analizando también las implicaciones y las características orográficas, geográficas, climáticas, demográficas, socioeconómicas, etc. de nuestra instalación.

9.1 Diseño general

Partiendo del conocimiento de estos datos previos iniciaremos la fase de diseño de nuestro sistema, sobre la que centraremos nuestros esfuerzos en el presente estudio pero para la que también deberemos considerar de manera decisiva, la naturaleza estratégica de la instalación a proteger, en las posteriores fases de implantación (ejecución de la instalación del sistema), operación y su posterior mantenimiento.

Un adecuado diseño condicionará absolutamente las citadas fases posteriores del proyecto.

Siguiendo la guía de buenas prácticas editada por el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) para la Elaboración de los Planes de Protección Específicos (PPE), el diseño del sistema de seguridad se deberá establecer con una protección multi-capa.

Un modelo de protección de acuerdo con el principio de "defensa en profundidad" en el que se aplicarán controles complementarios y superpuestos para lograr un mayor grado de protección.

Por ello, en línea con lo expuesto en la guía indicada, es conveniente articular la compartimentación de zonas de protección conforme a las necesidades de cada instalación, considerando al menos tres capas o zonas de protección, tanto en el ámbito físico que nos ocupa en el presente estudio como en el ámbito de la seguridad lógica.

Previa a la adopción de la compartimentación indicada hemos decidido continuar el análisis partiendo de dos premisas fundamentales para el diseño de un sistema. En primer lugar el sistema global debe ser conceptuado buscando su mayor efectividad y en segundo lugar debe estar basado en distintos niveles de riesgo.

- **Premisa de efectividad**, de los sistemas de seguridad en la que debemos optimizar criterios como la eficacia (funcionalidad), la eficiencia, la fiabilidad, la facilidad de mantenimiento, la sostenibilidad, la capacidad de adecuación a situaciones cambiantes, la durabilidad, la capacidad de recuperación frente a situaciones no previstas (resiliencia), etc.
- **Niveles de riesgo** que dentro de la naturaleza de las infraestructuras a proteger, se habrán establecido en la correspondiente identificación, análisis y evaluación de riesgos del Plan de Protección Específico (PPE) en función de las características de las diferentes áreas de la instalación, de su ubicación, de su criticidad, de su accesibilidad, de la presencia de personal, etc. (ver UNE-CLC/TS_50131-7=2005_V2 Guía Aplicación Sistemas de Alarma de Intrusión).

De acuerdo a la OM/316/2011, artículo 2.1.d, los Grados de seguridad de los sistemas a instalar en las denominadas infraestructuras críticas, serán de Grado 4. Esto es equivalente a instalaciones de alto riesgo, de acuerdo a los niveles de riesgo establecidos en la Norma UNE-EN 50131-1 (punto 6, Grados de Seguridad), de esta manera todo equipamiento a incorporar en el diseño de estas instalaciones debe estar certificado respecto a esta norma.

En correspondencia a estas dos premisas y a la compartimentación indicada, el presente capítulo aborda de forma orientativa los subsistemas convencionales de seguridad electrónica estableciendo en cada caso la conveniencia o no de la adopción de las posibles alternativas.

El diseño de cada subsistema tras el análisis descrito, se inicia con la elección de los elementos de protección que más se adecuen a las condiciones y características de la instalación.

En cada una de las zonas de protección establecidas se seleccionarán los elementos que bajo la premisa establecida de mayor efectividad, optimicen el aseguramiento de la detección y, mediante la configuración e interconexión adecuada, proporcionen el funcionamiento deseado.

Los subsistemas objeto de análisis en el presente estudio deberán ser complementados por medios de protección de seguridad física, cuya función esencial será proporcionar el retardo suficiente en la posible intrusión para que esta pueda ser detectada mediante los medios de protección electrónica por los sistemas de detección o de control de accesos, verificada por los sistemas de supervisión (p.e: Circuito Cerrado de Televisión), gestionada por los sistemas de Centralización y Gestión y pueda posibilitar la respuesta adecuada por subsistemas auxiliares como los de interfonía, megafonía, de iluminación u otros. Todo ello encaminado a garantizar la respuesta adecuada en tiempo y forma por los medios de respuesta personales (públicos y privados) no contemplados en este estudio.

Especial atención merecen en este estudio los sistemas que por su naturaleza posibilitan el funcionamiento de los subsistemas descritos y que a su vez son procesos básicos del mantenimiento del estado operativo de la organización que protegemos. Nos referimos por ejemplo al cableado de líneas de alimentación, a los sistemas de comunicaciones, a las interconexiones de señales de los distintos subsistemas de seguridad física, a los enlaces con los centros de control, a los puestos de vigilancia móviles o fijos, a los sistemas de alimentación eléctrica, etc.

No entraremos en la temporalidad o permanencia de los distintos subsistemas, dado que ello dependerá de la variabilidad del nivel de riesgo de nuestra instalación o de alguna parte de ellas y la consiguiente adaptación de nuestro sistema al citado nivel.

9.2 Modelo de Protección Multi-capa

En línea con lo expuesto, el criterio adoptado es el modelo de protección multi-capa. De acuerdo a dicho modelo nuestra instalación contará con una primera capa externa, que vendrá definida por un perímetro, que definiremos como el conjunto natural limitado que, en su conjunto, rodea o encierra un interés de seguridad en particular o blanco potencial completo. La protección que aplicaremos a dicho área la denominaremos en adelante protección perimetral y a los sistemas, elementos o subsistemas a implementar en dicho área, sistemas, elementos o subsistemas perimetrales.

Los controles físicos en la capa protectora externa o perimetral pueden consistir en vallas u otras barreras de protección, iluminación, señales y sistemas de detección de intrusos. Es el punto más externo en el que se utilizan las medidas de seguridad física para disuadir, detectar y retardar.

La capa media, vendrá definida por las superficies próximas a los edificios de nuestra instalación, los contornos de nuestras edificaciones, con las vulnerabilidades propias de los elementos practicables, como puertas, tragaluces o ventanas, y de los no practicables, como muros de construcción o superficies acristaladas. La protección que aplicaremos a esta área la denominaremos protección periférica y puede consistir en sistemas de iluminación de protección o sorpresiva, sistemas de detección de intrusión, cerraduras, rejas en puertas y ventanas, señales y barreras, protección de los tragaluces y los conductos de ventilación, sistemas de detección de penetración por suelos, paredes o techos, etc.

Por último, la capa o capas interiores, están diseñadas para hacer frente a un intruso que ha penetrado las capas de protección perimetral y periférica, pretende asegurar la detección y proporcionar la información necesaria para facilitar el seguimiento de la intrusión, para mantener localizado en todo momento al intruso.

9.2.1 Área perimetral

Según adelantábamos, por detección perimetral se entiende todo sistema de seguridad que, instalado en los límites de un espacio al aire libre, es capaz de detectar, localizar, visualizar o señalar cualquier intento de intrusión a través de la superficie o línea que determina el contorno de dicho espacio.

Indudablemente la precocidad en la detección constituye una ventaja decisiva de la vigilancia perimetral, favorece la interpretación de la intencionalidad del intruso o la puesta en fuga de éste, antes de que pueda aproximarse peligrosamente al bien a proteger.

Las condiciones ambientales desfavorables (nieve, granizo, niebla, animales en movimiento, objetos transportados por el viento, etc.) constituyen factores capaces de influenciar en la tasa de falsas alarmas, tanto más si el diseño del sistema y la elección, montaje o utilización de los elementos no se llevan a cabo considerando minuciosamente las exigencias y posibilidades reales de estos equipos y del entorno en el que deberán funcionar.

Si para la vigilancia en espacios cerrados se cuenta habitualmente, a efectos de detección, con fenómenos físicos característicos de la intrusión (apertura de puertas o ventanas, fractura de muros, desplazamientos del delincuente a través de zonas perfectamente delimitadas, etc.) en la vigilancia de zonas al aire libre, esta fenomenología no siempre resulta tan claramente perceptible para los equipos de detección ya sea porque la sensibilidad de los mismos deba reducirse para limitar las alarmas intempestivas o porque el criterio de detección resulte excesivamente selectivo y por ello incapaz de captar todas y cada una de las alternativas de que dispone el intruso (túnel bajo tierra, acceso por encima de la zona de vigilancia, fractura o escalo de la cerca, por el aire o buceando bajo la lámina de agua, etc.)

Teniendo en cuenta las prestaciones de los equipos de detección perimetral desarrollados hasta la fecha, no existe el "procedimiento ideal" capaz de resolver satisfactoriamente todos los casos de vigilancia en el exterior. Será necesario por lo tanto dado el elevado nivel de riesgo de las infraestructuras estudiadas y la predisposición a provocar alarmas injustificadas, que la protección perimetral de las infraestructuras críticas se proyecte conjugando las diferentes bondades de los distintos subsistemas de manera que se complementen mutuamente funcionando de manera coordinada. Especialmente relevante en esta área son los Sistemas de viodeovigilancia.

9.2.2 Área periférica

La protección periférica difiere de la perimetral en que su empleo queda limitado a las inmediaciones de edificaciones, en zonas menos influenciadas por el factor climatológico y ambiental.

Tras los sistemas de protección perimetral, los de tipo periférico son los que detectan el intento de intrusión con mayor precocidad, posibilitando con ello la activación de la alarma antes de que la proximidad del intruso al bien o a la zona más conflictiva, pueda resultar peligrosa.

Por concepto, los detectores empleados para la vigilancia de la periferia deben instalarse en lugares que frecuentemente están expuestos a condiciones ambientales particularmente desfavorables: la proximidad de personas, las trepidaciones ocasionadas por el paso de vehículos, las vibraciones provocadas por fenómenos meteorológicos, etc., y por lo tanto resultan especialmente perceptibles en los límites de la zona a vigilar, sobre todo cuando dichos límites coinciden con la línea de cerramiento del edificio. Los sistemas de control de acceso cobran especial relevancia en esta protección junto a los Sistemas de viodeovigilancia.

9.2.3 Área interior

Este tipo de detección es la más conocida y desarrollada, y a la que debido a su controlado campo de actuación más fiabilidad se le exige, dentro de ella los detectores volumétricos son los más característicos.

Se entiende por detección volumétrica todo sistema de vigilancia capaz de captar el desplazamiento del intruso, utilizando para ello una zona de influencia tridimensional, que cubra por lo menos un 80% del volumen del local a vigilar. Este sistema es también conocido como detección de movimientos, constituye una de las grandes familias de detectores denominados de presencia, junto a los de rotura y apertura.

Cualquiera que sea el procedimiento volumétrico elegido, el mismo está diseñado para captar el desplazamiento del intruso a partir de las perturbaciones que origina dicho movimiento en las condiciones ambientales.

Por lo general, son sistemas altamente seguros en cuanto a su aptitud para la detección, a pesar de que por captar fenómenos de naturaleza compleja y por emplear tecnología sofisticada capaz de detectar variaciones en la energía infrarroja, en el supuesto de detectores PIR de infrarrojos) o el análisis de ondas de baja amplitud y rangos de alta frecuencia, en los supuestos de detectores de microondas.

Al igual que en las protecciones precedentes los Sistemas de Viodeovigilancia como elemento de apoyo y verificación e incluso de detección y análisis, se presentan en la protección interior como elemento irrenunciable para el tipo de instalaciones que nos ocupa.

9.3 Subsistemas de seguridad electrónica convencionales

Como ya hemos indicado, en esta guía no abordaremos las Medidas de Protección Pasivas, es decir las encargadas de dificultar o retardar la materialización del riesgo, centrándonos en las Medidas de Protección Técnicas Activas o Electrónicas, que serán las encargadas de detectar e informar de la presencia de un riesgo.

A la amplia variedad de Medidas Técnicas Activas, que se diseñan y fabrican con el fin específico de servir a la seguridad de las personas y de los bienes, las vamos a denominar genéricamente Sistemas Electrónicos de Seguridad, y las definiremos como el conjunto de elementos electromecánicos y electrónicos que relacionados entre sí por una adecuada instalación nos proporcionan una información que contribuye al incremento del nivel de seguridad de un determinado entorno.

En esta categoría englobaremos todos los dispositivos y sistemas electrónicos que la tecnología actual pone a disposición de la protección contra los riesgos de carácter antisocial, tales como robo, atraco, hurto, sabotaje, secuestro, incendio, ataque a la Información, etc.

De todos ellos en el presente estudio nos centraremos en los **subsistemas de protección de intrusión, control de accesos, de videovigilancia y los de centralización.**

El procedimiento para el análisis de todos ellos, debe partir de una sinopsis previa que presente en una tabla o similar de manera esquemática y simplificada los elementos, componentes y/o características más significativas de cada subsistema, incluyendo una recomendación para su instalación en instalaciones de Grado III y Grado IV y especialmente en la protección de Infraestructuras Críticas, en áreas con niveles de riesgo diferenciados.

Esta metodología permite identificar y recomendar la utilización de uno u otro elemento en función del nivel de riesgo asignado a la zona donde se pretende instalar, existiendo elementos o detectores cuya instalación no sea recomendable en instalaciones o áreas de un nivel de riesgo alto pero sean asumibles en niveles de riesgo bajo.

Para el establecimiento de la recomendación para cada caso, se debe valorar su efectividad, evaluando conceptos como la eficacia, la fiabilidad o la resiliencia, asumiendo en cualquier caso que esta recomendación se realiza de manera genérica para cada elemento sin entrar en la casuística de que pudieran existir marcas o modelos concretos que pudieran presentar variaciones sustanciales en la valoración global.

9.3.1 Subsistemas de protección de intrusión

Cuando hablamos de subsistemas de protección de intrusión electrónicos podemos establecer tres grupos diferenciados, en función del papel principal que desempeñan en la globalidad del sistema de seguridad planteado en el Plan Específico de la Instalación que nos ocupa.

El primero y más extenso, recoge aquellos sistemas cuya función esencial es la Detección, el segundo agrupará los subsistemas preferentemente disuasorios y en tercer lugar los de supervisión. Todos ellos en cualquier caso podrán disponer de las funciones indicadas en mayor o menor medida.

9.3.1.1 Sistemas de detección de intrusión.

Básicamente un sistema de detección de intrusión, con independencia del tipo de instalación, está compuesto por un subsistema de alimentación, un subsistema de cableados o interconexionados, los sensores o detectores, los señalizadores y el subsistema de centralización.

Este esquema será prácticamente idéntico en los subsistemas de control de accesos, de videovigilancia, megafonía o interfonía, por lo que será el planteamiento a seguir de manera general en este estudio, prestándose una atención particular con un apartado individualizado para los subsistemas de cableados, alimentación eléctrica o de centralización.

De esta manera el criterio elegido para el análisis de los sistemas de detección de intrusión, será el ya adelantado en el *Modelo de Protección Multi-capa*, de acuerdo al que se establecía un área de detección perimetral que plantea una primera capa externa definida por nuestro perímetro y sus inmediaciones, y en el que en consecuencia se instalarán los detectores perimetrales, según se expone en la tabla 1.

Los detectores son los dispositivos encargados de informar a la central de alarmas o subsistema de centralización, de las variaciones en la magnitud que supervisan en las áreas protegidas, entendiendo por central de alarmas el equipo auto protegido, que integrado en un sistema electrónico de seguridad, es capaz de recibir y controlar información y generar señales de comunicación y/o de otros dispositivos.

De acuerdo a la naturaleza de las instalaciones objeto de protección, el nivel de protección asignado de acuerdo a la Norma UNE 50131-7 será, Grado 4 equivalente a Riesgo alto, donde la seguridad tiene prioridad sobre todos los demás factores. Se esperan intrusos con capacidad para planificar una intrusión con detalle y que dispongan de una gama completa de herramientas y equipos, incluyendo incluso medios de sustitución de componentes vitales del sistema.

De manera equivalente la legislación de seguridad privada recoge en la OM INT/316/2011 que el citado grado 4 considerado de alto riesgo, estará reservado entre otros a las denominadas infraestructuras críticas.

La normativa por tanto recogida en nuestra legislación refuerza la premisa expuesta de la fiabilidad de los sistemas a utilizar, garantía que en muchos casos y dada la no existencia de equipamiento con la certificación en grado 4, requerirá de procedimientos y algoritmos lógicos que sumando la sensibilidad de dos o más detectores, no penalice su fiabilidad. Se pretende por lo tanto, detectar más con mayor seguridad y con menos falsas alarmas.

Para ello en la tabla de detectores (ver Tabla 1) que se acompaña se incluyen tres distintas clasificaciones para los distintos tipo de detectores, con criterios complementarios que posteriormente posibiliten el uso conjunto de dos o más de ellos, con funcionamiento con lógica Y (And) y/o O (Or), áreas de detección solapadas y principios de funcionamiento diferente. De esta manera su utilización conjunta garantizará la máxima fiabilidad en la detección con los planteamientos lógicos adecuados de detección en una ventana de tiempo determinada.

La primera clasificación que se propone se basa en el criterio de la actitud del propio detector. De acuerdo a esto estableceremos:

- Detectores Activos (A, en la tabla): Aquellos que "generando una onda", evalúan posteriormente las modificaciones que en ella se producen para determinar si existe o no una situación susceptible de ser considerada como alarma. (Efecto Doppler).

- Detectores Pasivos (P, en la tabla): Aquellos que "no generan nada", sino que evalúan parámetros existentes en el medio que controlan y analizan sus fluctuaciones para determinar la existencia o no de una situación de alarma.

La segunda de las clasificaciones que vamos a utilizar se basa en el criterio de la zona de vigilancia del propio detector, entendiendo ésta como el espacio geométrico que vigila el detector. De acuerdo a esto existen Detectores Puntuales (P en la tabla), Detectores Lineales (L), Detectores Planares (S) y Detectores Volumétricos (V).

La tercera y última, y quizás la más extendida de todas ellas, se realiza en torno al criterio del emplazamiento o ubicación del detector, criterio ya elegido en el establecimiento de las áreas de implantación de las medidas expuesto en apartados anteriores, de acuerdo al que existirán Detectores Perimetrales, Detectores Periféricos y Detectores de Interior.

Basándose en estas clasificaciones, en la tabla 1 indicada, se incluyen cada uno de los detectores de las distintas áreas, estableciendo por ejemplo si se trata de un detector perimetral activo superficial o estamos hablando de un detector pasivo lineal. Estas circunstancias son las que deberemos tener en cuenta a la hora de solapar dos o más detectores, previendo que su principio de funcionamiento no pueda verse afectado por las mismas posibles interferencias meteorológicas, ambientales o intencionales. Preferentemente solaparemos un detector activo con uno pasivo, y un detector superficial con uno volumétrico, o un perimetral de superficie con uno enterrado, etc.

TABLA 1 (1)

DETECCIÓN PERIMETRAL

ESPACIO	UBICACIÓN		SISTEMA / ELEMENTO / DETECTOR	CLASIFICACIÓN DEL DETECTOR A/P	P/L/S/V	P/PF/I	INSTALACIÓN ESTRATÉGICA CON NIVEL DE RIESGO : ALTO	MEDIO	BAJO
Aire			Radares.	A	V	P	®		
			Análisis de vídeo	P	V	P/ PF / I	®		
Tierra	Superficie	Sobre Valla	Sistemas de Variación Tensión Mecánica.	P	L	P	®		
			Sistemas Inerciales.	P	S	P / PF		®	
			Sistemas de Cable Sensor (triboeléctrico, Microfónico, Magnético…)	P	S	P / PF		®	®
			Sistemas de detección de pérdida de continuidad	P	L	P / PF			®
			Sistemas de Fibra óptica	A	L	P / PF		®	®
			Sistemas de Campo Eléctrico. Radiofrecuencia – Capacitivos.	A	V	P	®	®	
		Junto A Valla	Sistemas de Campo Eléctrico – Radiofrecuencia – Capacitivos.	A	V	P	®	®	
			Barreras de Infrarrojos	A	S	P / PF		®	®
			Detectores de Infrarrojos Pasivos	P	v	P / PF		®	®
			Barreras de Microondas.	A	V	P		®	®
			Radares	A	V	P	®	®	
			Sistemas Laser	A	S	P	®	®	
			Análisis de vídeo.	P	V	P/ PF / I	®	®	®
	Enterrados		Presión – Neumáticos.	P	S	P	®	®	
			Campo Eléctrico – Radiofrecuencia.	A	V	P	®	®	
			Fibra óptica	A	S	P	®	®	
			Geófonos.- Geo-sísmicos	P	V	P	®	®	
Agua	Superficie / Lámina de Agua		Radares.	A	V	P	®		
			Análisis de vídeo.	P	V	P / PF /I	®	®	®
			Boyas / barreras flotantes sensorizadas	P	S	P	®	®	
	Subacuáticos		Sonares.	A	V	P	®		
			Radares.	A	V	P	®	®	
			Rejas y redes sensorizadas	P	S	S	®	®	

OBSERVACIONES	RECOMENDACIONES
Sistemas de alto coste.	Importancia en la definición del alcance de detección y del tamaño del objeto a detectar.
Importantes limitaciones en función de las condiciones meteorológicas.	Limitar su utilización a espacios muy delimitados
Importancia del estado y naturaleza del vallado sobre el que vayan montados, especialmente los sensores superficiales. Importante adaptabilidad a la orografía del terreno. Importancia cuando se pretende detectar antes de acceder al interior de los límites de la propiedad.	Precaución con vegetación próxima y con elementos próximos que posibiliten su salto. Precaución con la obtención y mantenimiento de una buena toma de tierra continua en Sistemas de Campo Eléctrico, Radiofrecuencia o Capacitivos. En instalaciones de alto riesgo se recomienda la instalación de dos o mas anillos de seguridad perimetral, basados en sistemas con distintos principios de funcionamiento y distintas áreas de detección, pero con la misma zonificación. Preferentemente un detector enterrado y uno o mas de superficie, al menos uno pasivo (P) y uno activo (A), y preferentemente uno volumétrico (V) y uno superficial (S).
Importantes limitaciones en función de la orografía del terreno, especialmente con vados y cambios de nivel, y la proximidad de vegetaciones cercanas. Prevalencia del factor disuasorio sobre el factor sorpresa.	Importancia del Circuito Cerrado de Televisión que posibilite la verificación y el seguimiento de la posible intrusión, y además permita la implantación de sistemas de análisis de video asociado a las imágenes captadas. En instalaciones de alto riesgo se recomienda la instalación de dos o mas anillos de seguridad perimetral, basados en sistemas con distintos principios de funcionamiento y distintas áreas de detección, pero con la misma zonificación. Preferentemente un detector enterrado y uno o mas de superficie, al menos uno pasivo (P) y uno activo (A), y preferentemente uno volumétrico (V) y uno superficial (S).
Importante analizar la naturaleza y tipos del terreno, y los cambios de composición en la definición de zonas. Prevalencia del factor sorpresa. Sistemas mas inmunes a las variaciones ambientales y meteorológicas.	
Importante incidir en modelos tierra/agua.	Importancia del Circuito Cerrado de Televisión que posibilite la verificación y el seguimiento de la posible intrusión, y además permita la implantación de sistemas de análisis de video asociado a las imágenes captadas.
Analizar posibles zonas de brumas y nieblas.	
Incorpora una barrera física a la propia detección	
Analizar problemática de las comunicaciones inalámbricas entre detectores.	Especialmente diseñado para la detección de buceadores y de vehículos submarinos tripulados y no tripulados
Incorpora una barrera física a la propia detección	

TABLA 1 (2)

	ESPACIO	UBICACIÓN	SISTEMA / ELEMENTO / DETECTOR	CLASIFICACIÓN DEL DETECTOR A/P	P/L/S/V	P/PF/I	INSTALACIÓN ESTRATÉGICA CON NIVEL DE RIESGO : ALTO	MEDIO	BAJO
DETECCIÓN PERIFÉRICA	Periferia: Puertas, Ventanas, Muros…. (Elementos Practicables y no Practicables)	Detectores de rotura	Sísmicos	p	S	P	®	®	
			Detectores Rotura de vidrio activos.	P	S	P	®	®	®
			Detectores Rotura de vidrio pasivos.	P	V	P / PF / I	®	®	®
		Detectores de apertura	Contactos y Balances Magnéticos	P	P / S	P / PF / I	®	®	®
			Finales de Carrera -Disp. Electro-mecánicos	P	P / S	P / PF / I		®	®
DETECCIÓN DE INTERIOR	Interiores	Detectores de Presencia	Detectores Infrarrojos	P	V	I	®	®	®
			Detectores de Microondas	A	V	I		®	®
			Detectores Duales Infrarrojos y Microondas	P	V	I	®	®	®
			Detectores de Ultrasonidos	A	V	I			®
			Detectores laser	A	V	I	®	®	
SISTEMAS DISUASORIOS			Iluminación Sorpresiva	A	V	P / PF			®
			Sistemas de Megafonía	A	V	P / PF	®	®	®
			Generadores de humo	A	V	I	®	®	®
			Cañones Sónicos Aéreos	A	V	P	®		
			Cañones Sónicos Subacuáticos	A	V	P	®		
SISTEMAS DE SUPERVISIÓN Y VIGILANCIA			Drones (UAS - RPAS)	A	V	P / PF / I	®		
			Vehículos subacuáticos no tripulados (UUS)	A	V	P	®		

Detector Activo	*A*	*Detector Puntual*	*P*	*Detector Perimetral*	*P*
Detector Pasivo	*P*	*Detector Lineal*	*L*	*Detector Periférico*	*PF*
		Detector Superficial	*S*	*Detector de Interior*	*I*
		Detector Volumetrico	*V*		

OBSERVACIONES	RECOMENDACIONES
Utilización equipamiento con homologación en GRADO 4 para IC	Se recomienda la adopción de detectores de rotura y apertura en todos los elementos aperturables.
Utilización equipamiento con homologación en GRADO 4 para IC	
Utilización equipamiento con homologación en GRADO 4 para IC	Evaluar la conveniencia de lógicas OR ó And en los detectores duales.
Generan una respuesta " normalmente" molesta al posible intruso que dificulta o imposibilita su actuación	No recomendado en IC, proporciona mas posibles beneficios que inconvenientes a un intruso profesional
	A evaluar en función de la capacidad de respuesta de la propia IC
Posibilidad de incorporar detectores y sistemas adicionales a los de supervisión	Evaluar posibles contramedidas por los riesgos que supone su utilización por el intruso

Centrándonos en el **área perimetral** en primer lugar se plantea la protección del espacio aéreo, en segundo la protección en tierra, bien sea ésta en superficie o en subsuelo y el tercero, en caso de su existencia, en el lado agua, donde se prestará atención a la detección sobre la lámina de agua o bajo ella.

Dado que la precocidad en la detección constituye una ventaja decisiva de la vigilancia perimetral, cuando se aborda la protección de una infraestructura clasificada como crítica se considera recomendable la instalación de algún sistema que permita la detección con anterioridad a la aproximación al vallado o linde de limitación de nuestra infraestructura crítica de manera que pueda establecerse un área de seguridad previa. Esta circunstancia, de detección sin protección física condiciona de manera decisiva la generación de alarmas no deseadas, que precisan de manera imprescindibles de los correspondientes sistemas de verificación por medios técnicos como los sistemas de videovigilancia o por medios personales a través de los medios de respuesta de la instalación.

Especial atención en esta área cobran los sistemas de videovigilancia que abordaremos posteriormente en un apartado específico.

Las condiciones ambientales desfavorables (nieve, granizo, niebla, animales en movimiento, objetos transportados por el viento, etc.) constituyen factores capaces de influenciar en la tasa de falsas alarmas, tanto más si la elección, montaje o utilización del sistema no se llevan a cabo considerando minuciosamente las exigencias y posibilidades reales de estos equipos y del entorno en el que deberán funcionar.

Esta circunstancia, aparte de exigir todo tipo de precauciones y meticulosidad en la realización del proyecto y de la propia instalación, obliga a considerar las respuestas del sistema como indicaciones de alerta, no pudiéndose interpretar como señales de alarma, en tanto no se haya comprobado el origen de las mismas. (Importancia de la videovigilancia para reforzar la función de verificación).

Ya en las proximidades del perímetro físico (vallado o muro) se podrán plantear sistemas perimetrales de superficie sobre el vallado o el muro o junto a él, posibilitando las alternativas que deberán ser analizadas sobre el contexto de cada instalación.

La valla metálica o similar, en definitiva cualquier elemento constructivo elástico capaz de transmitir vibraciones, tiene una doble función. Primero obstaculizar y retardar la intrusión y en segundo lugar, soportar al sistema de detección, de forma que éste pueda detectar las vibraciones que se originan en los intentos de intrusión a través de la misma.

Tanto los detectores instalados sobre la valla o muro de delimitación, como los instalados en superficie junto a ella, presentan junto a su principal función de detección una importante función disuasoria.

En la gran mayoría de los casos la adopción de detectores perimetrales de superficie ubicados junto al vallado exige con frecuencia trabajos adicionales de preparación del terreno, que debe ser llano y exento de vegetación en la zona de detección.

Por el contrario los detectores perimetrales enterrados, no gozan de la función disuasoria aportando como factor adicional al de la propia detección el sorpresivo. Como característica fundamental de este tipo de detectores es su total adaptabilidad a prácticamente cualquier tipo de topografía.

9.3.1.2 Sistemas disuasorios.

El segundo conjunto de subsistemas son los denominados sistemas disuasorios cuya principal prioridad es provocar el abandono en la intención agresora en el potencial intruso. Al margen del efecto disuasorio presente en muchos de los sistemas perimetrales tanto activos como pasivos, de forma preferente en estos últimos, en este conjunto de sistemas incluiremos sistemas reactivos cuyo funcionamiento y efectividad dependerá fundamentalmente de los sistemas de detección perimetral.

La función disuasoria se debe perseguir preferentemente en el área perimetral previa a nuestro perímetro, mediante actuaciones acústicas y/o visuales.

TABLA 2

		CLASIFICACIÓN DEL DETECTOR			INSTALACIÓN ESTRATÉGICA CON NIVEL DE RIESGO :				
SUBSISTEMA	SISTEMA / ELEMENTO / DETECTOR	A/P	P/L/S/V	P/PF/I	ALTO	MEDIO	BAJO	OBSERVACIONES	RECOMENDACIONES
SISTEMAS DISUASORIOS	Iluminación Sorpresiva	A	V	P / PF			®	Generan una respuesta "normalmente" molesta al posible intruso que dificulta o imposibilita su actuación	No recomendado en IC, proporciona mas posibles beneficios que inconvenientes a un intruso profesional
	Sistemas de Megafonía	A	V	P / PF	®	®	®		A evaluar en función de la capacidad de respuesta de la propia IC
	Generadores de humo	A	V	I	®	®	®		
	Cañones Sónicos Aéreos	A	V	P	®				
	Cañones Sónicos Subacuáticos	A	V	P	®				

Detector Activo	*A*	*Detector Puntual*	*P*	*Detector Perimetral*	*P*
Detector Pasivo	*P*	*Detector Lineal*	*L*	*Detector Periférico*	*PF*
		Detector Superficial	*S*	*Detector de Interior*	*I*
		Detector Volumetrico	*V*		

En el caso de actuaciones acústicas la detección activará la generación de una respuesta especialmente "molesta" al posible intruso que pueden ir desde la emisión de un mensaje a través de la megafonía instalada hasta la de señales acústicas, que alcanzan una onda electromagnética de 2100 hasta 3100 hertzios con un nivel de la presión acústica muy alta (en el entorno graduable de los 150 decibelios) y difícilmente soportable.

Cuando la función disuasoria buscada es visual, el objetivo perseguido puede depender de que lo pretendido sea informar al posible intruso de que ha sido detectado con un cambio del nivel de iluminación existente bien sobre iluminando el área en el que se ha producido la detección o bien por el contrario eliminando por completo la iluminación de dicha área.

En este último caso los sistemas de supervisión y vigilancia deberán garantizar el control con elementos de iluminación infrarroja o intensificadores de luz.

Como alternativa se deben considerar sistemas de generación de humo que cumplan con la norma UNE-EN 50131-8:2020 Sistemas de alarma. Sistemas de alarma de intrusión y atraco. Parte 8: Dispositivos de niebla de seguridad, aunque en estos casos su utilización se recomienda en las áreas periféricas y fundamentalmente de interior.

9.3.1.2 Sistemas de supervisión y vigilancia.

Por último los sistemas de supervisión tienen como función esencial la visualización de las áreas externas de nuestro perímetro vigilado incluyendo la citada área previa a nuestro perímetro. Esto circunstancia nos posibilita adelantarnos a la llegada del posible intruso a nuestro perímetro de seguridad posibilitando la obtención de información o imágenes, aunque de la misma manera implica la imposibilidad de una ubicación fija y la imprevisibilidad de posibles injerencias.

Se trata de dispositivos móviles dotados de muy diverso equipamiento tanto de detección como de supervisión, con distinta morfología en función del medio en el que operan, Tierra, Agua o Aire.

TABLA 3

		CLASIFICACIÓN DEL DETECTOR			INSTALACIÓN ESTRATÉGICA CON NIVEL DE RIESGO :				
SUBSISTEMA	SISTEMA/ELEMENTO /DETECTOR	A/P	P/L/S/V	P/PF/I	ALTO	MEDIO	BAJO	OBSERVACIONES	RECOMENDACIONES
SISTEMAS DE SUPERVISIÓN Y VIGILANCIA	Drones (UAS - RPAS) - AIRE	A	V	P/PF/I	®			Posibilidad de incorporar detectores y sistemas adicionales a los de supervisión, posible incorporación de IA con funcionamiento autónomo	Evaluar posibles contramedidas por los riesgos que supone su utilización o interceptación por el intruso
	Vehículos subacuáticos no tripulados (UUS) - AGUA	A	V	P	®				
	Robots automáticos - TIERRA	A	V	P/PF/I	®				

Detector Activo	*A*	*Detector Puntual*	*P*	*Detector Perimetral*	*P*
Detector Pasivo	*P*	*Detector Lineal*	*L*	*Detector Periferico*	*PF*
		Detector Superficial	*S*	*Detector de Interior*	*I*
		Detector Volumetrico	*V*		

En estos sistemas cobran especial relevancia los vehículos aéreos no tripulados denominados como drones, UAVs, UAS o RPAS entre otros muchos nombres. En cualquier caso se trata de aeronaves equipadas con distintas capacidades tecnológicas avanzadas que permitirán evaluar y reaccionar apropiadamente a los eventos detectados, mediante la realización de rondas de reconocimiento aleatorias o programadas, a la evaluación periódica del espacio aéreo físico y de comunicaciones, la geolocalización de elementos en tierra o en lámina de agua, etc.

La coordinación tierra-aire ha de ser perfecta para que el seguimiento y control de los objetivos a vigilar tengan éxito, siendo el tiempo de respuesta una variable sumamente importante y un factor que se potenciará enormemente gracias a las capacidades tecnológicas incorporadas al dron.

De igual manera existe la posibilidad de utilizar vehículos acuáticos no tripulados que proporcionen información similar sobre la lámina de agua o bajo ésta.

Por último, los robots terrestres, pueden adoptar distintas configuraciones incorporando al igual que sus parientes acuáticos o aéreos, muy distintas posibilidades tanto de detección como de supervisión

El funcionamiento de ellos puede realizarse de manera autónoma de acuerdo a unos parámetros preestablecidos o gestionados desde un centro de control local o remoto.

Detectado un riesgo que pueda suponer un peligro inminente que puede traducirse en daños a las infraestructuras y los individuos, los UAS o UUS, comunicarán a las fuerzas de respuesta el suceso proporcionando información sobre el tipo de amenaza, los datos detectados, vídeo del suceso, métricas de los sensores, localización GPS, individuos implicados, señales luminosas, señales sonoras, etc.

Frente a las evidentes ventajas que este tipo de sistemas proporciona a la seguridad de la instalación, es importante analizar también el riesgo que supone la utilización de este tipo de equipos por parte de los posibles intrusos, previendo las contramedidas adecuadas que imposibiliten el desplazamiento aéreo o acuático no autorizado.

Estos sistemas deben garantizar la detección y evaluación temprana, la identificación y la reacción apropiada. Un ejemplo de estos sistemas es un sistema de localización de dirección de radiofrecuencia para localizar las transmisiones de las señales de control del UAV. Una vez detectado y monitorizado el UAV podrá emplearse el sistema de perturbación electromagnética o jammer que puede hacer jamming selectivo sobre el UAV sin afectar a sistemas cercanos.

9.3.2 Sistemas de videovigilancia.

Haciendo de nuevo referencia a lo expuesto por la guía de buenas prácticas para la Elaboración de los Planes de Protección Específicos (PPE) editada por el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) y dando continuidad al ciclo de gestión continua de la seguridad, las agrupaciones propuestas son:

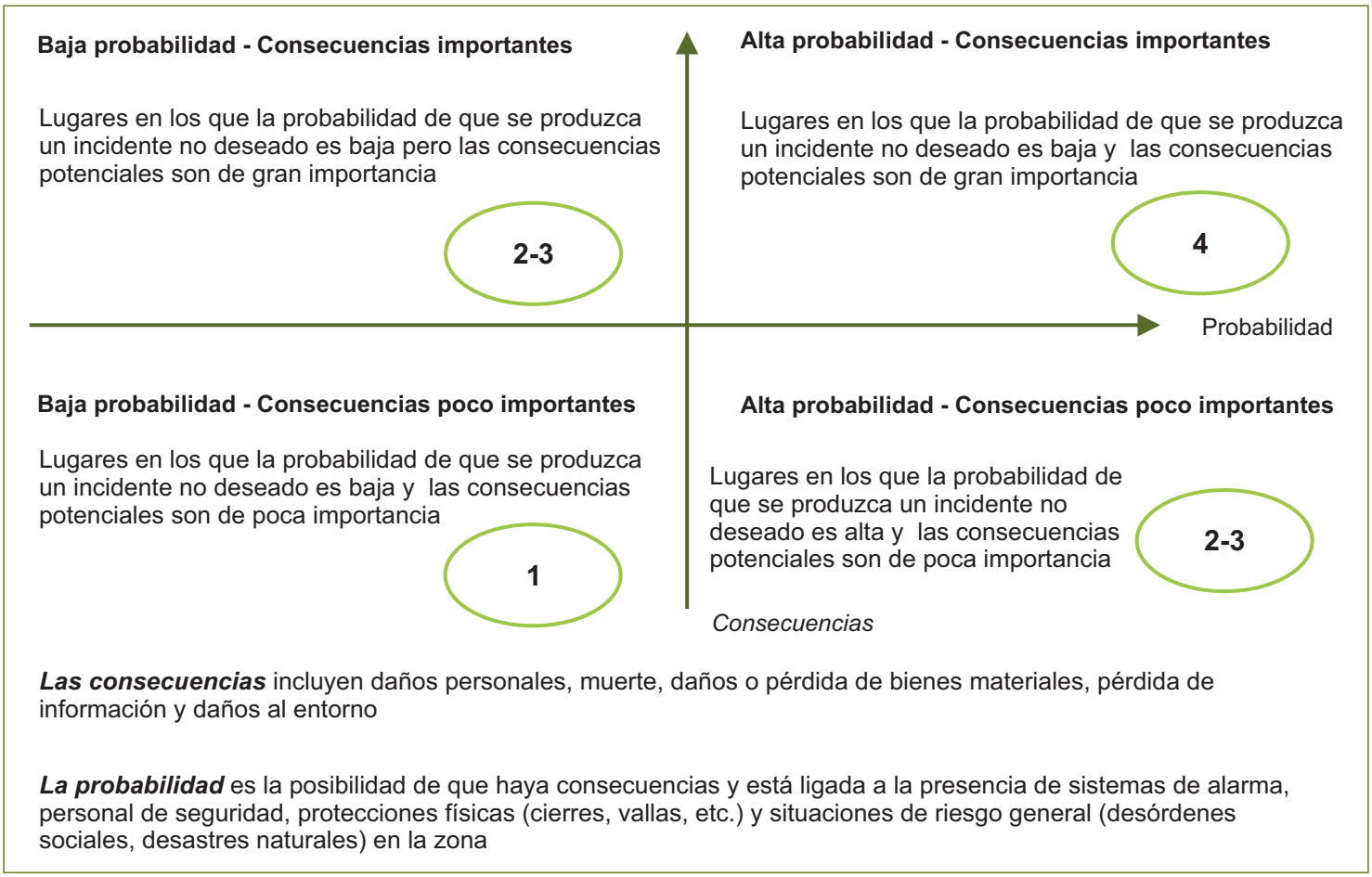
- Prevención y Detección
- Vigilancia y Monitorización
- Coordinación y Respuesta
- Continuidad y Contingencia.

Mientras que la Prevención y más concretamente la Detección, debe ser asumida por los sistemas de detección expuestos en el correspondiente apartado, la Vigilancia y Monitorización, será el principal propósito de los sistemas de videovigilancia (VSS) o de lo que hasta ahora denominábamos Circuito Cerrado de Televisión (CCTV).

Al igual que al hablar de los Sistema de Detección de Intrusión el nivel de protección asignado a las Instalaciones de Alto Riesgo de acuerdo a la Norma UNE 50131-1 debería ser Grado 4, de manera equivalente la legislación de seguridad privada española recoge en la OM INT/316/2011 que el citado Grado 4 estará reservado, entre otros, a las denominadas Infraestructuras Críticas.

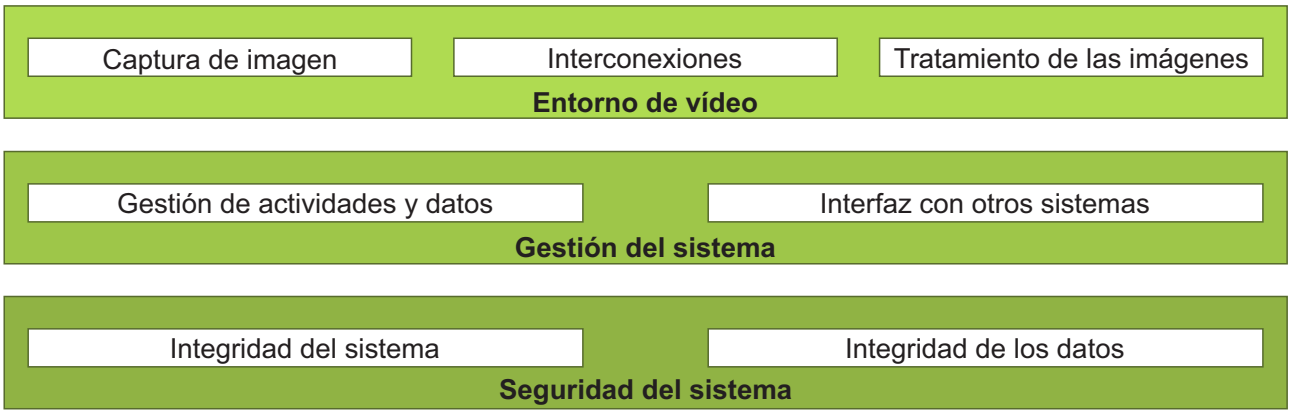
Desde el pasado mes de Diciembre de 2017, la norma EN 50132-1:2010 aludida en la citada OM INT/316/2011, referente a los Sistemas de Vigilancia (VSS) ó CCTV para uso en aplicaciones de seguridad, ha sido sustituida y actualizada por la UNE-EN 62676-1-1:2015.

Los grados establecidos para el VSS en la citada norma se han configurado teniendo en cuenta el nivel de riesgo dependiente de la probabilidad de que se produzca un incidente y del daño potencial causado por él, como se muestra en la figura anexa extraída de la citada Norma, estableciendo que el nivel de seguridad requerido se corresponde igualmente con un Grado 4, Riesgo Alto, es decir a escenarios con una alta probabilidad de que se produzca un incidente y con unas importantes consecuencias de llegar a producirse.



Fuente Norma EN 62676-1-1:2015

Cuando hablamos de un VSS en aplicaciones de seguridad y más concretamente en aplicaciones de alta seguridad como son las Infraestructuras Críticas, se debe asegurar un adecuado diseño en los tres bloques funcionales que constituyen los estadios de todo VSS, como se indica en la siguiente figura:



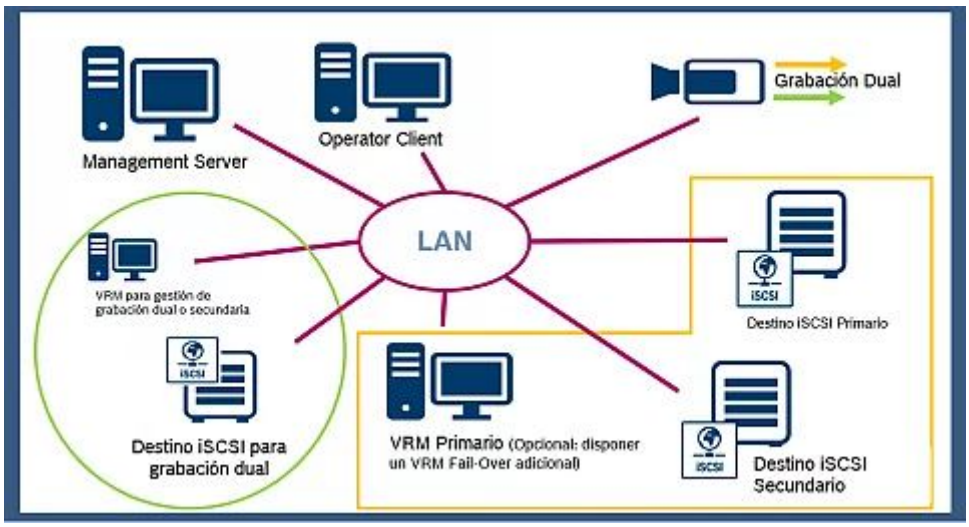
Fuente Norma EN 62676-1-1:2015

En efecto y tal y como expone la norma EN-62676-1, a la que nos remitiremos de manera habitual como referencia de nuestra legislación, el propósito de un VSS es el de capturar imágenes de una escena, gestionarlas y mostrarlas a un operador para su uso fácil y efectivo.

El conjunto de dispositivos, interconexiones y tratamientos constituye el entorno vídeo. Un sencillo ejemplo de ello se indica en la siguiente figura:

Fuente Norma EN 62676-1-1:2015

Es importante reseñar la rápida evolución que todos estos sistemas tienen en la actualidad, por ello el presente documento refleja los sistemas más habituales , de funcionamiento contrastado en el momento de su redacción, sin entrar en detalle de la definición de parámetros, circunstancia que exigiría la continua actualización en función del avance de los desarrollos tecnológicos y que además se ve agravada porque a diferencia de la familia UNE–EN 50131-1, la UNE EN 62676-1, no posibilita la normalización de los distintos componentes ni como consecuencia, su posible certificación.



Fuente Bosch Sistemas de Seguridad

El diseño de un adecuado VSS no dependerá tanto de la utilización de un equipamiento concreto, ni siquiera de un equipamiento con una homologación certificada de acuerdo a una norma, sino de la funcionalidad que proporciona al sistema de seguridad para el que está concebido.

La tabla anexa a este texto, pretende sintetizar los criterios de diseño de los sistemas de Protección de Infraestructuras Críticas, organizado de la siguiente forma:

- En las filas se han relacionado todos los sistemas de vídeo aplicables en los sistemas de Protección de Infraestructuras Críticas.

Se indican los siguientes sistemas en el entorno vídeo:

- Cámaras de espectro visible
- Domos PTZ
- Cámaras térmicas
- Posicionadores
- Sistemas de iluminación
- Carcasas para cámaras.
- Sistemas de vídeo embarcados.
- Sistemas de tratamiento de imágenes

Los siguientes para la Gestión del Sistema:

Sistemas de almacenamiento de imágenes

Sistemas de gestión

Y Elementos de detección y protección contra la manipulación de los sistemas de vídeo, como Seguridad del Sistema:

- Para cada uno de estos sistemas se han descrito los principales tipos de equipos disponibles en el mercado.
- En las columnas, se indica la idoneidad de uso de estos sistemas y equipos en función del riesgo asignado a la infraestructura. Se han establecido tres niveles de riesgo en función de los análisis de la instalación:
  - Alto
  - Medio
  - Bajo

Como criterio de idoneidad se han fijado los siguientes códigos:

- Sistema/equipo no recomendado. Este sistema no alcanza los niveles mínimos exigidos para este tipo de instalaciones.
- Recomendado. El sistema es idóneo para este tipo de instalaciones.
- Recomendado con observaciones. El sistema puede utilizarse para este tipo de instalaciones, pero deben cumplirse una serie de requisitos para su uso.
- Opcional. El sistema puede utilizarse en la instalación, pero no es obligatorio su uso.
- Obligatorio. El sistema debe ser empleado de forma obligatoria.
- Obligatorio con observaciones. El sistema debe utilizarse obligatoriamente y cumpliendo además un conjunto de requisitos.

Como complemento se añaden en el cuadro dos columnas con una serie de observaciones sobre cada sistema y de recomendaciones para su uso en los diferentes tipos de instalaciones.

A continuación se describen someramente los diferentes sistemas y su utilización en los grados de riesgo asignados a las infraestructuras críticas.


5G

TABLA 4 (1)

		SISTEMA	TIPO DE EQUIPO	INSTALACIÓN ESTRATÉGICA CON NIVEL DE RIESGO		
				ALTO	MEDIO	BAJO
ENTORNO VÍDEO.	CAPTURA DE IMÁGENES	CÁMARAS ESPECTRO VISIBLE	Cámara convencional B/N			R*
			Cámara convencional Color			R*
			Cámara convencional con conmutación automática Color - B/N		R*	R*
			Cámara convencional día / noche con leds Infrarrojos	R	R	R
		DOMOS PTZ	Domo día / noche			R*
			Domo día / noche con leds infrarrojos	R	R	R
		CÁMARAS TÉRMICAS	Cámara térmica	R	R	O
			Cámara termográfica	O	O	O
			Sistemas combinados cámara térmica - cámara día / noche	R	O	O
		POSICIONADORES	Posicionador para cámara	M	M	O
		ILUMINACIÓN	Foco luz blanca	M*	M*	M*
			Foco Infrarrojos	M*	M*	M*
		CARCASAS	Carcasa para interior anti-vandálica	M	M	M
			Carcasa para exterior (IP >= IP66) anti-vandálica	M	M	M

	No recomendado
R	Recomendado
R*	Recomendado cumpliendo los requisitos marcados en RECOMENDACIONES
O	Opcional
M	Obligatorio
M*	Obligatorio en las condiciones indicadas en RECOMENDACIONES

OBSERVACIONES	RECOMENDACIONES
Requieren de iluminación suficiente, por lo que no son admisibles en zonas no iluminadas de instalaciones de riesgo medio / alto	No recomendado si no es en combinación de focos infrarrojos con alcance suficiente para toda la zona vigilada
Requieren de iluminación suficiente, por lo que no son admisibles en zonas no iluminadas de instalaciones de riesgo medio / alto	No recomendado si no es en combinación de focos de luz blanca con alcance suficiente para toda la zona vigilada, siempre que se admitan éstos por criterio de discreción del sistema. La iluminación debe estar siempre garantizada
Importante emplear dispositivos con alta sensibilidad. Requieren de focos infrarrojos, por lo tanto presentan riesgo de sabotaje por eliminación de éstos	Requieren de focos infrarrojos con alcance suficiente para toda la zona vigilada
Importante emplear dispositivos con alta sensibilidad y relación señal / ruido.	Obligatorio si no existen focos infrarrojos. El alcance de los leds debe ser suficiente para iluminar toda la zona vigilada
Solamente admisible en zonas constantemente iluminadas de instalaciones de riesgo bajo	No recomendado. Pérdida de prestaciones en condiciones de muy baja iluminación
	Adecuado como apoyo a otros sistemas de visión fijos. El alcance de los leds debe ser suficiente para iluminar toda la zona vigilada
Adecuado en instalaciones de riesgo bajo si su empleo es económicamente aceptable	En instalaciones de riego medio / alto deben emplearse en combinación de sistemas automáticos de detección de incidentes sobre la imagen
Opcional. Coste económico de implantación elevado	Deben utilizarse en combinación con sistemas de análisis de la información que permitan utilizarla para detección de incidentes
	Recomendado si el diseño del sistema lo requiere (verificación visual humana, grabación de imágenes, seguimiento de objetivos, etc.)
Obligatorio con cámaras especiales si se necesita seguimiento de objetivo o visualización de detalles	En instalaciones de riesgo bajo puede resultar económicamente más interesante emplear domos PTZ
No deben utilizarse si no es posible o no es admisible iluminar la zona por la noche	Obligatorio para cámaras color en condiciones de escasa iluminación
Deben diseñarse para cubrir la totalidad del área vigilada	Obligatorio para cámaras B/N o de conmutación automática en condiciones de escasa iluminación
Obligatorio en todos los casos	Deben protegerse también acometidas de cable
Obligatorio en todos los casos	Deben protegerse también acometidas de cable

TABLA 4 (2)

		SISTEMA	TIPO DE EQUIPO	INSTALACIÓN ESTRATÉGICA CON NIVEL DE RIESGO ALTO	MEDIO	BAJO
ENTORNO VÍDEO.	INTERCONEXIONES		TRATADO EN EL APARTADO DE INTERCONEXIONES CABLEADOS Y COMUNICACIONES			
	TRATAMIENTO DE LAS IMÁGENES	ANÁLISIS	Detección de movimiento sobre vídeo			R*
			Análisis de imágenes para detección automática de incidentes (penetración en zona, salida de zona, merodeo, objeto abandonado, manipulación, etc.)	M	M	O
			Reconocimiento de matrículas de vehículos	M	M	O
			Reconocimiento de rostros	R	O	O
		ALMACENAMIENTO DE IMÁGENES	Videograbador digital "stand-alone"			M*
			Videograbador digital comunicable en red TCP/IP	M	M	M
			Sistema de videograbación redundantes	M	R	O
			Matriz de vídeo	M*	M*	M*
			Monitores para presentación de vídeo	M*	M*	M*
GESTIÓN DEL SISTEMA			Sistema de gestión de vídeo (VMS)	M	M	M
SEGURIDAD DEL SISTEMA		DETECCIÓN Y PROTECCIÓN CONTRA MANIPULACIÓN	Detección de manipulación de la cámara (pérdida de vídeo, cambio de enfoque, imagen degradada)	M	M	M
			Detección de manipulación de los equipos de transmisión de imágenes	M	M	M
			Sistema detección de movimiento próximo al emplazamiento de la cámara	M	M	M
			Sistema disuasorio de aproximación al emplazamiento de la cámara	R	O	O

	No recomendado
R	Recomendado
R*	Recomendado cumpliendo los requisitos marcados en RECOMENDACIONES
O	Opcional
M	Obligatorio
M*	Obligatorio en las condiciones indicadas en RECOMENDACIONES

OBSERVACIONES	RECOMENDACIONES
TRATADO EN EL APARTADO DE INTERCONEXIONES CABLEADOS Y COMUNICACIONES	
Requiere de un ajuste correcto en función de la instalación	Debido a la tasa de falsas alarmas y a la no clasificación automática de objetos e incidentes, no se considera adecuado en instalaciones de riesgo medio / alto o en instalaciones de riesgo bajo si el número de instalaciones supervisadas es alto
Debe configurarse de forma adecuada para cumplir los requisitos de alcance y tasa de falsas alarmas	
Debe estar asociado a los sistemas de control de acceso al perímetro exterior	
Recomendado en zonas de acceso muy restringido en combinación con el sistema de control de acceso para verificación del personal	
No recomendable. En su lugar deben instalarse equipos de vídeo-grabación comunicables	Solo admisible en una instalación aislada y permanentemente vigilada por personal in-situ
Obligatorio en todos los casos	
	En instalaciones de alto riesgo debe garantizarse un nivel alto de tolerancia a fallos de los equipos de grabación
Obligatorio en centros de control remotos cuando el número de cámaras supera al de monitores	El número de monitores físicos o virtuales debe ser el adecuado al número total de instalaciones vigiladas. Deben reservarse monitores físicos o virtuales para la visualización de las últimas alarmas en tiempo real
Obligatorio en centros de control remotos con un número elevado de emplazamientos a supervisar	
Obligatorio en todos los casos	
Obligatorio en todos los casos	
Obligatorio en todos los casos	
Obligatorio en todos los casos	
Recomendado en casos en los que sea importante retardar la manipulación de componentes esenciales del sistema	

9.3.2.1 Entorno Vídeo

Centrándonos en el entorno vídeo, la captura de la imagen en los VSS aplicados a seguridad se realiza fundamentalmente en el espectro visible y en el térmico tal y como se expone en la tabla adjunta y los Datos de imagen obtenidos pueden ser analógicos o digitales, aunque de manera mayoritaria y con una tendencia irreversible su utilización se va limitando al mundo digital.

En la citada tabla se exponen los equipos más habituales utilizados en los VSS en el campo de la seguridad y las recomendaciones y observaciones a tener en cuenta a la hora de su selección en función de los posibles niveles de riesgo del entorno donde será instalada dentro de nuestra IC. Como criterio a tener en cuenta deberemos asegurar que el equipo tenga la suficiente precisión y proporcione los detalles suficientes para permitir a los usuarios extraer la información apropiada (ISO 12233)

Las conexiones y comunicaciones necesarias en el entorno vídeo serán tratadas en el apartado de subsistemas auxiliares. Las comunicaciones describen las señales de datos de vídeo y control que se intercambian entre los componentes del VSS y las conexiones abordan los medios utilizados para el transporte de las señales de comunicación. Tanto las conexiones como las comunicaciones deben estar garantizadas tanto si se trata de interconexiones dedicadas, situaciones deseables en supuestos de alto riesgo en IC, como si se trata de redes compartidas con otras aplicaciones. Su diseño preverá reducir al mínimo la posibilidad de perdidas, retrasos o modificaciones de la señal y las interconexiones deberán estar controladas de manera permanente, de acuerdo a los límites establecidos en la EN 62676-1, en su apartado 6.1.2 referido a "Interconexiones".

Como último elemento de análisis en el entorno vídeo, el tratamiento de las imágenes incluye el análisis, almacenamiento y presentación de las señales de vídeo, o lo que es lo mismo de una secuencia de imágenes.

Todo el equipamiento a instalar en el área perimetral deberá estar diseñado para cumplir con la clase ambiental IV descrita en la EN 62676., en su apartado 7.1.5.

9.3.2.2 Captura de Imagen.

Cámaras de espectro visible

Son las cámaras de CCTV clásicas equipadas con sensores capaces de capturar imágenes

Debe realizarse un diseño adecuado de las ópticas de las que deben disponer para cubrir toda la escena a vigilar y prescribir correctamente su ubicación y posicionamiento, ya que estos dispositivos son fijos.

Todas estas cámaras requieren iluminación suficiente, ya sea ambiental o autónoma y se ven afectadas por el nivel de iluminación general y por las condiciones adversas de visibilidad: humo, niebla, lluvia intensa, nieve, etc. Por tanto, deberá tenerse en cuenta que si pueden darse estas condiciones adversas, esta parte del sistema funcionará con prestaciones degradadas.

Domos móviles

Son dispositivos de captura de imágenes similares a los anteriores pero que presentan la característica de poder mover o variar la escena vigilada a voluntad del usuario o del sistema de gestión de imágenes (PTZ, pan – tilt – zoom). En cuanto a la captura de imágenes es aplicable todo lo mencionado para cámaras de espectro visible.

En el caso más general, estos dispositivos permiten un movimiento del objetivo de 360º en horizontal y al menos 90º en vertical. Además permiten variar el enfoque para estrechar o ampliar el ángulo de visión de la escena. Es importante tener en cuenta para el diseño las características de zoom óptico y digital, la velocidad de desplazamiento, la sensibilidad y la relación señal/ruido.

En el caso de los domos es muy importante tener en cuenta el nivel de iluminación general o emplear domos que dispongan de leds para iluminar la zona visualizada por el objetivo.

Se recomienda su uso como apoyo a los sistemas de detección fijos, especialmente indicado para las tareas de verificación de alarmas, seguimiento de objetivos, etc.

Cámaras térmicas

La luz visible, detectable para el ojo humano y que las cámaras estándar pueden detectar y mostrar, precisa una fuente de luz como el sol o un proyector. Incluso las cámaras diurnas/nocturnas, que utilizan el espectro cercano al infrarrojo, necesitan algo de luz para funcionar, ya sea natural o procedente de una lámpara infrarroja especial.

Una cámara térmica no necesita una fuente de luz, ya que cualquier objeto con una temperatura superior a los cero grados Kelvin emite radiación térmica. Incluso objetos muy fríos, como el hielo, emiten radiación térmica. Cuanto más caliente esté el objeto, mayor radiación emite. Cuanto mayor sea la diferencia de temperatura en un escenario, más nítida será la imagen ofrecida por la cámara térmica.

La ventaja de las cámaras térmicas es que detectan de forma rápida e inequívoca los incidentes que se produzcan en su campo de visión. Son resistentes y el exceso de luz no las ciega ni se estropean cuando reciben la luz de un puntero láser. Proporcionan una primera línea de defensa perfecta que activa las acciones posteriores, mejorando de manera espectacular la eficacia del sistema de vigilancia.

Las cámaras térmicas son inmunes a la mayoría de los problemas con las condiciones de iluminación, sombras normales, etc., lo que las hace perfectas para el análisis de vídeo. Consiguen mucha más precisión que las cámaras convencionales en la mayoría de las aplicaciones de vídeo inteligente.

9.3.2.3 Tratamiento de las Imágenes.

Aunque un VSS no tiene por qué contener necesariamente las funciones de análisis, almacenamiento y presentación, cuando hablamos de Protección de Infraestructuras Críticas este apartado cobra una vital importancia dada la característica forense que posteriormente nos posibilitará la trazabilidad y auditoria de las señales.

En efecto en los VSS no solo es importante poder detectar incidentes o visualizar imágenes en tiempo real, sino poder realizar análisis posteriores de lo sucedido y captado por las cámaras que componen el sistema, de ahí la importancia de los equipos o sistemas de almacenamiento de imágenes. Estos dispositivos deben almacenar la información captada de forma segura y permitir un acceso rápido posterior para su análisis.

Durante este estadio los sistemas a utilizar nos permitirán cambiar las imágenes capturadas, modificando por ejemplo su resolución, frecuencia de imágenes o la compresión.

Para la Protección de Infraestructuras Críticas solamente se consideran aceptables los equipos basados en almacenamiento digital de las imágenes.

Los dispositivos más simples permiten la visualización en tiempo real o almacenada en el propio equipo. Son lo que se denomina sistemas "Stand-alone". Este tipo de sistemas solamente serán admisibles en Protección de Infraestructuras Críticas de bajo riesgo con personal dedicado a la vigilancia "in-situ". En todos los demás casos, deberán utilizarse equipos comunicables mediante protocolos TCP/IP.

Además en los casos de infraestructuras de alto riesgo, deberán preverse sistemas con dispositivos de almacenamiento redundante, con el objetivo de minimizar la posibilidad de pérdida de imágenes almacenadas por fallo en los dispositivos de almacenamiento.

Los sistemas de captura de imágenes pueden utilizarse no solo para visualizar determinadas zonas de la instalación en tiempo real o para grabar los incidentes. También pueden utilizarse como sensores orientados a la detección automática de incidentes. Es el caso de los sistemas de detección de incidencias basados en análisis de imágenes.

Para este tipo de infraestructuras están especialmente indicados los sistemas basados en la combinación de cámaras de visión térmica y dispositivos de detección basados en el análisis de las imágenes térmicas.

Podemos distinguir los siguientes sistemas de tratamiento de imágenes:

- Sistemas de detección de movimiento sobre imágenes.
- Sistemas de análisis de imágenes y detección automática de incidentes basada en diferentes reglas: paso por zona, merodeo, entrada o salida, abandono de objeto, retirada de objeto, etc.
- Sistemas de reconocimiento de placas de identificación de vehículos.
- Sistemas de reconocimiento de rostros.

En infraestructuras de riesgo alto serán obligatorios los sistemas de reconocimiento de matrículas de vehículos en los accesos a la instalación y de detección automática de incidentes en los perímetros.

Por último la presentación de la información es la muestra de imágenes de vídeo como imágenes individuales o como secuencia de imágenes de vídeo consecutivas de forma que un operador pueda verlas.

Algunos ejemplos de dispositivos para la presentación de la información incluyen las pantallas de los monitores o proyectores. Gracias a la capacidad de mostrar una multitud de fuentes a través de un mosaico de dispositivos de visualización aparecen los videowalls, donde el contenido visual de alta definición puede compartirse para realizar importantes análisis y toma de decisiones.

Para su composición se pueden utilizar cubos de proyección, proyectores y dispositivos de visualización de pantalla plana LED y LCD.

9.3.2.4 Gestión del Sistema

La interfaz de usuario es fundamental en la gestión de actividades y datos en un VSS, pues de ella depende la operatividad, comodidad de uso y seguridad real del VSS.

Cuando el VSS adquiere dimensiones difíciles de manejar desde un puesto de operador, se hace necesario disponer de un sistema de gestión. El sistema de gestión tiene la misión de coordinar el funcionamiento de todos los dispositivos y facilitar la utilización y el acceso a la información para los usuarios.

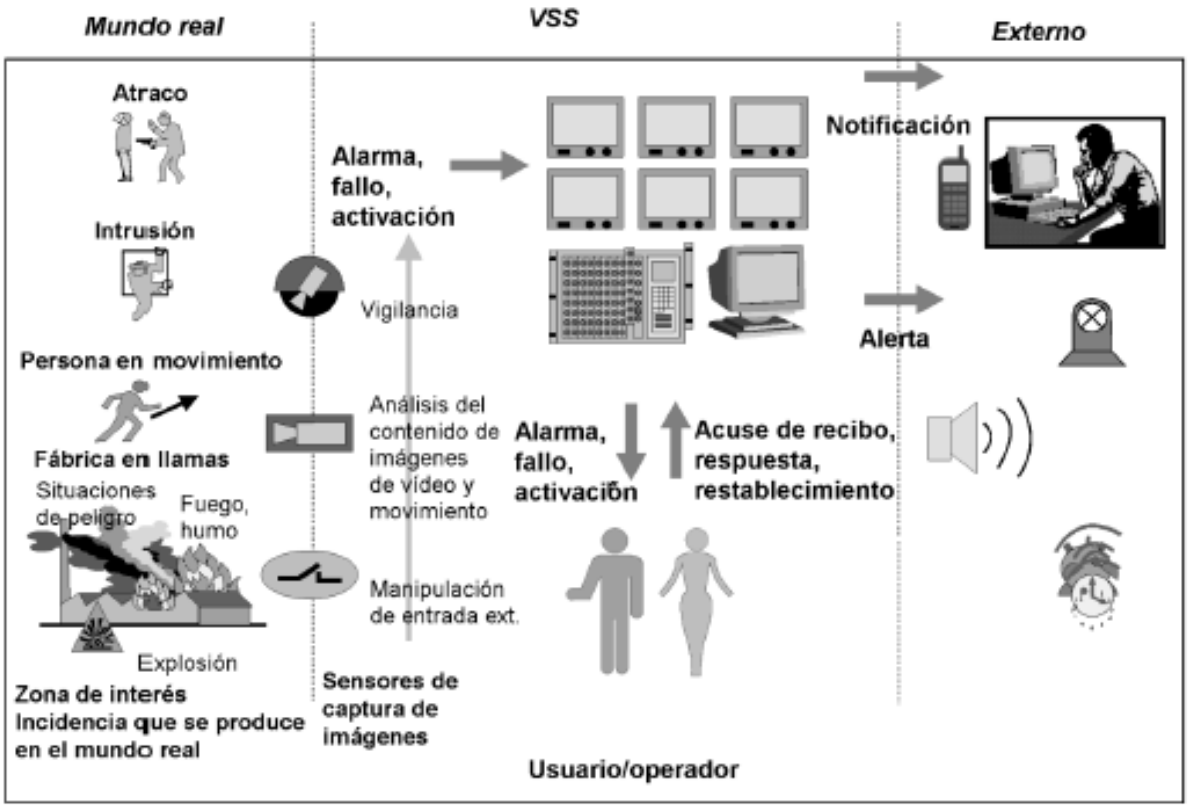
Los sistemas de gestión pueden ir desde las matrices de monitores y consolas de mando hasta los sistemas de gestión soportados por servidores y aplicaciones informáticas. Estos últimos permiten un acceso rápido a las imágenes de las diferentes cámaras, visualización automática de incidentes, posicionamiento automático de cámaras móviles, búsqueda selectiva de incidentes, acceso rápido a imágenes almacenadas, etc.

Cuando ese sistema debe manejar además de los datos de vídeo otros datos adquiridos, como datos de audio o metadatos, la gestión de la información hace necesaria e imprescindible la herramienta de un sistema de gestión de vídeo, VMS (Video Manager System).

Para la gestión de un VSS en la Protección de Infraestructuras Críticas se considera obligatorio la implantación de un sistema de gestión de vídeo, VMS (Video Manager System).

Además de la gestión de los datos el VMS a implementar debe garantizar el correcto tratamiento de las incidencias que se produzcan en el emplazamiento y las actuaciones de los usuarios.

Una incidencia, entendiendo por tal la aparición de una situación de riesgo, debe activar un procedimiento de alarma en el VSS. La activación del procedimiento, provoca la ejecución de tareas de nuestro VSS.



Fuente Norma EN 62676-1-1:2015

De igual forma un adecuado VMS debe permitir la interconexión con otros sistemas, ya sean estos de seguridad o de sistemas relacionados con ésta o de control de otros sistemas ajenos e independientes a la seguridad (security) como pudieran ser "escadas" de control productivo o sistemas de seguridad informática o comunicaciones.

9.3.2.5 Seguridad del Sistema

El sistema de vídeo vigilancia es un elemento clave en la protección de una infraestructura. Por lo tanto, debe estar protegido contra la manipulación o sabotaje.

La seguridad del Sistema debe comprender la integridad del sistema y la integridad de los datos.

La integridad del sistema comprende la seguridad física del sistema y el control físico y lógico al VSS. Esto requiere que constructivamente los equipos estén diseñados contra la manipulación pero además el sistema en su conjunto tiene que ser capaz de detectar estas condiciones para alerta al personal de vigilancia.

El propósito por tanto del sistema es la protección contra interferencias intencionadas e involuntarias del funcionamiento normal del VSS

Esto implica que el sistema obligatoriamente debe contemplar las siguientes acciones:

- Detección de manipulación en las cámaras: pérdida de señal de vídeo, cambio de escena, imagen degradada.
- Detección de manipulación de los equipos de almacenamiento de imágenes: fallo en los dispositivos de almacenamiento, fallo de comunicaciones, acceso no autorizado a sus envolventes, etc.
- Sistemas de detección de aproximación y accesos no autorizados a los emplazamientos de cámaras y al sistema en conjunto.
- Sistemas de detección de intento de manipulación de los armarios de conexionado o alimentación de cámaras.
- Sistemas de identificación de datos que garanticen la fuente de datos, la hora, la fecha, la ubicación, …
- Sistemas de autenticación de datos que prevengan contra la modificación, borrado o inserción de datos no reales.
- Sistemas de protección de los datos que prevengan el acceso no autorizado a las bases de datos, previendo su duplicidad y su grado de disponibilidad.

TABLA 5 (1)

		SISTEMA	EQUIPO	GRADO 1: Riesgo bajo
ENTORNO VÍDEO	CAPTURA DE IMÁGENES	CÁMARAS ESPECTRO VISIBLE	Cámara convencional B/N	Adecuado si la iluminación general es baja o se utilizan focos infrarrojos
			Cámara convencional Color	Adecuado si la iluminación general es suficiente para la sensibilidad de la cámara en cualquier condición y momento del día (requiere de focos de luz blanca en condiciones de baja iluminación)
			Cámara convencional con conmutación automática Color - B/N	Adecuado. Requieren de focos infrarrojos
			Cámara convencional día / noche con leds Infrarrojos	Adecuado
		DOMOS PTZ	Domo día / noche	Adecuado adaptando el alcance máximo a la zona a vigilar, con programación automática de rondas y con iluminación suficiente para la sensibilidad de la cámara
			Domo día / noche con leds infrarrojos	Adecuado adaptando el alcance máximo a la zona a vigilar, con programación automática de rondas
		CÁMARAS TÉRMICAS	Cámara térmica	Adecuado si su empleo es económicamente aceptable
			Cámara termográfica	Opcional. Económicamente poco interesante
			Sistemas combinados cámara térmica - cámara día / noche	Opcional. Económicamente poco interesante
		POSICIONADORES	Posicionador para cámara	Opcional. Económicamente puede resultar más interesante emplear domos PTZ
		ILUMINACIÓN	Foco luz blanca	Obligatorio para cámaras color en condiciones de escasa iluminación
			Foco Infrarrojos	Obligatorio para cámaras B/N o de conmutación automática en condiciones de escasa iluminación
		CARCASAS	Carcasa para interior anti-vandálica	Opcional
			Carcasa para exterior (IP >= IP66) anti-vandálica	Opcional

GRADO 2: Riesgo bajo a medio	GRADO 3: Riesgo medio a alto	GRADO 4: Riesgo alto
Adecuado si la iluminación general es baja o se utilizan focos infrarrojos	No recomendado si no es en combinación de focos infrarrojos con alcance suficiente para toda la zona vigilada	No recomendado si no es en combinación de focos infrarrojos con alcance suficiente para toda la zona vigilada
Adecuado si la iluminación general es suficiente para la sensibilidad de la cámara en cualquier condición y momento del día (requiere de focos de luz blanca en condiciones de baja iluminación)	No recomendado si no es en combinación de focos de luz blanca con alcance suficiente para toda la zona vigilada	No recomendado si no es en combinación de focos de luz blanca con alcance suficiente para toda la zona vigilada, siempre que se admitan éstos por criterio de discreción del sistema. La iluminación debe estar siempre garantizada
Adecuado. Requieren de focos infrarrojos	Adecuado. Requieren de focos infrarrojos con alcance suficiente para toda la zona vigilada	Adecuado. Requieren de focos infrarrojos con alcance suficiente para toda la zona vigilada
Adecuado	Obligatorio si no existen focos infrarrojos. El alcance de los leds debe ser suficiente para iluminar toda la zona vigilada	Obligatorio si no existen focos infrarrojos. El alcance de los leds debe ser suficiente para iluminar toda la zona vigilada
Adecuado adaptando el alcance máximo a la zona a vigilar, con programación automática de rondas y con iluminación suficiente para la sensibilidad de la cámara	No recomendado. Pérdida de prestaciones en condiciones de muy baja iluminación	No recomendado. Pérdida de prestaciones en condiciones de muy baja iluminación
Adecuado adaptando el alcance máximo a la zona a vigilar, con programación automática de rondas	Adecuado como apoyo a otros sistemas de visión fijos	Adecuado como apoyo a otros sistemas de visión fijos
Adecuado si su empleo es económicamente aceptable	Recomendado en combinación de sistemas automáticos de detección de incidentes sobre la imagen	Recomendado en combinación de sistemas automáticos de detección de incidentes sobre la imagen
Opcional. Económicamente poco interesante	Opcional. Deben utilizarse en combinación con sistemas de análisis de la información que permitan utilizarla para detección de incidentes	Opcional. Deben utilizarse en combinación con sistemas de análisis de la información que permitan utilizarla para detección de incidentes
Opcional. Económicamente poco interesante	Opcional	Recomendado si el diseño del sistema lo requiere (verificación visual humana, grabación de imágenes, seguimiento de objetivos, etc.)
Opcional. Económicamente puede resultar más interesante emplear domos PTZ	Obligatorio con cámaras especiales si se necesita seguimiento de objetivo o visualización de detalles	Obligatorio con cámaras especiales si se necesita seguimiento de objetivo o visualización de detalles
Obligatorio para cámaras color en condiciones de escasa iluminación	Obligatorio para cámaras color en condiciones de escasa iluminación	Obligatorio para cámaras color en condiciones de escasa iluminación. No deben utilizarse si no es posible o no es admisible iluminar la zona por la noche
Obligatorio para cámaras B/N o de conmutación automática en condiciones de escasa iluminación	Obligatorio para cámaras B/N o de conmutación automática en condiciones de escasa iluminación	Obligatorio para cámaras B/N o de conmutación automática en condiciones de escasa iluminación
Recomendado	Obligatorio	Obligatorio
Recomendado	Obligatorio	Obligatorio

TABLA 5 (2)

	SISTEMA		EQUIPO	GRADO 1: Riesgo bajo
ENTORNO VÍDEO	INTERCONEXIONES		TRATADO EN EL APARTADO DE INTERCONEXIONES CABLEADOS Y COMUNICACIONES	
	TRATAMIENTO DE LAS IMÁGENES	ANÁLISIS	Detección de movimiento sobre vídeo	Recomendado si se requiere un sistema automático de detección de incidentes asociado al vídeo
			Análisis de imágenes para detección automática de incidentes (penetración en zona, salida de zona, merodeo, objeto abandonado, etc.)	Opcional. Económicamente poco interesante
			Reconocimiento de matrículas de vehículos	Opcional. Económicamente poco interesante
			Reconocimiento de rostros	Opcional
		ALMACENAMIENTO	Videograbador digital "stand-alone"	Obligatorio
			Videograbador digital comunicable en red TCP/IP	Opcional
			Sistema de videograbación redundantes	Opcional
		PRESENTACIÓN DE LAS IMÁGENES	Matriz de vídeo	Opcional
			Monitores para presentación de vídeo	Opcional
	GESTIÓN DEL SISTEMA		Sistema de gestión de vídeo (VMS)	Opcional
SEGURIDAD DEL SISTEMA	DETECCIÓN Y PROTECCIÓN CONTRA MANIPULACIÓN		Detección de manipulación de la cámara (pérdida de vídeo, cambio de enfoque, imagen degradada)	Opcional
			Detección de manipulación de los equipos de transmisión de imágenes	Opcional
			Sistema detección de movimiento próximo al emplazamiento de la cámara	Opcional
			Sistema disuasorio de aproximación al emplazamiento de la cámara	Opcional

GRADO 2: Riesgo bajo a medio	GRADO 3: Riesgo medio a alto	GRADO 4: Riesgo alto
TRATADO EN EL APARTADO DE INTERCONEXIONES CABLEADOS Y COMUNICACIONES		
Recomendado si se requiere un sistema automático de detección de incidentes asociado al vídeo	Adecuado si la tasa de falsas alarmas es admisible	No adecuado por tasa de falsas alarmas y no clasificación automática de objetos e incidentes
Opcional. Económicamente poco interesante	Recomendado	Obligatorio cuando se necesite de un sistema automático de detección de incidentes basado en vídeo
Opcional. Económicamente poco interesante	Recomendado en combinación de los sistemas de control de acceso al perímetro exterior	Recomendado en combinación de los sistemas de control de acceso al perímetro exterior
Opcional	Opcional	Recomendado en zonas de acceso muy restringido en combinación con el sistema de control de acceso para verificación del personal
Obligatorio	No recomendado. Emplear en su lugar DVR comunicables	No recomendado. Emplear en su lugar DVR comunicables
Opcional	Obligatorio	Obligatorio
Opcional	Recomendado	Obligatorio
Opcional	Opcional	Obligatorio en centros de control remotos cuando el número de cámaras supera al de monitores
Opcional	Obligatorio en centros de control remotos con un número elevado de emplazamientos a supervisar	Obligatorio en centros de control remotos con un número elevado de emplazamientos a supervisar
Opcional	Obligatorio en caso de un número importante de emplazamientos a supervisar	Obligatorio
Recomendado	Obligatorio	Obligatorio
Opcional	Obligatorio	Obligatorio
Opcional	Recomendado	Obligatorio
Opcional	Opcional	Recomendado en casos en los que sea importante retardar la manipulación de componentes esenciales del sistema

9.3.3 Subsistema de control de accesos

Se define en este documento las líneas generales a tener en cuenta para la instalación de un sistema de control de accesos, capaz de monitorizar todos los aspectos relacionados con la seguridad de las personas que acuden a trabajar a una instalación tipo así como de los visitantes que diariamente accederán a la misma.

De manera sintética un subsistema de Control de Accesos estará conformado por diferentes elementos, cada uno operando en forma autónoma, pero integrados bajo una misma plataforma, lo cual permitirá monitorizar en forma integrada e inteligente cada uno de éstos.

El sistema de control de accesos estará basado en elementos de hardware; microcontroladores y lectores, así como los accesorios específicos para cada uno de los accesos controlados, según el elemento de control propuesto; puertas, pasillos de circulación, accesos a rampas, etc.

Este sistema permitirá regular y restringir el acceso a determinadas áreas consideradas críticas, tanto por su función, como por su ocupación.

En aquellas áreas donde se requiera conocer con certeza la entrada y salida confirmada de un usuario (así como la activación de la función de anti retorno –anti passback-), contarán con lector de entrada y de salida, pulsador de salida consentida, contacto magnético, cerradero eléctrico y pulsador de salida de emergencia.

En los restantes accesos contarán con lector de entrada, pulsador de salida consentida, contacto magnético, cerradero eléctrico y pulsador de salida de emergencia.

En aquellas áreas que requieran un nivel adicional de seguridad, los lectores de acceso estarán dotados de un teclado, requiriendo el paso de una tarjeta y la introducción de un número PIN, y en casos específicos, donde así se requiera por la criticidad del área, se dispondrá de lectores biométricos de cualquiera de las tecnologías disponibles (huella, reconocimiento facial, reconocimiento iris, patrón venoso, y otros).

Los lectores a ser instalados serán de última generación, capaces de leer tarjetas del tipo y tecnología que se requiera en función del nivel de seguridad exigido.

Cada usuario del sistema tendrá un código único, asignado a la tarjeta de identificación, el cual no es repetible, asociando en forma inequívoca el portador de la tarjeta con ésta.

Para recolectar las señales de los dispositivos que conforman el sistema de control de accesos se dispondrá de controladoras autónomas con capacidad instalada para el número de lectores requerido en cada una de las plantas.

La tipología y capacidad de las controladoras dependerá del número lectoras, entradas digitales y salidas de relé requeridas y/o una segunda controladora tipo modular, para función únicamente accesos controlando una única puerta con opción para control de entrada y/o control de entrada y salida.

Las entradas digitales correspondientes a contactos magnéticos asociados a las puertas, así como los pulsadores de salida consentida, son independientes a las entradas digitales indicadas anteriormente, por lo que la totalidad de dichas entradas estará disponible para los elementos de intrusión.

En ambos casos, las comunicaciones entre las controladoras y el servidor de gestión se realizarán a través de un puerto Ethernet (TCP/IP).

La controladora dispondrá localmente de la base de datos asociada a ella, por lo que aún en el caso de una fallo de comunicaciones con el servidor del sistema, seguirá totalmente operativa, almacenado todos los eventos asociados. Una batería de soporte interno permitirá mantener la base de datos en la controladora aún cuando hayan fallado la alimentación eléctrica y las comunicaciones con el servidor.

Una vez recuperada las comunicaciones, cada controladora procederá a transferir al servidor los registros que no fueron enviados a éste durante el fallo, evitando de esta forma el perder información importante relativa a los eventos transcurridos durante esta incidencia.

Asociado a cada lector integrado en la controladora modular se dispondrá de un módulo de interfase a través del cual se recibirán las señales del contacto magnético y del pulsador de salida consentida. Un relé controlado por el sistema y ubicado en este módulo, enviará la alimentación eléctrica al cerradero para el control de apertura y cierre de la puerta o el comando para la apertura de un pasillo motorizado, etc.

Las comunicaciones entre estos módulos y la controladora se realizarán mediante un conexionado categoría 5 o 6 y con cable tipo FTP. El protocolo de comunicaciones será supervisado, lo que permitirá conocer a través de un software de monitorización, el estado propio lector y del cable de comunicaciones, así como cualquier intento de sabotaje, tanto del propio cable como del lector.

Para las controladoras de dos lectores, no será necesario el módulo de interfase ya que dicha controladora dispone de las entradas requeridas para el contacto magnético y el pulsador de salida consentida, así como un relé de salida para el control de la apertura de la puerta.

Los diferentes elementos de intrusión; contactos magnéticos, detectores de movimiento, etc., serán conectados directamente a las controladoras (entradas digitales), supervisando –a través de 4 estados– la condición operacional y las comunicaciones con estos.

A través del software de control se podrá gestionar cada acceso, asignando a los usuarios autorizados, ya sea por grupos, individualmente, por categorías, por horarios, etc. El sistema de gestión es totalmente flexible para adaptarlo a las necesidades del usuario.

La siguiente imagen muestra la configuración del sistema de control de accesos para una puerta dada.

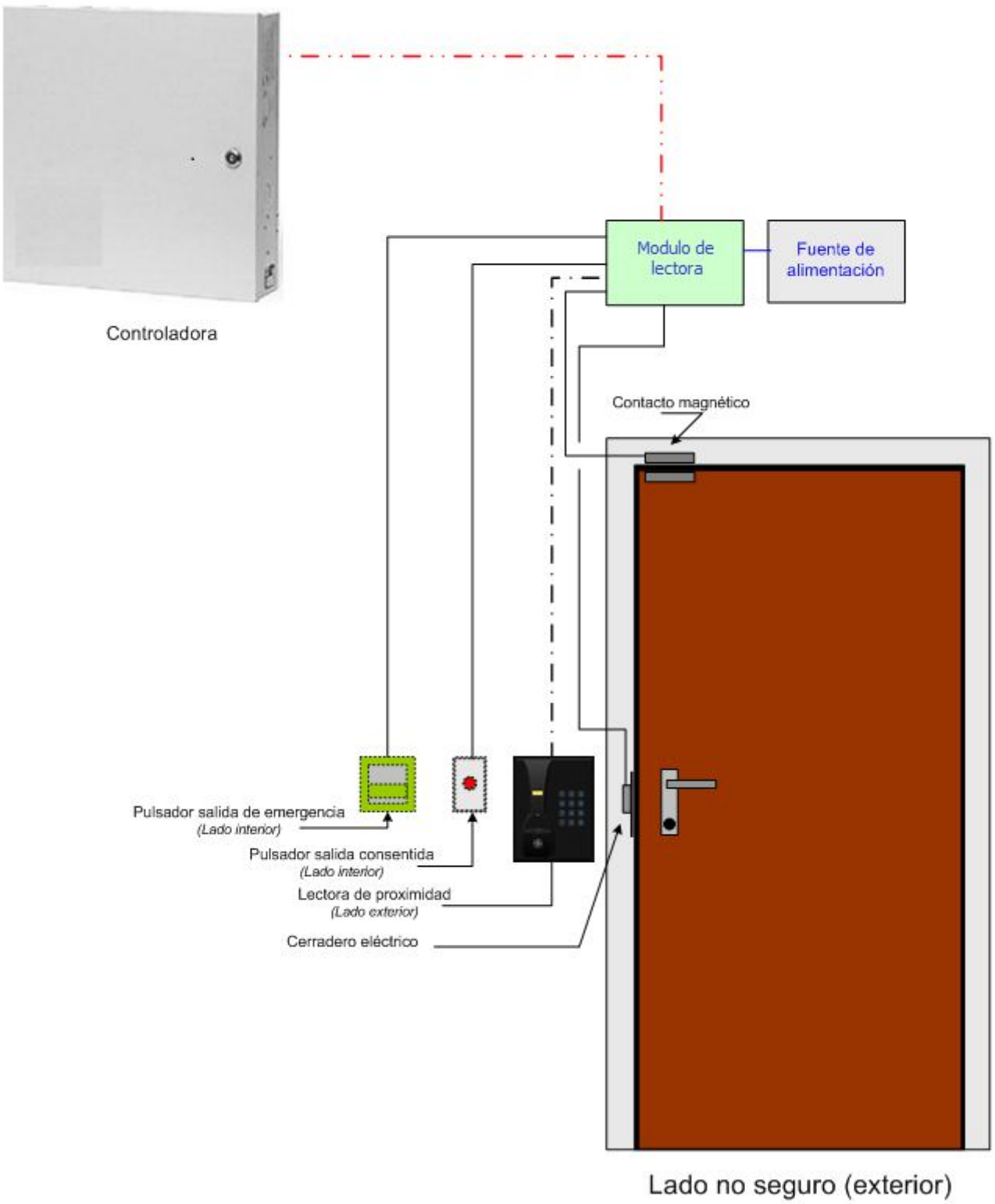


Figura: Configuración del sistema de control de accesos para una puerta.

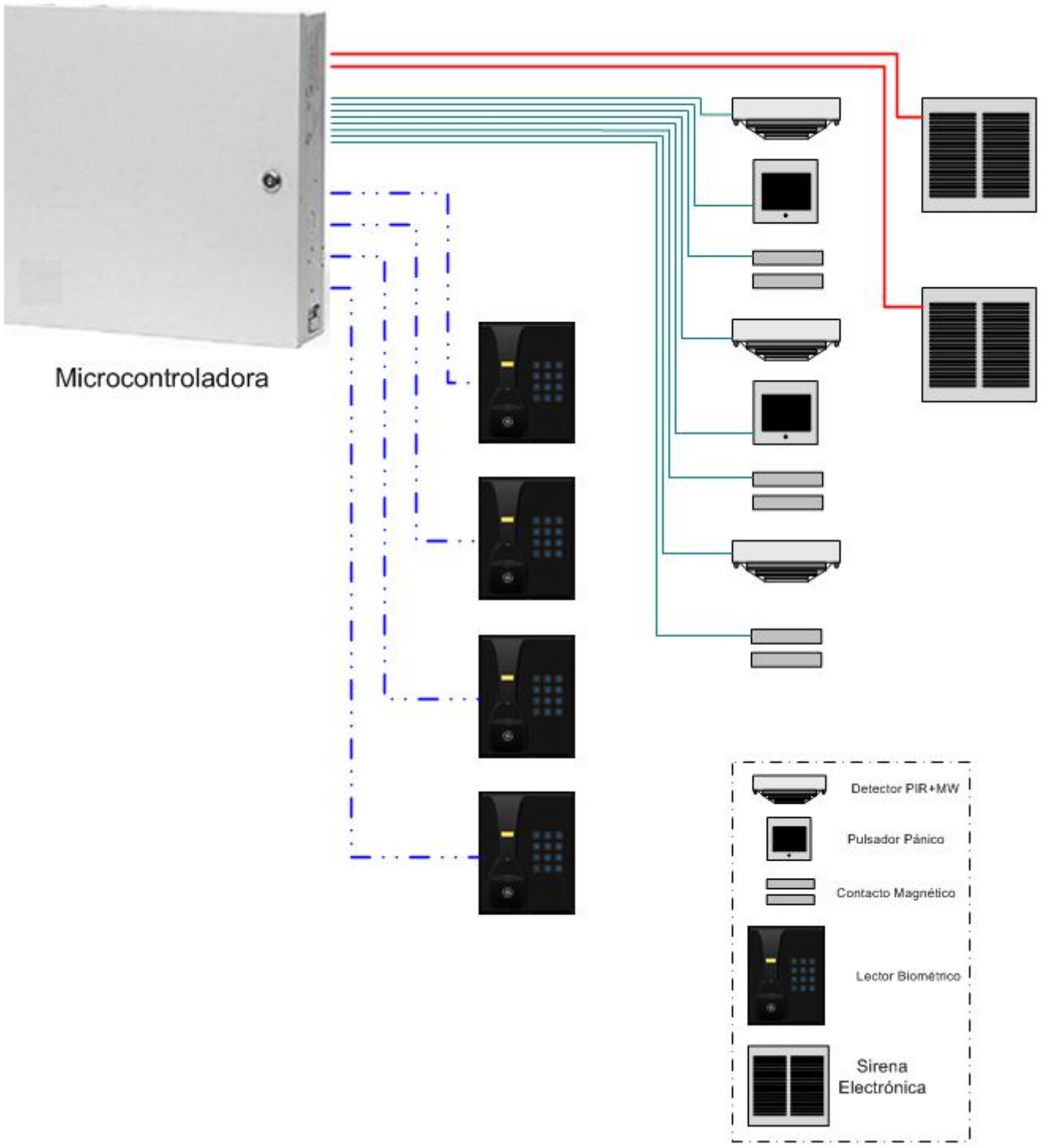


Figura: Integración de los elementos de control de accesos e intrusión a la controladora

Las entradas asociadas a los sistemas de intrusión serán gestionadas como tal, pudiendo ser agrupadas en zonas, las cuales a su vez podrán ser armadas y desarmadas en forma manual desde el software de control o en forma automática, mediante temporización o asociadas a los lectores de control de accesos.

El software de gestión será detallado en el siguiente apartado correspondiente a la centralización del sistema.

9.3.3.1 Comunicación Controladora-Lector y OSDP

Si bien tradicionalmente los protocolos de comunicación utilizados son Wiegand y Clock/Data, se recomienda el uso de sistemas que implementen protocolos de seguridad avanzada basados en OSDP.

El Protocolo de Dispositivos Abiertos Supervisados (OSDP) es una norma de comunicaciones de control de acceso desarrollada por la Asociación de la Industria de la Seguridad (SIA) para mejorar la interoperabilidad entre el control de acceso y los productos de seguridad.

OSDP especifica el protocolo de comunicación entre lectores y controladores, eliminando la necesidad de 'controladores propietarios' cuando se utilizan controladores y lectores de terceros al simplificar la forma en que se comunican esos dispositivos. Las funciones comunes están estandarizadas, incluida la forma en que se envían, formatean y cifran los datos de las credenciales.

También están estandarizadas características avanzadas como qué mensajes muestra el lector, cómo funcionan los LED o el sabotaje integrado, o incluso cómo funciona la verificación biométrica bidireccional.

Beneficios de OSDP:

- Comunicación bidireccional, incluida la retroalimentación mostrada por el lector
- Integración biométrica estandarizada con sistemas de acceso
- Manejo de grandes cantidades de datos de credenciales
- Versión 'Secure Channel' de OSDP que admite el cifrado de datos, a partir de la versión 2.1.7 de OSDP, se utiliza cifrado AES de 128 bits en los datos entre el lector y el controlador.

9.3.4 Subsistema de Centralización

El subsistema de centralización representa el nudo gordiano de los Centros de Seguridad y Vigilancia, porque en ellos se combinan y optimiza la información de los distintos subsistemas y se presenta para su gestión y control de manera integrada.

Podemos definir como un sistema de centralización, de sistemas de seguridad, como aquel que integra en una misma plataforma de gestión, distintos subsistemas, permitiendo una gestión más proactiva, ágil y efectiva en su uso, apoyando estos subsistemas con elementos de planimetría y señalética visual.

El presente capítulo describe la funcionalidad requerida por este tipo de sistemas si bien se deberá complementar con lo descrito en lo referente a la norma UNE-EN 50398, descrita anteriormente y es fundamental la intervención del Ingeniero de Seguridad.

La elección del sistema requiere la inversión del tiempo necesario, ya que, tanto la implantación como un posible cambio posterior de la estructura a implementar, conllevaría pérdidas económicas en el equipamiento y en la formación de su personal.

Para llevar a cabo la elección del sistema de Centralización, en la "Etapa de Trabajo" de Planificación de la instalación (ver UNE-EN 50398) deberemos tener en cuenta los siguientes aspectos:

- Arquitectura de la solución integral de seguridad
- Mecanismos de alta disponibilidad
- Software de gestión y módulos de integración

Gestión de infraestructura IT y comunicaciones

Existe una creciente tendencia a la participación de los equipos de seguridad de la información y áreas IT en la gestión de la infraestructura de comunicaciones e informática sobre la que se despliegan los sistemas de seguridad (servidores, puestos cliente, red, etc.), por lo que se recomienda que en la fase de diseño de centralización de sistemas se consensuen los aspectos indicados a continuación así como las políticas, medidas de seguridad IT y OT, alta disponibilidad, mecanismos de copia de seguridad y respaldo, bastionado de PCs, etc., de aplicación sobre la red, equipos y sistemas de seguridad.

A través de este marco de trabajo conjunto el desarrollo de las siguientes fases permitirá el cumplimiento y verificación de los requisitos IT, favoreciendo una integración sobre los sistemas de gestión, mantenimiento y respuesta global de la infraestructura.

9.3.4.1 Arquitectura

Esta etapa es la más importante de todas, ya que su elección condicionará el futuro del equipamiento y de las opciones posteriores del entorno informática y de gestión.

Para ello definiremos los siguientes sistemas de control en función de su arquitectura:

Sistema Distribuido

Consistente en el enlace, por medio de una red de comunicaciones, de diversos nodos distribuidos físicamente, dotados de capacidad de proceso y enlazados a sensores y/o actuadores.

Estos sistemas se caracterizan por que el proceso de control tiene lugar en estos nodos de manera coordinada. Las redes de comunicaciones orientadas al enlace de estos nodos son conocidas también como buses de comunicaciones o redes multiplexadas. Un nodo es un procesador autónomo con su propio hardware: procesador (CPU), memoria, oscilador de reloj, interfaz de comunicaciones, e interfaz hacia el subsistema que controla.

Entre las distintas ventajas que aporta el sistema de control distribuido, contamos con:

- Un aumento de la confiabilidad al sistema. Esta arquitectura tiene redundancia, en el caso de que fallara uno de los sistemas, los demás continúan funcionando.
- El crecimiento de la empresa es soportable, ya que se pueden realizar tantas copias del sistema como centros dispuestos en diferentes lugares geográficos.
- Tomas de decisiones locales. La lógica de negocio y las tomas de decisiones en cada lugar son independientes unas de otras.
- La distribución de datos no está centralizada en la empresa. En el caso de que la lógica de negocio es la de tener datos locales para las tomas de decisiones, el sistema distribuido es idóneo, en caso contrario, recomendamos optar por un sistema centralizado.
- El uso del ancho de banda local, permite tener una interfaz amigable. Este sistema sólo consume el ancho de la banda de una red local.
- La velocidad de respuesta es alta, siempre que los datos se encuentren en la red local.

Y sus desventajas

- El soporte local para esta tecnología, requiere que, por cada lugar geográfico, se debe tener personal para dar soporte tecnológico a esta arquitectura.
- Sirva como consejo que una mala distribución de los datos, es peor que un sistema centralizado, ya que requiere un uso en exceso de la red y una ampliación de sus características.
- Costo y complejidad del SW (software).
- Costo en llevar los cambios del SW a cada lugar, para la realización del mantenimiento.
- La integridad de los datos requiere de un control más complejo.
- El sistema requiere de otra área de la tecnología, SW de seguridad, protección y de redes, independiente de la de gestión de datos de la explotación.

No obstante, existen razones adicionales por las que es preferible la elección de un sistema distribuido, tales como el de menor tiempo de diseño y menores costes de operación y mantenimiento.

Sistema Centralizado

En un sistema de control centralizado existe un único controlador donde confluyen todas las señales de entrada a muestrear, se procesan realizando todos los algoritmos necesarios de control y se generan todas las señales necesarias de salida.

Los sistemas centralizados dan lugar a costosos y pesados cableados punto a punto (desde cada sensor o actuador hasta el sistema centralizado) y a la utilización de redes analógicas (4-20mA) tanto para la conexión de sensores dedicados a la captación de señales de entrada como para la activación de indicadores.

Una de las razones principales para la migración desde los sistemas centralizados a los sistemas distribuidos fue la necesidad de simplificación y normalización del cableado, basándose en la filosofía de la sustitución de cobre (costosos cableados punto a punto) por nodos inteligentes enlazados por un bus serie sobre par trenzado de baja sección.

Entre las ventajas que encontramos en este tipo de sistemas contamos con:

- Un único punto de control. Mayor control de seguridad y protección de la información en un solo punto.
- Fácil de mantener. Se adapta a empresas con muchos cambios de requerimientos. Con un fácil despliegue de los cambios. El mantenimiento y soporte se centraliza en un solo punto, con el consiguiente ahorro de costes.
- Tomas de decisiones. Esta arquitectura es primordial en las tomas de decisiones centralizadas, desde cualquier otro punto, llamado de lógica de negocio de la empresa centralizada.

Y entre las desventajas, podemos identificar las siguientes:

- Interfaz de usuario poco llamativo. Por el uso de la red amplia, se evita tener pantalla con imágenes, ya que se debe controlar el uso de ancho de banda de la red.
- Velocidad de repuestas lenta, dependiendo de la conexión de la red a la central.
- Debe existir un mecanismo de respaldo o copia del sistema centralizado, en caso de contingencia muy estricta, ya que, con la muerte del sistema central, pues igualmente moriría el sistema a nivel general.
- El crecimiento depende de los equipos que lo soporta. Si la empresa crece de forma exponencial, el equipo deberá ir sustituyéndose, en función de dichos cambios.

No obstante, en nuestro estudio se ha de tener en cuenta otra serie de factores tales como la robustez del sistema, su arquitectura, la telegestión, la gobernabilidad o el control desde puntos remotos.

9.3.4.2 Mecanismos de alta disponibilidad

Servidor Redundante de Alta Disponibilidad

Este sistema, está basado en un conjunto de servidores principal-secundario, con redundancia en caliente y servicios de clusterización que permiten habilitar disponibilidad del sistema en un 99%.

Esta solución ha de combinar de forma conjunta el software y el hardware. Los servidores deberán disponer de múltiples CPUs con doble fuente de alimentación y doble tarjeta de red. Esta solución se puede aplicar tanto en entornos LAN como WAN. El tiempo de recuperación es imperceptible por el operador usuario.

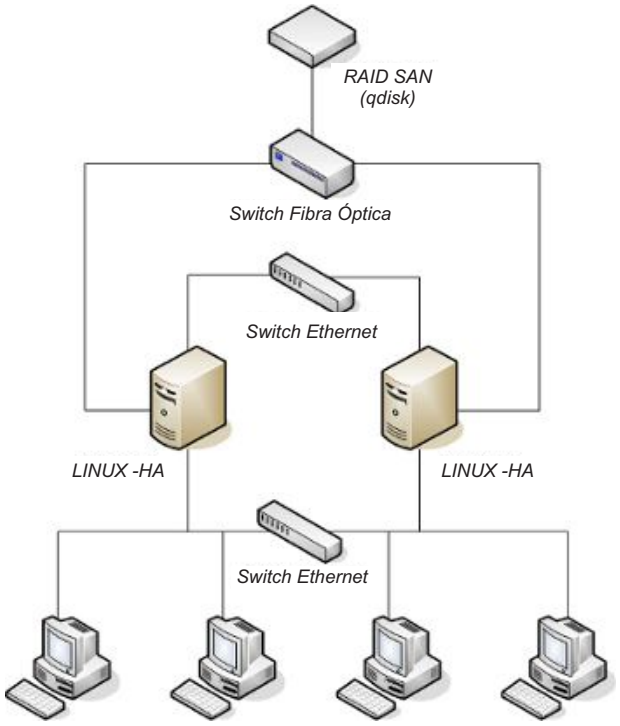
Se recomienda utilizar un RAID 6++ un RAID SAN FC es posible que prefiera asignar una unidad lógica a la base de datos y evitar el coste de un RAID SAN dedicado.

En este caso debe considerar que las bases de datos consumen una gran cantidad de recursos de disco y es posible que creen interferencias con los otros usuarios del SAN.

Para la comunicación entre los nodos del clúster se utiliza una red privada (física o una VLAN) que sirve tanto para los dispositivos de fencing, encargados de apagar un nodo cuando falla como para la comunicación de Linux-HA (Heartbeat).

El clúster necesita también un disco lógico de quorum que sirve como un importante apoyo para determinar que nodo del clúster es el que está fallando.

El siguiente gráfico está basado en un sistema de disco SAN sobre fibra óptica. Actualmente es una de las opciones más caras, pero también es la que mayor rendimiento proporciona. El disco compartido se aloja en un RAID SAN FC.

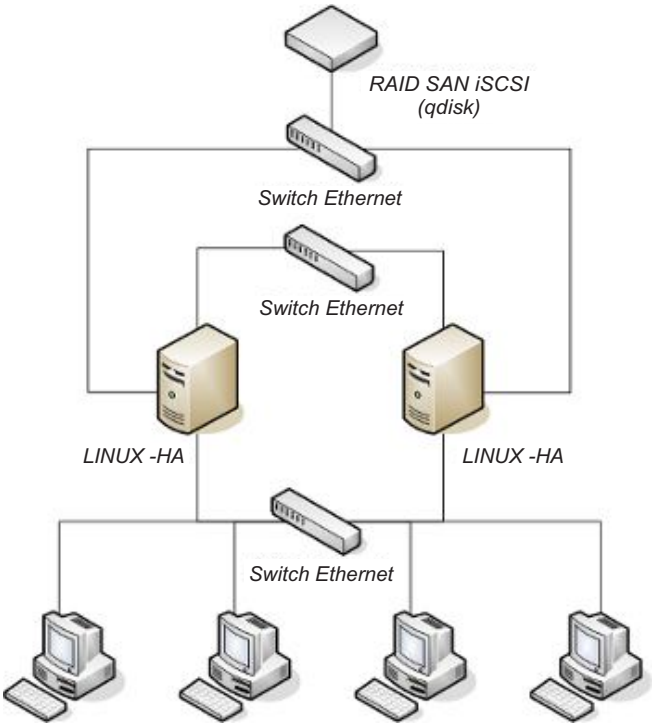


Servidor Redundante Estándar

En este caso, el sistema está basado en un conjunto de servidores principal- secundario, con redundancia en caliente y servicios de clusterización.

Esta solución sólo incluye requerimientos especiales de Software. Su aplicación se realiza en entornos LAN. El tiempo de recuperación es imperceptible por el operador -usuario.

En el siguiente gráfico, el sistema está basado en un sistema de Disco SAN sobre iSCSI. En esta configuración se sustituye el RAID SAN FC por un RAID iSCSI, más económico, que funciona sobre Ethernet Gigabit. Aunque el ancho de banda disponible entre los servidores y el disco SAN es considerablemente menor, también lo es el coste total de clúster ya que tampoco es necesario el SWITCH FC ni las tarjetas FC.

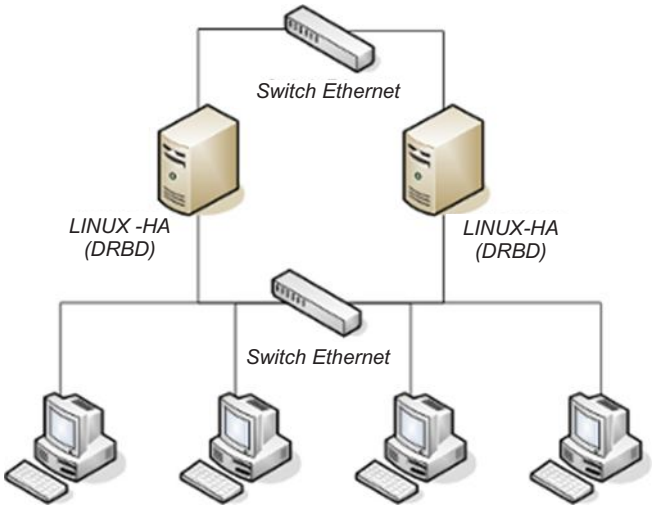


iSCSI es un protocolo IP que básicamente permite ejecutar comandos SCSI sobre una LAN. El rendimiento del protocolo se puede ver considerablemente afectado si no se ejecuta en una red dedicada (física o VLAN). Suele considerarse como una alternativa de bajo coste frente a la fibra óptica (FCP).

Servidor de BackUp

Finalmente, este último sistema está basado en un conjunto de servidores principal- secundario (redundancia en frío). El servidor de respaldo permanece inactivo y sólo es puesto en servicio una vez que el principal ha caído. Requiere de respaldos periódicos - BackUps de la base de datos con una periodicidad mínima diaria. El tiempo de restauración puede durar varias horas.

En el siguiente gráfico, nos basaremos en un sistema de DRDB – RAID 1 sobre Ethernet. Finalmente, puede eliminarse el RAID SAN por completo y utilizar DRDB, un software de duplicado de disco a través de la red. DRDB puede verse como un RAID-1 de red. Los nodos del clúster comparten la base de datos mediante el duplicado de los datos del nodo activo al nodo pasivo en lugar de utilizar el mismo disco de SAN.



Obviamente esta es la configuración más económica de las tres ya que sustituimos el RAID SAN por dos discos duros convencionales y un cable directo que une los dos nodos del clúster. No obstante, se trata de una solución real de alta disponibilidad y puede tenerse en cuenta, sobre todo cuando se cuenta con un presupuesto ajustado.

9.3.4.3 Software de gestión y módulos de integración

Una vez seleccionada la arquitectura y mecanismo de alta disponibilidad, pasaremos a la elección del software de gestión. La variedad de aplicaciones en el mercado está creciendo conforme a la demanda y se puede elegir de una extensa gama de fabricantes, donde en algún caso son plataformas desarrolladas sobre sistemas de vídeo y control de accesos.

La plataforma de centralización, normalmente se compone de una herramienta de desarrollo y personalización, al que se pueden añadir una serie de módulos opcionales, que permiten cubrir las necesidades puntuales de cualquier instalación.

Atendiendo a los distintos subsistemas de integración que incluyen los softwares del mercado, identificaremos las necesidades a valorar en cada subsistema que lo compone, indicando las características necesarias, en función de nuestra Infraestructura Crítica a proteger:

CCAA (Control de Accesos)

Número de Puertas. Seleccionar el software en función del número de puertas que debamos controlar, teniendo en cuenta cada uno de los inmuebles que controle el Sistema (sede principal y sucursales), y sus posibles ampliaciones en inmuebles.

Niveles de seguridad. Según el estado de alerta, deberemos aumentar o disminuir el requerimiento de acceso. Así pues, un sistema elevado podrá requerir una doble habilitación (p.ej. tarjeta y huella dactilar o código en el teclado y reconocimiento facial, o en situaciones de alerta máxima, además de lo anterior, autorizar la apertura remota por un operador que pueda identificar al usuario a través de la cámara).

Cerraduras. Otra de las características de estos accesos puede nacer por no tener la misma cerradura para todas las puertas, pero con lectores con accesos individuales por cada empleado, permitiendo dar altas y bajas de empleados, con el consiguiente ahorro de costes en mantenimiento y amaestramiento de bombillos.

Uso amigable. La elección de lectores puede facilitar a los usuarios el no tener que recordar códigos, con las consiguientes falsas alertas o recodificaciones. Las nuevas tecnologías ayudan a que las huellas dactilares, venas, oculares, faciales, etc. evitan el llevar tarjetas o memorizar codificaciones para cada usuario, minimizando los riesgos por pérdidas o sustracciones.

Control de Presencia. El sistema a escoger puede incluir sistemas complementarios de control de presencia o de horario, evitando equipamiento redundante.

Cuartos de Seguridad. El disponer de usuarios con distintos perfiles, permitirá autorizar el acceso a distintos cuartos de seguridad restringida, incluso en franjas horarias, tales como despachos, almacenes, cajas fuertes, armarios informáticos, etc.

Control de visitas. Existen sistemas que, además de lo anteriormente descrito, permiten tener un control del personal visitante e incluso su ubicación dentro de las infraestructuras.

Acceso en instalaciones. Algunos de estos sistemas permiten integrar los accesos en aparcamientos, uso de ascensores, entradas de vehículos y su seguimiento. Sirva como ejemplo, la posibilidad de registrar una visita a la I.C. (infraestructura crítica) a través del parking, registrando su huella dactilar, reconocimiento facial, etc. y a partir de este registro, dirigirle hacia zona de aparcamiento, ascensores o planta de personal donde se le vaya a atender.

Gráficos de pantalla. Tan importante como las herramientas que ayudarán a los usuarios a gestionar los niveles de seguridad es la sencillez de interpretación en pantalla, que permita una toma de decisiones rápida y adecuada.

CCTV

Número de cámaras. Seleccionar el software en función del número de cámaras que debamos controlar y teniendo en cuenta cada uno de los inmuebles que controle el Sistema (sede principal y sucursales), y sus posibles ampliaciones en inmuebles.

Cuadrantes. Los niveles de selección y de alerta por pantalla que puedan confeccionar los operadores es uno de los factores más relevantes.

Ancho de banda. Algunas aplicaciones requieren mucho ancho de banda para poder trabajar, ralentizando o encareciendo los costes de instalación.

Nivel de detalle. Una gran definición de las imágenes obtenidas aporta la información necesaria para la toma de decisiones. Las cámaras podrán tener una gran resolución, pero el nivel de detalle mostrado en el monitor y la gestión de las mismas, son elementos muy relevantes a la hora de la selección.

Búsqueda de elementos de control y objetos perdidos. Esta opción es de gran importancia, ya que permite disponer de un control rápido de lo que pueda estar ocurriendo o ya haya ocurrido.

Videoanálisis. Los sistemas de cámaras pueden generar sistemas de alerta y para evitar un alto índice de FAR (falsas alarmas) el SW (software) de gestión ha de ser de gran calidad.

INTRUSIÓN

Número de sinópticos. Seleccionar el software en función del número de elementos de detección del sistema de intrusión y sus estados.

Integración entre los sistemas de CCTV e Intrusión. Ambos han de complementarse, permitiendo identificar de forma inmediata la intrusión, apoyada con la parte visual.

El SW de gestión ha de permitir la ampliación de nuevos elementos de seguridad que puedan ir apareciendo en el mercado, bajo cualquier estándar, siempre que estos resulten de interés para la defensa de nuestra I.C., en otras palabras, el SW ha de ser escalable y ampliable y no ser un equipamiento cerrado, ya que la evolución de la I.C. ha de tener su contraprestación en el equipamiento de defensa.

Detección temprana y alerta confirmada. La posibilidad de confirmación del suceso seguro es uno de los retos de los SW de gestión, ya que el tiempo de detección es vital para disponer de una respuesta adecuada. Así pues, la combinación de elementos pasivos con activos, ralentizarán los accesos o salidas del recinto y su detección nos ayudará a disponer de las medidas de respuesta para la zona en el que haya sido detectado.

CIBERSEGURIDAD

Detección combinada. Todos los elementos anteriormente descritos han de combinarse también con un sistema de protección contra ciberataques. La posibilidad de que se produzca un ciberataque en las proximidades de la I.C. puede conllevar una vulnerabilidad de los sistemas de seguridad locales posibilitando brechas que permitan el acceso a su interior.

Detección estructurada por capas. Otra de las características del sistema ha de tener una combinación de varias capas de seguridad, podrá proteger fácilmente a los usuarios en cualquier lugar, a la vez que simplifica la implementación y la administración de la protección, protegiendo:

- Todos los ordenadores, dispositivos móviles y servidores de la red.
- Sucursales y usuarios remotos conectados a través de VPN.
- Servidores web y de correo electrónico, e incluso usuarios de wifi.

Interrelación con otras herramientas de SW. La necesidad y la rápida evolución de los sistemas informáticos ha de tener una continuada revisión de los sistemas y una rápida implementación de los mismos, que permita seguir protegiendo los sistemas de la I.C.

Compatibilidad y metodología. El sistema ha de ser rígido en su estabilidad y fácil de implementarse con las políticas empresariales de seguridad para los empleados y servicios contratados.

VISUALIZACIÓN E INTERFAZ

Multipantalla. El sistema ha de disponer de múltiples sistemas de visualización, tanto en Video-Wall, interrelación entre pantallas, redireccionando los entornos o duplicándolos para el uso de nuevos operadores de monitorización.

Iconografía propia. El sistema ha de permitir un diseño de iconos reconocibles por el usuario, que mejore los tiempos de gestión y no haya de aprender nuevas leyendas, con los posibles errores que pudieran derivarse.

Continuidad de gestión. El sistema ha de permitir disponer de herramientas de control intermedias, pudiendo desplazarse entre puntos de control con elementos portátiles, tales como smartphones, tablets, o cualquier otro gadget de pantalla. Sirva, por ejemplo, la necesidad de seguir gestionando un control de accesos fuera de un entorno no operativo (por avería), hasta su reposición o reubicación en un nuevo emplazamiento.

9.3.5 Sistemas de alimentación

Fuente de energía para proporcionar la alimentación principal.

Obligadamente debe cumplir los requisitos impuestos por el vigente Reglamento Electrotécnico de Baja Tensión e Instrucciones Técnicas complementarias aplicables.

9.3.5.1 SAI-UPS.

A fin de cumplimentar los requerimientos impuestos por la Norma UNE-EN 50131-6 para la alimentación de los Sistemas de Protección de las Instalaciones Críticas podrá recurrirse a la instalación de:

- SAIs que se encarguen de recargar Baterías para la alimentación de emergencia del Sistema de Seguridad por un mínimo de 120 horas (Tipo B de las soluciones definidas en la UNE-EN 50131-6).
- SAIs que constituyan la fuente principal de alimentación del Sistema de Seguridad, por lo que deberá poder efectuarlo, como mínimo, durante un año (Tipo C de las soluciones definidas en la UNE-EN 50131-6).

Dichos SAIs deberán cumplir los requisitos funcionales exigidos en las Normas UNE-EN 50131-1 y UNE-EN 50131-6 para los que presten servicio a Sistemas de Grado Cuatro en dichos Tipos.

9.3.5.2 Grupos electrógenos.

A fin de cumplimentar los requerimientos impuestos por la Norma UNE-EN 50131-6 para la alimentación de los Sistemas de Protección de las Instalaciones Críticas podrá recurrirse a la instalación de:

- Grupos Electrógenos que se encarguen de recargar Baterías para la alimentación de emergencia del Sistema de Seguridad por un mínimo de 120 horas (Tipo B de las soluciones definidas en la UNE-EN 50131-6).
- Grupos Electrógenos que constituyan la fuente principal de alimentación del Sistema de Seguridad, por lo que deberá poder efectuarlo, como mínimo, durante un año (Tipo C de las soluciones definidas en la UNE-EN 50131-6).

Dichos Grupos Electrógenas deberán:

- Cumplir los requisitos funcionales exigidos en las Normas UNE-EN 50131-1 y UNE-EN 50131-6 para los que presten servicio a Sistemas de Grado Cuatro en dichos Tipos.
- Su lugar de instalación deberá estar insonorizado y provisto de una salida de gases canalizada al exterior, además de estar bien ventilado, para evitar que el motor del Grupo se deteriore rápidamente. Además, la ventilación de la Sala deberá garantizar el ingreso de aire fresco y la salida de aire caliente sin restricciones.

9.3.5.3 Fuentes de alimentación.

A fin de cumplimentar los requerimientos impuestos por la Norma UNE-EN 50131-6, los Sistemas de Protección de las Instalaciones Críticas podrán contar con Fuentes de Alimentación integradas en los propios Equipos componentes del Sistema o con Fuentes de Alimentación Independientes (Grupos Electrógenos o S.A.Is, para los que ya se han indicado los requisitos a reunir), destinadas a alimentar a la totalidad o parte del Sistema ya sea de modo permanentemente o en caso de cesar el suministro principal por cualquier causa.

Las Fuentes integradas en los Equipos componentes del Sistema (Tipo A de la Norma UNE-EN 50131-6:2008) deben cumplir con los requisitos, criterios de rendimiento y procedimientos de ensayo impuestos para ellas en la Norma antedicha y, en consecuencia, deben estar certificadas por un Organismo de Acreditación reconocido según la Norma UNE-EN 45011:1998, y deberán cumplir los siguientes requisitos:

- Duración mínima de la alimentación de emergencia proporcionada: 60 horas
- Tiempo máximo de recarga: 24 horas.

10 Certificación de la instalación

La norma en vigor Orden INT/316/2011, de 1 de febrero, sobre funcionamiento de los sistemas de alarma en el ámbito de la seguridad privada, establece en su artículo 4 la obligatoriedad del proyecto y certificado de instalación en los siguientes términos:

1. El proyecto de instalación, al que hace referencia el artículo 42 del Reglamento de Seguridad Privada, estará elaborado de acuerdo con la Norma UNE-CLC/TS 50131-7. En ella, se determinan las características del diseño, instalación, funcionamiento y mantenimiento de sistemas de alarma de intrusión, con los cuales se pretende conseguir sistemas que generen un mínimo de falsas alarmas.

2. 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.

Atendiendo a lo indicado en la presente guía, las instalaciones Grado 3 y 4 deberían incluir en el certificado la referencia explícita al cumplimiento con las normas técnicas asociadas a los subsistemas de seguridad que componen el sistema combinado e integrado de alarmas, en línea con lo establecido por la norma 50398.

Se propone a continuación el modelo de certificado con cláusula que hace referencia al cumplimiento anteriormente descrito, esta cláusula deberá ser adaptada según las características particulares de cada instalación.

> *"6º.- Que en línea con los sistemas de seguridad indicados los Sistemas de Control de Accesos, de Videovigilancia (CCTV), los posibles sistemas combinados y las distintas interacciones entre unos y otros han sido diseñados e instalados de acuerdo al correspondiente proyecto de instalación realizado en conformidad con las Normas vigentes en cada uno de los casos."*

Modelo Propuesto de "CERTIFICADO DE ENTREGA DE INSTALACION DE SEGURIDAD"

CERTIFICADO DE ENTREGA DE INSTALACION DE SEGURIDAD

D. **……** técnico de **xxxxxxxxxxxxxxxxxxxxxxxxx** empresa inscrita en el registro de Empresas de Seguridad con el número xxxxx, domiciliada en C/ xxxxxxxxxxx.

CERTIFICA:

1º.- Que la ejecución de la instalación de seguridad efectuada para _____

_____ con número de contrato/oferta _____ ha sido realizada bajo la dirección y control de **xxxxxxxxxxxxxxx.**, de acuerdo con el proyecto contratado y con la documentación técnica que define los aparatos y dispositivos que la integran.

2º.- Que dicho sistema de seguridad, de acuerdo con la información aportada por su titular y los riesgos analizados por **xxxxxxxxxxxxxx**cumple la finalidad preventiva y protectora acordada con el cliente.

3º.- Que reuniendo el sistema de seguridad las condiciones y requisitos de la vigente Normativa de Seguridad Privada, se entrega a ……., en representación de su titular, junto con los manuales que son preceptivos, para que se dediquen, debidamente conservados, al fin destinado.

4º.- Que los controles y pruebas efectuadas en la instalación del sistema de seguridad, han sido plenamente satisfactorias, no habiéndose apreciado deficiencias en el funcionamiento de la instalación.

5º.- Que para la instalaciones con conexión a C.R.A., los controles y pruebas efectuadas han sido plenamente satisfactorias, no habiéndose apreciado deficiencias en la transmisión o recepción en la Central Receptora de las señales de alarma, provocadas desde la instalación, y que dicho sistema de seguridad reúne los requisitos exigidos por la normativa vigente para su conexión a Central de Alarmas, siendo su número de contrato de Conexión a la Central receptora de alarmas de **xxxxxxxxxxxxxxxxxx** el **……..**

En este supuesto, el cliente viene obligado por la normativa de seguridad privada a realizar un contrato de mantenimiento.

6º.- Que en línea con los sistemas de seguridad indicados los Sistemas de Control de Accesos, de Videovigilancia (CCTV), los posibles sistemas combinados y las distintas interacciones entre unos y otros han sido diseñados e instalados de acuerdo al correspondiente proyecto de instalación realizado en conformidad con las Normas vigentes en cada uno de los casos

7ª Que igualmente el proyecto de instalación global ha sido realizado de conformidad con la Norna UNE-CLC/TS 50131-7

7º.- Los elementos y dispositivos instalados cumplen con lo especificado en la Orden INT/316/2011

8º.- El grado del sistema de seguridad de acuerdo a lo especificado en la Orden INT/316/2011

es: **GRADO ___**

Para que conste, y a efectos de dar cumplimiento a lo dispuesto en el artículo 42 del Reglamento de Seguridad Privada, y, en su caso, la normativa de protección de datos de carácter personal, expido el presente en ……., a…… de …… de 20…….

Conforme **EL CLIENTE** Por **xxxxxxxxxxxxxxxxxxx**,

Fdo.:_____ Fdo.: D. _____

ANEXO I – LISTADO DE MATERIALES INSTALADOS

CLIENTE: …….

UBICACIÓN: …….

ELEMENTO	UDS	GRADO(*)	MARCA	MODELO

(*) Según Orden INT/316/2011

Para que conste, y a efectos de dar cumplimiento a lo dispuesto en el artículo 42 del Reglamento de Seguridad Privada, expido el presente en …….. a …….. de ……de 202

Conforme **EL CLIENTE**

Por **xxxxxxxxxxxxxxxxxxx.**,

Fdo.: D._____

Fdo: _____

11 Glosario de términos

BMS: Acrónimo del término inglés Building Management System, sistemas de gestión de edificios permite la automatización y el control centralizado de los inmuebles para convertirlos en edificios inteligentes.

CCAA: Sistema de Control de Accesos de Seguridad

CCF: Acrónimo del término inglés "Central Control Facility" que hace referencia a los equipos utilizados para los propósitos de control y/o de señalización que se conectan a una o más aplicaciones y que están atendidos habitualmente por personal de operación.

CCTV: Sistema de Circuito Cerrado de Televisión

CNPIC: Centro Nacional de Protección de Infraestructuras Críticas es el Órgano del Ministerio del Interior encargado del impulso, la coordinación y supervisión de todas las actividades que tiene encomendadas la Secretaría de Estado de Seguridad en relación con la Protección de Infraestructuras Críticas en el territorio nacional.

ENS: Esquema Nacional de Seguridad El Real Decreto 3/2010, de 8 de enero, regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

IICC: Infraestructuras críticas según lo establecido en Ley PIC 8/2011.

Ley PIC: Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

IAS: Acrónimo del término inglés "Intrusion Alarm Systems" sistemas de alarma de detección de intrusión.

FAT: Acrónimo del término inglés "Factory Acceptance Test" o ensayos de aceptación en fábrica.

iSCSI: Abreviatura de Internet SCSI es un estándar que permite el uso del protocolo SCSI sobre redes TCP/IP. iSCSI es un protocolo de la capa de transporte definido en las especificaciones SCSI-3.

LAN: Red de área local por sus siglas en inglés Local Area Network.

Normas UNE: Normas UNE son un conjunto unificado de normas técnicas creadas por los Comités Técnicos de Normalización o CTN. De estos comités forman parte diferentes sectores dentro de la actividad productiva o de comercialización.

Normas EN: Normas Europeas, que elaboran, proponen y desarrollan los expertos de los diferentes Estados Miembros, de los sectores industriales o tecnológicos dentro de la estructura de normalización del Comité Europeo de Normalización (CEN).

Normas UNE-EN: Son la versión oficial en español de las normas europeas. Son normas adoptadas y armonizadas tras la aprobación del órgano especifico dentro de la estructura de normalización nacional de AENOR.

OSDP: Open Supervised Device Protocol o Protocolo de Dispositivos Abiertos Supervisados es una norma de comunicaciones de control de acceso desarrollada por la Asociación de la Industria de la Seguridad (SIA) para mejorar la interoperabilidad entre el control de acceso y los productos de seguridad.

PPE: Plan de Protección Específico según establece la Ley PIC 8/2011 y el Real Decreto 704/2011 que la desarrolla.

OT: Operational Technology.

PSO: Plan de Seguridad del Operador según establece la Ley PIC 8/2011 y el Real Decreto 704/2011 que la desarrolla.

RAID: Acrónimo del inglés que significa Redundant Array of Independent Disks, literalmente «matriz de discos independientes redundantes.

SAN: Storage Area Network, red de alta velocidad independiente y dedicada que interconecta y suministra depósitos compartidos de dispositivos de almacenamiento a varios servidores.

SAT: Acrónimo del término inglés "Site Acceptance Test" o ensayos de aceptación en el emplazamiento.

SCI: Sistema de Control Industrial.

SAI-UPS: Sistema de Alimentación Ininterrumpida), también conocido por sus siglas en inglés, UPS (Uninterrupted Power Supply).

SCSI: Interfaz de sistemas informáticos pequeños, más conocida por el acrónimo inglés SCSI (Small Computer System Interface).

UCSP: Unidad Central de Seguridad Privada es el servicio del Cuerpo Nacional de Policía (CNP) encargado de las relaciones y el control del sector de la Seguridad Privada.

VMS: Sistema de gestión de vídeo del inglés Video Management System.

VPN: Red privada virtual, del inglés Virtual Private Network.

VSS: Sistema de videovigilancia del inglés Video Surveillance System.

12 Anexo I.- Serie UNE-EN 50531-x

Se detallan a continuación las características especiales que deben cumplir los dispositivos de fábrica para cumplir con la especificación establecida por la norma **UNE-EN 50131-x** en lo relativo a grados 3 y 4.

EN-50131-1 Sistemas de Alarma.- Requisitos del sistema.

6. Grados de Seguridad.

Grado 3, Riesgo medio a alto.

Grado 4, Riesgo Alto.

8. Requisitos funcionales.

8.1.4 Constatación de fallos. Tabla 1, Fallos.

8.3. Utilización.

8.3.2. Autorización. Tabla 3, Requisitos relativos a los códigos de autorización.

8.3.5. Prohibición de la activación. Tabla 4, Prohibición de la activación.

8.3.6. Derogación de la Prohibición de la activación. Tabla 5, condiciones de la derogación de la Prohibición de la activación.

8.3.9. Reactivación. Tabla 6, Reactivación.

8.4. Procesamiento de señales. Tabla 7, Procesamiento de las señales.

8.5. Señalizaciones. Tabla 8, señalización.

8.5.2. Disponibilidad de las Señalizaciones. Tabla 9, señalizaciones disponibles.

8.6. Notificación. Tabla 10, requisitos relativos a la notificación.

8.7.2. Detección de la manipulación. Tabla 12, Detección de la manipulación, componentes a incluir. Tabla 13, Modalidad a detectar.

8.7.3. Supervisión de sustitución. Tabla 14. Cuando el sistema de alarma se encuentre activado o desactivado, y se detecte sustitución, se debe generar señal de manipulación Opcional en Grado 3, Obligatoria en Grado 4.

8.7.4. Supervisión de sustitución, tiempo de respuesta. Tabla 15.

8.8.3. Supervisión de enlaces. Tabla 16. Duración máxima autorizada para enlace INDISPONIBLE, Grado 3, 100 seg. Grado 4, 10 seg.

8.8.4.1. Integridad del enlace. Comunicación periódica. Tabla 17. Intervalo máximo permitido entre señales o mensajes de comunicación periódica, Grado 3, 100 seg. Grado 4, 10 seg.

8.8.4.2. Verificación durante el procedimiento de activación. Tabla 18. Tiempo máximo desde la recepción de la última señal o mensaje, Grado 3, 60 seg. Grado 4, 10 seg.

8.8.5. Seguridad de la comunicación. Tabla 19. Los sistemas de grado 4 deben incluir los medios para detectar el retardo, la modificación, la sustitución o la perdida de cualquier señal o mensaje, de forma obligatoria. En Grado 3, es opcional.

8.8.6. Señales o mensajes a generar. Tabla 20.

8.10. Registro de incidencias. Número mínimo de incidencias, Grado 3, 500 Incidencias. Grado 4, 1000 incidencias. Persistencia mínima de la memoria ante corte de la alimentación, Grado 3 y Grado 4, 30 días. Incidencias a registrar, tabla 22.

9. Fuentes de alimentación.

Duración mínima de la fuente de alimentación de emergencia:

Tipo A, recargable, Grado 3 y 4, 60 horas. (tiempo máximo de la recarga en ambos casos, 24 horas).

Tipo B, no recargable, Grado 3 y 4, 120 horas.

EN-50131-2-2 Sistemas de Alarma.- Detectores de intrusión. Detectores infrarrojos pasivos.

4.1. Procesamiento de incidencias. Tabla 1.

4.2. Detección.

4.2.1. Características de funcionamiento de la detección. Tabla 3.

4.2.2. Señalización de la detección. En Grado 3 y 4 el indicador debe de poderse activar y desactivar a distancia en el Nivel 2 de acceso.

4.3. Requisitos de funcionamiento.

4.3.1. Intervalo de tiempo entre señales o mensajes de intrusión. El tiempo entre señales de intrusión deben de ser para Grado 3, 30 seg. Para Grado 4, 15 seg.

4.5. Seguridad frente a la manipulación. Tabla 4.

4.6. Requisitos eléctricos. Estos requerimientos no son aplicables a los detectores que tiene fuente de alimentación interna tipo C (ver Norma EN-50131-6)

6.3. Ensayos de paseo.

6.3.5. Verificar características de detección con movimiento intermitente. Para Grados 3 y 4, el movimiento intermitente debe consistir en el SWT caminado 1m a una velocidad de un 1m/seg. parándose y continuando durante 5 seg. antes de continuar, repitiéndose hasta atravesar todo el área de detección.

6.3.6. Verificar las características de detección próxima. Los ensayos comienzan para Grado 3 y 4 a una distancia de 0,5m+/-0,05m, desde el eje vertical del detector.

6.5. Autoensayos. Criterios de superación/fallo Para detectores de Grado 3 y 4, se supervisa el detector durante el autoensayo local. Para Grado 4 también se supervisa el detector durante el autoensayo a distancia.

6.8.2. Cambio lento de tensión de alimentación y límites del intervalo de tensión de alimentación. Generación de señal de intrusión y no señal de fallo. Para Grado 3 y 4 la tensión se baja en escalones de 0,1 V/seg. a pasos no mayores de 10mV hasta que se genere señal de fallo. Deben también generar una señal de fallo antes de no generar una señal de intrusión.

EN-50131-2-3 Sistemas de Alarma.- Detectores de Intrusión. Requisitos para detectores de microondas.

4. Requisitos de funcionamiento.

4.1. Tratamiento de incidencias. Tabla 1.

4.2.1. Funcionamiento de la detección. Tabla 3.

4.2.2. Indicación de la detección. En los Grados 3 y 4, el indicador de generación de mensaje de intrusión debe ser capaz de activarse y desactivarse a distancia en el Nivel de acceso 2.

4.2.3. Reducción significativa del alcance. Los detectores de Grado 4 deben de detectar reducción significativa del alcance o área de cobertura debida.

4.3. Requisitos de funcionamiento.

4.3.1. Intervalo de tiempo entre señales o mensajes de intrusión. Los detectores cableados deben de ser capaces de proporcionar una señal de intrusión no más tarde de 15 seg. después del final de la señal precedente. Los detectores inalámbricos en Grado 3, 30 seg. En Grado 4, 15 seg.

4.5. Seguridad frente a la manipulación.

4.5.5. Detección del enmascaramiento. (Reorientación del detector nunca superior a 5°) Tabla 4.

4.6. Requisitos eléctricos. (Estos requisitos no son aplicables a los detectores que tienen fuente de alimentación tipo C, ver Norma EN-50131-6). Tabla 5.

6.3. Ensayos de paseo.

6.3.6. Verificar las características de detección próxima. Los ensayos comienzan para Grado 3 y 4 a una distancia de 0,5m+/-0,05m, desde el eje vertical del detector.

6.5. Autoensayos. Criterios de superación/fallo Para detectores de Grado 3 y 4, se supervisa el detector durante el autoensayo local. Para Grado 4 también se supervisa el detector durante el autoensayo a distancia.

6.8.2. Cambio lento de tensión de alimentación y límites del intervalo de tensión de alimentación. Generación de señal de intrusión y no señal de fallo. Para Grado 3 y 4 la tensión se baja en escalones de 0,1 V/seg. a pasos no mayores de 10mV hasta que se genere señal de fallo. Deben también generar una señal de fallo antes de no generar una señal de intrusión.

EN-50131-2-4 Sistemas de Alarma.- Detectores de Intrusión. Requisitos para detectores combinados de infrarrojos pasivos y microondas.

*Los mismos requisitos y parámetros de ensayo de EN-50131-2-2 y EN-50131-2-3.

EN-50131-2-5 Sistemas de Alarma.- Detectores de Intrusión. Requisitos para detectores combinados de infrarrojos pasivos y ultrasónicos.

*Los mismos requisitos y parámetros de ensayo de EN-50131-2-2 y EN-50131-2-3.

EN-50131-2-6 Sistemas de Alarma.- Detectores de Intrusión. Contactos de apertura (magnéticos).

4. Requisitos de Funcionamiento.

4.1. Incidencias. Tabla 1.

4.2. Señales o mensajes. Tabla 2.

4.3. Detección.

4.3.2. Señalización de la detección. Para Grado 3 y 4 un detector debe de ser capaz de recibir los comandos de activación y desactivación remota de la indicación cuando el indicador esté presente.

4.4. Requisitos de funcionamiento.

4.4.1 Intervalo de tiempo entre señales o mensajes de intrusión. El tiempo entre señales de intrusión deben de ser para Grado 3, 30 seg. y para Grado 4, 15 seg.

4.5. Seguridad frente a la manipulación.

4.5.2. Prevención del acceso no autorizado al interior del detector a través de las tapas y orificios existentes. Para detectores de Grado 3 y 4, todas las tapas que dan acceso a los componentes que pudieran afectar adversamente al funcionamiento del detector, deben equiparse con un dispositivo de detección de manipulación.

4.6. Requisitos eléctricos. Tabla 3.

4.7. Clasificación y condiciones ambientales. Para todos los grados, el detector no debe generar o verse afectado por las condiciones y niveles de severidad de CEM definidos en las Normas EN 50130-4 y EN 61000-6-3.

6.6. Seguridad frente a la manipulación.

6.6.4. Resistencia a la interferencia de campo magnético. (ensayo especifico para Grados 3 y 4).

EN-50131-3 Sistemas de Alarma.- Equipo de Control y señalización.

8. Requisitos funcionales.

8.1.4. Fallo. Tabla 1.

8.3. Operación.

8.3.2. Autorización.

8.3.2.2.2. Claves digitales. En Grados 3 y 4 se deben incluir medios para evitar la aceptación de códigos copiados de datos interceptados (desde un lugar a más de 1 m del CIE).

8.3.2.2.3. Claves biométricas. Tabla 2.

8.3.2.3. Utilización de métodos de autorización en combinación. Tabla 3.

8.3.2.4. Detección de intentos repetitivos de autorización inválida. Tabla 4.

8.4. Procesamiento.

8.4.3. Monitotización del procesamiento del CIE. Tabla 5.

8.5. Señalización.

8.5.1. Generalidades. Tabla 6.

8.6. Salidas de notificación. Se debe de proporcionar los para notificar de manera remota el "acceso de nivel 3" en Grado 3.

8.7. Seguridad frente a la manipulación (detección/protección)

8.7.1. Protección frente a la manipulación. Tabla 7.

8.7.2. Detección de la manipulación. Tabla 8.

8.7.2.1. Acceso al interior de la envolvente. Tabla 9.

8.7.2.2. Retirada del montaje. Tabla 10.

8.10. Registro de Incidencias. Tabla 11. En los CIE de Grado 3 y 4, se deben proporcionar los medios para almacenar el registro de incidencias de manera permanente.

8.10.2. Registro de las incidencias en el ARC u otro emplazamiento remoto. En grado 3 y 4, cuando la transmisión de las incidencias haya fallado se deben transferir a un componente del I&HAS apropiado para su almacenamiento hasta que la transferencia sea posible.

11.3. Ensayo funcional reducido.

11.5. Nivel de acceso.

11.6.2.1. Ensayos de la clave digital.

d) Procedimiento de ensayo.

1) El número de códigos validos debe ser: 50 para grado 3, 100 para grado 4.

11.7.9. Monitorización del procesamiento del CIE.

b) principio. Tabla 29.

EN-50131-4 Sistemas de Alarma.- Dispositivos de advertencia.

5. Requisitos.

5.1. Funcionales.

5.1.1. Respuestas. Tabla 1.

5.2. Manipulación.

5.2.1. Protección. Tabla 5.

5.2.2. Detección. Tabla 6 y 7.

5.6. Eléctricos.

5.6.3. Autoalimentación.

5.6.3.2. Tiempo en espera del dispositivo acumulador. Tabla 8.

5.6.3.3. Velocidad de recarga. Tabla 9.

5.7. Requisitos de auto ensayo.

5.7.1.1. Generalidades. Tabla 10.

EN-50131-5-3 Sistemas de Alarma.- Requisitos para los equipos de interconexión que usan técnicas de radiofrecuencia.

4. Requisitos generales.

4.1. Inmunidad a la atenuación. Tabla 1.

4.2. Inmunidad a la colisión.

4.2.1 Requisitos relativos a la tasa de colisión. Nivel de confianza en las transmisiones de alarma y supervisión. Tabla 2. Para asegurarse de trasnmisiones satisfactorias en Grado 3 y 4, se debe de dar acuse de recibo a todos los tipos de mensajes (alarma, supervisión, etc) por el equipo receptor al equipo transmisor.

4.2.2. Requisitos realtivos a la relación de caudal. Tabla 3.

4.3. Inmunidad a la sustitución no intencionada e intencionada de componentes y mensajes. Tabla 4.

4.3.1. Inmunidad a la sustitución no intencionada e intencionada de componentes. Para los equipos de Grado 4, el CIE debe disponer de medios para detectar la sustitución.

4.3.2. Inmunidad a la sustitución intencionada de mensajes. Para los equipos de grado 3 y grado 4, el equipo receptor debe tener autenticación de mensajes. Tabla 5.

4.4. Inmunidad a interferencias.

4.4.3. Interferencias para los grados 3 y 4. Tabla 8.

4.5. Requisito para la supervisión de enlaces de RF.

4.5.1. Requisito para la detección de un fallo de comunicación periódica. En los grados 3 y 4, se debe evitar la puesta en servicion cuando el último mensaje de comunicación periódica desde cualquier equipo de transmisión exceda el periodo de la tabla 10.

4.5.2. Requisito para la detección de interferencias. Tabla 11, 12 y 1

5. Ensayos.

5.1.5.1. Ensayo de inmunidad a la sustitución de componentes de Grado 3 y 4. Se debe realizar el ensayo en cámara anecoica apantalada

5.1.6.3. Ensayos de interferencias para equipos de Grado 3 y 4. Se debe colocar el equipo como se muestra en el ANEXO B.

5.1.7.1. Ensayos para la detección de un fallo de comunicación periódica en un enlace.

a) Condiciones suplementarias de ensayo para verificar los enlaces entre un equipo transmisor y el CIE.

Para Grados 3 y 4, se debe verificar ue se impide al CIE su entrada en servicio según los tiempos de la tabla 10.

5.1.7.2. Ensayos para la detección de interferencias. Tabla 15.

EN-50131-6 Sistemas de Alarma.- Fuentes de alimentación.

4. Requisitos funcionales.

4.2. Supervisión de la fuente de alimentación. Tabla 1.

4.3. Periodo de reserva.

4.4. Recarga en una fuente de alimentación del Tipo A.

5. Diseño.

5.1. Protección frente a sobretensiones. Para los Grado 3 y 4, debe incorporarse una protección de las fuentes de alimentación que evite que la tensión continua de salida sobre pase la tensión máxima de alimentación de salida, a fin de evitar daños a otros componentes del sistema.

5.3. Protección frente a la descarga profunda. En aquellos casos en los que la descarga profunda del dispositivo acumulador pueda provocar daños a dicho dispositivo, en los grados 3 y 4 se deberá incorporar protección frente a la descarga profunda.

5.6. Seguridad frente a la manipulación.

5.6.1. Protección frente a la manipulación

5.6.2. Detección de la manipulación

5.6.2.1. Apertura de la envolvente.

5.6.2.3. Penetración en la envolvente. En el caso de una fuente de alimentación de Grado 4, debe de ser imposible la penetración en su envolvente con una herramienta que forme un agujero mayor de 4 mm sin que se genere una señal de manipulación.

8.1.5. Plan de ensayo.

Ensayos	Apartado	Grado 3	Grado 4
Inspección de la documentación	8.2.1	ABC	ABC
Marcado	8.2.2	ABC	ABC
Carga máxima	8.2.3	ABC	ABC
Variación gradual de la carga	8.2.4	ABC	ABC
Variación de la carga	8.2.5	ABC	ABC
Cortocircuito	8.2.6	ABC	ABC
Sobrecarga	8.2.7	ABC	ABC
Carga	8.2.8	A	A
Retención de la carga	8.2.9	A	A
Ondulación residual	8.2.10	AB	AB
Fallo de la fuente de alimentación externa	8.2.11	AB	AB
Fallo del dispositivo acumulador	8.2.12	AB	AB
Tensión baja del dispositivo acumulador	8.2.13	ABC	ABC
Tensión baja de salida	8.2.14	ABC	ABC
Tensión alta de salida	8.2.15	Op	ABC
Protección frente a la descarga profunda	8.2.16	ABC	ABC
Protección frente a la manipulación	8.2.17	ABC	ABC
Detección de la manipulación	8.2.18	ABC	ABC
NOTA – A, B Y C se refieren a los tipos de fuente de alimentación que se definen en 4.1			

EN-50131-7 Sistemas de Alarma.- Guía de aplicación.

4.1. Estructura de grados.

4.1.3. Grado 3: Riesgo medio a alto. Se esperan intrusos familiarizados con el IAS y que tengan una gama amplia de herramientas y equipo electrónico portátil.

4.1.4. Grado 4: Riesgo alto. A utilizar cuando la seguridad tiene prioridad sobre todos los demás factores. Se esperan intrusos con capacidad o recursos para planificar una intrusión con detalle y que tengan una gama completa de equipos, incluyendo medios de sustitución de componentes vitales en el IAS.

7.3. Propuesta de diseño del sistema.

7.3.2. Emplazamiento del equipo.

7.3.2.1. Emplazamiento del CIE. En los IAS de Grado 3 y 4 que activan, cualquier subsistema debería establecer también el subsistema que supervisa el área en la cual se sitúa el CIE.

ANEXO E. Niveles de supervisión.

A considerar	Grado 3	Grado 4
Puertas perimetrales	OP	OP
Ventanas	OP	OP
Otras aberturas	OP	OP
Paredes		P
Techos y tejados		P
Suelos		P
Sala		T
Objeto (alto riesgo)		S

O = Abertura P = Penetración T= Atrapado
S = Objeto que requiere especial consideración

ANEXO G. Estudio técnico.

G.20. Equipo de control y señalización y fuentes de alimentación.

xii) encaminamiento de la fuente de alimentación al IAS vía: Conexión a la red de alimentación mediante una acometida de derivación con fusible (recomendado para los IAS de Grado 3 y 4).

G.25. Dispositivo de aviso interno.

i) proximidad al CIE o ACE (en los IAS de Grado 3 y 4).

Dinamizando la Industria de la Seguridad

Asociación Española de Empresas de Seguridad

C/Alcalá, 99 2ºA - 28009 Madrid

Telf. 915 765 225

www.aesseguridad.es

aes@aesseguridad.es

@aes_seguridad

@aesseguridad2021