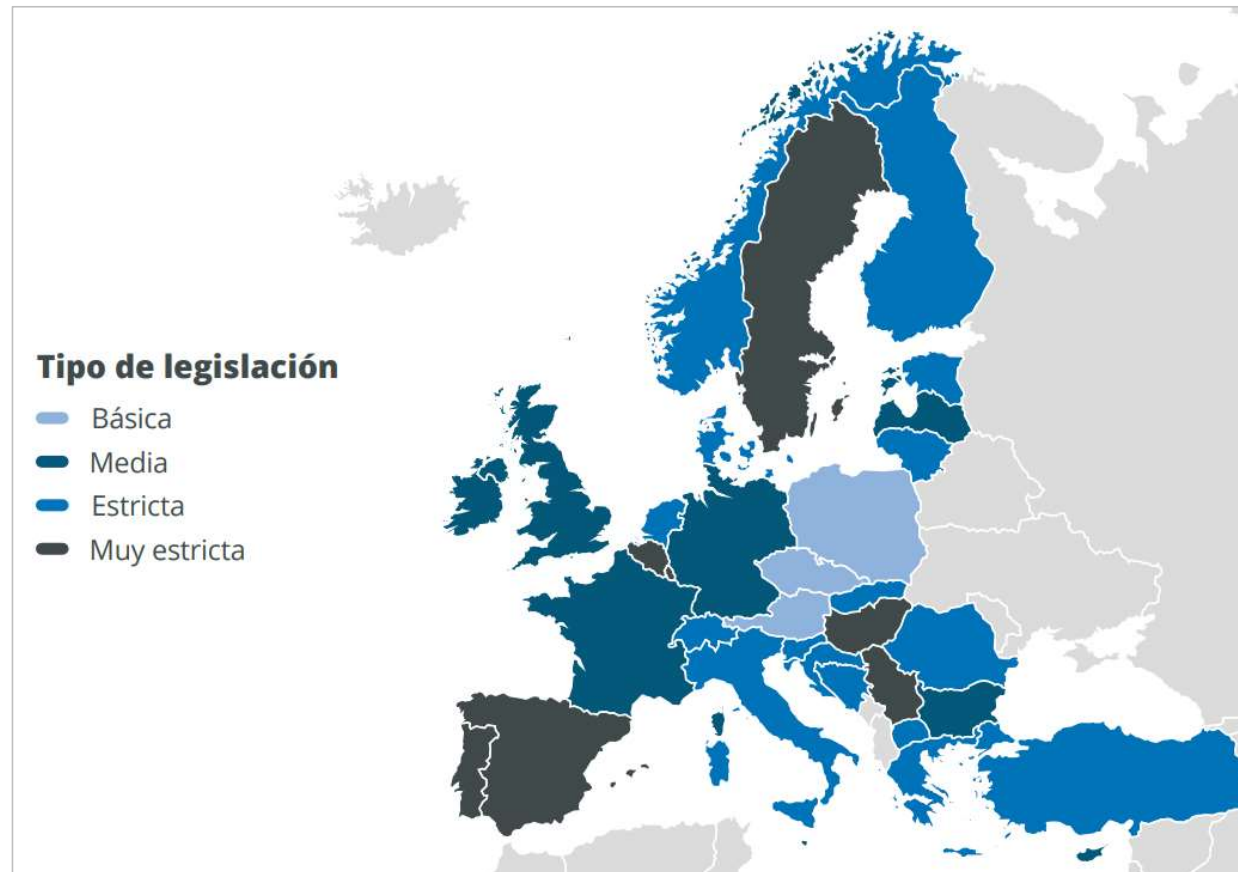




JORNADA SOBRE VIGLANCIA Y SISTEMAS DE SEGURIDAD

Badajoz, Diciembre de 2023



FUENTE: INFORME APROSER (El sector de la Seguridad Privada en España – 2022)

- En lo que respecta a **instalaciones y medidas de seguridad**, se concreta:
 - **Quiénes pueden realizar las mismas**: Únicamente las empresas de seguridad autorizadas podrán realizar las operaciones de instalación y mantenimiento de aparatos, dispositivos o sistemas de seguridad y alarma, cuando éstos pretendan conectarse a una central de alarmas, centros de control o de videovigilancia.
 - Cuáles deben ser las **características de los elementos que las integran (Normas UNE-EN 50xxx) y los contenidos y especificaciones de los proyectos de instalación (Norma UNE-CLC/TS 50131-7)**.
 - Se determinan los diferentes **Grados de Seguridad** (desde el 1 hasta el 4), que están determinados por el valor a proteger y por la capacidad técnica de los intrusos para intentar eludir y sabotear los sistemas.
 - En qué deben consistir las preceptivas **revisiones de mantenimiento de los sistemas**.
 - Se establecen los pasos a seguir o **protocolo de actuación** para considerar que una **alarma está correctamente verificada**, tanto por medios técnicos como humanos, y pueda ser comunicada a las Fuerzas y Cuerpos de Seguridad.
 - Se establecen los **plazos de adecuación** de aquellos sistemas que fueron instalados antes de la fecha de entrada en vigor de la presente Orden.
 - **Formación** del personal.

Principales consideraciones al respecto



BOLETÍN OFICIAL DEL ESTADO



Núm. 42

Viernes 18 de febrero de 2011

Sec. I. Pág. 18325

CAPÍTULO V

Formación del personal

Artículo 18. *Personal para el servicio de verificación de alarmas.*

Las empresas de seguridad responderán de que los vigilantes de seguridad encargados de la verificación personal de las alarmas cuenten con una formación específica para este tipo de servicios, de acuerdo con lo establecido a este respecto en la normativa sobre personal de seguridad privada, impartida en centros de formación autorizados.

Artículo 19. *Personal de instalación y mantenimiento.*

Las empresas de seguridad responderán de que, la formación de los responsables de los proyectos de instalación elaborados, así como la de los técnicos y operarios encargados de su ejecución, implique el conocimiento exhaustivo del contenido de las Normas UNE-EN 50131 y siguientes, de forma que cualquier instalación de seguridad se ajuste a lo establecido en ellas.

Artículo 20. *Personal de centrales de alarmas.*

Las empresas de seguridad responderán de que la formación de los operadores y demás personal dedicado al tratamiento de las señales de alarma que reciban las centrales, procedentes de los sistemas conectados a ellas, cuenten con una formación técnica y operativa específica, que les permita cumplir, como mínimo, con los procedimientos de actuación exigidos en esta Orden.



I. DISPOSICIONES GENERALES

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

7133 Orden ITC/1142/2010, de 29 de abril, por la que se desarrolla el Reglamento regulador de la actividad de instalación y mantenimiento de equipos y sistemas de telecomunicación, aprobado por el Real Decreto 244/2010, de 5 de marzo.

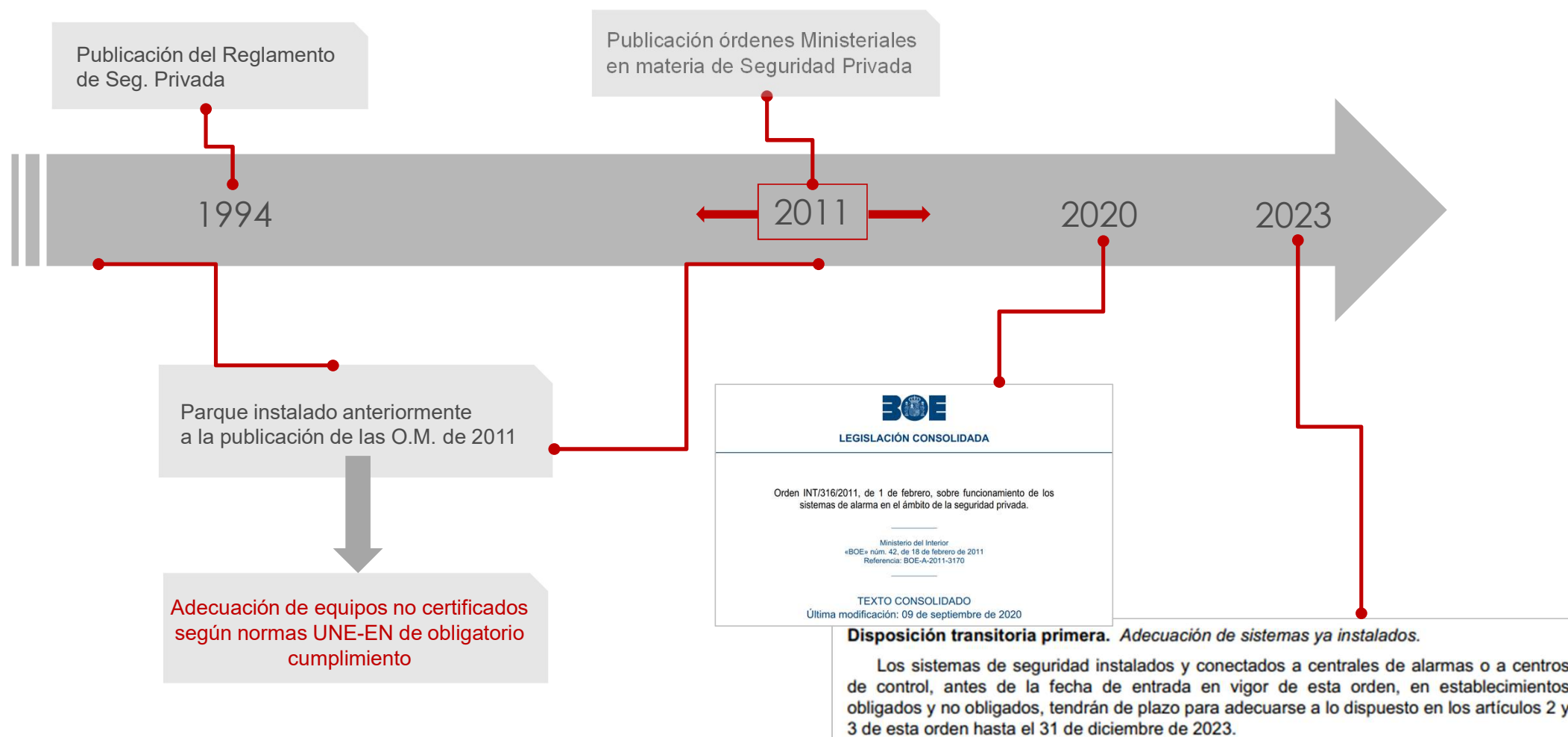
f) Tipo F: Instalaciones de infraestructuras de telecomunicación de nueva generación y de redes de telecomunicaciones de control, gestión y seguridad en edificaciones o conjuntos de edificaciones.

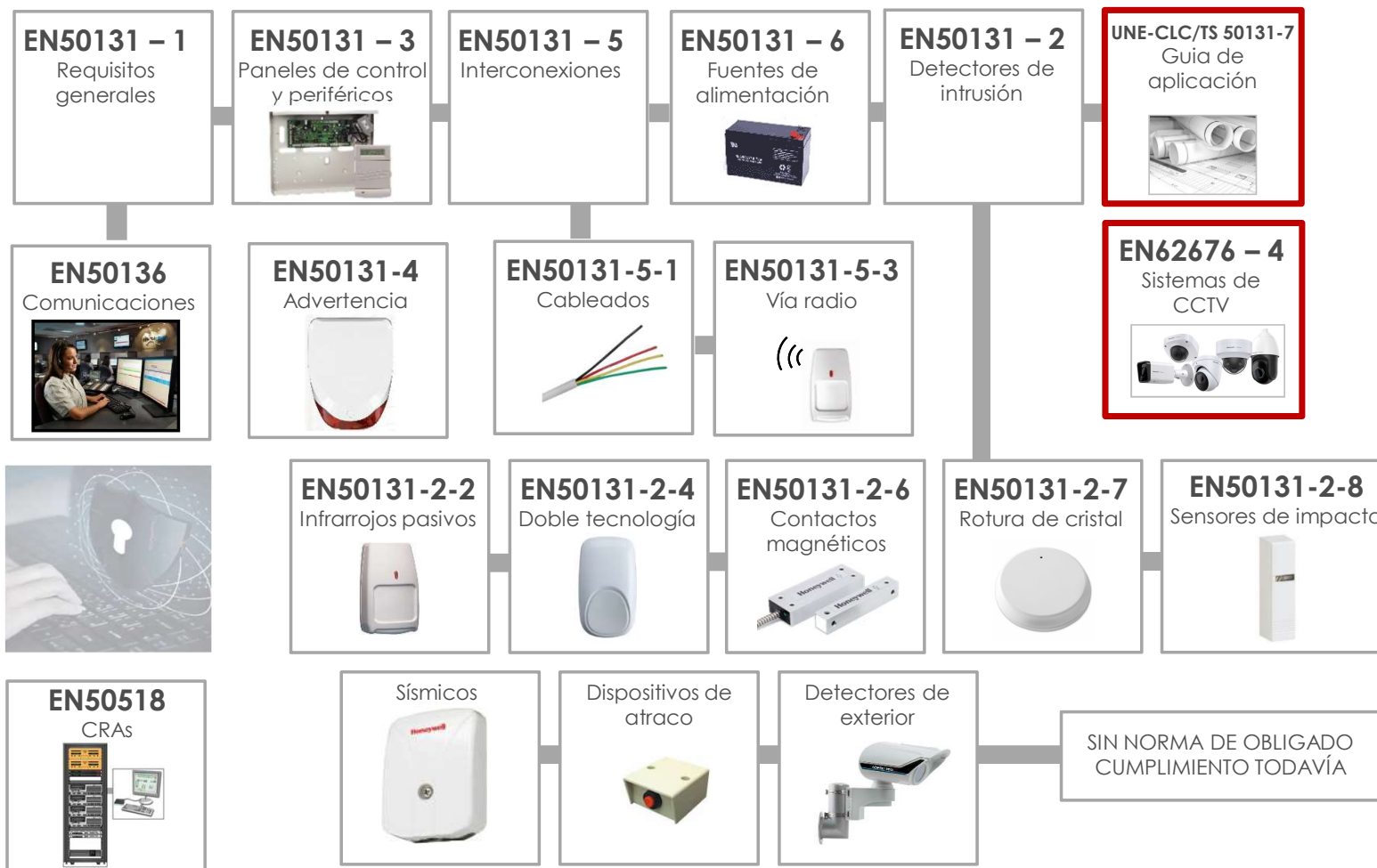
Definición: Instalaciones, incluida su puesta a punto y mantenimiento, de infraestructuras de telecomunicación en edificaciones o conjuntos de edificaciones ejecutadas mediante tecnologías de acceso ultrarrápidas (fibra óptica, cable coaxial y pares trenzados categoría 6 o superior), e integración en las mismas de equipos y dispositivos para el acceso a los servicios de radiodifusión sonora y televisión, sistemas de portería y videoportería electrónicas, sistemas de videovigilancia, control de accesos y equipos técnicos electrónicos de seguridad excluida la prestación del servicio de conexión a central de alarmas, así como de redes, equipos y dispositivos para la gestión, control y seguridad que sirvan como soporte a los servicios ligados al Hogar Digital y su integración con las redes de telecomunicación.

Equipamiento: Las empresas instaladoras que trabajen este tipo de instalaciones deberán disponer, como mínimo, de los equipos de rango de medida y precisión adecuados que incorporen las funcionalidades de medida incluidas en los siguientes aparatos: multímetro, medidor de tierra, medidor de aislamiento, medidor de intensidad de campo con pantalla y posibilidad de realizar análisis espectral y medidas de tasa de error sobre señales digitales QPSK y COFDM, simulador de frecuencia intermedia (5-2150 MHz), medidor selectivo de potencia óptica y testeador de fibra óptica monomodo para FTTH, equipo para empalme o conectorización en campo para fibra óptica monomodo y analizador/certificador para redes de telecomunicación de categoría 6 o superior.



Plazos de adecuación de los sistemas







UNE-EN 50131-1:2008

Sistemas de alarma. Sistemas de alarma contra intrusión y atraco. Parte 1: Requisitos del sistema

UNE

Vigente 16 / 04 / 2008

Leer

ICS

13.320 / Sistemas de alarma y de alerta

CTN

CTN 108/SC 79/Sistemas de alarma

ANULACIONES

Anula a UNE-EN 50131-1 CORR:2004

Anula a UNE-EN 50131-1:1998

MODIFICACIONES

Es modificada por UNE-EN 50131-1:2008/A1:2010

Es modificada por UNE-EN 50131-1:2008/A2:2017

Es modificada por UNE-EN 50131-1:2008/A3:2021

UNE-EN 50131-1 CORR:2004

Sistemas de alarma. Sistemas de alarma de intrusión. Parte 1: Requisitos generales.

UNE

Anulada 01 / 05 / 2009

Leer

ICS

13.320 / Sistemas de alarma y de alerta

CTN

CTN 108/SC 79/Sistemas de alarma

ANULACIONES

Anula a UNE-EN 50131-1 CORR:2003

Es anulada por UNE-EN 50131-1:2008

CORRECCIONES

Corrige a UNE-EN 50131-1:1998

Aprobación del material

- Cualquier elemento o dispositivo que forme parte de un sistema de alarma de los recogidos por la normativa de seguridad privada, deberá cumplir, como mínimo, el grado y características establecidas en la Normas UNE-EN 50xxx que corresponda.
- Los productos deberán estar fabricados con arreglo a las Normas y contar con la evaluación de conformidad de Organismos de Control acreditados.



afnor CERTIFICATION

Organisme certificateur
AFNOR Certification
11, rue Jean-Jacques Rousseau
93571 La Plaine Saint-Denis Cedex
FRANCE
Tél : (01) 41 41 41 41
Fax : (01) 41 41 41 41
Site internet : www.afnor-cert.com

CNPP
Organisme certificateur
CNPP Cert.
Rue de la Grande Vallée - CS 22045
77000 La Courbe-Val
FRANCE
Tél : (01) 70 00 00 00
Fax : (01) 70 00 00 00
Site internet : www.cnpp-cert.com

MATERIELS DE SECURITE ELECTRONIQUES - DETECTION D'INTRUSION
EQUIPOS DE SEGURIDAD ELECTRONICA - INTRUSION
CERTIFICAT / CERTIFICADO N° 123000-11

HONEYWELL SECURITY UK LTD
Newhouse Industrial Estate
Motherwell ML1 1SS
LANARKSHIRE - SCOTLAND

est autorisée à apposer les marques NF et ASP sur le produit selon les conditions définies dans le référentiel de certification NF324-HS8 (rév. 20) / Se autoriza a poner las marcas NF y ASP en el producto que se indica a continuación según las condiciones definidas en el referencial de certificación NF324-HS8 (rév. 20) :

Marque commerciale / Marca comercial : HONEYWELL
Reference commerciale / Modelo : CPDS
Type de produit / Gama de productos : Clavier de commande avec lecteur de badge de proximité
Tectado de control con lector de placas de proximidad

Ce certificat atteste / Este certificado atesta :
- que le produit désigné est conforme aux normes listées sur le présent certificat, telles que spécifiées dans le référentiel de certification NF 324 - H 58,
que el producto designado cumple con las normativas listadas en este certificado, como especificado en el referencial de certificación NF324-HS8,
- que le système installé de la société a été évalué conformément au référentiel de certification NF 324 - H 58
que el sistema de control de la empresa se ha evaluado conforme al referencial de certificación NF324-HS8

Caractéristiques certifiées essentielles / Características esenciales certificadas	
Niveau de sécurité / Nivel de Seguridad	Boucliers / Escudos : 3
Liens avec la centrale / Enlaces con la central de alarmas	Grade / Grado : 3
Classe d'environnement / Clase medioambiental	Fibre / Fibra
	Radio
	II

Synthese des normes produits appliquées / Resumen de los estándares de productos aplicados
EN 60181-1 ; EN 60181-2

Ce produit est conforme associé aux centrales certifiées NF324-ASP et est de niveau de sécurité supérieur ou égal aux centrales auxquelles il est associé. Sa référence figure sur les certificats des centrales.
Este producto está certificado en conjunto con las centrales certificadas NF324-ASP con el nivel de seguridad igual o superior a los que está asociado. Su referencia se puede encontrar en los certificados de las centrales.

Ce certificat n'est valable que sous réserve des résultats des contrôles effectués par AFNOR Certification et CNPP Cert. qui peuvent prendre toute sanction conformément aux règles générales de la marque NF, au référentiel général HD de la marque ASP et au référentiel de certification NF 324 - H 58. Este certificado solo es válido acompañado del ensayo que le sigue y está sujeto a los resultados de los controles realizados por AFNOR Certification y CNPP Cert. Quiénes pueden tomar las medidas sancionadoras de acuerdo con las reglas generales de la marca NF, el reglamento general HD de la marca ASP y el referencial de certificación NF324-HS8.

Ce certificat est valable jusqu'au 19/07/2026. Este certificado es válido hasta 19/07/2026.
Il annule et remplace tout certificat antérieur. Este certificado anula y reemplaza cualquier certificado anterior.

Date de prise d'effet, le 19/07/2023

Julien HIZO
Directeur Général d'AFNOR Certification
General Manager of AFNOR Certification

Christophe BODIN
Directeur CNPP Cert.
Manager of CNPP Cert.

Ce document comporte 1 page / Este documento contiene una página (PDF) / 16-12 10400000

Page 1



Certificados de producto, consideraciones a tener en cuenta

afnor
CERTIFICATION
Organisme certificateur
AFNOR Certification
11, rue Francis de Pressensé
93571 LA PLAINE SAINT-DENIS Cedex
FRANCE (33) 1 41 42 80 00
Site Internet : <http://www.marque-nf.com>

CNPP
Organisme certificateur
CNPP Cert.
Route de La Chapelle-Henriette - CS 22285
27950 LA CHAPELLE LONGUEVILLE
FRANCE (33) 3 32 53 83 43
Site Internet : <http://www.cnpp.com>

MATERIELS DE SECURITE ELECTRONIQUES - DETECTION D'INTRUSION
EQUIPOS DE SEGURIDAD ELECTRONICA - INTRUSION

CERTIFICAT/CERTIFICADO N° 123000-10

HONEYWELL SECURITY UK LTD
Newhouse Industrial Estate
Motherwell ML15SB
LANARKSHIRE - SCOTLAND

est autorisée à apposer les marques NF et A2P sur le produit selon les conditions définies dans le référentiel de certification NF324-H58 (rev. 20) : Se autoriza a poner las marcas NF y A2P en el producto que se indica a continuación según las condiciones definidas en el referencial de certificación NF324-H58 (rev. 20) :

Marque commerciale / Marca comercial : HONEYWELL
Référence commerciale / Modelo : CP037
Type de produit / Gama de productos : Clavier
Teclado

Ce certificat atteste / Este certificado atesta :
- que le produit désigné est conforme aux normes listées sur le présent certificat, telles que spécifiées dans le référentiel de certification NF 324 - H 58,
que el producto designado cumple con las normativas listadas en este certificado, como especificado en el referencial de certificación NF324-H58,
- que le système qualité de la société a été évalué conformément au référentiel de certification NF 324 - H 58
que el sistema de calidad de la empresa se ha evaluado conforme al referencial de certificación NF324-H58

Caractéristiques certifiées essentielles / Características esenciales certificadas	
Niveau de sécurité Nivel de Seguridad	Boucliers / Escudos : 3 Grade / Grado : 3
Liaisons avec la centrale Enlaces con la panel de alarma	Filaire Cableada
Classe d'environnement Clase medioambiental	II

Synthèse des normes produits appliquées / Resumen de los estándares de productos aplicados
EN 50131-1 ; EN 50131-3

Ce produit est conforme associé aux centrales certifiées NF&A2P et est de niveau de sécurité supérieur ou égal aux centrales auxquelles il est associé. Sa référence figure sur les certificats des centrales.
Este producto está certificado en conjunto con paneles certificados NF&A2P/EN con el nivel de seguridad igual o superior a los paneles a los que está asociado. Su referencia se puede encontrar en los certificados de los paneles.

Ce certificat n'est valable que sous réserve des résultats des contrôles effectués par AFNOR Certification et CNPP Cert. peuvent prendre toute sanction conformément aux règles générales de la marque NF, au référentiel général H0 de la marque A2P au référentiel de certification NF 324 - H 58. Este certificado sólo es válido acompañado del anexo que le sigue y está sujeto a los resultados de los controles realizados por AFNOR Certification y CNPP cert. Quienes pueden tomar las medidas sancionadoras de acuerdo con las reglas generales de la marca NF, el reglamento general H0 de la marca A2P y el referencial de certificación NF324-H58.

Ce certificat est valable jusqu'au 18/07/2026. Este certificado es válido hasta 18/07/2026.
Il annule et remplace tout certificat antérieur. Este certificado anula y reemplaza cualquier certificado anterior.

Date de prise d'effet, le 19/07/2023

Julien NIZARD
Directeur Général d'AFNOR Certification
General Manager of AFNOR Certification

Christophe BODIN
Directeur CNPP Cert.
Manager of CNPP Cert.

Ce document comporte 1 page/ Este documento contiene una página (MCP F 16-13 M-04/2023)

Caractéristiques certifiées essentielles / Características esenciales certificadas	
Niveau de sécurité Nivel de Seguridad	Boucliers / Escudos : 3 Grade / Grado : 3
Liaisons avec la centrale Enlaces con la panel de alarma	Filaire Cableada
Classe d'environnement Clase medioambiental	II

- Grado de seguridad.
- Clase ambiental:
 - Clase II – instalados en interior sin temperatura fija.
 - Clase IV – instalados en exterior sin temperatura fija.



Ce certificat est valable jusqu'au 18/07/2026. Este certificado es válido hasta 18/07/2026.
Il annule et remplace tout certificat antérieur. Este certificado anula y reemplaza cualquier certificado anterior.

Date de prise d'effet, le 19/07/2023

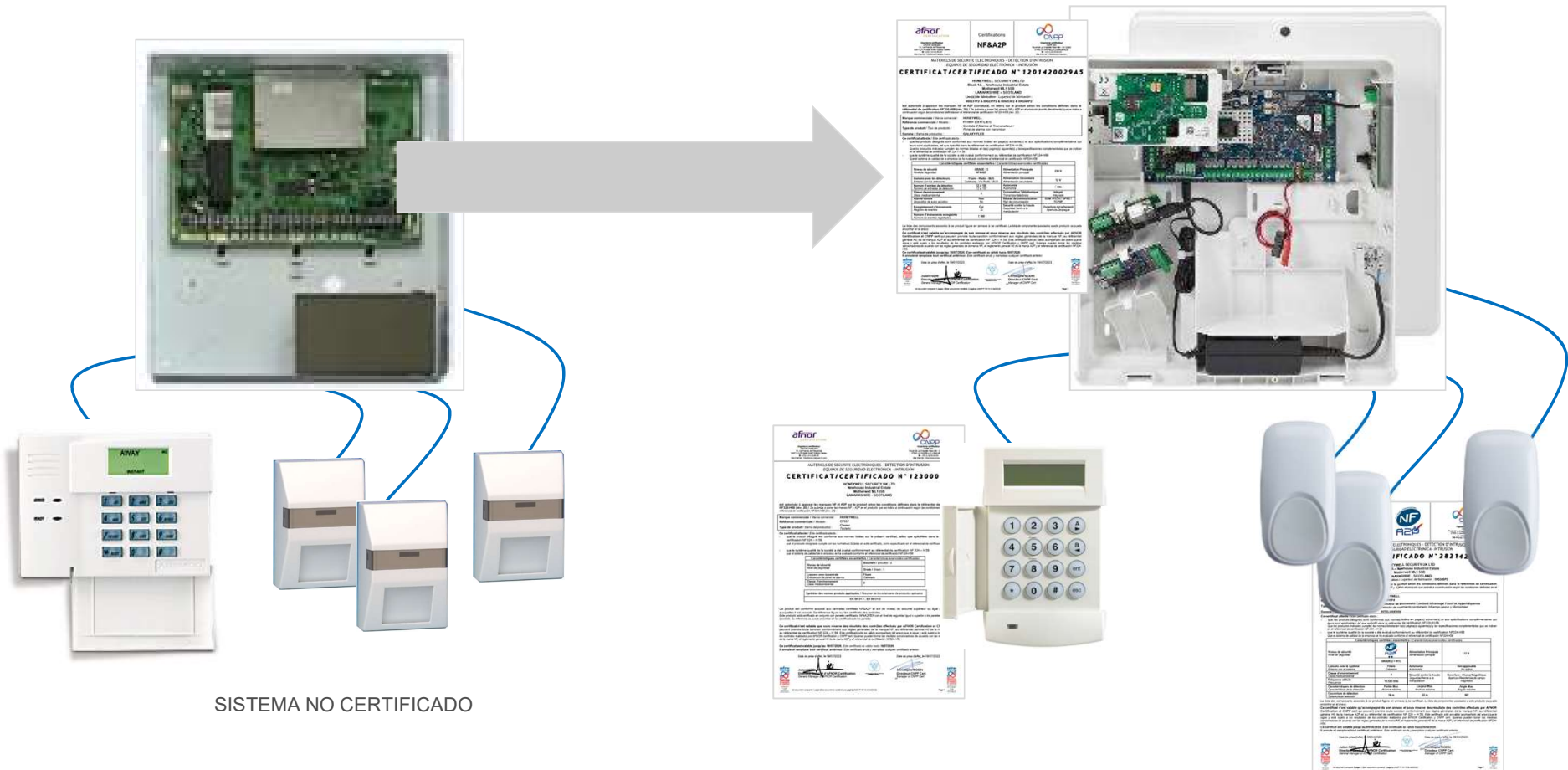
Julien NIZARD
Directeur Général d'AFNOR Certification
General Manager of AFNOR Certification

Christophe BODIN
Directeur CNPP Cert.
Manager of CNPP Cert.

Ce document comporte 1 page/ Este documento contiene una página (MCP F 16-13 M-04/2023)

- Periodo de validez. Si un equipo certificado no se recertifica por decisión del fabricante (obsolescencia, línea de producto sustitutiva), no será necesaria su sustitución durante su vida útil de funcionamiento.

Adecuación de sistemas ¿sólo se trata de esto?



UNE CLC/TS 50131-7 V2

Referencia para el diseño de sistemas anti – intrusión



BOE
LEGISLACIÓN CONSOLIDADA

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

Ministerio del Interior
«BOE» núm. 42, de 18 de febrero de 2011
Referencia: BOE-A-2011-3170

TEXTO CONSOLIDADO
Última modificación: 09 de septiembre de 2020

Relación de Normas UNE o UNE-EN que resultan de aplicación en los sistemas de alarma

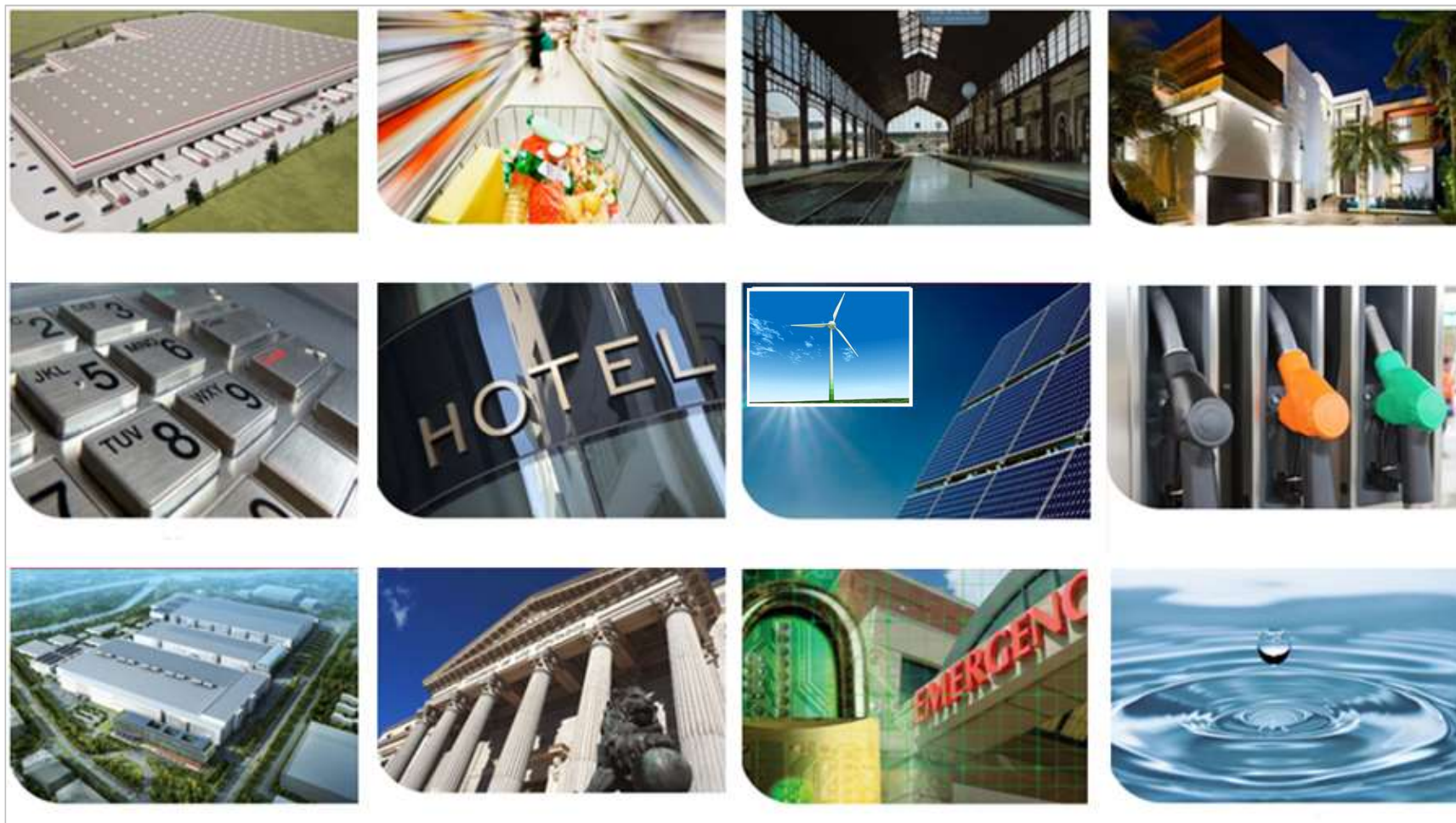
Denominación	
temas de alarma. Parte 4: Compatibilidad electromagnética. Norma de familia de producto: Requisitos de inmunidad para componentes de sistemas de detección de incendios, intrusión y alarma social.	
temas de alarma. Parte 4: Compatibilidad electromagnética. Norma de familia de producto: Requisitos de inmunidad para componentes de sistemas de detección de incendios, intrusión y alarma social.	
temas de alarma. Parte 4: Compatibilidad electromagnética. Norma de familia de producto: Requisitos de inmunidad para componentes de sistemas de detección de incendios, intrusión y alarma social.	
temas de alarma. Parte 5: Métodos de ensayo ambiental.	
temas de alarma. Sistemas de alarma contra intrusión y atraco. Parte 1: Requisitos del sistema.	
temas de alarma. Sistemas de alarma contra intrusión y atraco. Parte 1: Requisitos del sistema.	
temas de alarma. Sistemas de alarma de intrusión y atraco. Parte 2-2: Detectores de intrusión. Detectores de infrarrojos pasivos.	
temas de alarma. Sistemas de alarma de intrusión y atraco. Parte 2-3: Requisitos para detectores de microondas.	
temas de alarma. Sistemas de alarma de intrusión y atraco. Parte 2-4: Requisitos para detectores combinados de infrarrojos pasivos y microondas.	
Sistemas de alarma. Sistemas de alarma de intrusión y atraco. Parte 2-5: Requisitos para detectores combinados de infrarrojos pasivos y ultrasónicos.	
Sistemas de alarma. Sistemas de alarma de intrusión y atraco. Parte 2-6: Contactos de apertura (magnéticos).	
Sistemas de alarma. Sistemas de alarma de intrusión y atraco. Parte 3: Equipo de control y señalización.	
Sistemas de alarma. Sistemas de alarma de intrusión y atraco. Parte 4: Dispositivos de advertencia.	
Sistemas de alarma. Sistemas de alarma de intrusión. Parte 5-3: Requisitos para los equipos de interconexión que usan técnicas de radiofrecuencia.	
Sistemas de alarma. Sistemas de alarma de intrusión. Parte 5-3: Requisitos para los equipos de interconexión que usan técnicas de radiofrecuencia.	
Sistemas de alarma. Sistemas de alarma de intrusión. Parte 6: Fuentes de alimentación.	
Sistemas de alarma. Sistemas de alarma de intrusión y atraco. Parte 6: Fuentes de alimentación.	
Sistemas de alarma. Sistemas de alarma de intrusión y atraco. Parte 8: Sistemas/dispositivos de niebla de seguridad.	
Sistemas de alarma. Sistemas de alarma de intrusión. Parte 2-2: Requisitos para los detectores de infrarrojos pasivos.	
Sistemas de alarma. Sistemas de alarma de intrusión. Parte 2-3: Requisitos para detectores de microondas.	
Sistemas de alarma. Sistemas de alarma de intrusión. Parte 2-4: Requisitos para los detectores combinados de infrarrojos pasivos y de microondas.	
Sistemas de alarma. Sistemas de alarma de intrusión. Parte 2-5: Requisitos para los detectores combinados de infrarrojos pasivos y ultrasónicos.	
Sistemas de alarma. Sistemas de alarma de intrusión. Parte 2-6: Requisitos para contactos de apertura (magnéticos).	
Sistemas de alarma. Sistemas de alarma de intrusión. Parte 3: Equipo de control y señalización.	
Sistemas de alarma. Sistemas de alarma de intrusión. Parte 7: Guía de aplicación	
Sistemas de alarma. Sistemas de vigilancia CCTV para uso en aplicaciones de seguridad. Parte 1: Requisitos del sistema.	
Sistemas de alarma. Sistemas de vigilancia CCTV para uso en aplicaciones de seguridad. Parte 2-1: Cámaras en blanco y negro.	
Sistemas de alarma. Sistemas de vigilancia CCTV para uso en aplicaciones de seguridad. Parte 4-1: Monitores en blanco y negro.	
Sistemas de alarma. Sistemas de vigilancia CCTV para uso en aplicaciones de seguridad. Parte 5: Transmisión de vídeo.	
Sistemas de alarma - Sistemas de vigilancia CCTV para uso en aplicaciones de seguridad. Parte 7: Guía de aplicación.	
Sistemas de alarma. Sistemas de vigilancia CCTV para uso en aplicaciones de seguridad. Parte 7: Guía de aplicación.	
Sistemas de alarma. Sistemas de control de accesos de uso en las aplicaciones de seguridad. Parte 1: Requisitos de los sistemas.	
Sistemas de alarma. Sistemas de control de accesos de uso en las aplicaciones de seguridad. Parte 1: Requisitos de los sistemas.	

Anomalías detectadas I

- No realizar los proyectos de instalación o realizarlos sin ajustarse a la Norma UNE-CLC/TS 50131-7 (art. 4.1 Orden INT/316)

JORNADA VIRTUAL MARZO 2021
Inspector Juan Campaña Santiago

Nuevos sistemas / Adecuación de sistemas



**SEGURPRI**
Monográfico N° 13
Octubre 2011



PREGUNTAS MÁS FRECUENTES (F.A.Q.)
ORDENES MINISTERIALES

Desde la publicación en el Boletín Oficial del Estado, el pasado 18 de febrero, de las cinco nuevas órdenes ministeriales, muchas han sido las preguntas planteadas a esta Unidad Central de Seguridad Privada por parte de empresas, asociaciones, sindicatos, personal, etc., bien sobre dudas, aclaración, o interpretación del articulado de las mismas

Con las respuestas que a las mismas se han realizado, se han elaborado el presente monográfico de SEGURPRI, esperando que sirva de ayuda y referencia para el resto del sector de seguridad privada.

1

UNIDAD CENTRAL DE SEGURIDAD PRIVADA

DIRECCIÓN GENERAL DE LA POLICÍA Y DE LA GUARDIA CIVIL
Comisaría General de Seguridad Ciudadana

20.- ¿Será obligatorio el elaborar un proyecto de instalación en todos los clientes, sean obligados o no, siempre que se vayan a conectar?

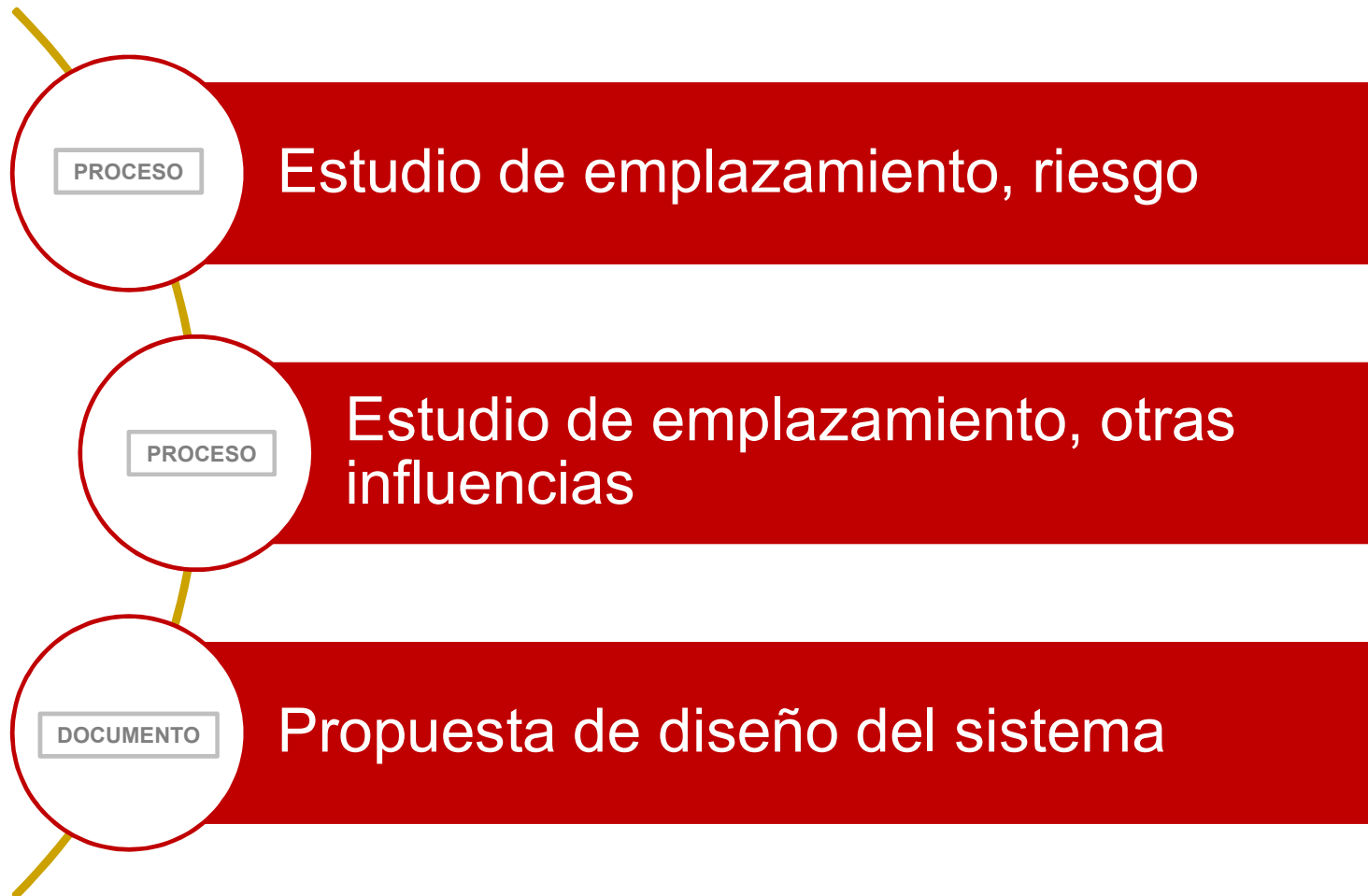
Conforme a lo previsto en el artículo 42 del Reglamento de Seguridad Privada y el artículo 4 de la Orden INT 316/2011, el proyecto de instalación es obligatorio para todos los sistemas que vayan a conectarse a la Central de Alarmas o a un centro de control o de videovigilancia, independientemente de que sean o no establecimientos obligados a adoptar medidas de seguridad específicas.

12.- ¿Cómo definir el Grado de seguridad de una instalación?, ¿quién define los parámetros para las de Grado 3? ¿Sólo los instaladores con el estudio de seguridad o interviene la policía en algún proceso?

Los grados de seguridad de las instalaciones, en los distintos tipos de establecimientos o locales, vienen recogidos en el artículo 2 de la Orden INT 316 de 2011, diferenciando el grado 4 para la infraestructuras críticas, el Grado 3 para los establecimientos obligados, y el 2 para el resto de sistemas que se pretendan conectar a una central de alarmas.

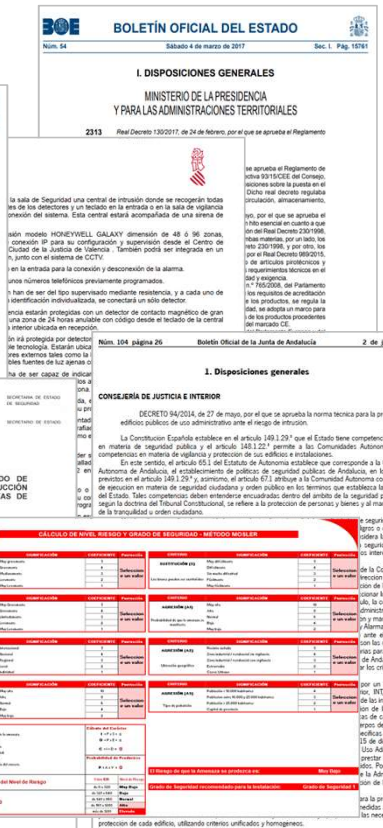
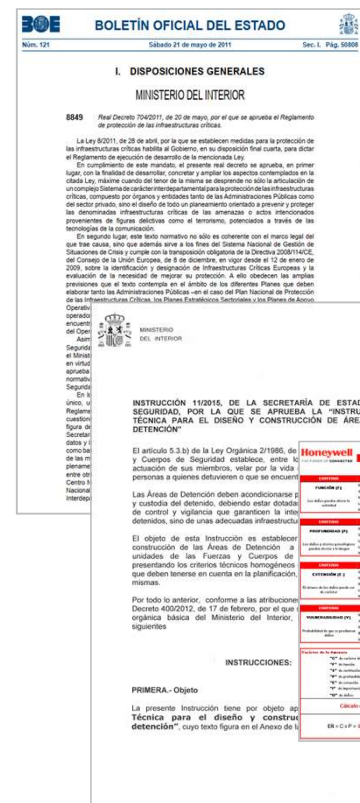
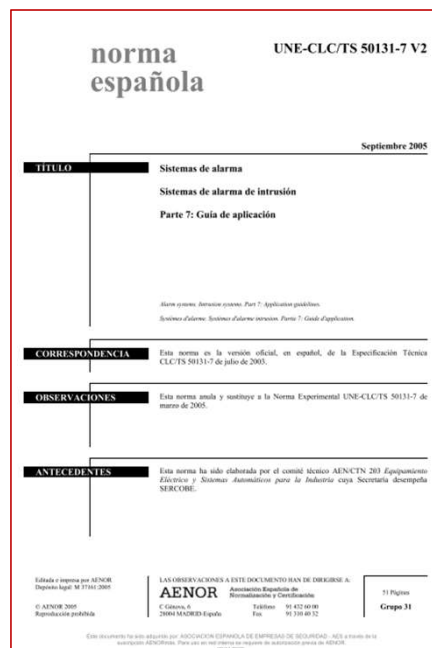
Respecto a la posible intervención de las unidades territoriales de seguridad privada en los proyectos de instalación, es un aspecto que recoge el artículo 42.2 del Reglamento de Seguridad Privada cuando habla de *“proyectos de instalación, con niveles de cobertura adecuados a las características arquitectónicas del recinto y del riesgo a cubrir, de acuerdo con los criterios técnicos de la propia empresa instaladora y, eventualmente, los de la dependencia policial competente, todo ello con objeto de alcanzar el máximo grado posible de eficacia del sistema, de fiabilidad en la verificación de las alarmas, de colaboración del usuario, y de evitación de falsas alarmas”*.

Por otra parte es muy importante el estudio en los proyectos de instalación a través de la Guía de aplicación de la norma UNE EN-50131-7, que nos va a determinar según el riesgo, el Grado de aplicación en cada caso, que como mínimo será siempre el exigido en la Orden mencionada.



Análisis de riesgos para determinar el grado de seguridad

- Se deberá presentar al cliente una propuesta de diseño, donde se determinará el grado de seguridad requerido, así como la selección de los componentes que satisfagan el grado y la clase ambiental apropiados, debiéndose prestar especial atención a la necesidad de reducir al mínimo la generación de falsas alarmas



Grados y clasificación ambiental según UNE CLC/TS 50131-7 V2

- Estructura de Grados:
 - **Grado 1**, riesgo bajo: se esperan intrusos que tengan poco conocimiento de los sistemas de seguridad y dispongan de una gama limitada de herramientas fácilmente disponibles.
 - **Grado 2**, riesgo bajo a medio: se esperan intrusos que tengan un conocimiento limitado de los sistemas de seguridad y con uso de una gama general de herramientas e instrumentos portátiles.
 - **Grado 3**, riesgo medio a alto: se esperan intrusos familiarizados con los sistemas de seguridad y que tengan una gama amplia de herramientas y equipo electrónico portátil.
 - **Grado 4**, riesgo alto: 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 del sistema contra intrusión.
- Clasificación ambiental:
 - **Tipo I**: Interiores, pero restringido a ambiente residencial / de oficinas.
 - **Tipo II**: Interiores en general (áreas de ventas, tiendas, restaurantes, escaleras, áreas de fabricación, ensamblaje, almacenes).
 - **Tipo III**: Exteriores pero resguardados de la lluvia y el sol directos, o interiores con condiciones ambientales extremas (plantas de garaje, cobertizos, muelles de carga).
 - **Tipo IV**: Exteriores en general.

Grado de Seguridad



Clase ambiental

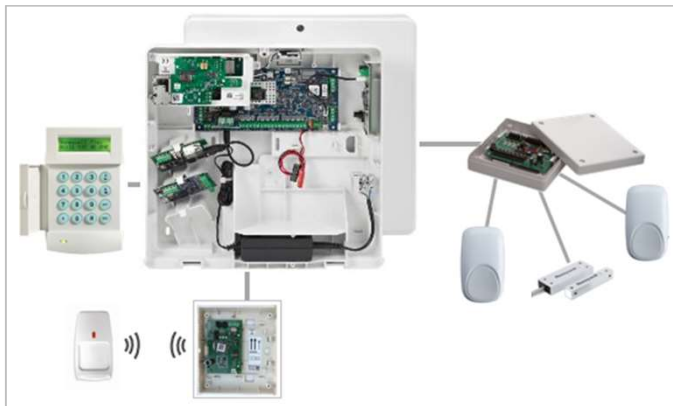




Estudio técnico

- Para estar seguros de que el Sistema de Seguridad proporciona y es coherente con las características detalladas en la propuesta de diseño, diferentes cuestiones se deben considerar durante el estudio técnico:

INTERCONEXIONES: - CABLEADAS ESPECÍFICAS - INALÁMBRICAS



CONSIDERACIONES SOBRE LOS DETECTORES SEGÚN SU TECNOLOGÍA



EQUIPOS DE CONTROL Y SEÑALIZACIÓN, FUENTES DE ALIMENTACIÓN, SISTEMAS DE TRANSMISIÓN DE ALARMAS, DISPOSITIVOS DE AVISO



En la propuesta de diseño

Comentarios acerca del estudio del emplazamiento de los detectores

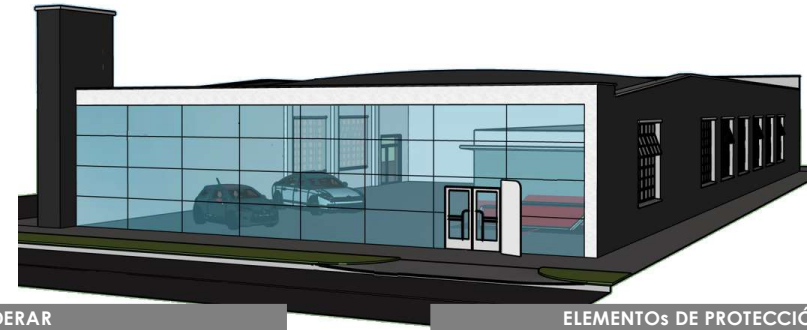
- El objetivo de la siguiente tabla es proporcionar una guía al diseñador respecto al tipo de intrusión que puede esperarse en los distintos puntos de las instalaciones supervisadas.

Niveles de supervisión				
A considerar	Grado 1	Grado 2	Grado 3	Grado 4
Puertas perimetrales	O	O	OP	OP
Otras aberturas		O	OP	OP
Paredes				P
Techos y tejados				P
Suelos				P
Sala	T	T	T	T
Objeto (alto riesgo)			S	S

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

- Esta guía no debe considerarse como una lista exhaustiva de todos los métodos de intrusión que podrían darse, puesto que las condiciones variarán de unas instalaciones a otras. Puede ser necesario considerar la prestación de supervisión contra métodos de intrusión no contemplados en la tabla. Similarmente, puede haber circunstancias en las que el diseñador considere que determinados métodos de intrusión no son aplicables a todas las instalaciones supervisadas o parte de ellas.

A CONSIDERAR		TIPO DETECTOR - TECNOLOGÍA
Abertura	O	Magnético
Penetración	P	Sísmico, Inercial, Rotura de cristal
Atrapado	T	Volumétrico
Especial consideración	S	Sísmico, Detector Exterior, Pulsador



ZONAS A CONSIDERAR

Ruta de entrada y salida
Zona de ventas
Zona de taller
Zona administrativa
Almacén
Escaparates, zona de exposición
Puertas y cierres metálicos
Recinto caja fuerte y caja fuerte

T
T
T
T
T/O
S
O
T/O/S

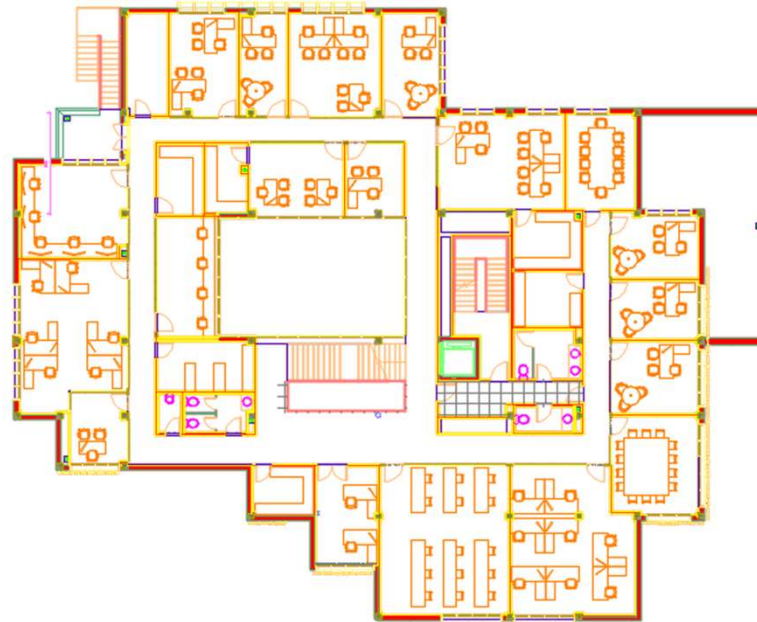
ELEMENTOS DE PROTECCIÓN

Volumétrico
Volumétrico
Volumétrico
Volumétrico
Volumétrico / Magnético
Microfónico - rotura de cristal
Magnético
Volumétrico / Magnético / Sísmico

O=Abertura, P=Penetración; T=Atrapado, S=Objeto de especial consideración

Plan de instalación / propuesta modificada

- **El plan de instalación** debe basarse en la propuesta de diseño y considerar los aspectos identificados en el estudio de la preinstalación.
- Se debe especificar donde se va a colocar cada componente y como debe emplazarse.
- Se deben especificar los detalles de las interconexiones requeridas y, si fuera cableado, también los tipos de cables y la ruta de éstos.
- **Puede ocurrir que haya que realizar una modificación en la propuesta**, bien por necesidades del cliente, bien porque en el estudio de preinstalación se vea que es necesario. Cualquier cambio debe ser consensuado con el cliente y quedar registrado.







Documento “tal como se instaló”

- Debe ser un registro preciso del sistema de seguridad, incluyendo toda la información relativa al equipo instalado y a su emplazamiento. Debiéndose reflejar cualquier cambio que se hubiera realizado durante el proceso de instalación si se hubiera considerado necesario.
- Si correspondiera por el tamaño y la complejidad del sistema de seguridad, este documento debería incluir también detalles de todos los tipos de cables utilizados y sus canalizaciones.
- Cuando se declare que el sistema de seguridad o cualquiera de sus componentes cumplen con cualquier legislación, reglamento, o especificaciones nacionales o europeas, todas estas declaraciones deben incluirse en el certificado de conformidad.
- Instrucciones de funcionamiento del sistema, con suficiente nivel de detalle para reducir al mínimo la posibilidad de operación incorrecta: cuestiones a tener en cuenta a la hora de conectar el sistema, detalle de los diferentes procesos (conexiones, desconexiones, anulaciones de zona, procedimientos de prueba, ...). Así como alguna operativa concreta que especifique el fabricante de los equipos.
- Datos de la empresa instaladora.
- Datos de la empresa de mantenimiento.
- Datos de la central receptora de alarmas.
- Datos de la empresa encargada de acudir a la atención de las alarmas.
- Detalles sobre todos los procedimientos relativos a la verificación de las alarmas.
- Instrucciones y documentación necesaria en cuanto a los procesos de verificación.

Anomalías detectadas

- No informar a los usuarios del funcionamiento de los sistemas y el número de revisiones preceptivas, ni incluir en contrato el número de mantenimientos que se contratan



Mantenimiento de los sistemas

Revisiones preventivas cada trimestre, no debiendo, en ningún caso, transcurrir más de cuatro entre dos sucesivas (Art. 43.1 Reglamento de Seguridad Privada)

Una anual, sin que transcurran más de catorce meses, cuando los sistemas permitan la comprobación de cada uno de los elementos del sistema desde la Central de Alarmas (Art. 43.2 Reglamento de Seguridad Privada)

Acorde anexos II y III Orden INT/316/2011



BOLETÍN OFICIAL DEL ESTADO



Núm. 42 Viernes 18 de febrero de 2011 Sec. I. Pág. 18329

Tipo	Numero	Año	Denominación
UNE-EN	50136-2-3	1998	Sistemas de alarma. Sistemas y equipos de transmisión de alarma. Parte 2-3: Requisitos para los equipos usados en sistemas con transmisores digitales que hacen uso de la red telefónica pública conmutada.
UNE-EN	50136-2-4	1998	Sistemas de alarma. Sistemas y equipos de transmisión de alarma. Parte 2-4: Requisitos para los equipos usados en sistemas con transmisores de voz que hacen uso de la red telefónica pública conmutada.
UNE-CLC/TS	50136-4	2005 V2	Sistemas de alarma. Sistemas y equipos de transmisión de alarma. Parte 4: Equipos anunciadores usados en centrales receptoras de alarma.
UNE-CLC/TS	50136-7	2005 V2	Sistemas de alarma. Sistemas y equipos de transmisión de alarma. Parte 7: Guía de aplicación.
UNE CLC/TS	50398	2005 V2	Sistemas de alarma. Sistemas de alarma combinados e integrados.

ANEXO II

Mantenimiento presencial anual de sistemas electrónicos de seguridad

Equipos	Acciones	Periodicidad (*)
Objetivo	Realizar un completo test del estado y de la funcionalidad de un sistema. Se deberá preparar por parte de la empresa mantenedora un impreso estándar en la que reflejar, además del tipo de CIE (marca, modelo, etc.) y del resto de elementos utilizados, los resultados de las pruebas efectuadas con el fin de evitar el posible olvido de alguna de ellas. Sirva esta guía para su confección. Una copia de este impreso deberá ser entregada al usuario, debidamente firmada por el técnico, al finalizar las pruebas.	Anual
Situación de pruebas	Antes de iniciar el proceso de mantenimiento de un sistema, el técnico, identificándose debidamente, informará a la CRA, que situará el sistema en estado de pruebas, registrando las señales recibidas de forma automática, pero sin cursar su trámite. Deberá obtenerse inicialmente el registro de incidencias del sistema de modo que, si su capacidad lo permite, reproduzca los últimos 15 días. Al final del test se obtendrá otro registro de incidencias del periodo de pruebas para comprobar que todas han sido llevadas a cabo correctamente. Igualmente, al final del test se comprobará con la CRA si todas las señales de alarma generadas han alcanzado su destino.	Anual
Alimentación del sistema	Las comprobaciones han de efectuarse sobre la fuente de alimentación (PS) de la propia CIE y también sobre otras posibles fuentes de alimentación auxiliares que el sistema emplee de forma tanto centralizada como distribuida, siendo necesario abrir las cajas de los equipos implicados. Verificar: Posibles anomalías de alimentación. Suministro de c.a. Toma de tierra. Tensión de la c.c. de las salidas. Id. retirando la c.a. (sólo baterías). Tensión de carga de la batería. Antigüedad de la batería (sus99). Provocar un fallo red de c.a. y. Provocar también un fallo de b. Comprobar su señalización local a la CRA (cotejar con CRA al Nota: La notificación del fallo de m. Comprobarlo consultando la pro	

Anomalías detectadas

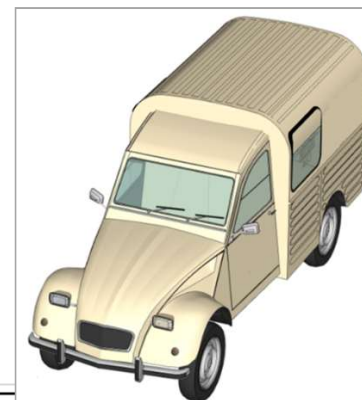
No realización de los mantenimientos contratados con sus clientes o no realizarlos conforme al ANEXO II de la Orden INT/316/2011

Mantenimiento de los sistemas

Ejemplos de acciones a realizar



Mantenimiento periódico de los sistemas contra intrusión conforme a anexos II y III de la Orden del Ministerio del Interior INT/316/2011, de 1 de febrero																	
INSTALACIÓN: 	FECHA: 																
VERIFICACIÓN MANTENIMIENTO PRESENCIAL																	
EQUIPOS Y COMPROBACIONES A REALIZAR	UDS. REALIZADO																
CENTRAL DE INTRUSIÓN - Estado y funcionamiento del támpor (grados 2 y 3) y del posible despegue (grado 3). - Estado de los elementos de cierre del panel (bisagras, tornillos, ...). - Aspecto general del interior (conexiones, cableado, ...). - Alimentación (realizar procesos indicados en apartado "fuentes de alimentación").	SI																
FUENTE/S DE ALIMENTACIÓN - Verificar suministro de C.A. y toma de tierra. - Verificar tensión en las salidas auxiliares. - Desconectar A.C., verificar funcionamiento y tensión de las baterías (aprox. 12Vcc +/- 5%). - Verificar tensión de carga de las baterías (aprox. 13,8Vcc +/- 5%). - Antigüedad de las baterías (sustituir si es más de 6 años). - Provocar un fallo de C.A. y reponerlo tras 1 minuto (o el tiempo programado como notificación de fallo en el panel). - Provocar un fallo de baterías y reponerlo tras 1 minuto. - Comprobar señalización de las averías en local (teclado/s) y las transmisiones de alarma a la C.R.A., así como las restauraciones, comparando la información facilitada por la C.R.A. con el registro de incidencias del panel.																	
COMUNICACIONES - VÍA PRIMARIA - Provocar una o más alarmas y comprobar el correcto curso de la llamada a la C.R.A. - Observar que el tiempo de comunicación sea correcto. - Desconectar A.C., verificar funcionamiento y tensión de las baterías (aprox. 12Vcc +/- 5%).																	
COMUNICACIONES - VÍA/S DE BACKUP - Desconectar la vía de comunicación primaria y comprobar que, al cabo de un cierto tiempo, su fallo es comunicado por la vía de comunicación alternativa. - Provocar algunas alarmas y comprobar que son debidamente transmitidas por la vía/s alternativa/s. - Reconectar la vía primaria.																	
TECLADO/S - Comprobar el display, teclas y el zumbador interno. - Ver el estado del támpor de apertura (grados 2 y 3) y el antidespegue (grado 3). - Verificar posibles problemas de funcionamiento preguntando a los usuarios.																	
DETECTORES, DIFERENTES TECNOLOGÍAS - Comprobar la cobertura de los detectores volumétricos y el funcionamiento de los elementos que exijan una activación manual. - Comprobar que los posibles cambios en la distribución del mobiliario, material almacenado, carteles colgantes, etc... no afecten a la cobertura de los detectores de movimiento. - Poniendo el sistema en modo test, comprobar mediante el zumaboadr del teclado y la posible ayuda de un colaborador, la correcta activación de todos y cada uno de los elementos que puedan ser examinados por este medio (volumétricos, contactos magnéticos, pulsadores de atraco, ...). - Comprobar el resto de elementos mediante el procedimiento más adecuado: sísmicos (herramienta de prueba específica o percusión), inerciales (percusión), rotura de cristal (herramienta específica de test), ... - Con el sistema desarmado, comprobar aleatoriamente la activación del támpor de algunos detectores (grados 2 y 3) y la transmisión de estas incidencias a la C.R.A. - Enmascarar los detectores volumétricos de este tipo (grado 3) y comprobar su reacción y la transmisión de esta incidencia a la C.R.A. - Verificar la activación de los elementos comprobados mediante el registro de incidencias del sistema.																	
<table border="1"> <thead> <tr> <th>DETECTOR VOLUMÉTRICO</th> <th>SELEC</th> </tr> </thead> <tbody> <tr> <td>DETECTOR VOLUMÉTRICO D.T. ANTIMASKING</td> <td>SELEC</td> </tr> <tr> <td>CONTACTO MAGNÉTICO</td> <td>SELEC</td> </tr> <tr> <td>DETECTOR DE ROTURA DE CRISTAL</td> <td>SELEC</td> </tr> <tr> <td>DETECTOR INERCIAL</td> <td>SELEC</td> </tr> <tr> <td>DETECTOR SÍSMICO</td> <td>SELEC</td> </tr> <tr> <td>PULSADOR DE ATRACO</td> <td>SELEC</td> </tr> <tr> <td>DETECTOR DE EXTERIOR</td> <td>SELEC</td> </tr> </tbody> </table>		DETECTOR VOLUMÉTRICO	SELEC	DETECTOR VOLUMÉTRICO D.T. ANTIMASKING	SELEC	CONTACTO MAGNÉTICO	SELEC	DETECTOR DE ROTURA DE CRISTAL	SELEC	DETECTOR INERCIAL	SELEC	DETECTOR SÍSMICO	SELEC	PULSADOR DE ATRACO	SELEC	DETECTOR DE EXTERIOR	SELEC
DETECTOR VOLUMÉTRICO	SELEC																
DETECTOR VOLUMÉTRICO D.T. ANTIMASKING	SELEC																
CONTACTO MAGNÉTICO	SELEC																
DETECTOR DE ROTURA DE CRISTAL	SELEC																
DETECTOR INERCIAL	SELEC																
DETECTOR SÍSMICO	SELEC																
PULSADOR DE ATRACO	SELEC																
DETECTOR DE EXTERIOR	SELEC																
OPERATIVA HABITUAL - Armar el sistema (esta acción debería llevarla a cabo alguno de los usuarios habituales con su código). Si están habilitadas particiones, áreas o grupos, esta acción se deberá realizar por cada una de ellas. Comprobar la duración de los tiempos de salida. - Generar una alarma de robo y comprobar la activación de la/s sirena/s.																	
SELEC																	





A MEDIDA QUE LOS EDIFICIOS SE VUELVEN CADA VEZ MÁS Y MÁS DIGITALES, LAS ORGANIZACIONES ESTÁN CADA VEZ MÁS EXPUESTAS A LAS AMENAZAS DE CIBERSEGURIDAD. PARA AYUDAR A DEFENDERSE DE POSIBLES PÉRDIDAS FINANCIERAS, O DAÑOS A LA IMAGEN CAUSADOS POR ESTE TIPO DE ATAQUES, SE DEBE IMPLEMENTAR UNA ESTRATEGIA FUERTE DE PROTECCIÓN, QUE CONTEMPLA TODOS LOS PUNTOS POSIBLES POR DONDE SE PUEDAN PRODUCIR LOS PROBLEMAS Y COMO ATAJARLOS.

**INTRUSIÓN – VÍDEO –
CONTROL DE ACCESOS**

LOGÍSTICA

El hackeo informático amenaza al sector de la logística

<https://logistica.cdecomunicacion.es/noticias/sectoriales/55433/hackeo-informatico-amenaza-logistica>

LA NUEVA ESPAÑA

Por qué los hospitales son el nuevo objetivo de los ciberdelincuentes y cómo afecta a los pacientes?

<https://www.lne.es/salud/guia/2022/10/01/hospitales-son-nuevo-objetivo-ciberdelincuentes-76381568.html>

ADMINISTRACIÓN PÚBLICA DIGITAL

Las administraciones públicas son objetivo prioritario de los Ciberataques

<https://administracionpublicadigital.es/actualidad/2023/10/las-administraciones-publicas-son-objetivo-prioritario-de-los-ciberataques>

DIARIO DE SEVILLA

Las estafas informáticas casi duplican ya a los robos convencionales en Sevilla

https://www.diariodesevilla.es/sevilla/estafas-informaticas-duplican-robos-Sevilla_0_1854115168.html

HISCOX

El 54% de las empresas españolas del sector retail reconocen haber sufrido algún ciberataque

<https://www.hiscox.es/el-54-de-las-empresas-espanolas-del-sector-retail-reconocen-haber-sufrido-algun-ciberataque>

EUROPA PRESS

Air Europa sufre un ciberataque que expone datos bancarios de clientes y aconseja cancelar tarjetas

<https://www.europapress.es/economia/noticia-air-europa-sufre-ciberataque-expone-datos-bancarios-clientes-20231010101627.html>

LOSNEGOCIOS.ES

Joyerías Rabat se enfrenta al peor ataque cibernético de su historia

https://www.losnegocios.es/joyerias-rabat-enfrenta-peor-ataque-cibernetico-historia_102984.htm

EL CONFIDENCIAL

Un grupo “hacker” bloquea durante horas las páginas web de bancos españoles

https://www.elconfidencial.com/empresas/2023-07-21/grupo-hacker-bloquea-horas-paginas-web-bancos-espanoles_3704704/



CONTEMPLAR EL CIBERATAQUE EN LOS ANÁLISIS DE RIESGOS

Honeywell



ALGUNOS ASPECTOS CLAVE EN EL DISEÑO



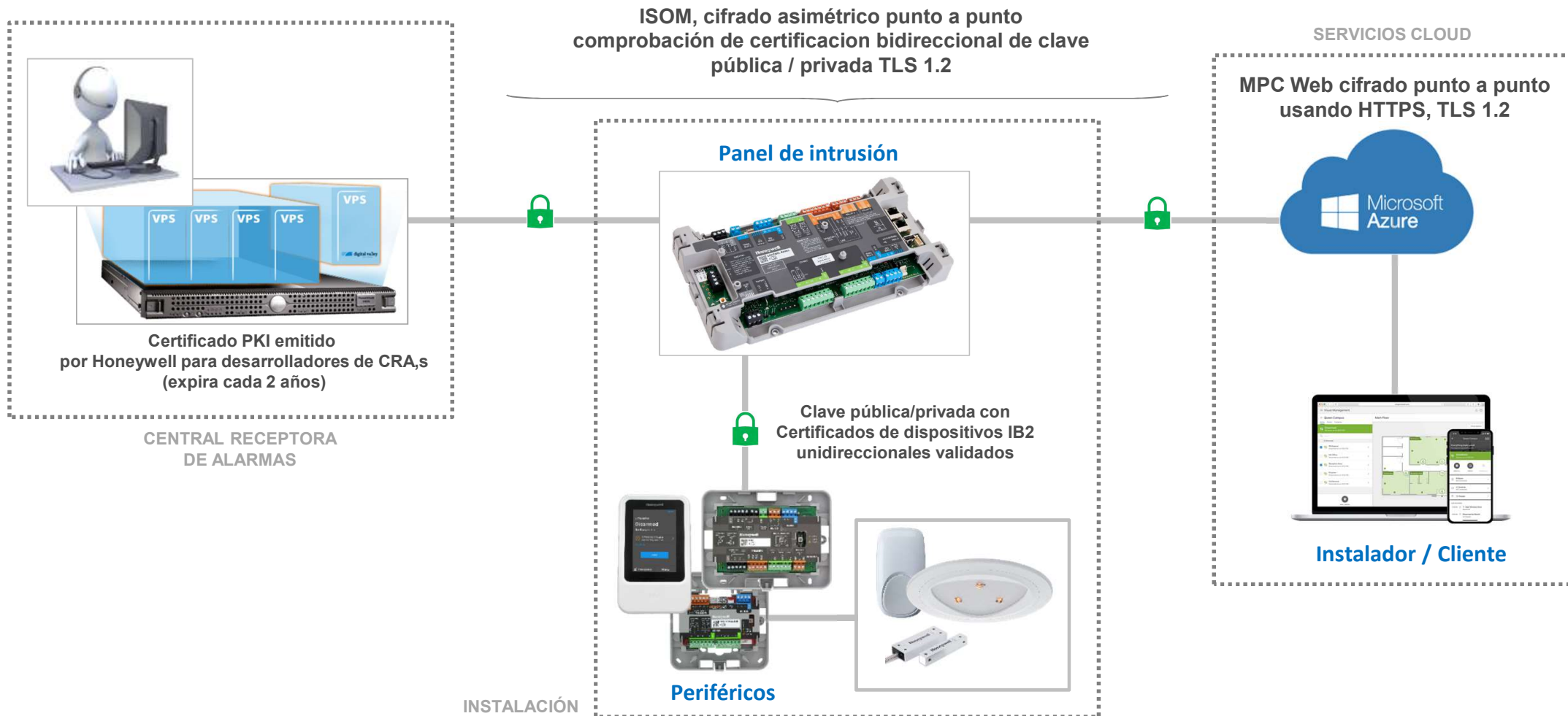


Tipo de ataque	Explicación
Ataque de intermediario	Es un ataque en que el atacante transmite en secreto y posiblemente altera la comunicación entre dos partes que creen que se están comunicando entre sí.
Ataque de escalada de privilegios	Es el acto de explotar un error, un fallo de diseño o una supervisión de la configuración en un sistema operativo, o una aplicación de software, para obtener un acceso elevado a los recursos que normalmente están protegidos frente al acceso por parte de una aplicación o usuario.
Ataque de phishing	Es un intento de obtener información sensible, al fingir el atacante que es una entidad confiable en una comunicación electrónica.
Ataque de sniffing	Consiste en la lectura no autorizada de información que se transmite o almacena normalmente en texto sin formato.
Ataque de reproducción	Es una forma de ataque a la red en el que una transmisión se repite o retrasa de forma maliciosa o fraudulenta.
Ataque de keylogging	Es la acción de grabar o registrar de manera encubierta las teclas que se pulsan en un teclado, de manera que puedan ser reproducidas posteriormente sin el conocimiento del usuario.
Ataque por fuerza bruta	Consiste en múltiples intentos de adivinar las credenciales de acceso de un usuario válido.
Ataque de denegación de servicio	Ataque DoS, implica inundar la máquina o el recurso objetivo con solicitudes supérfluas en un intento de sobrecargar el sistema e interrumpir el funcionamiento normal.
Ataque de denegación de servicio distribuido	Ataque DDoS, es un ataque de denegación de servicio por parte de más de una fuente.
Ataque de malware	Consisten en la introducción de software hostil o intrusivo, incluyendo virus de ordenador, gusanos, troyanos, ransomware, spyware, adware, scareware y otros programas intencionalmente dañinos con la intención de interrumpir el funcionamiento normal de sistema operativo y/o interceptar la funcionalidad de aplicaciones legítimas.
Exploit de raíz	Consiste en obtener el acceso al sistema operativo subyacente.
Ataque de ingeniería inversa	Es un intento de descubrir las vulnerabilidades y debilidades del sistema rompiendo la estructura de una aplicación legítima.

Amenazas habituales a la seguridad cibernética

Protección ante ataques externos

Ejemplo paneles MAXPRO Intrusion



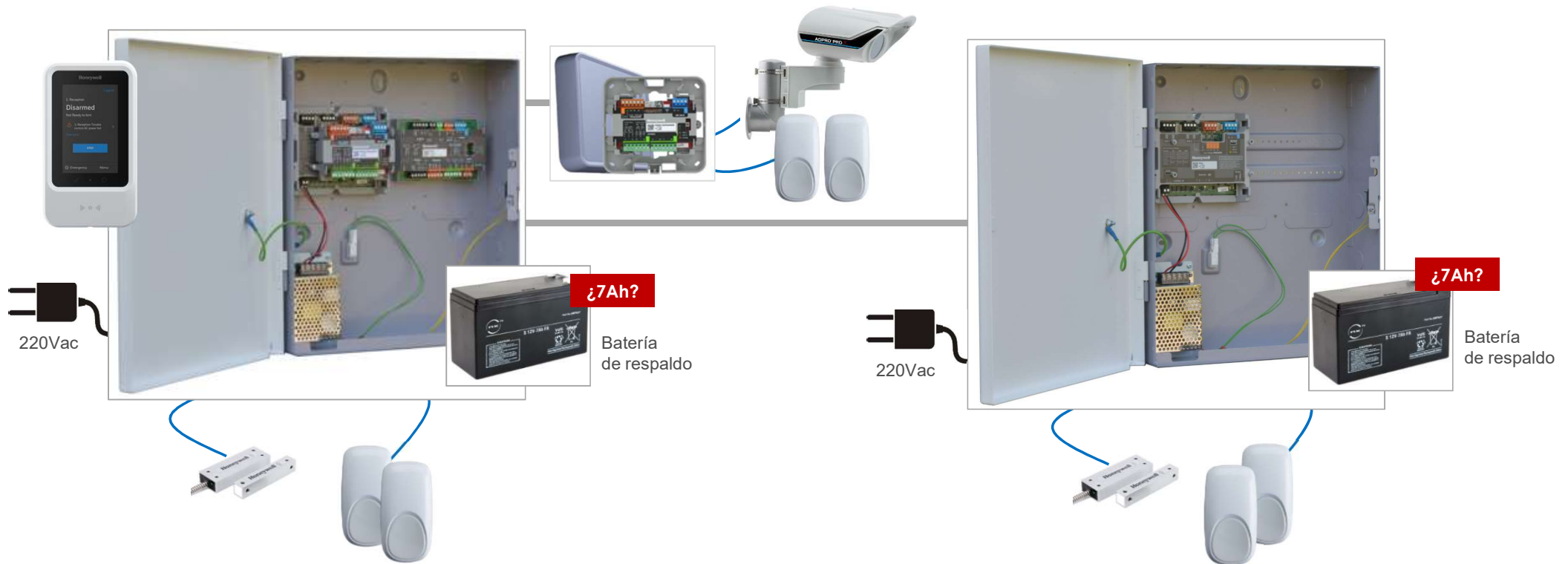
Alimentación del sistema

Determinar capacidad de baterías y la necesidad de alimentadores auxiliares



Claves para el cálculo:

- Número de elementos de consumo continuo (necesitan 12Vcc para su funcionamiento) que son capaces de alimentar el panel de intrusión y las fuentes de alimentación auxiliares si fueran precisas.
- Determinar fuente/es de alimentación en el caso de que se necesitaran.
- Calcular baterías de respaldo atendiendo a normativa.



UNE-EN 50131-1:2008/A3:2021 Requisitos del sistema

Fuentes de alimentación



Duración mínima de la fuente de alimentación de emergencia

Fuente de alimentación	Grado 1	Grado 2	Grado 3	Grado 4
Tipo A	12 horas	12 horas	60 horas	60 horas
Tipo B	24 horas	24 horas	120 horas	120 horas

Para las fuentes de alimentación del tipo A y B en los sistemas de grados 3 y cuando se notifica un fallo en la fuente de alimentación primaria a un centro de recepción de alarmas o a otro centro de control remoto, la duración de la alimentación de emergencia puede reducirse a la mitad

Para las fuentes de alimentación del tipo A y B , cuando se proporciona una fuente de alimentación primaria complementaria, con cambio automático entre la fuente de alimentación primaria y la fuente de alimentación primaria complementaria, los periodos indicados pueden reducirse a 4 horas

Fuente de alimentación de emergencia (tipo A) - Duración de recarga

	Grado 1	Grado 2	Grado 3	Grado 4
Tiempo máximo de recarga	72 horas	72 horas	24 horas	24 horas

Honeywell

REF.	Descripción	Consumo (mA)		Total Consumo (mA)	
		Consumo	6%	Unidades	Consumo
MPIP2000	Panel Serie 2000	230	243,8	1	243,8
MPIP3000	Panel Serie 3000	270	286,2	0	0
MPICLTEE	Módulo GPRS 4G	45	47,7	1	47,7
MPIKTSPRX	Teclado proximidad	75	79,5	1	79,5
MPIKTSMF	Teclado proximidad Mifare	110	116,6	0	0
MPIDC1	Módulo accesos	60	63,6	0	0
MPIEOP4	Módulo 4 relés	15	15,9	0	0
MPIEIOB4E	Expansor de zonas	35	37,1	2	74,2
TOTAL EQUIPOS DE CONTROL				445,2	
DT8016AF4	Detector volumétrico Grado 3	9	9,54	12	114,48
033430.01	Detector volumétrico Grado 3	6	6,36	0	0
DT8320AF4	Detector volum. 360º Grado 3	15	15,9	0	0
DT8016AF4-SN	Detector volumétrico Grado 3 V-Plex	4	4,24	0	0
DT8320AF4-SN	Detector volum. 360º Grado 3 V-Plex	6	6,36	0	0
SCT100	Detector sísmico	3	3,18	2	6,36
LUMINAX	Lector de proximidad	40	42,4	0	0
ADPRO	Detector exterior hasta 60 metros	60	63,6	0	0
TOTAL DETECCIÓN				120,84	
TOTAL CONSUMO				566,04	
Consumo máximo salidas					
				MPIP2000	MPIP3000
AUX1	1500 mA	1100 mA			
AUX2		1100 mA			
V-Plex 1	128 mA	128 mA			
V-Plex 2		128 mA			

Herramientas para el cálculo de consumos

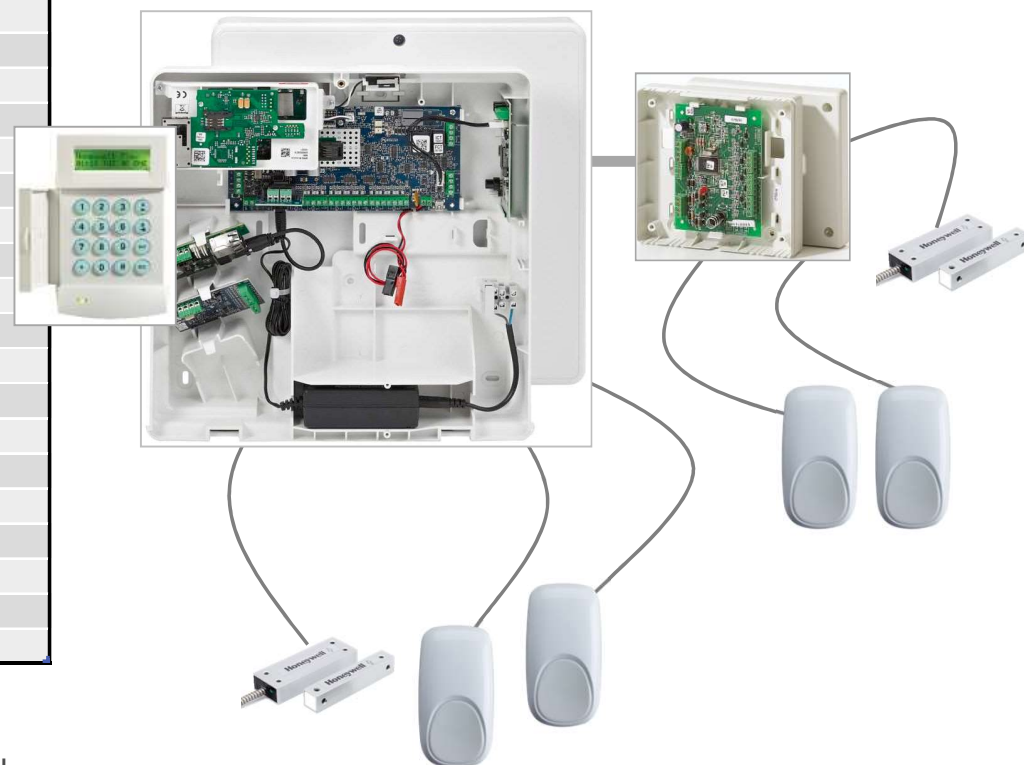
UNE-EN 50131-1:2008/A3:2021 Requisitos del sistema Señalización



Señalización	Grado 1	Grado 2	Grado 3	Grado 4
Sistema Activado / Parcialmente activado	M	M	M	M
Sistema Desactivado	M	M	M	M
Condición de alarma de atraco	M	M	M	M
Identificación de la zona de atraco	M	M	M	M
Condición de alarma de intrusión	M	M	M	M
Identificación de la zona de intrusión	M	M	M	M
Identificación del detector de intrusión*	M	M	M	M
Identificación condición de alarma del detector	M	M	M	M
Inhibido	M	M	M	M
Aislado	M	M	M	M
Condiciones de fallo	M	M	M	M
Condición de manipulación	M	M	M	M
Enmascaramiento	Op	Op	M	M
Reducción de alcance	Op	Op	Op	M
Señalización (es) en espera	M	M	M	M
Señalización de alerta	M	M	M	M
Activación	Op	Op	Op	Op
Fin de la activación	M	M	M	M
Señalización de entrada	M	M	M	M
Fin de la desactivación	M	M	M	M

M = Obligatorio / Op = Opcional

* La identificación del detector de intrusión está destinada a permitir al usuario determinar la causa de la condición de alarma contra intrusos. En UNE-EN 50131-1:2008/A2 2017, se elimina la condición anterior de que se aplicaba sólo a detectores con capacidades de procesamiento.



Supervisión de la disponibilidad de las interconexiones por cable

	Grado 1	Grado 2	Grado 3	Grado 4
Control de la disponibilidad	Op	Op	M	M
Periodo máximo de indisponibilidad continua de la interconexión	30 segundos	30 segundos	10 segundos	2 segundos

Verificación de las comunicaciones

	Grado 1	Grado 2	Grado 3	Grado 4
Intervalos máximos permitidos	100 segundos	100 segundos	60 segundos	10 segundos

Señales o mensajes que se generarán en respuesta a la monitorización

	Grado 1	Grado 2	Grado 3	Grado 4
Si es posible, identificar la condición específica como fallo	T o F	T o F	T	T

T = señal de Tamper / F = señal de Fallo

Supervisión de la integridad de las interconexiones

	Grado 1	Grado 2	Grado 3	Grado 4
Corte de todos los hilos	M	M	M	M
Corte de algún hilo	Op	M	M	M
Cortocircuito de todos los hilos	Op	M	M	M
Cortocircuito de algún par de hilos	Op	M	M	M

Estas condiciones aplican a los cables utilizados para la interconexión entre dos componentes del sistema

M = Obligatorio / Op = Opcional



UNE-EN 50131-1:2008/A3:2021 Requisitos del sistema Detección de la manipulación



Deteccion de la manipulación - Componentes a incluir

Componentes	Grado 1	Grado 2	Grado 3	Grado 4
CIE - Equipo de control y señalización	M	M	M	M
ACE - Equipo auxiliar de control	M	M	M	M
SPT - Equipo de transmisión de alarma	M	M	M	M
WD - Dispositivo de aviso	M	M	M	M
PS - Fuente de alimentación	M	M	M	M
Dispositivos contra los atracos (a)	Op	M	M	M
Detecores de intrusión (b)	Op	M	M	M
Cajas de unión	Op	Op	M	M

Op = Opcional / M = Obligatorio

(a) No se requiere que los ACE y los dispositivos de atraco cumplan los requisitos de esta tabla

(b) En ciertos grados puede ser necesario proteger los dispositivos contra la manipulación con una

Deteccion de la manipulación - Medios para detectarla

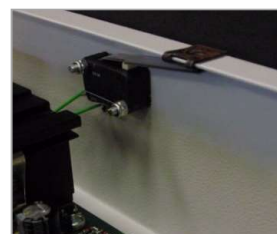
Medios	Grado 1	Grado 2	Grado 3	Grado 4
Apertura por medios normales	M	M	M	M
Retirada del montaje (equipos inalámbricos)	Op	M	M	M
Retirada del montaje (equipos cableados)	Op	Op	M (c)	M
Penetración del WD audible	Op	Op	Op	M (a)
Penetración del CIE/ACE/SPT	Op	Op	Op	M (a)
Ajuste de la orientación del detector	Op	Op	M (b)	M (b)

Op = Opcional / M = Obligatorio

(a) Se aplica al CIE, ACE, SPT, WD cuando están situados fuera del local vigilado

(b) Cuando el ajuste de la orientación es posible

(c) Opcional para las cajas de unión y los contactos de apertura



Detectores sísmicos, a tener en cuenta



Dispositivo para test externo:
Permite el test de todos los
que están en su radio de
acción (5 metros)



Sísmico



Dispositivo para test interno

Orden INT/316/2011, de Febrero

ATM1 Area

Settings

Sensors

Outputs

Test

Seismic Sensor Test

TEST NOW

☐ Schedule Daily Test

Last test result: 31 May 2021, 10:54 AM

TOTAL	SUCCESS
02	01
Name	Zone No
Zone 1	1
Zone 5	5

Ejemplo de programación en panel

Panel I/O

Zones

Outputs

Diagnostics

0 Unassigned

Reset All

Basic View

Zone No	Zone Name	Response Type	Area	Bypassable
1	Zone 1	23 - Seismic	ATM1 Area	Yes
2	Zone 2	12 - 24 Hour Personal Assistance	Area1-MPIP3000E_1	Yes
3	Zone 3	15 - CO Detector	Area1-MPIP3000E_1	Yes
4	Zone 4	17 - 24 Hour Trouble	Area1-MPIP3000E_1	Yes
5	Zone 5	22 - Non-Security Response	Area1-MPIP3000E_1	Yes
6	Zone 6	23 - Seismic	ATM1 Area	Yes
7	Zone 7	25 - Holdup Type 2	Area1-MPIP3000E_1	Yes
8	Zone 8	34 - Fire	Area1-MPIP3000E_1	Yes
9	Zone 9	35 - Not Used	Area1-MPIP3000E_1	Yes
10	Zone 10	3 - Perimeter	Area1-MPIP3000E_1	Yes

CANCEL

SAVE AND SYNC

BOE BOLETÍN OFICIAL DEL ESTADO Núm. 42 Viernes 18 de febrero de 2011 Sec. I. Pág. 18332		
Equipos	Acciones	Periodicidad (*)
Funciones automáticas de test	Batería: La batería se comprobará también de forma automática y, en caso de fallo, éste será transmitido a la CRA. Red de c.a: La red de c.a. estará también supervisada. Cualquier fallo deberá ser comunicado a la CRA, con un posible retardo. Un corte accidental del suministro eléctrico de poca duración no debe tener incidencia sobre el sistema. Registro de incidencias: Deberá ser obtenido bidireccionalmente, permitiendo analizar posibles fallos.	Trimestral
Funciones avanzadas de autotest	Sísmicos: Los sísmicos pueden ser comprobados de forma periódica y automática y, de producirse un fallo, éste será comunicado a la CRA. Para ello, cada sísmico debe poseer una cerámica de test en su interior o en sus inmediaciones que generará una vibración de corta duración al ser activada mediante una salida del CIE. Esta vibración generará una señal de alarma que será ignorada como tal por la central, sin embargo, si esta señal de alarma no se produjera, su omisión sí sería interpretada como fallo. Detectores y contactos Los detectores de movimiento y los contactos magnéticos montados sobre puertas y ventanas practicadas habitualmente se activan cuando el sistema se encuentra desarmado. Sus señales de alarma llegan a la central pero son ignoradas en estas circunstancias, no obstante, pueden emplearse para determinar un posible fallo de uno de estos elementos.	Trimestral

Detectores sísmicos, comentario acerca de UNE-EN 50131-2-8



Norma Española
UNE-EN 50131-2-8

Diciembre 2017
Versión corregida, Septiembre 2020

Sistemas de alarma

Sistemas de alarma de intrusión y atraco

Parte 2-8: Detectores de intrusión

Detectores de impactos

Esta norma ha sido elaborada por el comité técnico CTN 108 Seguridad física y electrónica. Sistemas de protección y alarma, cuya secretaria desempeña AES.



EXTRACTO DEL DOCUMENTO UNE-EN 50131-2-8



Asociación Española
de Normalización
Génova, 6 - 28004 Madrid
915 294 900
info@une.es
www.une.es

1 Objeto y campo de aplicación

Esta norma europea trata los detectores de impactos instalados en edificios para detectar el impacto o serie de impactos provocados por un ataque con fuerza a una barrera física (por ejemplo, puertas o ventanas).

Especifica cuatro grados de seguridad de I a IV (según la Norma EN 50131-1), detectores inalámbricos o con cable específicos o no específicos y cuatro clases de usos ambientales de I a IV (según la Norma EN 50130-5).

Esta norma no incluye los requisitos de los detectores de impactos destinados a la detección de ataques de penetración a cajas fuertes y cámaras acorazadas mediante perforación, corte o lanza térmica.

Esta norma no incluye los requisitos de los detectores de impactos destinado al uso en exteriores.

El detector de impactos necesita cumplir con todos los requisitos del grado de seguridad especificado.

Las funciones adicionales a aquellas obligatorias especificadas en esta norma pueden ser incluidas en el detector siempre y cuando no afecten negativamente al correcto funcionamiento de las funciones obligatorias.

Esta norma no trata los requisitos para el cumplimiento de las directivas reguladoras tales como la directiva de CEM, la directiva de baja tensión, etc., salvo en el caso de que especifica las condiciones del equipo para el ensayo de susceptibilidad CEM, como se requiere en la Norma EN 50130-4.

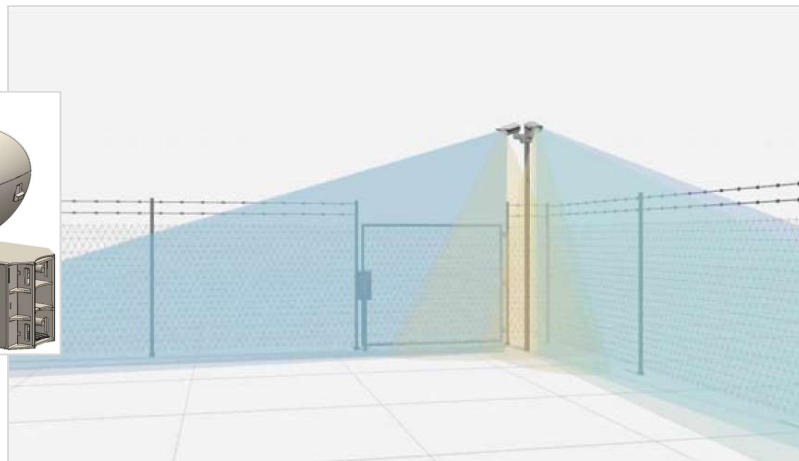
Esta norma no es aplicable a las interconexiones del sistema.



Equipos aún no normalizados

▪ Orden INT/314/2011. Disposición transitoria única:

- Cuando un sistema de alarma necesite utilizar componentes que en el momento de su instalación no estén disponibles en el mercado, según lo establecido en la normativa sobre funcionamiento de los sistemas de alarma en el ámbito de la seguridad privada, se permitirá su conexión, siempre que tales elementos no influyan negativamente en su funcionamiento operativo.
- La permanencia de tales elementos en el sistema estará condicionada a la posible aparición de la especificación técnica que lo regule y a su disponibilidad en el mercado. Transcurrido el periodo de carencia de diez años establecido, se deberá disponer del pertinente certificado emitido por el fabricante y exhibirse.



Protección perimetral



Dispositivos de atraco

Comentario sobre las comunicaciones de alarma

- **Pregunta)** ¿Dónde dice que las instalaciones de grado 3 o de grado 4 estén obligadas a tener 2 vías de comunicación?. Únicamente donde se hace referencia parecida es en el artículo 12 “alarma confirmada”, en la norma 50136 no dice nada al respecto.
- **Respuesta)** Ni en las nuevas Órdenes Ministeriales, ni las Normas UNE EN sobre sistemas de alarma exigen que los sistemas de Grado 3 o de Grado 4 tengan obligatoriamente que contar con doble vía de comunicación, siendo esta obligación dependiente de las distintas opciones que permite la Norma, acerca de las características y los tipos y elementos que se van a instalar.

Supervised Premises Transceiver MPIP3000E - Alarm panel with integrated single path SPT (Ethernet) MPIP2100E - Alarm panel with integrated single path SPT (Ethernet) MPIP2000E - Alarm panel with integrated single path SPT (Ethernet) MPICLTEE – 4G module (provides radio based secondary transmission path for a dual path SPT) <i>In order to provide an EN 50136 compliant ATS, the SPT must be used in conjunction with a receiving centre transceiver (RCT) which complies with the requirements of EN 50136-3.</i>	ATS Category: Ethernet/4G: DP4 Ethernet: SP5 SPT Classification: Type Z Equipment type - Fixed Environmental Class II	EN 50136-2: 2013 EN 50131-10: 2014 Including the related requirements of: EN 50136-1:2012 + A1: 2018 EN 50130-4: 2011 + A1: 2014 EN 50130-5: 2011
--	---	--

Ejemplo certificado MAXPRO Intrusion, apartado comunicaciones

DIRECCIÓN GENERAL DE LA POLICÍA Y DE LA GUARDIA CIVIL
 Comisaría General de Seguridad Ciudadana



SEGURPRI

Monográfico N° 13 Octubre 2011





PREGUNTAS MÁS FRECUENTES (F.A.Q.)
 ORDENES MINISTERIALES

Desde la publicación en el Boletín Oficial del Estado, el pasado 18 de febrero, de las cinco nuevas órdenes ministeriales, muchas han sido las preguntas planteadas a esta Unidad Central de Seguridad Privada por parte de empresas, asociaciones, sindicatos, personal, etc., bien sobre dudas, aclaración, o interpretación del articulado de las mismas

Con las respuestas que a las mismas se han realizado, se han elaborado el presente monográfico de SEGURPRI, esperando que sirva de ayuda y referencia para el resto del sector de seguridad privada.

Criterios de funcionamiento de la transmisión

- Las condiciones de atraco, de alarma de intrusión, de manipulación y de fallo, así como las otras condiciones, se deben notificar mediante un sistema de transmisión de alarma y/o un dispositivo de aviso audible de acuerdo con los requisitos especificados en las tablas: requisitos sobre la notificación (UNE-EN 50131-1:2008/A2:2017) y tiempos máximos de notificación (UNE-EN 50136-1:2012/A1:2019)

NOTIFICACIÓN DE ALARMAS	Grado 2						Grado 3					Grado 4			
	A	B	C	D	E	F	A	B	C	D	E	A	B	C	D
Sirena normal	2	Op	Op	Op	Op	Op	2	Op	Op	Op	Op	2	Op	Op	Op
Sirena autoalimentada	Op	1	Op	Op	1	Op	Op	1	Op	Op	Op	Op	1	Op	Op
Comunicador (categoría ATS)	SP2	SP2	DP1	SP3	Op	DP2	SP3	SP3	DP2	SP4	DP3	SP5	SP5	DP4	SP6

	SP1	SP2	SP3	SP4	SP5	SP6	DP1	DP2	DP3	DP4
Fallo de la vía primaria	32 días	25 horas	30 min	3 min	90 seg	20 seg	25 horas	30 min	3 min	90 seg
Fallo de la vía secundaria (la primaria está operativa)	Op	Op	Op	Op	Op	Op	50 horas	25 horas	25 horas	5 horas
Fallo de la vía alternativa (la primaria ha fallado)	Op	Op	Op	Op	Op	Op	25 horas	30 min	3 min	90 seg
Fallo de todas las vías al mismo tiempo	32 días	25 horas	30 min	3 min	90 seg	20 seg	25 horas	31 min	4 min	3 min

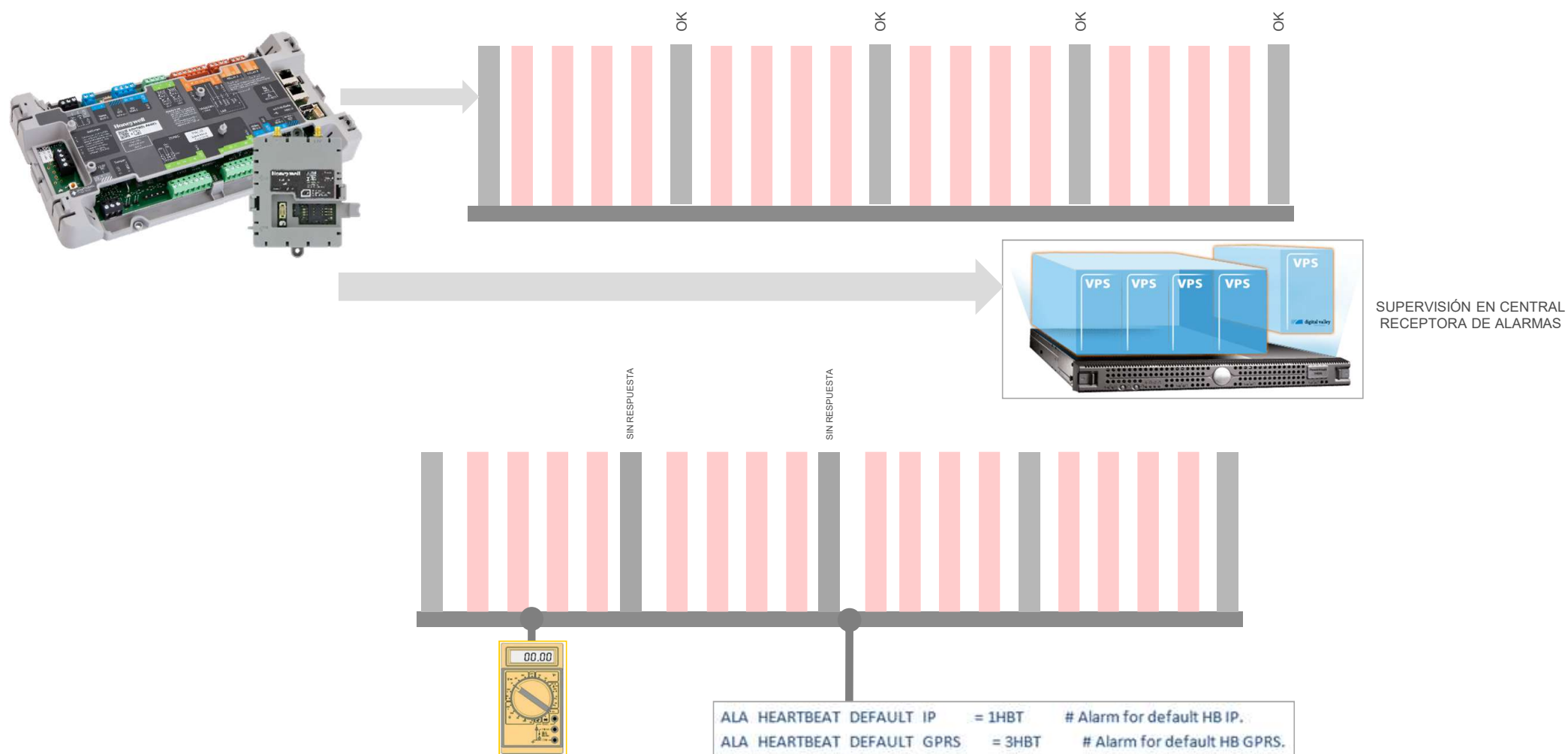


Categoría del transmisor de alarmas (ATS):

- Ethernet / 4G: DP4 – Sistemas con doble vía de comunicación
- Ethernet: SP5 – Sistemas con sólo una vía de comunicación

(Comunicaciones MAXPRO Intrusion)

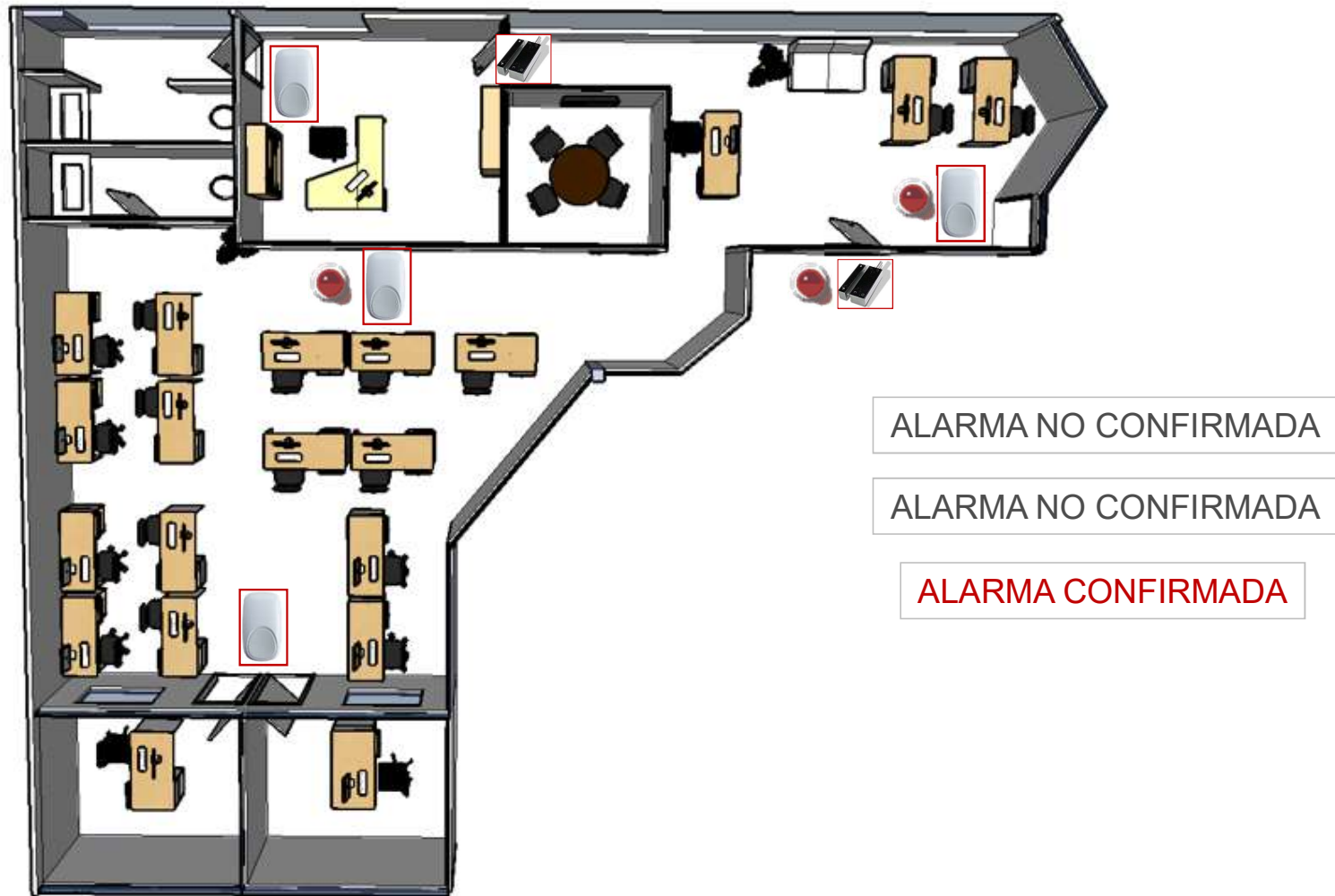
Ejemplo de supervisión de las comunicaciones

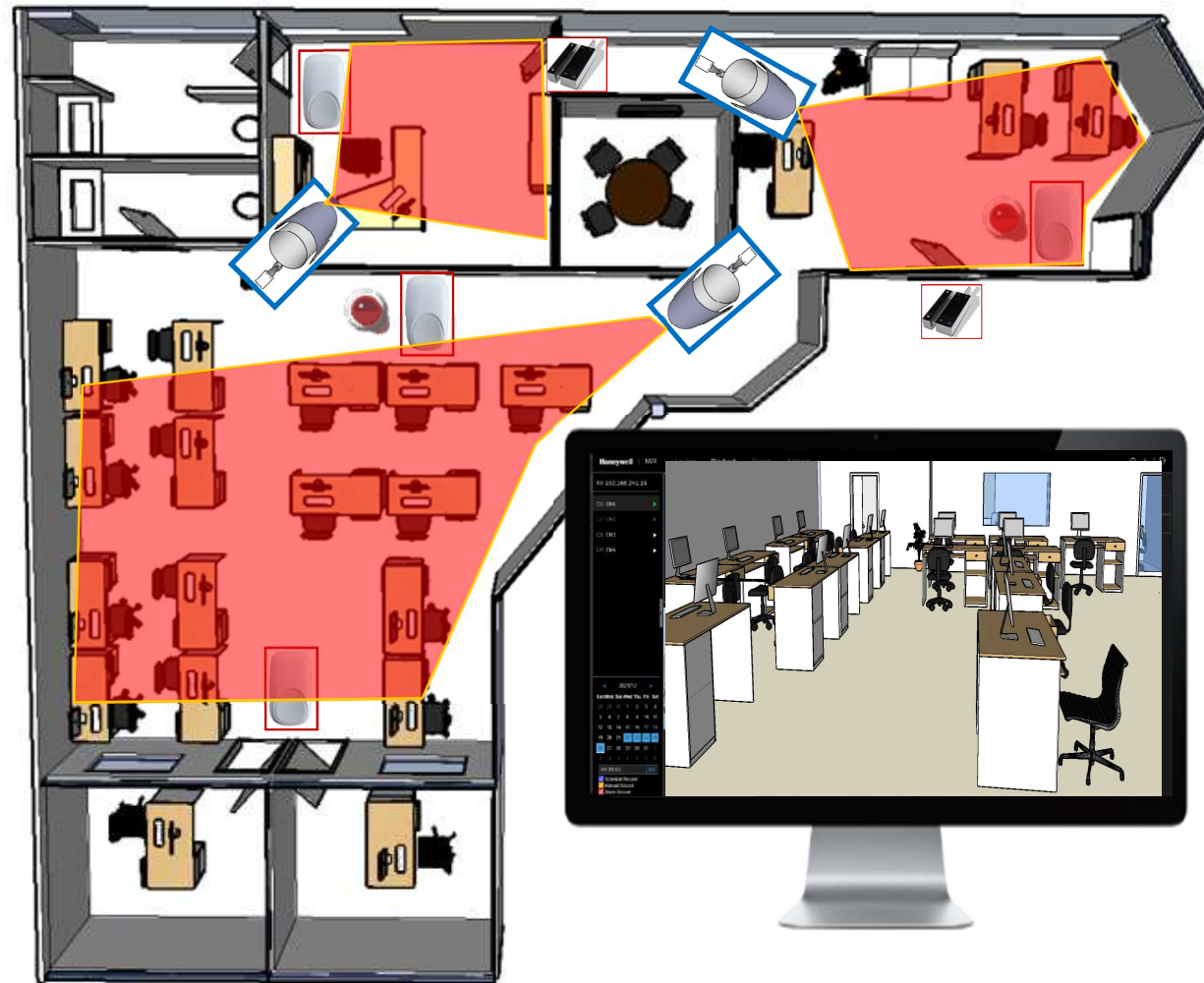


- De conformidad con lo dispuesto en el Reglamento de Seguridad Privada (Art. 48), cuando se produzca una alarma, las centrales de alarma deberán proceder de inmediato a su verificación, utilizando, para que esta sea considerada válida, todos o algunos de los procedimientos técnicos o humanos establecidos en el presente Capítulo, comunicando seguidamente, al servicio policial correspondiente, las alarmas reales producidas.



Verificación secuencial, ejemplo instalación Grado 2





Honeywell



SISTEMAS DE VIDEOVIGILANCIA, CLAVES DE DISEÑO

UNE – EN 62676-4:2015

Referencia para el diseño de sistemas de videovigilancia





LEGISLACIÓN CONSOLIDADA

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

Ministerio del Interior
«BOE» núm. 42, de 18 de febrero de 2011
Referencia: BOE-A-2011-3170

TEXTO CONSOLIDADO
Última modificación: 09 de septiembre de 2020

Relación de Normas UNE o UNE-EN que resultan de aplicación en los sistemas de alarma

Denominación
Compatibilidad electromagnética. Norma de familia de producto: Requisitos de inmunidad para detección de incendios, intrusión y alarma social.
Compatibilidad electromagnética. Norma de familia de producto: Requisitos de inmunidad para detección de incendios, intrusión y alarma social.
Compatibilidad electromagnética. Norma de familia de producto: Requisitos de inmunidad para detección de incendios, intrusión y alarma social.
Métodos de ensayo ambiental.
Sistemas de alarma contra intrusión y atraco. Parte 1: Requisitos del sistema.
Sistemas de alarma contra intrusión y atraco. Parte 1: Requisitos del sistema.
Sistemas de alarma de intrusión y atraco. Parte 2-2: Detectores de intrusión. Detectores de infrarrojos pasivos.
Sistemas de alarma de intrusión y atraco. Parte 2-3: Requisitos para detectores de microondas.
Sistemas de alarma de intrusión y atraco. Parte 2-4: Requisitos para detectores combinados de infrarrojos pasivos
Sistemas de alarma de intrusión y atraco. Parte 2-5: Requisitos para detectores combinados de infrarrojos pasivos
Sistemas de alarma. Sistemas de alarma de intrusión y atraco. Parte 2-6: Contactos de apertura (magnéticos).
Sistemas de alarma. Sistemas de alarma de intrusión y atraco. Parte 3: Equipo de control y señalización.
Sistemas de alarma. Sistemas de alarma de intrusión y atraco. Parte 4: Dispositivos de advertencia.
Sistemas de alarma. Sistemas de alarma de intrusión. Parte 5-3: Requisitos para los equipos de interconexión que usan técnicas de radiofrecuencia.
Sistemas de alarma. Sistemas de alarma de intrusión. Parte 5-3: Requisitos para los equipos de interconexión que usan técnicas de radiofrecuencia.
Sistemas de alarma. Sistemas de alarma de intrusión. Parte 6: Fuentes de alimentación.
Sistemas de alarma. Sistemas de alarma de intrusión y atraco. Parte 6: Fuentes de alimentación.
Sistemas de alarma. Sistemas de alarma de intrusión y atraco. Parte 8: Sistemas/dispositivos de niebla de seguridad.
Sistemas de alarma. Sistemas de alarma de intrusión. Parte 2-2: Requisitos para los detectores de infrarrojos pasivos.
Sistemas de alarma. Sistemas de alarma de intrusión. Parte 2-3: Requisitos para detectores de microondas.
Sistemas de alarma. Sistemas de alarma de intrusión. Parte 2-4: Requisitos para los detectores combinados de infrarrojos pasivos y de microondas.
Sistemas de alarma. Sistemas de alarma de intrusión. Parte 2-5: Requisitos para los detectores combinados de infrarrojos pasivos y ultrasónicos.
Sistemas de alarma. Sistemas de alarma de intrusión. Parte 2-6: Requisitos para contactos de apertura (magnéticos).
Sistemas de alarma. Sistemas de alarma de intrusión. Parte 3: Equipo de control y señalización.
Sistemas de alarma. Sistemas de alarma de intrusión. Parte 7. Guía de aplicación
Sistemas de alarma. Sistemas de vigilancia CCTV para uso en aplicaciones de seguridad. Parte 1: Requisitos del sistema.
Sistemas de alarma. Sistemas de vigilancia CCTV para uso en aplicaciones de seguridad. Parte 2-1: Cámaras en blanco y negro.
Sistemas de alarma. Sistemas de vigilancia CCTV para uso en aplicaciones de seguridad. Parte 4-1: Monitores en blanco y negro.

UNE-EN 62676-4:2015

UNE

Sistemas de videovigilancia para utilización en aplicaciones de seguridad. Parte 4: Directrices de...

01 / 05 / 2015

Vigente

UNE-EN.	50133-1/A1.	2004	Sistemas de alarma. Sistemas de control de accesos de uso en las aplicaciones de seguridad. Parte 1: Requisitos de los sistemas.
---------	-------------	------	--

Sistemas de videovigilancia

Protección ante ataques externos



Estándar del sector de tarjetas de pago para prevenir el fraude y las infracciones de información



Garantiza características que permiten acreditar funciones de control de ataques externos



Estándar de encriptación



Protocolo criptográfico que permite una comunicación segura

1

Determina la prohibición de la instalación de equipos de Videovigilancia y Comunicaciones que no la cumplan*, no impactando en otras áreas de la seguridad electrónica

2

No se puede instalar contenido ni materiales de empresas y subsidiarias no NDAA

3

Generalmente diseñados pensando en la Ciberseguridad

4

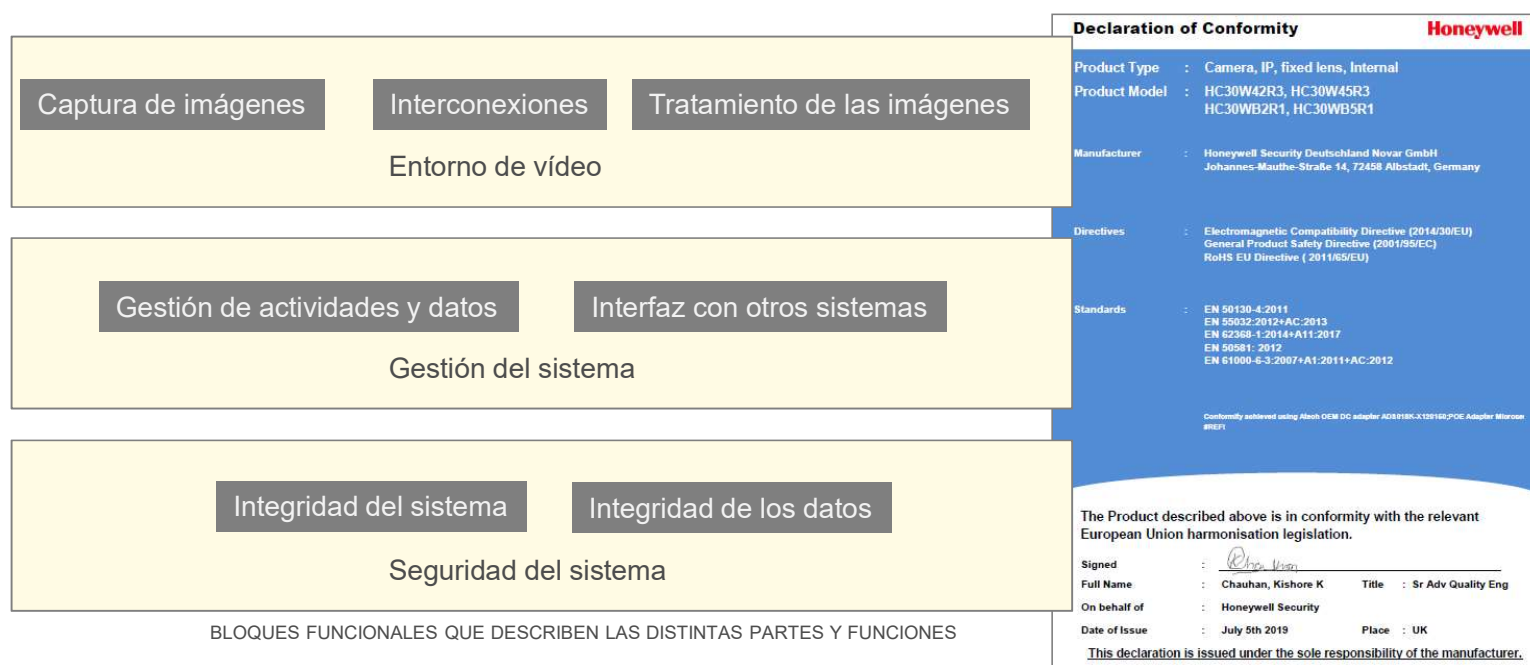
No todas las soluciones NDAA son Ciberseguras



* Ciertas compañías chinas y sus subsidiarias



- Un sistema de CCTV (VSS) normalmente está compuesto por dispositivos analógicos y digitales, así como de software. Ya que la tecnología y, con ella, los equipos de los VSS y sus funcionalidades se desarrollan y cambian rápidamente, esta norma no define aparatos individuales ni sus requisitos. En su lugar se define y describe a un VSS como un conjunto de partes funcionales y las relaciones que existen entre ellas.





- Antes de realizar el diseño del sistema de CCTV hay que analizar el propósito para el que se diseña, **las necesidades del cliente y las amenazas frente a las que nos vamos a encontrar**; siguiendo estas premisas se conseguirá el sistema más adecuado para controlar los posibles riesgos identificados.



- Los sistemas de videovigilancia se clasifican en grados que describen el nivel de seguridad requerido. Tienen en cuenta el nivel de riesgo, que depende de la probabilidad de que se produzca un incidente y del daño potencial causado.

	Baja probabilidad - Consecuencias importantes	Alta probabilidad - Consecuencias improtantes	
Grados 2-3	Lugares en los que la probabilidad de que se produzca un incidente no deseado es baja pero las consecuencias potenciales son de gran importancia	Lugares en los que la probabilidad de que se produzca un incidente no deseado es alta y las consecuencias potenciales son de gran importancia	Grado 4
	Baja probabilidad - Consecuencias poco importantes	Alta probabilidad - Consecuencias poco importantes	
Grado 1	Lugares en los que la probabilidad de que se produzca un incidente no deseado es baja y las consecuencias potenciales son de poca importancia	Lugares en los que la probabilidad de que se produzca un incidente no deseado es alta y las consecuencias potenciales son de poca importancia	Grados 2-3

Las consecuencias incluyen daños personales, muerte, daños o pérdida de bienes materiales, pérdida de información y daños al entorno

La probabilidad es la posibilidad de que haya consecuencias y está ligada a la presencia de sistemas de alarma, personal de seguridad, protecciones físicas y situaciones de riesgo general (desórdenes sociales, desastres naturales) en la zona

A 3D architectural rendering of a modern office interior. The space is divided into several areas: a large open-plan office with desks and chairs, a reception area with a long counter, and a meeting room with a large table and chairs. The office has large windows on the right side, providing natural light. The overall design is clean and professional.



IMAGINACIÓN	ALTO
Capillos	Oscilador - 6/1ps
Cajón automático	Identificar - 12,3/1ps
Cable de freno	Oscilador - 12,3/1ps
Zona de confusión de buseta	Reconocer - 6/1ps
Aperturamiento, acceso de vehículos	Vision - 12,3/1ps
Compartimiento, garaje	Oscilador - 6/1ps
Aperturamiento, acceso de peatones	Identificar - 12,3/1ps
Receptor de efectivo	Oscilador - +P.T. 12,3/1ps
Revolución de la llave	Identificar - 12,3/1ps
Combinación de bisagras y escomeros	Reconocer - 6/1ps
Soportes para escaleras	Reconocer - 6/1ps
Receptor de la llave	Oscilador - 6/1ps
Puerta cliente	Identificar - 12,3/1ps
Puerta de emergencia	Identificar - 12,3/1ps
Puerta de acceso	Oscilador +P.T. 12,3/1ps
Receptor de cheque	Reconocer - 12,3/1ps
Artículo de alto valor	Reconocer - 12,3/1ps
Interior del ascensor	Reconocer - 6/1ps
Receptor de carga	Reconocer - 6/1ps
Perímetro	Detectar - 2/1ps
Cable de telefonía	Reconocer - 6/1ps
Interior de la cabina	Detectar - 2/1ps
Alarmado	Oscilador - 12,3/1ps
Parada de taxis	Oscilador +P.T. 6/1ps
Alarma de incendio	Oscilador - 12,3/1ps
Acceso a los baños	Oscilador - 6/1ps

- **Controlar:** este nivel de detalle es suficiente para detectar una multitud de personas sobre una área amplia, observar el número, la dirección y la velocidad con que se desplazan.
- **Detectar (25 píxeles por metro):** con este nivel de detalle, el operador puede responder a una señal de alerta, buscar en la pantalla la presencia de una persona y confirmar o descartar su existencia con un alto nivel de certeza.
- **Observar (63 píxeles por metro):** Se pueden observar características particulares, como el tipo de ropa, el color, etc. También es posible tener una visión del entorno que rodea a la persona.
- **Reconocer (125 píxeles por metro):** Se puede determinar, con un alto nivel de certeza, si la persona visualizada es o no alguien que se conoce.
- **Identificar (250 píxeles por metro):** de este modo se puede identificar a una persona más allá de cualquier duda razonable.



¿Ver una escena y saber
que está ocurriendo algo?

OBSERVAR
63ppm



¿Ver un suceso y determinar
exactamente que está ocurriendo?

RECONOCER
125ppm

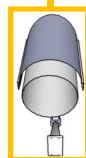
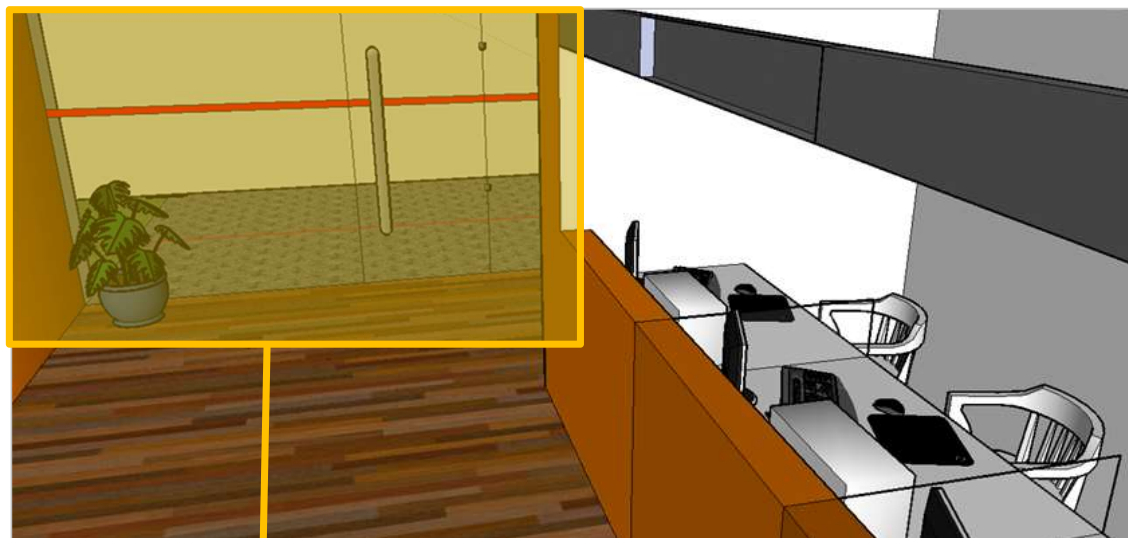


¿Identificar exactamente
a la persona implicada?

IDENTIFICAR
250ppm

Ejemplo cámara controlando puerta de acceso

Identificar = 250ppm



CÁMARA A "N" METROS DE DISTANCIA
Y A "N" METROS DE ALTURA DEL
"BLANCO"

Vestibulo calle	Observar + PTZ - 12,5 fps
Conexiones de escaleras y ascensores	Observar - 6 fps
Soportes para bicicletas	Reconocer - 6 fps
Pista de baile	Observar - 6 fps
Puerta cliente	Identificar - 12,5 fps
Puertas de emergencia	Identificar - 12,5 fps



25 PPM: DETECTAR
Puede distinguir información tal como formas, color, tamaño o género, pero no puede distinguir caras o letras



63 PPM: OBSERVAR
Puede detectar información tal como caras o matrículas (funciones de videoanálisis)

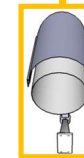
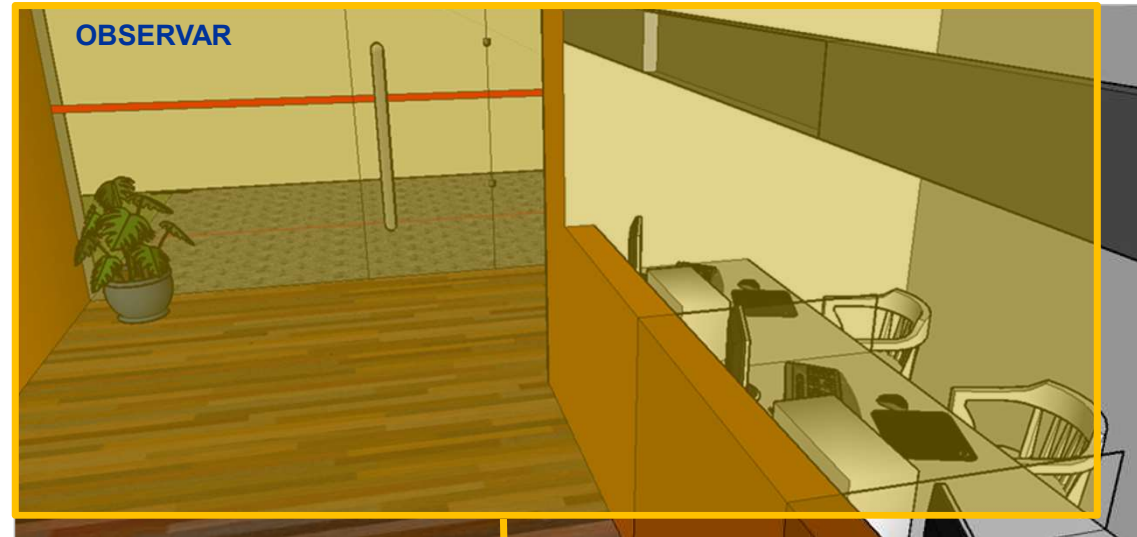
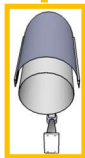
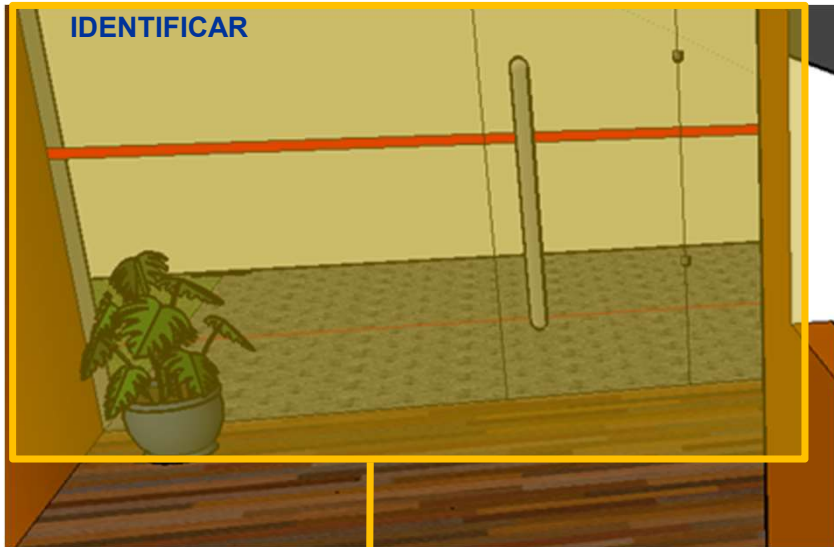


125 PPM: RECONOCER
Puede detectar información tal como caras y datos de una matrícula



250 PPM: IDENTIFICAR
Información clara y detallada tal como color de ojos o cicatrices

Propósito de cada una de las cámaras,
¿lente y resolución adecuadas? ¿ajuste adecuado en lentes MFZ?



HC35W45R2

- * Cámara formato Minidomo IP, referencia HC35W45R2. Marca Honeywell o similar.
- * Cumplimiento NDAA, sección 889, PCI-DSS y TLS1.2 (seguridad ante ataques externos), acreditados mediante certificado de detección de vulnerabilidades. AES 128/256.
- * Sensor de imagen CMOS 1/2.7" con escaneo progresivo.
- * Resolución 5 Mpx. 1St: 2592 x 1944 / 2592 x 1520 / 1920 x 1080 / 1280 x 720.
- * **Lente 2,7-13,5mm**, DC- Iris, F1.6- F3.3 MFZ.
- * **Resolución y óptica ajustadas, en el momento de la puesta en marcha, para cumplir el propósito requerido (identificación, reconocimiento, observación).**
- * Iluminación mínima 0,005 Lux/F1.6 (Color, 30 IRE), 0 Lux/F1.6 con IR encendidos.
- * Iluminación mediante LEDs hasta 50 metros (smart IR).
- * Rango dinámico extendido 120 dB.
- * Triple streaming, 2 encriptados.
- * ONVIF S, ONVIF G, ONVIF T.
- * Ranura µSD para tarjeta de hasta 256 Gb (no incluida).
- * Alimentación PoE (IEEE 802.3at) (Class 0), 12 Vcc.
- * IP66/IP67 con nivel de resistencia al impacto IK10.
- * Analíticas incorporadas en la cámara: conteo de personas, multimerodeo, intrusión, detección de movimiento, detección de movimiento inteligente. Eventos asociados a salida digital, Email o grabación en tarjeta µSD.
- * 1 Entrada / 1 salida de alarma.



Acerca de la alimentación





UBICACIÓN "BLANCO"

Pasillos	Obs
Cajero automático	Ident
Zona de bar	Obs
Zonas de contenedores de basura	Rec
Aparcamiento, acceso de vehículos	VR
Aparcamiento, garage	Obs
Aparcamiento, acceso de peatones	Rec
Recuento de efectivo	Ident
Vestibulo calle	Obs
Conexiones de escaleras y ascensores	Obs
Soportes para bicicletas	Reconocer - 6 fps
Pista de baile	Observar - 6 fps
Puerta cliente	Identificar - 12.5 fps
Puertas de emergencia	Identificar - 12.5 fps
Fachada	Observar + PTZ - 12.5 fps
Puesto de socorro	Reconocer - 12.5 fps
Artículos de alto valor	Reconocer - 12.5 fps
Interior del ascensor	Reconocer - 6 fps
Muelle de carga	Rec
Perímetro	Def
Cabina de teléfono	Obs
Zona estéril	Def
Almacén	Rec
Parada de taxis	Obs
Cajas registradoras	Rec
Acceso a los baños	Rec



XO Storage Calculator rev.: 2.0						Results		
Cameras Recording (24/7)	Quantity	Image Resolution	Image Complexity and Motion	Number of Images Per Second	Days of online storage	Network data transfer	Storage capacity required (24/7 recording)	Storage Bandwidth
H.264	SET	SELECT	SELECT	SET	SET	Megabit/sec	Gigabyte	Megabyte/sec
Type 1	10	8Mpixel	Medium	25	15	158,40	25701,92	20,31
Type 2	0	CIF	Medium	0	0	0,00	0,00	0,00
Type 3	0	CIF	Medium	0	0	0,00	0,00	0,00
Type 4	0	CIF	Medium	0	0	0,00	0,00	0,00
Type 5	0	CIF	Medium	0	0	0,00	0,00	0,00
Type 6	0	CIF	Medium	0	0	0,00	0,00	0,00
Type 7	0	CIF	Medium	0	0	0,00	0,00	0,00
Type 8	0	CIF	Medium	0	0	0,00	0,00	0,00
Type 9	0	CIF	Medium	0	0	0,00	0,00	0,00
Type 10	0	CIF	Medium	0	0	0,00	0,00	0,00
Type 11	0	CIF	Medium	0	0	0,00	0,00	0,00
Total:	10	Cameras			TOTAL:	158,40 Mbps (Max:160)	25701,92 GB	20,31 MBps

- Capacidad de almacenamiento
- Procesador NVR
- Ancho de banda en la red

Identificación facial

- Recomendación y directrices para instalaciones de videovigilancia. **Fuente: Grupo de trabajo en identificación facial de la Red de Laboratorios Forenses Oficiales de España (RLFOE)**



La evaluación debe realizarse sobre los fotogramas extraídos del videograbador

Honeywell

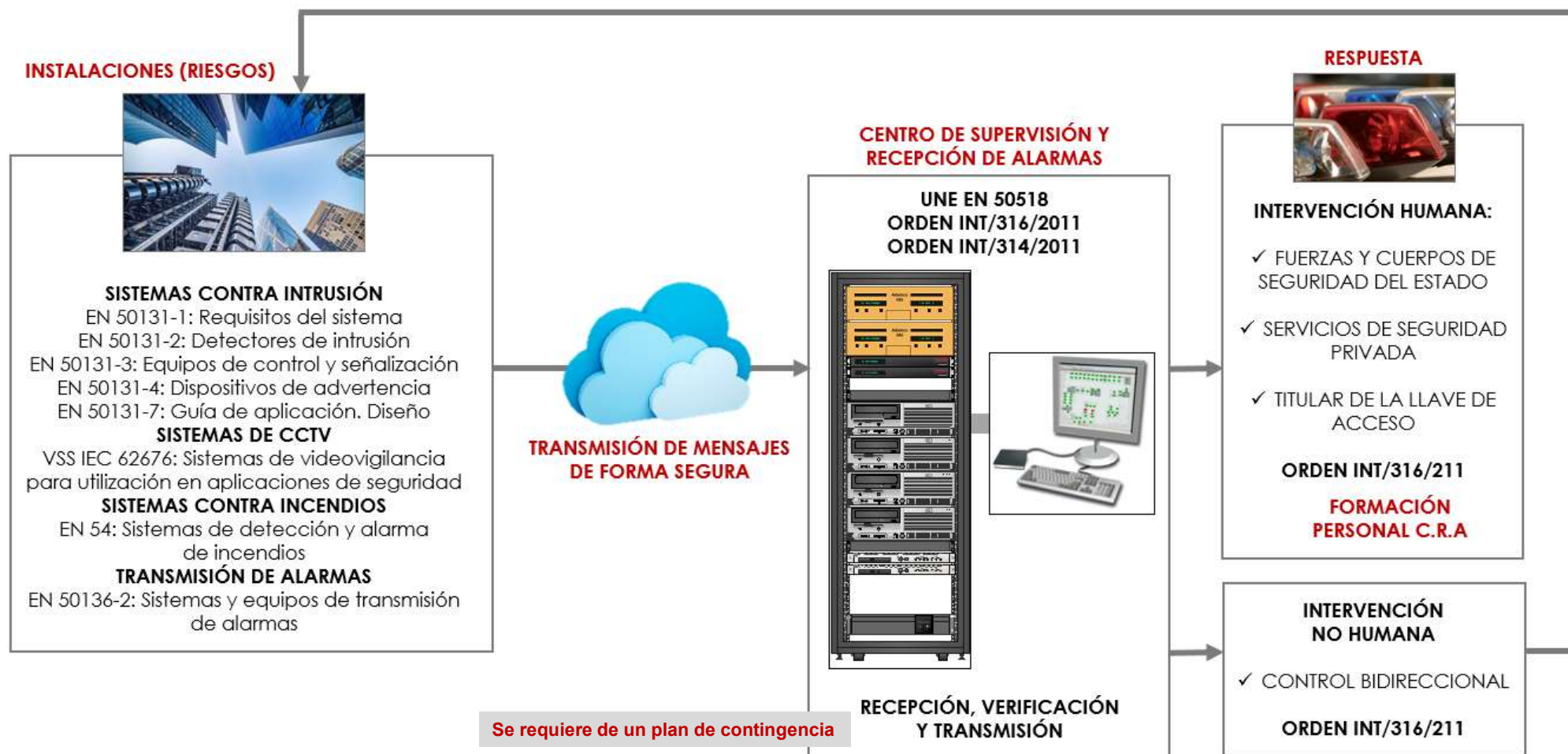


COMENTARIO ACERCA DE LOS SERVICIOS CLOUD, EVOLUCIÓN EN LOS SISTEMAS DE SEGURIDAD



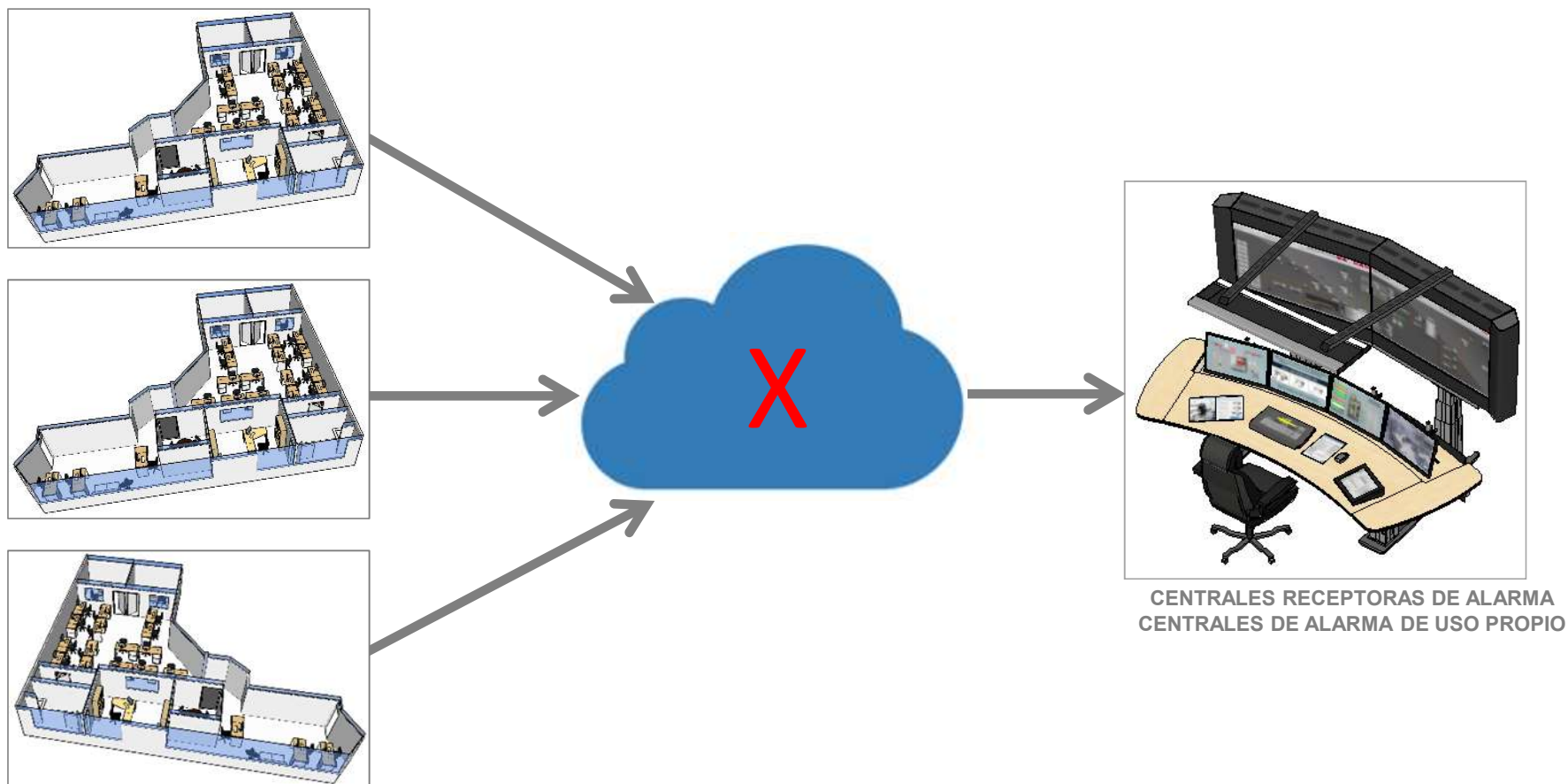
- Define todo lo concerniente a los Centros de Supervisión y Recepción de Alarmas en lo referente a las características constructivas de los recintos para contar con una infraestructura sólida.
- Establece, junto con la Orden INT/316/2011, los procesos y operativa para lograr la respuesta más eficaz a las alarmas.
- Habla de como utilizar la tecnología y medios necesarios de manera segura y fiable.





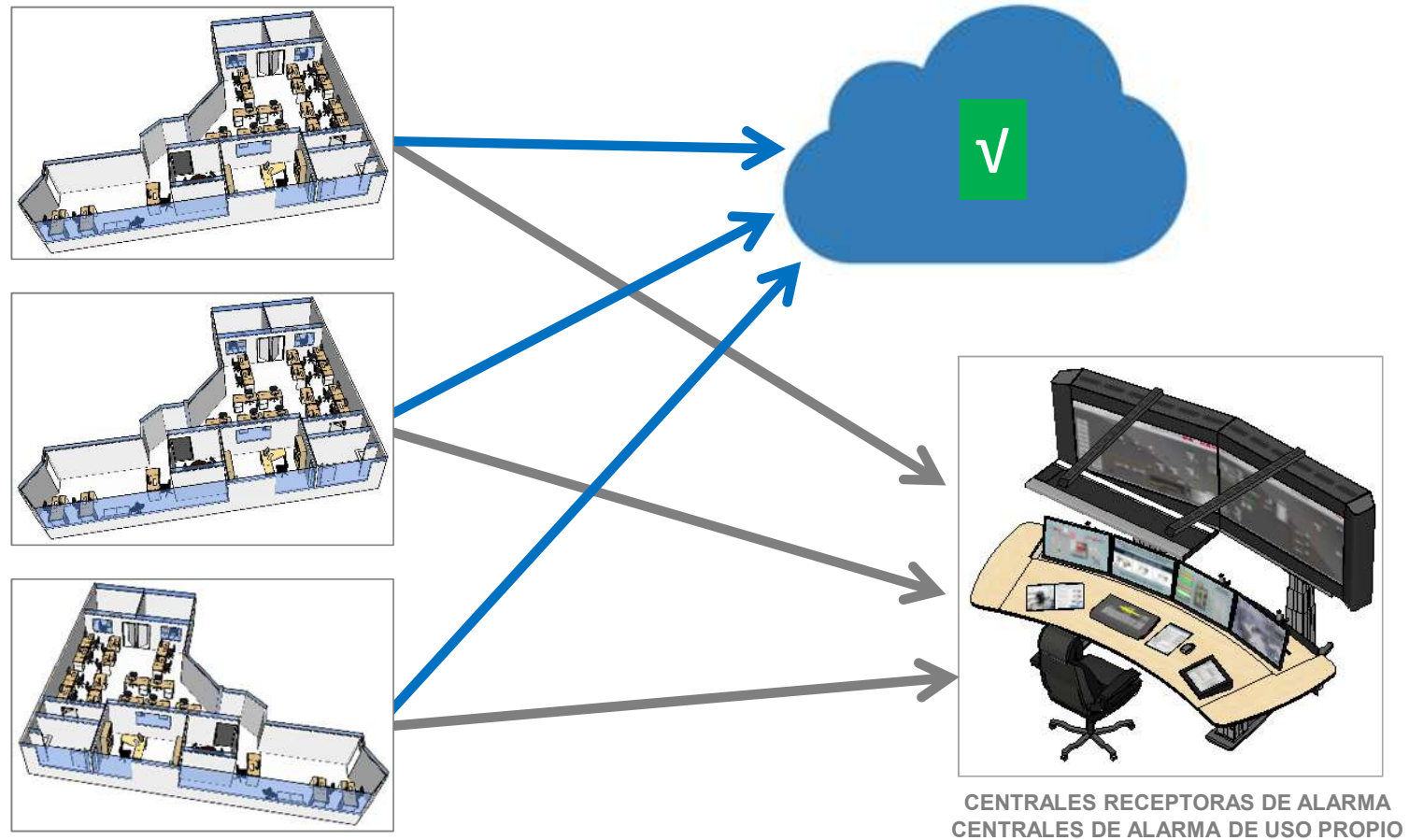
Claves para la elección de servicios Cloud

¿Dependencia de la nube?

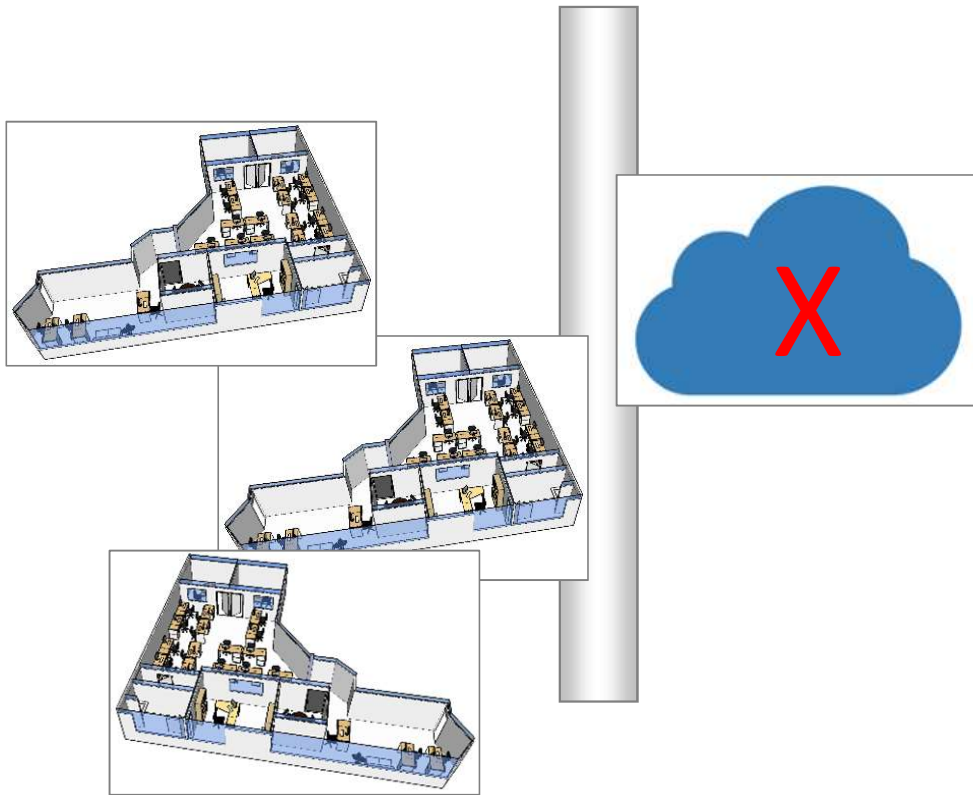


Claves para la elección de servicios Cloud

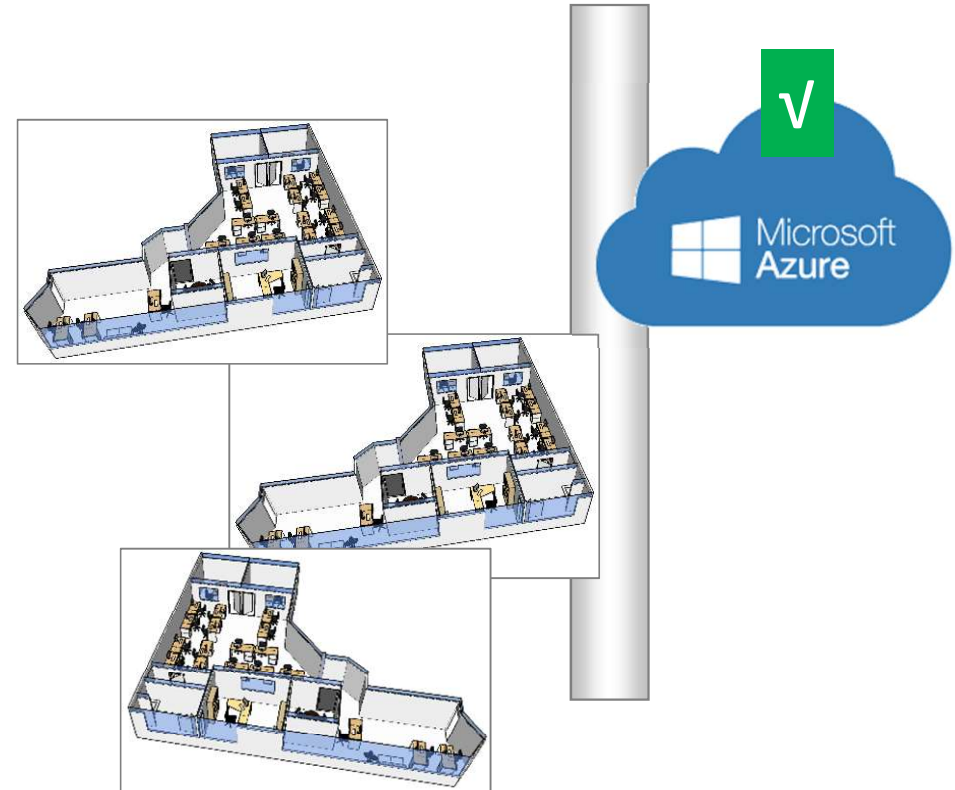
¿Información redundante?, plan de contingencia, servicios de valor añadido



Claves para la elección de servicios Cloud ¿Dónde están alojados los servidores?



CLOUD PROPIETARIO DE FABRICANTE



ACUERDO CON PARTNER TECNOLÓGICO

Claves para la elección de servicios Cloud ¿Integración entre sistemas?

