Honeywell

SISTEMAS DE VIDEOVIGILANCIA

LA IMPORTANCIA DEL DISEÑO EN LA INVESTIGACIÓN Y RESOLUCIÓN DEL DELITO Y EN LA VERIFICACIÓN DE ALARMAS

Juan José Nadales
Security Demand Generation
Honeywell | BUILDING AUTOMATION
+34 616 792 016
juan.jose.nadales@honeywell.com

HONEYWELL

NASDAQ: **HON** | ~**715** sites | ~**97,000** employees | **Charlotte, NC** headquarters | **Fortune 500** | 2022 Revenue: **~$35 B**

AEROSPACE TECHNOLOGIES

Nuestros productos se utilizan en prácticamente todas las plataformas de aeronaves comerciales y de defensa de todo el mundo e incluyen propulsión de aeronaves, sistemas de cabina de mando, comunicaciones por satélite y sistemas de energía auxiliar.

BUILDING AUTOMATION

Nuestros productos, software y tecnologías se encuentran en más de 10 millones de edificios en todo el mundo, ayudando a los clientes a garantizar que sus instalaciones sean seguras, energéticamente eficientes, sostenibles y productivas.

ENERGY & SUSTAINABILITY SOLUTIONS

Desarrollamos materiales avanzados, tecnologías de procesos, soluciones de automatización y software industrial que están revolucionando las industrias en todo el mundo.

Ayudamos a resolver los difíciles retos de la sostenibilidad y la transición energética en todos nuestros mercados

INDUSTRIAL AUTOMATION

Proporcionamos soluciones de apoyo a nuestros clientes para ayudarles a obtener resultados con mayores niveles de productividad y seguridad. Nuestra innovación impulsa soluciones de procesos, gestión del rendimiento de activos, ciberseguridad y automatización de almacenes y comercios

Honeywell Connected Enterprise

La Empresa Conectada de Honeywell (HCE) se estableció en 2018 para acelerar el desarrollo de software y soluciones de IIoT. Nos centramos en el desarrollo de software, desde la puerta de enlace hasta las aplicaciones de usuario final, aportando escala y capacidad en todo Honeywell. Estas nuevas ofertas se comercializan a través de los negocios de Honeywell.

BUILDING AUTOMATION | INNOVACIÓN Y TECNOLOGÍA

Sistemas de gestión de edificios

Controles precisos y optimización del uso de la energía, calefacción, refrigeración, humedad, utilización del espacio y software de gestión de edificios

Incendio

Sistemas de control y software relacionado, incluidos centrales de incendios, detectores de humo/CO, sistemas de megafonía y alarmas, detección de incendios por aspiración y alarmas de voz

Seguridad

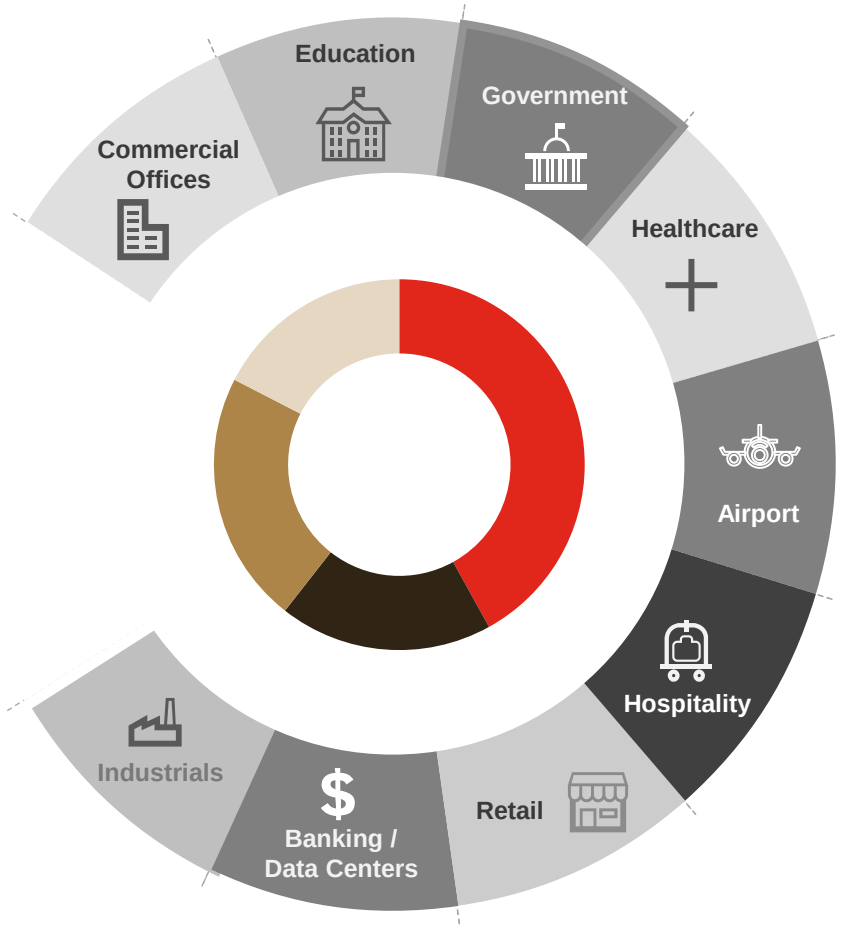
Sistemas de detección y software relacionado, incluidos intrusión, control de acceso, videovigilancia y verificación de alarmas para edificios e infraestructuras críticas

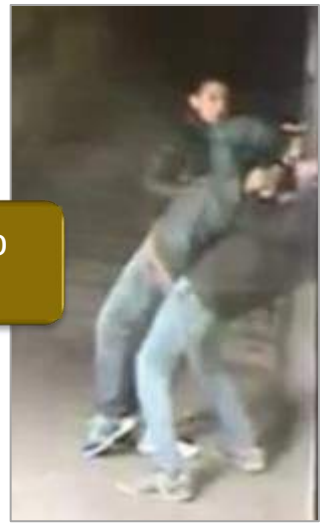
Soluciones para edificios

Software y hardware integrados para edificios y estructuras complejas, especializados en instalación, integración y servicio

Aire y Agua

Sistemas de purificación del aire y filtrado del agua





Autores del hecho delictivo captados por las cámaras

Investigación policial

Autores desconocidos

Autores conocidos

Diligencias de investigación (Instrucción)

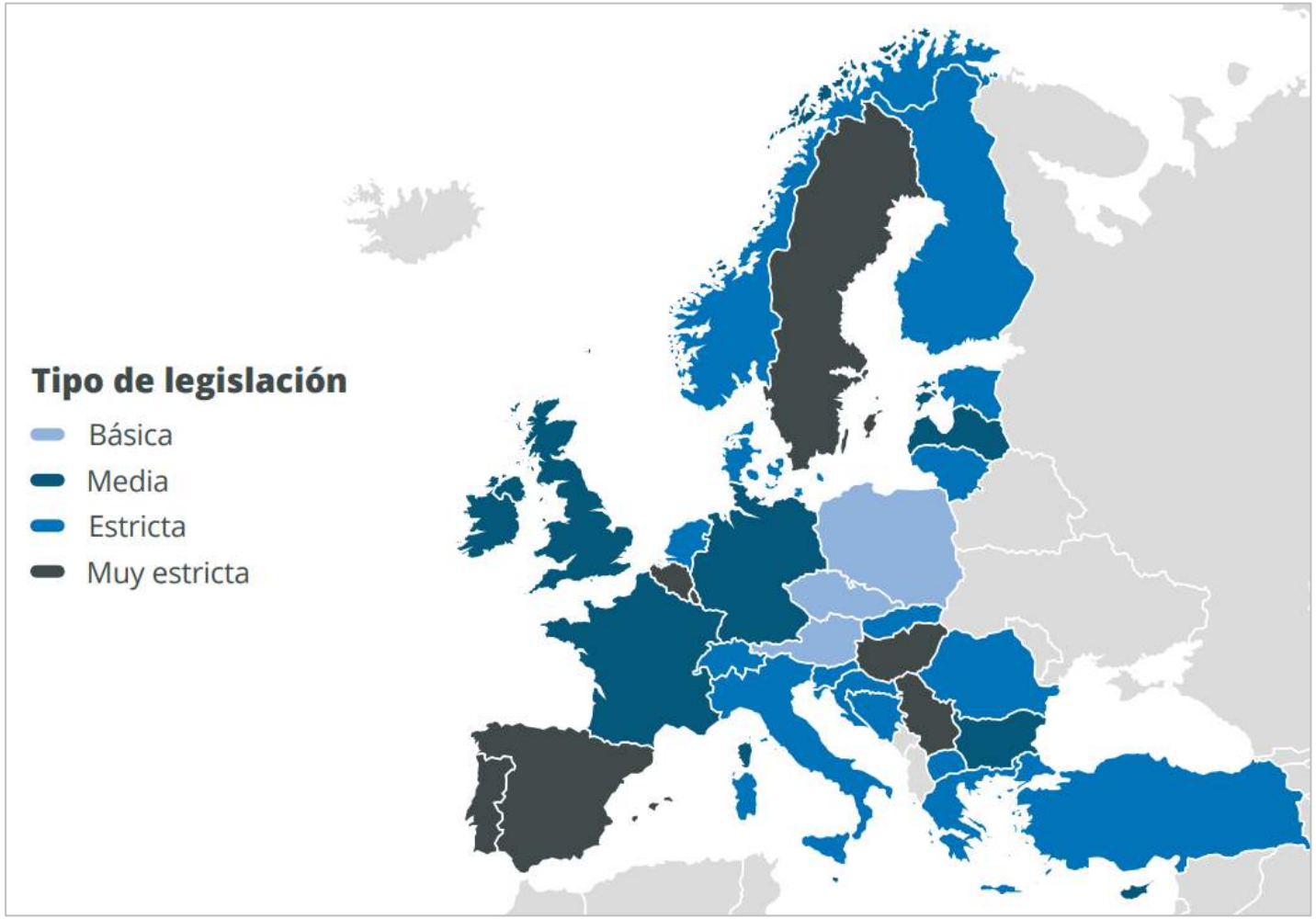
Puesta a disposición judicial

Solicitud pericial facial (identificación facial)

En el 70% de los casos imposibilidad de estudio por mala calidad de la imagen

La importancia del diseño en la investigación y resolución del delito

Legislación, marco normativo



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

- Orden INT/316/2011, de 1 de Febrero - En lo que respecta a **instalaciones y medidas de seguridad**, se concreta:
  - **Quienes 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.**

https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgseguridadciudadana_ucseguridadprivada.php

Orden INT/316/2011, de 1 de Febrero y comentario sobre empresas instaladoras no autorizadas

- En lo que respecta a **instalaciones y medidas de seguridad**, se concreta:
  - **Quienes 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.**

- Tipo C: Instalaciones de sistemas audiovisuales.

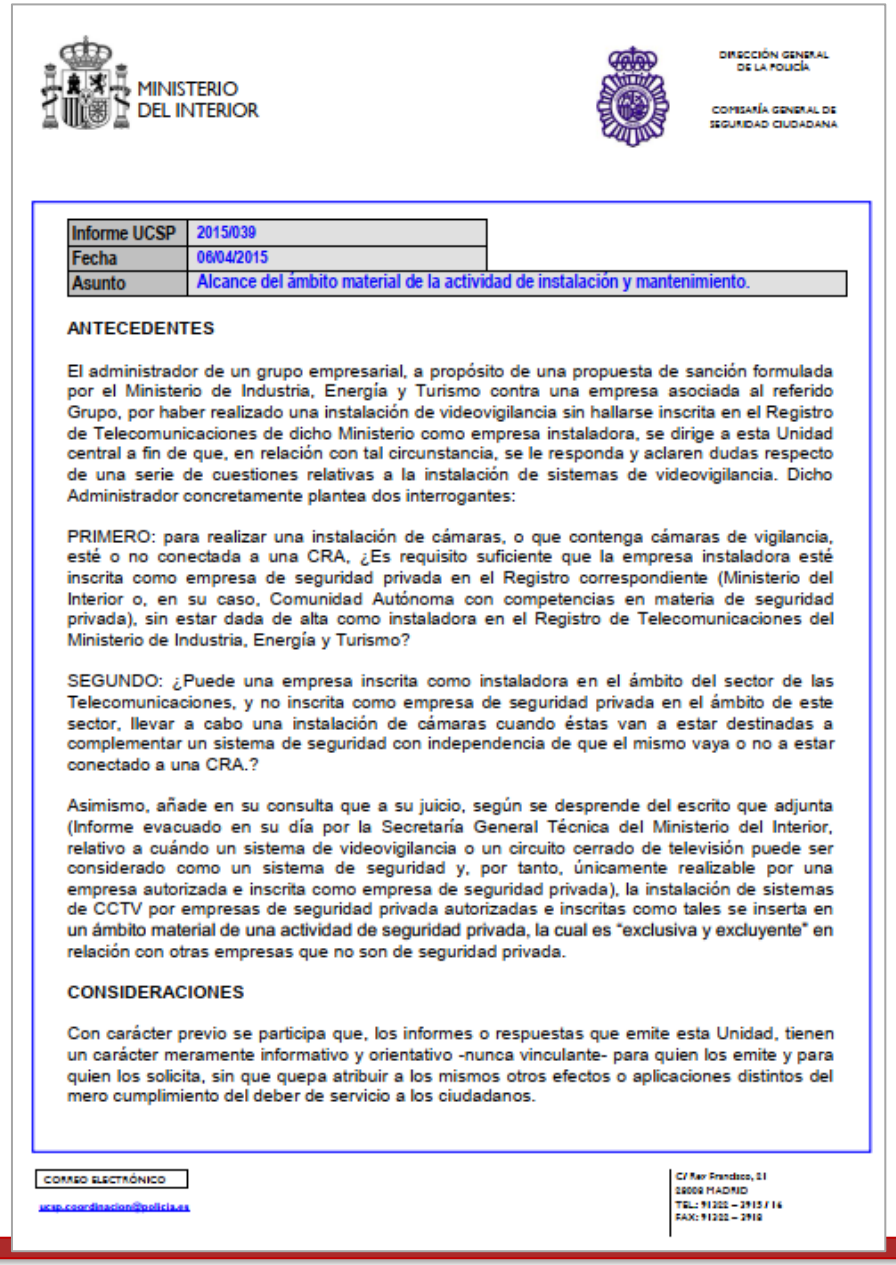
  Definición: Instalaciones públicas o privadas, incluida su puesta a punto y mantenimiento, de sistemas de videovigilancia excluida la prestación del servicio de conexión a centrales de alarmas, sistemas de circuito cerrado de televisión, megafonía, microfonía, sonorización, y montaje de estudios de producción audiovisual.

- 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 vídeoportería 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.

https://avancedigital.mineco.gob.es/RegistroInstaladores/Paginas/instalaciones.aspx

Comentario acerca de la obligatoriedad de las autorizaciones necesarias



MINISTERIO DEL INTERIOR

DIRECCIÓN GENERAL DE LA POLICÍA

COMISARÍA GENERAL DE SEGURIDAD CIUDADANA

Informe UCSP	2015/039
Fecha	06/04/2015
Asunto	Alcance del ámbito material de la actividad de instalación y mantenimiento.

ANTECEDENTES

El administrador de un grupo empresarial, a propósito de una propuesta de sanción formulada por el Ministerio de Industria, Energía y Turismo contra una empresa asociada al referido Grupo, por haber realizado una instalación de videovigilancia sin hallarse inscrita en el Registro de Telecomunicaciones de dicho Ministerio como empresa instaladora, se dirige a esta Unidad central a fin de que, en relación con tal circunstancia, se le responda y aclaren dudas respecto de una serie de cuestiones relativas a la instalación de sistemas de videovigilancia. Dicho Administrador concretamente plantea dos interrogantes:

PRIMERO: para realizar una instalación de cámaras, o que contenga cámaras de vigilancia, esté o no conectada a una CRA, ¿Es requisito suficiente que la empresa instaladora esté inscrita como empresa de seguridad privada en el Registro correspondiente (Ministerio del Interior o, en su caso, Comunidad Autónoma con competencias en materia de seguridad privada), sin estar dada de alta como instaladora en el Registro de Telecomunicaciones del Ministerio de Industria, Energía y Turismo?

SEGUNDO: ¿Puede una empresa inscrita como instaladora en el ámbito del sector de las Telecomunicaciones, y no inscrita como empresa de seguridad privada en el ámbito de este sector, llevar a cabo una instalación de cámaras cuando éstas van a estar destinadas a complementar un sistema de seguridad con independencia de que el mismo vaya o no a estar conectado a una CRA.?

Asimismo, añade en su consulta que a su juicio, según se desprende del escrito que adjunta (Informe evacuado en su día por la Secretaría General Técnica del Ministerio del Interior, relativo a cuándo un sistema de videovigilancia o un circuito cerrado de televisión puede ser considerado como un sistema de seguridad y, por tanto, únicamente realizable por una empresa autorizada e inscrita como empresa de seguridad privada), la instalación de sistemas de CCTV por empresas de seguridad privada autorizadas e inscritas como tales se inserta en un ámbito material de una actividad de seguridad privada, la cual es "exclusiva y excluyente" en relación con otras empresas que no son de seguridad privada.

CONSIDERACIONES

Con carácter previo se participa que, los informes o respuestas que emite esta Unidad, tienen un carácter meramente informativo y orientativo -nunca vinculante- para quien los emite y para quien los solicita, sin que quepa atribuir a los mismos otros efectos o aplicaciones distintos del mero cumplimiento del deber de servicio a los ciudadanos.

CORREO ELECTRÓNICO

ucsp.coordinacion@policia.es

C/ Rey Francisco, 21
28008 MADRID
TEL.: 91322 – 2915 / 16
FAX: 91322 – 2910

El administrador de un grupo empresarial, a propósito de una propuesta de sanción formulada por el Ministerio de Industria, Energía y Turismo contra una empresa asociada al referido Grupo, por haber realizado una instalación de videovigilancia sin hallarse inscrita en el Registro de Telecomunicaciones de dicho Ministerio como empresa instaladora, se dirige a esta Unidad central a fin de que, en relación con tal circunstancia, se le responda y aclaren dudas respecto de una serie de cuestiones relativas a la instalación de sistemas de videovigilancia. Dicho Administrador concretamente plantea dos interrogantes:

De lo dispuesto en las legislaciones de referencia, se infiere claramente que para el ejercicio de la actividad de instalación y mantenimiento de sistemas de telecomunicación (las cámaras de videovigilancia y los circuitos cerrados de televisión forman parte de ella), es obligatoria la inscripción de la empresa interesada en el Registro de Empresas Instaladoras de Telecomunicación (como empresa instaladora en el ámbito del sector de las telecomunicaciones, sin conexión a centrales de alarmas) y que cuando se vayan a conectar tales sistemas (de videovigilancia CCTV) para uso en aplicaciones de seguridad a centrales de alarmas, centros de control o de videovigilancia por la misma, entonces habrá de hallarse obligatoriamente inscrita, además, en el Registro Nacional de Seguridad Privada o autonómico que corresponda (como empresa autorizada en el ámbito del sector de la seguridad privada) y solo en tal caso se podrá llevar a cabo la instalación y mantenimiento de tales sistemas para uso en aplicaciones de seguridad privada.

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

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

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

TECNOLOGÍA PARA TU EMPRESA.ES

La Ciberseguridad en el Data Center es de suma importancia

https://tecnologiaparatuempresa.ituser.es/seguridad/2023/04/la-ciberseguridad-en-el-datacenter-es-de-suma-importancia

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

Medidas de seguridad y encriptación segura de transmisión

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

Chip TPM
Encriptación de secuencias de vídeo

NIS2 DIRECTIVE COMPLIANT

Cumplimiento de NDAA

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

https://blink.ucsd.edu/technology/security/ndaa/index.html

Documentación de los equipos

Garantía de que se cumplen los requisitos de Ciberseguridad

CÁMARAS IP
SERIE 35

Cámaras con tecnología inteligente avanzada para proteger sus instalaciones

Haga que sus instalaciones sean inteligentes y seguras con las cámaras de la Serie 35 de Honeywell, perfectas para pequeñas y medianas empresas. Estas cámaras están disponibles en una amplia gama de formatos y resoluciones y ofrecen análisis inteligente integrado, una claridad de imagen excepcional, integración flexible del sistema, transmisión segura de datos y fácil instalación.

CALIDAD DE IMAGEN HD SUPERIOR, HASTA 8 MP

- Disponible en resoluciones desde 2 MP (2592x1944) hasta 8 MP (3840x2160)
- True WDR (120 dB) garantiza imágenes sin reflejos
- La función Día/Noche Real proporciona imágenes en colores vivos durante el día e imágenes nítidas en blanco y negro durante la noche mediante un filtro de corte IR extraíble
- Excelente rendimiento con luz baja con reducción de ruido 2D/3D, ahorro de almacenamiento y ancho de banda gracias al Smart Codec(1)
- No incluyen contenido ni material de ninguna empresa o sus subsidiarias prohibidos por la Sección 889 de la Ley de Autorización de Defensa Nacional (NDAA, por sus siglas en inglés) de EE. UU. y puede utilizarse como parte de sistemas de vídeo que cumplan con los requisitos establecidos por la sección 889 de la NDAA

SOLUCIÓN FLEXIBLE DE VIGILANCIA

- Una amplia gama de formatos, lentes y opciones de zoom para todo tipo de instalaciones, incluidos micro domo, mini domo, mini domo eyeball, bullet y domo PTZ
- H.265 (2), H.264, Smart Codec(1) y MJPEG compatibles con transmisión triple
- La tecnología Smart IR proporciona una distribución uniforme de los LED IR en escenas nocturnas o con poca luz
- A prueba de agua/polvo (IP66/IP67) e IK10 (depende del modelo)
- Compatibilidad con ONVIF Perfil S, G, T
- Cifrado de transmisión: cámara a MAXPRO y NVR Serie 35 bajo AES/256 que asegura la privacidad de datos
- Recuento de personas, detección de intrusión, merodeo y detección de movimiento inteligente para aumentar el conocimiento de la situación y reducir las falsas alarmas

FÁCIL DE INSTALAR Y UTILIZAR

- La alimentación integrada a través de Ethernet (Power over Ethernet, PoE) elimina la necesidad de una fuente de alimentación independiente y el cableado correspondiente
- Entradas de 12VCC cuando no se dispone de PoE
- Configuración remota, ajustes de zoom motorizados y enfoque automático mediante cliente web o desde el NVR
- Múltiples opciones de montaje para una amplia gama de aplicaciones de seguridad
- Múltiples idiomas GUI(3) (14 países)

(1) Cubierta por una o más reivindicaciones de las patentes enumeradas en patentlist.honeywell.com
(2) Smart Codec ahorra hasta un 50% en uso de banda y almacenamiento en comparación con H.264/H.265 estándar según la external
(3) Se pueden cambiar compuestos en árabe, checo, holandés, inglés, francés, alemán, italiano, japonés, coreano, polaco, portugués(Brasil), ruso, español y turco

APLICACIONES DE MERCADO

Estas cámaras versátiles y con un amplio número de características están diseñadas para ayudar a proteger sus instalaciones, evitar robos en tiendas, fraudes, vandalismo y otras posibles amenazas a la seguridad. Son perfectas para comercio minorista interior y exterior, oficinas, pequeñas y medianas empresas, salas de juegos y más.

ALMACENAMIENTO DE VÍDEO INTEGRADO

- Admite tarjetas microSD (Clase 10) de hasta 256 GB para el almacenamiento local de vídeo (tarjeta no incluida).

DETECCIÓN DE MOVIMIENTO INTELIGENTE

- La detección de movimiento inteligente, en comparación con la detección de movimiento tradicional que solo detecta cambios de píxeles y generalmente presenta una mayor tasa de falsas alarmas, está diseñada para generar una alarma cuando el algoritmo de IA (inteligencia artificial) reconoce el objeto como una persona o un vehículo.

Honeywell

Honeywell

HONEYWELL COMERCIAL SECURITY
715 Peachstreet St. NE
Atlanta, GA. 30308
www.honeywell.com

June 24, 2022

NATIONAL DEFENSE AUTHORIZATION ACT 2019 (SECTION 889)

The John S. McCain National Defense Authorization Act 2019 (NDAA) is a United States federal law which specifies the budget, expenditures and policies of the U.S. Department of Defense. Within NDAA 2019, Section 889a, prohibits the U.S. government from procuring video and telecommunication equipment from certain Chinese companies and their subsidiaries. Section 889b prohibits the U.S. Government from conducting business with or extending with organizations that use video and telecommunication equipment from these certain Chinese companies, regardless of the size of the contract or grant.

The Honeywell 30 Series, 35 Series, 60 Series and 70 Series cameras are designed for use as part of video systems which comply with NDAA 2019, Section 889. In addition to the 30/35/60/70 Series cameras, our MAXPRO® and Pro-Watch® VMS/NVR ranges, our 30/35 Series Embedded NVRs and our ADPRO iFT/iFT-E IP NVRs follow our extensive cyber testing process and do not contain components from any of the companies highlighted in NDAA 2019, Section 889. Together with the Series 30/35/60/70 cameras they can be used to provide video systems compliant with NDAA 2019, Section 889. These ranges are well suited for SMB, entry-level enterprise and critical applications where compliance is essential, such as government, utilities, premium commercial, campuses and retail.

NDAA 2019 Section 889 is focused on video surveillance and telecommunications equipment. It does not impact other areas of security. Honeywell access control solutions are cyber tested, do not contain components from banned suppliers, and are not addressed by NDAA 2019 Section 889. Honeywell Pro-Watch, WINPAK and other access software and hardware can continue to be sold to and used by federal agencies or other businesses wishing to implement security solutions compliant with NDAA 2019 Section 889.

Specific Honeywell products that can be used as part of NDAA Section 889 compliant systems are:
- 30 Series IP Cameras
- 35 Series IP Cameras
- 60 Series IP Cameras
- 30 Series Embedded NVRs
- 35 Series Embedded NVRs
- MAXPRO® and Pro-Watch® VMS & NVRs
- ADPRO iFT/iFT-E IP NVRs
- Pro-Watch® Integrated Security and Access control
- WINPAK® Access Control

Yours sincerely,

OFFICE OF THE BIOMETRICS AND SURVEILLANCE CAMERA COMMISSIONER

SECURE BY DEFAULT

Secure by Default Self-Certification

THIS IS TO CERTIFY THAT

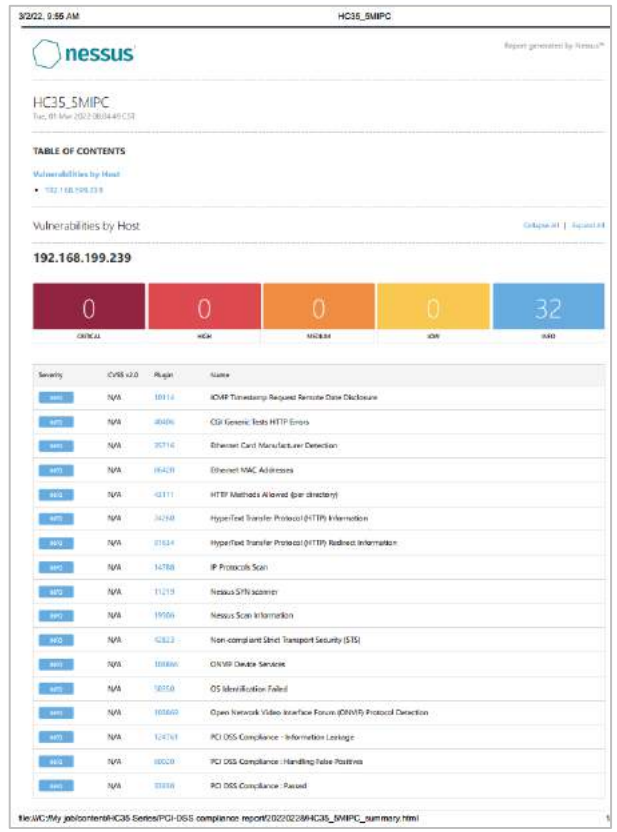
Honeywell

Has self-certified that their product(s) listed below are Secure by Default.

Series 35

25th March 2022
DATE OF ISSUE

Fraser Sampson
BIOMETRICS AND SURVEILLANCE CAMERA COMMISSIONER



3/2/22, 9:55 AM HC35_5MIPC

nessus

HC35_5MIPC

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.199.239

0	0	0	0	32
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	Plugin	Name
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	46180	CGI Generic Tests HTTP Errors
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	91634	HyperText Transfer Protocol (HTTP) Redirect Information
INFO	N/A	14788	IP Protocols Scan
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	42823	Non-compliant Strict Transport Security (STS)
INFO	N/A	168980	ONVIF Device Services
INFO	N/A	50350	OS Identification Failed
INFO	N/A	168982	Open Network Video Interface Forum (ONVIF) Protocol Detection
INFO	N/A	117651	PCI DSS Compliance : Information Leakage
INFO	N/A	66029	PCI DSS Compliance : Handling False Positives
INFO	N/A	33814	PCI DSS Compliance : Passed

file:///C:/My jobs/content/HC35 Series/PCI-DSS compliance report/20220228/HC35_5MIPC_summary.html 1

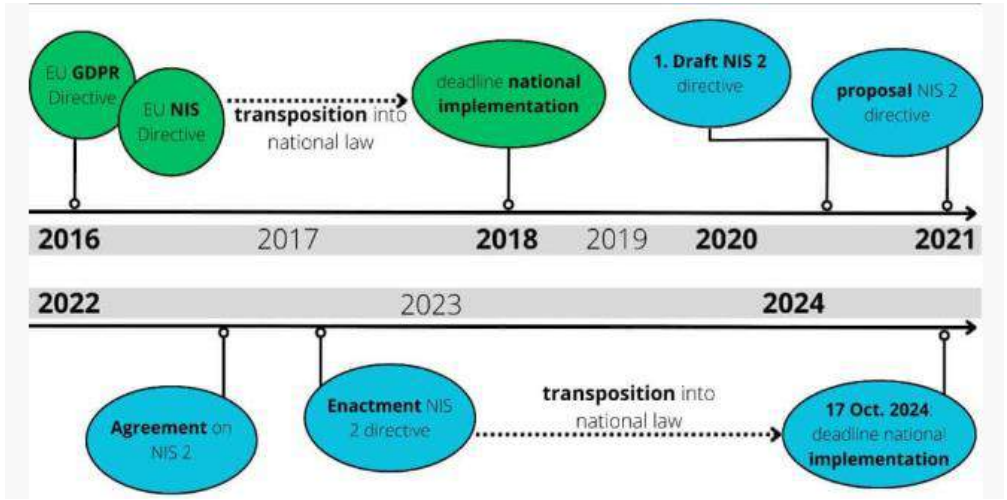
Directiva NIS2, relativa a medidas de Ciberseguridad

Concebida para proteger las infraestructuras esenciales frente a todo tipo de amenazas cibernéticas en Europa.

La **Directiva (UE) 2022/2555, conocida como NIS2**, relativa a las medidas destinadas a **garantizar un elevado nivel común de Ciberseguridad en toda la Unión Europea**, establece una serie de obligaciones de para los Estados miembros, así como medidas para la gestión de riesgos de Ciberseguridad y obligaciones de notificación para las entidades en su ámbito de aplicación.

Para el 17 de Octubre de 2024, todos los países miembros de la UE deben adoptar y publicar las medidas necesarias para cumplirla.

Una de las novedades más importantes introducidas por la Directiva es el amplio espectro de sectores mercantiles involucrados, distinguiéndose entre **Entidades Esenciales y Entidades Importantes.**



Directiva NIS2, sectores involucrados

Entidades Esenciales:

- Energía
- Sanidad
- Transporte
- Banca
- Mercados Financieros
- Gestión del agua potable
- Aguas residuales
- Infraestructuras digitales
- Gestión de servicios TIC
- Administración Pública
- Espacio

Entidades Importantes:

- Servicios postales
- Servicios de mensajería
- Gestión de residuos
- Productos químicos
- Alimentación
- Fabricación
- Proveedores digitales
- Investigación

Directiva NIS2, requerimientos

https://www.boe.es/doue/2022/333/L00080-00152.pdf

1. Notificación de incidentes cibernéticos.
2. Mantenimiento de las medidas de seguridad adecuadas.
3. Identificación y evaluación de riesgos.
4. Seguridad de los productos y servicios.
5. Cooperación con las autoridades supervisoras.
6. Planificación de emergencias y respuesta a incidentes.
7. Sanciones en caso de infracción.
8. Cooperación entre Estados miembros.

Directiva (EU) 2022/2555, algunos ejemplos de Entidades

4. Producción, transformación y distribución de alimentos		Empresas alimentarias, tal como se definen en el artículo 3, punto 2, del Reglamento (CE) n.º 178/2002 del Parlamento Europeo y del Consejo ([3]), que se dediquen a la distribución al por mayor y a la producción y transformación industriales

2) «Empresa alimentaria», toda empresa pública o privada que, con o sin ánimo de lucro, lleve a cabo cualquier actividad relacionada con cualquiera de las etapas de la producción, la transformación y la distribución de alimentos.

3. Banca		Entidades de crédito, tal como se definen en el artículo 4, punto 1, del Reglamento (UE) n.º 575/2013 del Parlamento Europeo y del Consejo ([15])

HAN ADOPTADO EL PRESENTE REGLAMENTO:

PARTE PRIMERA

DISPOSICIONES GENERALES

TÍTULO I

OBJETO, ÁMBITO DE APLICACIÓN Y DEFINICIONES

Artículo 1

Ámbito de aplicación

El presente Reglamento establece normas uniformes sobre los requisitos prudenciales generales que las entidades supervisadas conforme a la Directiva 2013/36/UE deberán cumplir en relación con lo siguiente:

a) Los requisitos de fondos propios relativos a elementos del riesgo de crédito, del riesgo de mercado, del riesgo operativo y del riesgo de liquidación.

b) Los requisitos destinados a limitar las grandes exposiciones.

c) Una vez haya entrado en vigor el acto delegado a que se refiere el artículo 460, los requisitos de liquidez relativos a elementos del riesgo de liquidez plenamente cuantificables, uniformes y normalizados.

d) Los requisitos de información relativos a las letras a), b) y c), y en materia de apalancamiento.

encima de lo exigido por el presente Reglamento, o apliquen medidas más estrictas que las previstas en el mismo.

Artículo 4

Definiciones

1. A efectos del presente Reglamento se entenderá por:

1) «Entidad de crédito»: una empresa cuya actividad consista en recibir del público depósitos u otros fondos reembolsables y en conceder créditos por cuenta propia.

2) «Empresa de inversión»: una persona tal como se define en el artículo 4, apartado 1, punto 1, de la Directiva 2004/39/CE que está sujeta a lo dispuesto en dicha Directiva, excepto:

a) las entidades de crédito;

b) las empresas locales;

c) las empresas no autorizadas a prestar el servicio auxiliar referido en el punto 1, de la parte B del anexo I de la Directiva 2004/39/CE, que presten únicamente uno o varios de los servicios y actividades de inversión enumerados en los puntos 1, 2, 4 y 5 de la parte A del anexo I de la citada Directiva, y a las que no se permite tener en depósito dinero o valores de sus clientes y que, por esta razón, nunca puedan hallarse en situación deudora respecto de dichos clientes.

Directiva (EU) 2022/2555, algunos ejemplos de Entidades

6. Agua potable		Suministradores y distribuidores de aguas destinadas al consumo humano, tal como se definen en el artículo 2, punto 1, letra a), de la Directiva (UE) 2020/2184 del Parlamento Europeo y del Consejo ([22]), excluidos los distribuidores para los que la distribución de aguas destinadas al consumo humano sea una parte no esencial de su actividad general de distribución de otros bienes y productos básicos

Artículo 2

Definiciones

A efectos de la presente Directiva se entenderá por:

1) «agua destinada al consumo humano»:

a) todas aquellas aguas, ya sea en su estado original, ya sea después del tratamiento, utilizadas para beber, cocinar, preparar alimentos y otros usos domésticos, en locales tanto públicos como privados, sea cual fuere su origen e independientemente de que se suministren a través de una red de distribución, de una cisterna o envasadas en botellas u otros recipientes, incluidas las aguas de manantial;

b) todas las aguas utilizadas en empresas alimentarias para fines de fabricación, tratamiento, conservación o comercialización de productos o sustancias destinados al consumo humano;

5. Sector sanitario		— Prestadores de asistencia sanitaria, tal como se definen en el artículo 3, letra g), de la Directiva 2011/24/UE del Parlamento Europeo y del Consejo ([18])
		— Laboratorios de referencia de la UE, tal como se definen en el artículo 15, del Reglamento (UE) .../...del Parlamento Europeo y del Consejo ([19])
		— Entidades que realizan actividades de investigación y desarrollo de medicamentos, tal como se definen en el artículo 1, punto 2, de la Directiva 2001/83/CE del Parlamento Europeo y del Consejo ([20]) roductos farmacéuticos de base y especialidades farmacéuticas a que se refiere la sección C, división 21, de la roductos sanitarios que se consideran esenciales en situaciones de emergencia de salud pública («lista de pro- les durante la emergencia de salud pública») en el sentido del artículo 22 del Reglamento (UE) 2022/123 del l Consejo ([21])

Artículo 3

Definiciones

A los efectos de la presente Directiva, se entenderá por:

a) «asistencia sanitaria»: los servicios relacionados con la salud prestados por un profesional sanitario a pacientes para evaluar, mantener o restablecer su estado de salud, incluidos la receta, dispensación y provisión de medicamentos y productos sanitarios;

b) «asegurado»:

i) las personas, incluidos los familiares y sus supérstites, contempladas en el artículo 2 del Reglamento (CE) nº 883/2004, que sean aseguradas en la acepción del artículo 1, letra c) de dicho Reglamento, y

f) «profesional sanitario»: todo doctor en medicina, enfermero responsable de cuidados generales, odontólogo, matrona o farmacéutico a tenor de lo dispuesto en la Directiva 2005/36/CE u otro profesional que ejerza actividades en el sector de la asistencia sanitaria que estén restringidas a una profesión regulada según se define en el artículo 3, apartado 1, letra a), de la Directiva 2005/36/CE, o toda persona considerada profesional sanitario conforme a la legislación del Estado miembro de tratamiento;

g) «prestador de asistencia sanitaria»: toda persona física o jurídica que dispense legalmente asistencia sanitaria en el territorio de un Estado miembro;

NIS2 COMPLIANT CYBER SECURITY

SECURE DEVELOPMENT LIFE CYCLE PROCESS

Honeywell has developed a robust system for considering security at the outset of product conception and during development, as well as responding to potential vulnerabilities in existing products. This system, Honeywell's Secure Software Development Lifecycle (SSDLC) initiative, has evolved and grown even more robust over the past few years.

Honeywell takes product security seriously. Our products go through a robust and comprehensive penetration testing regimen. In some cases, additional independent security testing is conducted. The criteria for this additional testing as well as which products or offerings are selected for this are closely held proprietary information.

We have a robust and comprehensive Secure Development Life Cycle (SDLC) based on best practices and industry standards that includes the following:

- Security Risk Assessment based on the threat environment faced by a particular product or offering as well as the technical features and customer needs
- Security Requirements and security controls based on industry standards and guidelines such as BSIMM, ISA/IEC 99/62443, ISO 27001, PCI DSS, GDPR, OWASP, applicable local laws and regulations, and others depending on the product or offering and the Security Risk Assessment
- Privacy Impact Assessments
- Threat Modeling
- Secure by Design, Privacy by Design and Secure Coding standards and practices
- Static Application Security Testing (SAST, also known as source code scanning) to enforce secure design and coding practices. We scan for OWASP Top 10 and SANS Top 25 vulnerabilities as well as for language-specific quality measures. Current SAST tools include SonarQube and Coverity depending on product and language needs.
- Binary scanning to identify open source usage and potential vulnerabilities.
- A formal Risk Management Policy that requires specific mitigation timelines based on severity
- Review and approval of cybersecurity by senior leadership prior to product shipment
- Lifecycle support and customer notification for security updates.

An audit team of Honeywell performs checks to ensure that security deliverables required under Honeywell's Secure Development Life Cycle processes are completed.

Honeywell completes training programs for its employees on the company's security process and on specific cybersecurity concerns and solutions.

All software engineers in Honeywell receive formal training on the Secure Development Life Cycle process and general cyber/product security topics.

NETWORK AND INFORMATION SECURITY DIRECTIVE 2 (NIS2)

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive)

The EU cybersecurity requirements introduced in 2016 by NIS Directive were updated and strengthened by the NIS2 Directive that came into force in 2023. In the light of increased digitalization with growing cyber-attacks and an evolving overall cybersecurity threat landscape, EU has introduced more stringent supervisory measures with incident response capacities and stricter enforcement requirements by expanding them to new sectors and entities.

By 17 October 2024, all EU member countries must adopt and publish the measures necessary to comply with the NIS2 Directive and they shall apply those measures from 18 October 2024.

Honeywell

PRO-WATCH® ECOSYSTEM

INTEGRATED SECURITY PLATFORM

- Highest security thanks to cryptographic coprocessor
- TLS 1.2 encryption
- Point to point encryption with OSDPv2
- Dual authentication and Biometrics
- Audit and compliance reporting
- Transparent mode access control
- Traceability of IT assets

MB-SECURE PRO ECOSYSTEM

INTEGRATED INTRUSION AND ACCESS CONTROL

- Highest security thanks to cryptographic coprocessor
- AES 128-bit encryption
- Encrypted Ethernet connection
- TLS 1.2 encryption and 2-fold authentication
- IT room security with dual authentication

MAXPRO® CLOUD ECOSYSTEM

INTEGRATED VIDEO, INTRUSION AND ACCESS CONTROL

- Software as a Service (SaaS) managed by Azure
- All data encrypted with TLS1.2 AES256 bit between host and server
- 2-factor authentication
- Point to point encryption with OSDP V2
- Audit and compliance recording
- Dual authentication for data rooms (card + pin)

VIDEO SURVEILLANCE

35, 60 AND 70 SERIES IP CAMERAS
35 SERIES AND MAXPRO NVRS

- Highest security thanks to cryptographic coprocessor
- Built-in FIPS/TPM certificated encryption chipsets
- All encrypted communications (HTTPS) with Web and Mobile Clients
- Point to point encryption of the video stream for perimeter protection

Obligatoriedad de la elaboración de un proyecto para cualquier tipo de instalación











https://share.vidyard.com/watch/NBM1Y1FLTP4t7cxqArnSyG

Normas UNE-EN 62676 para utilización en sistemas de videovigilancia en aplicaciones de seguridad

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
			Parte 4: Compatibilidad electromagnética Norma de famili temas de detección de incendios, intrusión y alarma social.
			Parte 4: Compatibilidad electromagnética. Norma de famil temas de detección de incendios, intrusión y alarma social.
			Parte 4: Compatibilidad electromagnética. Norma de famil temas de detección de incendios, intrusión y alarma social.
			Parte 5: Métodos de ensayo ambiental.
			Sistemas de alarma contra intrusión y atraco. Parte 1: Rec
			Sistemas de alarma contra intrusión y atraco. Parte 1: Rec
			Sistemas de alarma de intrusión y atraco. Parte 2-2: Detec
			Sistemas de alarma de intrusión y atraco. Parte 2-3: Requ
			Sistemas de alarma de intrusión y atraco. Parte 2-4: Requ
			Sistemas de alarma de intrusión y atraco. Parte 2-5: Requ
			Sistemas de alarma de intrusión y atraco. Parte 2-6: Cont
			Sistemas de alarma de intrusión y atraco. Parte 3: Equipo
			Sistemas de alarma de intrusión y atraco. Parte 4: Disposi
UNE-EN.	50131-5-3.	2005	Sistemas de alarma. Sistemas de alarma de intrusión. Parte 5-3: Requisitos pa radiofrecuencia.
UNE-EN.	50131-5-3.	2005/A1:2008	Sistemas de alarma. Sistemas de alarma de intrusión. Parte 5-3: Requisitos pa radiofrecuencia.
UNE-EN.	50131-6.	1999	Sistemas de alarma. Sistemas de alarma de intrusión. Parte 6: Fuentes de alim
UNE-EN.	50131-6.	2008	Sistemas de alarma. Sistemas de alarma de intrusión y atraco. Parte 6: Fuente
UNE-EN.	50131-8.	2009	Sistemas de alarma. Sistemas de alarma de intrusión y atraco. Parte 8: Sistem
UNE-CLC/TS.	50131-2-2.	2005 V2	Sistemas de alarma. Sistemas de alarma de intrusión. Parte 2-2: Requisitos pa
UNE-CLC/TS.	50131-2-3.	2005 V2	Sistemas de alarma. Sistemas de alarma de intrusión. Parte 2-3: Requisitos pa
UNE-CLC/TS.	50131-2-4.	2005 V2	Sistemas de alarma. Sistemas de alarma de intrusión. Parte 2-4: Requisitos pa microondas.
UNE-CLC/TS.	50131-2-5.	2005 V2	Sistemas de alarma. Sistemas de alarma de intrusión. Parte 2-5: Requisitos pa ultrasónicos.
UNE-CLC/TS.	50131-2-6.	2005 V2	Sistemas de alarma. Sistemas de alarma de intrusión. Parte 2-6: Requisitos pa
UNE-CLC/TS.	50131-3.	2005 V2	Sistemas de alarma. Sistemas de alarma de intrusión. Parte 3: Equipo de contr
UNE-CLC/TS.	50131-7.	2005 V2	Sistemas de alarma. Sistemas de alarma de intrusión. Parte 7. Guía de aplicac
UNE-EN.	50132-1.	2010	Sistemas de alarma. Sistemas de vigilancia CCTV para uso en aplicaciones de
UNE-EN.	50132-2-1.	1998	Sistemas de alarma. Sistemas de vigilancia CCTV para uso en aplicaciones de
UNE-EN.	50132-4-1.	2002	Sistemas de alarma. Sistemas de vigilancia CCTV para uso en aplicaciones de
UNE-EN.	50132-5.	2002	Sistemas de alarma. Sistemas de vigilancia CCTV para uso en aplicaciones de
UNE-EN.	50132-7 CORR.	2004	Sistemas de alarma - Sistemas de vigilancia CCTV para uso en aplicaciones de
UNE-EN.	50132-7.	1997	Sistemas de alarma. Sistemas de vigilancia CCTV para uso en aplicaciones de
UNE-EN.	50133-1 CORR.	1998	Sistemas de alarma. Sistemas de control de accesos de uso en las aplicaciones
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.

UNE-EN IEC 62676-2-33:2022	UNE	Sistemas de videovigilancia para utilización en aplicaciones de seguridad. Parte 2-33: Enlace...	01/10/2022	Vigente
UNE-EN IEC 62676-5:2018	UNE	Sistemas de videovigilancia para utilización en aplicaciones de seguridad. Parte 5: Especificaciones d...	01/09/2018	Vigente
UNE-EN 62676-1-1:2015	UNE	Sistemas de videovigilancia para utilización en aplicaciones de seguridad. Parte 1-1: Requisitos del...	29/07/2015	Vigente
UNE-EN 62676-3:2015	UNE	Sistemas de videovigilancia para utilización en aplicaciones de seguridad. Parte 3: Interfaces...	01/03/2015	Vigente
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 IEC 62676-2-31:2019	UNE	Sistemas de videovigilancia para utilización en aplicaciones de seguridad. Parte 2-31: Transmisión y...	01/10/2019	Vigente
UNE-EN 62676-2-2:2014	UNE	Sistemas de videovigilancia para utilización en aplicaciones de seguridad. Parte 2-2: Protocolos de...	01/03/2014	Vigente
UNE-EN IEC 62676-2-32:2019	UNE	Sistemas de videovigilancia para utilización en aplicaciones de seguridad. Parte 2-32: Control de...	01/10/2019	Vigente
UNE-EN 62676-1-2:2014	UNE	Sistemas de videovigilancia para utilización en aplicaciones de seguridad. Parte 1-2: Transmisión de...	01/04/2014	Vigente
UNE-EN 62676-3:2015/AC:2018-08	UNE	Sistemas de videovigilancia para utilización en aplicaciones de seguridad. Parte 3: Interfaces...	01/10/2018	Vigente
UNE-EN 62676-1-2:2014/AC:2015	UNE	Sistemas de videovigilancia para utilización en aplicaciones de seguridad. Parte 1-2: Transmisión de...	01/06/2015	Vigente
UNE-EN 62676-2-1:2014	UNE	Sistemas de videovigilancia para utilización en aplicaciones de seguridad. Parte 2-1: Protocolos de...	01/03/2014	Vigente

UNE –EN 62676-1-1. Descripción funcional del VSS

- 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.

BLOQUES FUNCIONALES QUE DESCRIBEN LAS DISTINTAS PARTES Y FUNCIONES

- No existen certificados de producto ya que los procesos de certificación necesitan unos plazos superiores a la evolución tecnológica. Lo que sí es importante es seguir los pasos para la elaboración del proyecto (UNE – EN 62676-4:2015)

UNE –EN 62676-1-1. Grados de seguridad

- 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.

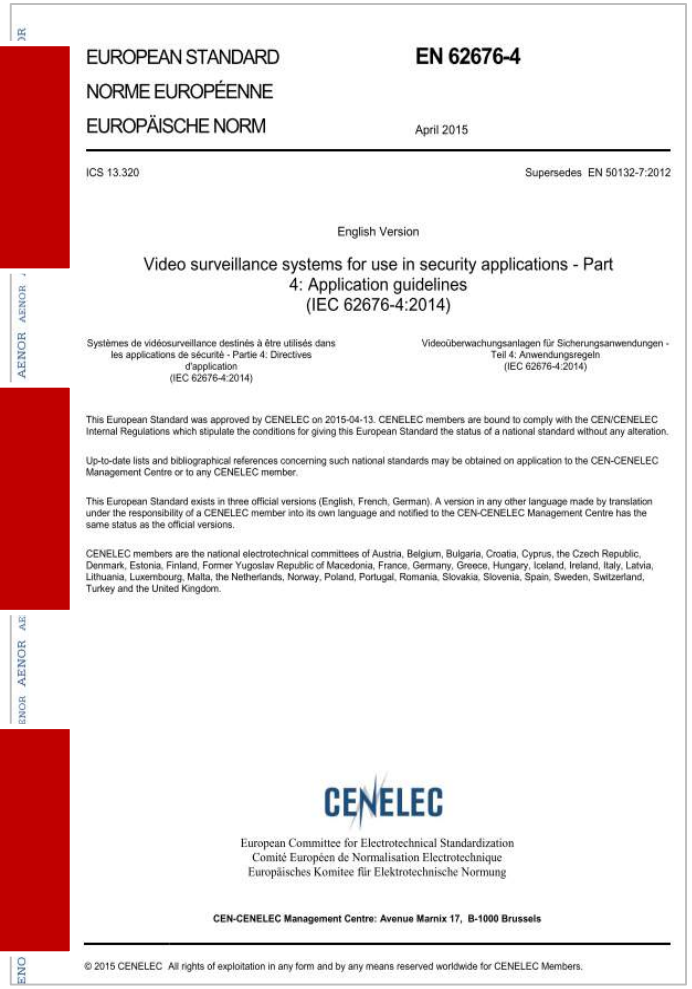
	Baja probabilidad - Consecuencias importantes	**Alta probabilidad - Consecuencias improtantes**
Grados 2-3	Lugares en los que la probabilidad de que se produzca un incidente no deseado es baja pero las consecuencias potenciales son de gran importancia	Lugares en los que la probabilidad de que se produzca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

UNE – EN 62676-4:2015. Directrices de aplicación, referencia para el diseño de sistemas

- Evaluación de riesgo y grado de seguridad
- Documento “requisitos del sistema del CCTV y sus componentes”
- Instalación y puesta en marcha



EUROPEAN STANDARD **EN 62676-4**

NORME EUROPÉENNE

EUROPÄISCHE NORM April 2015

ICS 13.320 Supersedes EN 50132-7:2012

English Version

Video surveillance systems for use in security applications - Part 4: Application guidelines
(IEC 62676-4:2014)

Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité - Partie 4: Directives d'application
(IEC 62676-4:2014)

Videoüberwachungsanlagen für Sicherungsanwendungen - Teil 4: Anwendungsregeln
(IEC 62676-4:2014)

This European Standard was approved by CENELEC on 2015-04-13. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

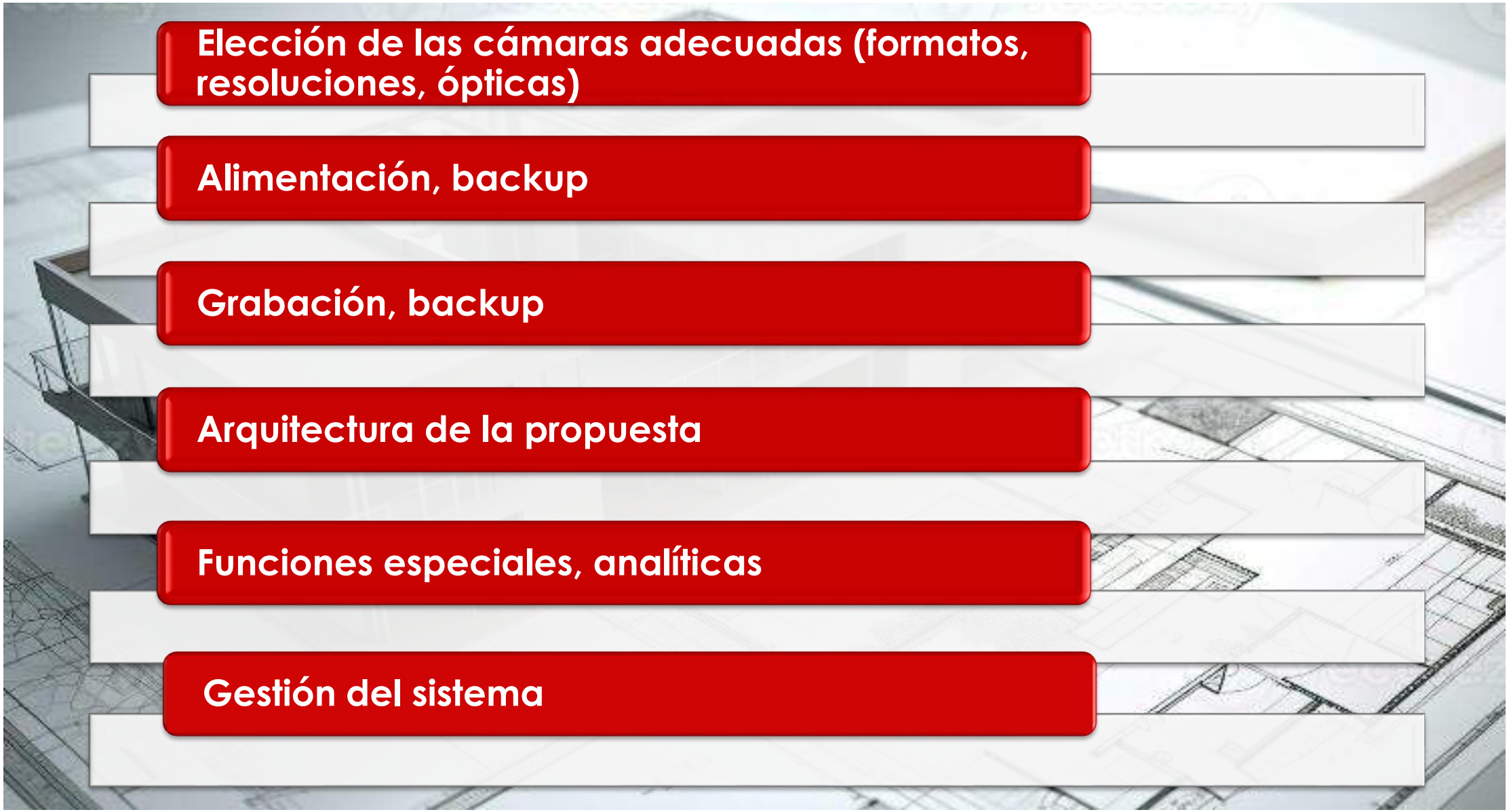
This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

CENELEC

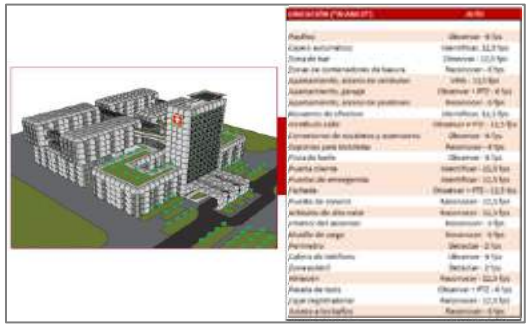
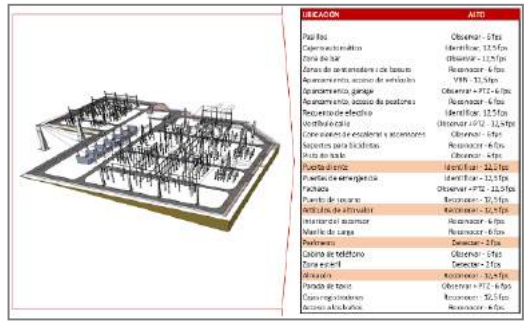
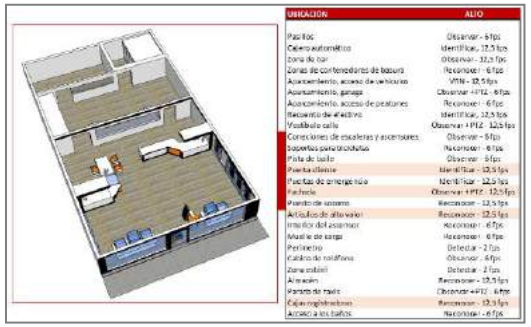
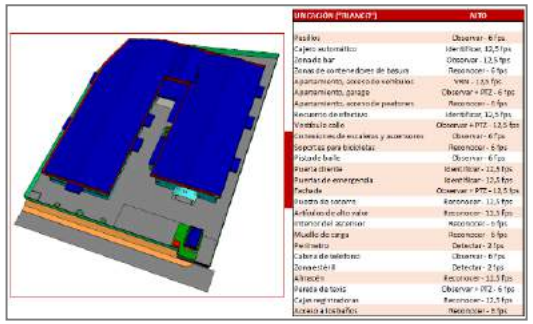
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels


Elección de las cámaras adecuadas (formatos, resoluciones, ópticas)
Alimentación, backup
Grabación, backup
Arquitectura de la propuesta
Funciones especiales, analíticas
Gestión del sistema

Inicio del proyecto, propósito de cada una de las cámaras (UNE – EN 62676-4:2015)

UBICACIÓN "BLANCO"	PROPÓSITO DE LA CÁMARA
Pasillos	Observar
Cajero automático	Identificar
Zona de bar	Observar
Zonas de contenedores de basura	Reconocer
Aparcamiento, acceso de vehículos	Ver - grabar la matrícula
Aparcamiento, garage	Observar + opción cámara móvil
Aparcamiento, acceso de peatones	Reconocer
Recuento de efectivo	Identificar
Vestíbulo calle	Observar + opción cámara móvil
Conexiones de escaleras y ascensores	Observar
Soportes para bicicletas	Reconocer
Pista de baile	Observar
Puerta cliente	Identificar
Puertas de emergencia	Identificar
Fachada	Observar + opción cámara móvil
Puesto de socorro	Reconocer
Artículos de alto valor	Reconocer
Interior del ascensor	Reconocer
Muelle de carga	Reconocer
Perímetro	Detectar
Cabina de teléfono	Observar
Zona estéril	Detectar
Almacén	Reconocer
Parada de taxis	Observar + opción cámara móvil
Cajas registradoras	Reconocer
Acceso a los baños	Reconocer

Propósito de cada una de las cámaras

- **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.

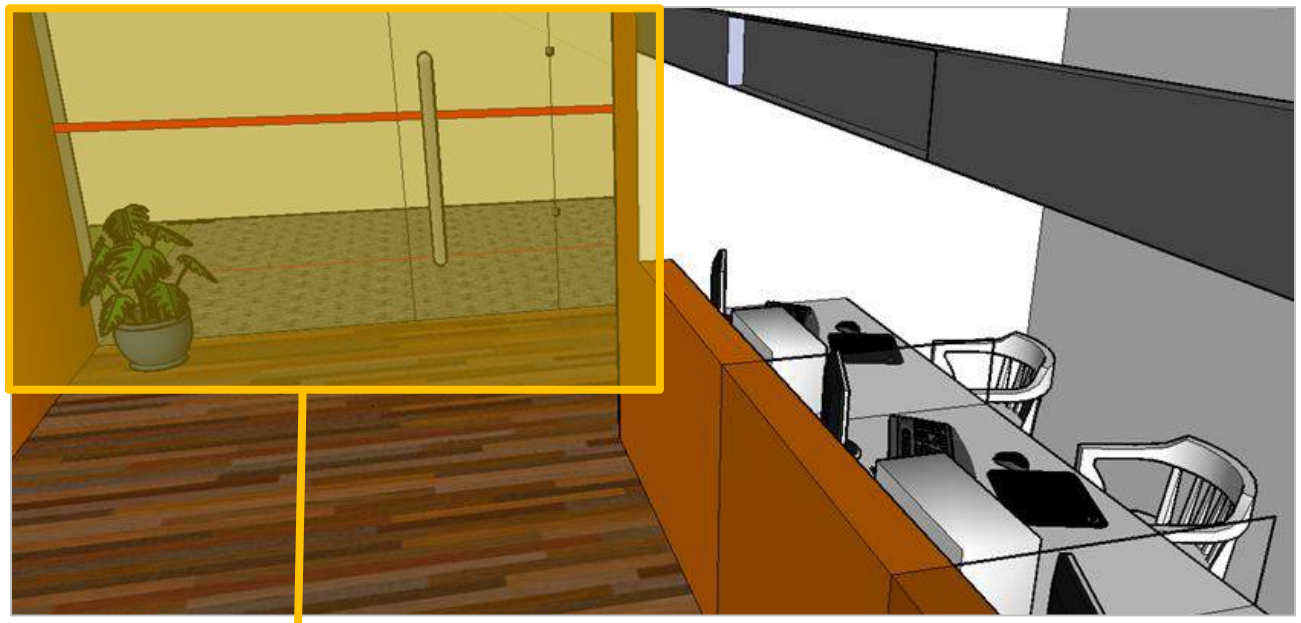
¿Ver una escena y saber que está ocurriendo algo?
OBSERVAR
63ppm

¿Ver un suceso y determinar exactamente que está ocurriendo?
RECONOCER
125ppm

¿Identificar exactamente a la persona implicada?
IDENTIFICAR
250ppm

Píxeles por metro – Nivel de detalle en función a la distancia

Ejemplo cámara controlando “puerta cliente” – 250 ppm



CÁMARA A “N” METROS DE DISTANCIA Y A “N” METROS DE ALTURA DEL “BLANCO”

Vestíbulo 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

HERRAMIENTA DE DISEÑO

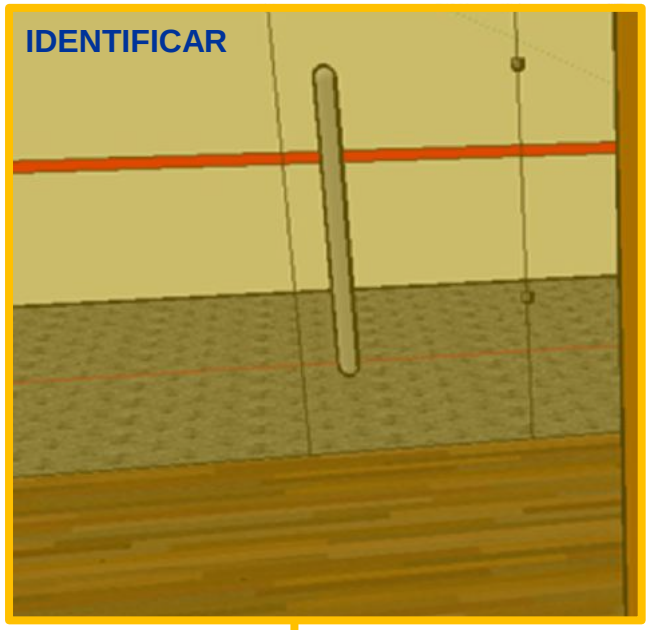
25 PPM: DETECTAR
Puede distinguir información tal como formas, color, tamaño o género, pero no puede distinguir caras o letras

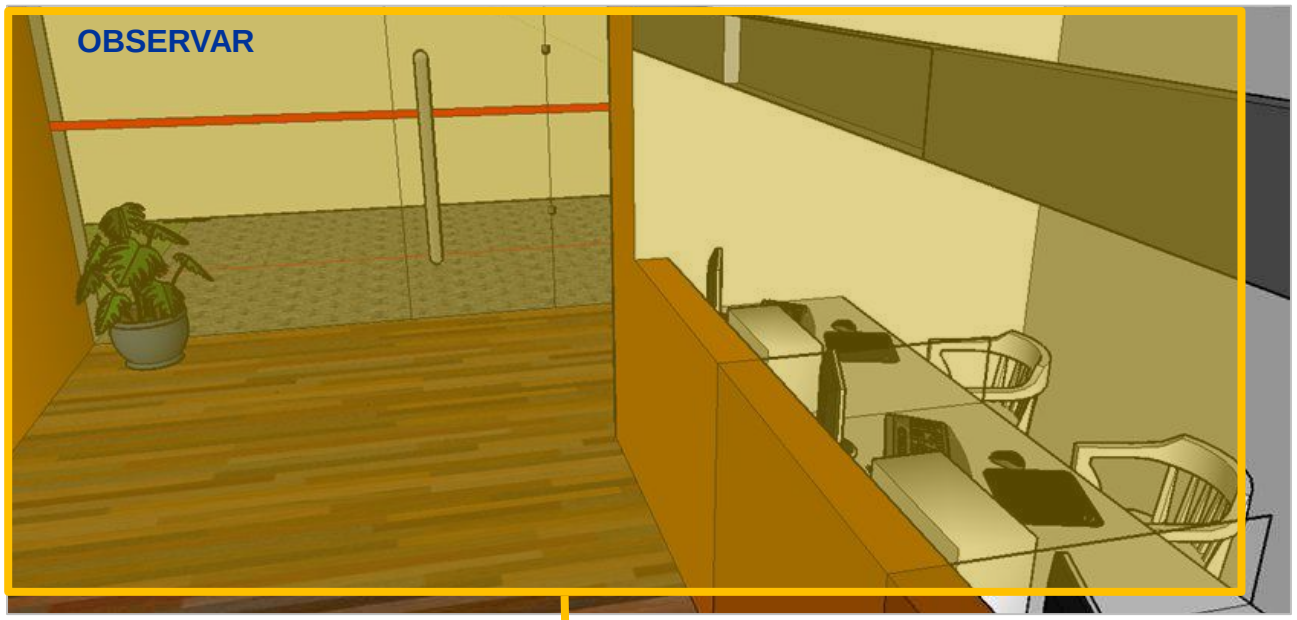
63 PPM: OBSERVAR
Puede detectar información tal como caras o matrículas (funciones de videoanálisis)

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

¿Lente y resolución adecuadas?, ¿ajuste adecuado de lentes MFZ?

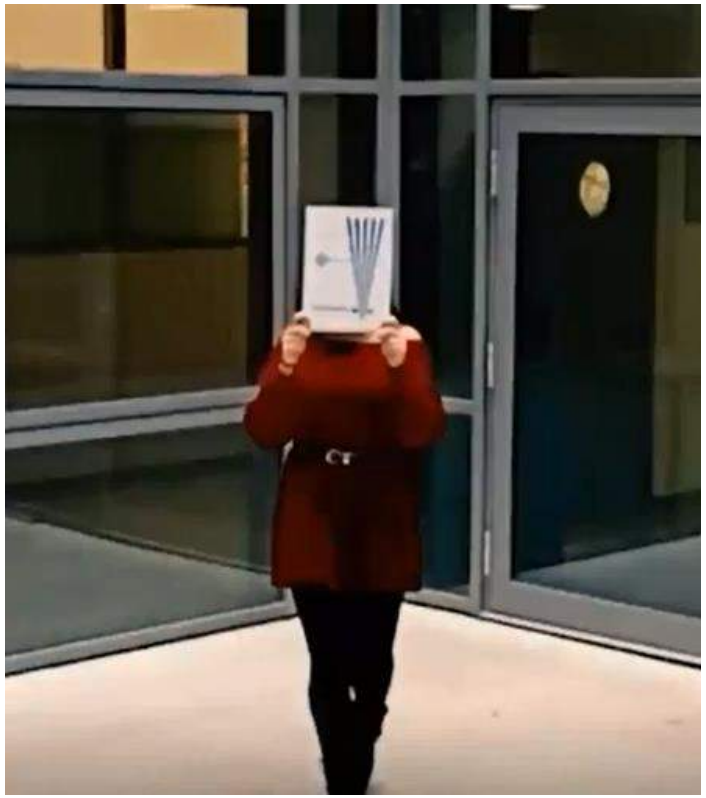




* Cámara formato Minidomo IP, referencia HC35W45R2. Marca Honeywell o similar.
* Cumplimiento NDAA, sección 889, PCI-DSS y TLS1.2 (seguridad ante ataques externos), acreditados mediante certificado de detección de vulnerabilidades. AES 128/256.
* Sensor de imagen CMOS 1/2,7" con escaneo progresivo.
* 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 incluída).
* 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.

Identificación facial, herramienta para el ajuste

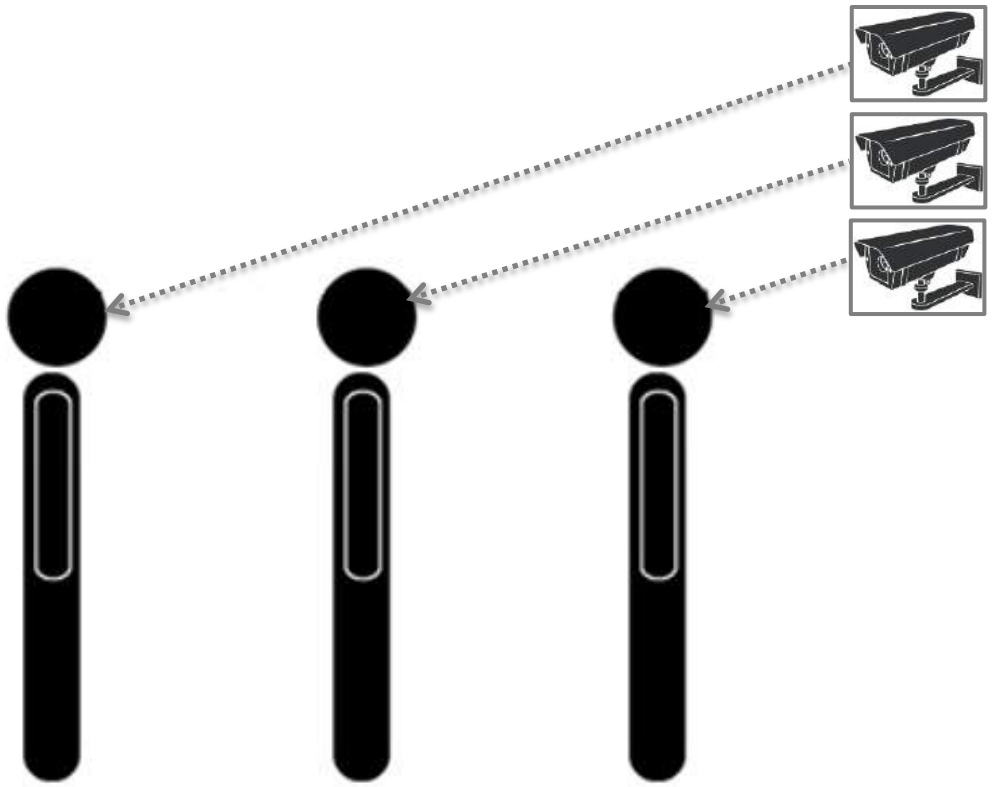
- Recomendación y directrices para instalaciones de videovigilancia. **Fuente: Grupo de trabajo en identificación facial de la Red de Laboratorios Forenses Oficiales de España (RLFOE)**



La evaluación debe realizarse sobre los fotogramas extraídos del videograbador

Identificación facial, altura de instalación de las cámaras Vs distancia del “blanco”

- Los resultados de la tabla indican cual sería la instalación máxima de la cámara según la distancia entre la cámara y la zona obligada de paso (blanco).
- Cálculos realizados considerando una persona de 170 cm de altura



Distancia al blanco	Altura de instalación
1 metro	1,86 metros
1,50 metros	2 metros
2 metros	2,13 metros
2,50 metros	2,16 metros
3 metros	2,40 metros
3.50 metros	2,53 metros
4 metros	2,67 metros
4,50 metros	2,80 metos
5 metros	2,93 metros
5,50 metros	3,07 metros
6 metros	3,20metros
6,50 metros	3.34 metros
7 metros	3,47 metros
7,50 metros	3, 60 metros
8 metros	3,74 metros

Elección de la cámara adecuada, algunas cuestiones a tener en cuenta

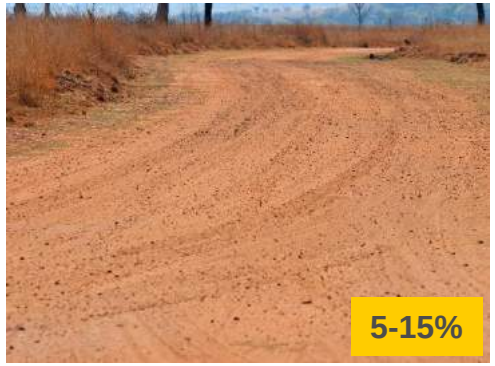
Importancia de la iluminación de apoyo si fuera necesaria y comentario acerca de la reflectancia

- La reflectancia se expresa en porcentaje e indica la cantidad de luz reflejada en una superficie.
- Este dato es importante para tener en cuenta a la hora de la instalación de cámaras con leds IR o focos IR de apoyo, ya que indicará que rendimiento real vamos a obtener en condiciones de poca o nula iluminación (reducción del alcance de visión).
- Algunos escenarios y su grado de reflectancia orientativo:

Zona asfaltada

Superficie acristalada

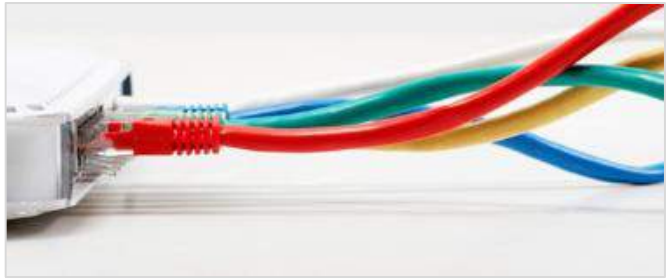
Tierra



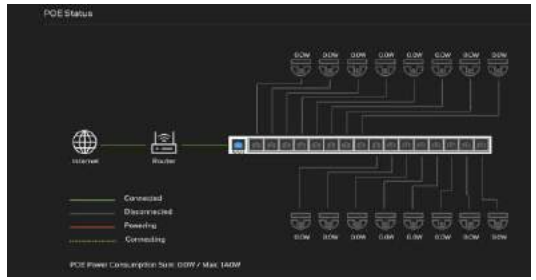
Césped

Alimentación de las cámaras, diferentes opciones

PoE



Control de consumos de las cámaras



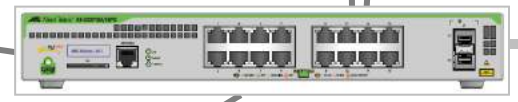
Alimentador estandar

Fuente de alimentación con batería de respaldo (monitorizada en sistema contra intrusion)

Alimentación de backup mediante SAI. Elección del equipo adecuado


6W


6W


70W


6W


6W


6W


4,1W

200W


4,1W

Cálculo de Potencia Aparente del SAI (VA)

VA SAI = Consumo del Sistema / Factor de Potencia

308,2 / 0,6 = 513,66

Determinar tiempo de autonomía que se considere razonable

* Utilizar 0,6 como constante para el factor de potencia

Grabación, diferentes opciones

Opción de grabación en tarjeta µSD en la propia cámara
- Grabación en caso de alarma, fallo en NVR o fallo en la red

Grabación en local
- Dimensionado de discos duros en función a necesidades del cliente
- Interfaces eSATA (1, 2, 4, …)
- Opciones estandar y RAID

Servidor NAS
- Exportación de clips de vídeo

Opción de grabación en Cloud
- Grabación de cámaras determinadas en caso de alarma

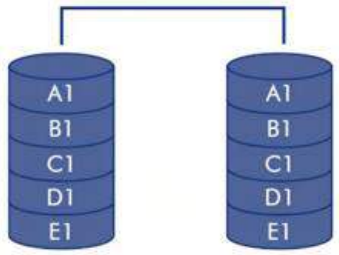
Grabación redundante (UNE – EN 62676-1-1)

Almacenamiento: El VSS debe poder	1	2	3	4
Hacer copias de seguridad de los datos y/o grabaciones redundantes			X	X
Hacer funcionar un dispositivo de almacenamiento seguro frente al fallo (por ejemplo RAID 5, espejo contínuo) o cambiar de forma automática a un soporte de almacenamiento a otro en caso de que se produzca un fallo de almacenamiento				X

NIS2 DIRECTIVE COMPLIANT

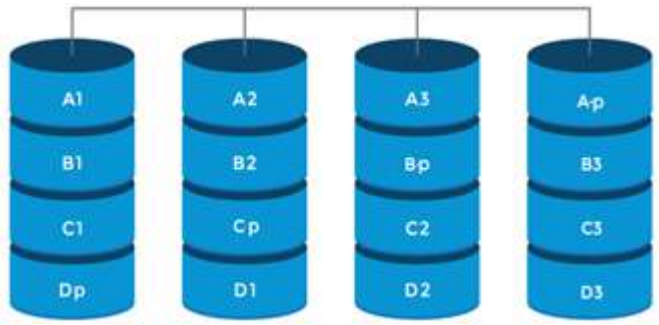
RAID Support

RAID 1



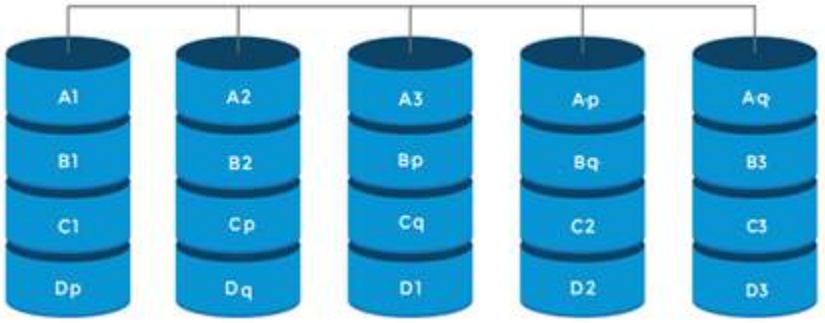
Mínimo 2 HDDs
Backup de datos

RAID 5



Mínimo 3 HDDs
Soporte restauración de datos
Puede fallar 1 HDD

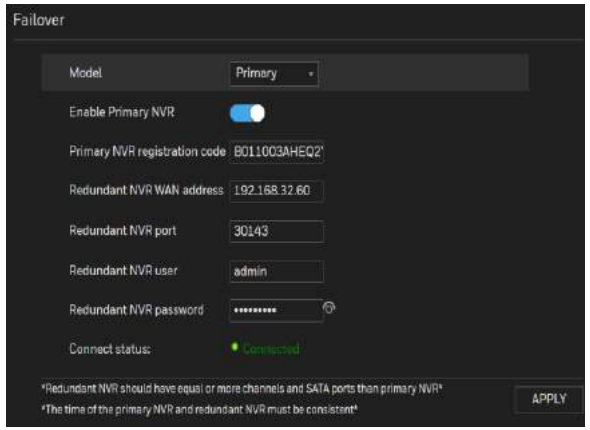
RAID 6

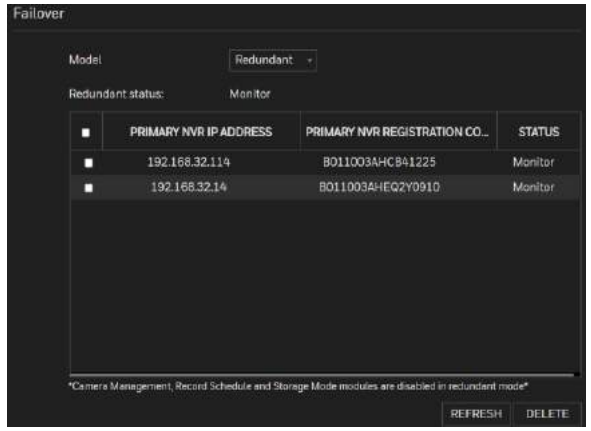


Mínimo 4 HDDs
Soporte restauración de datos
Pueden fallar 2 HDDs

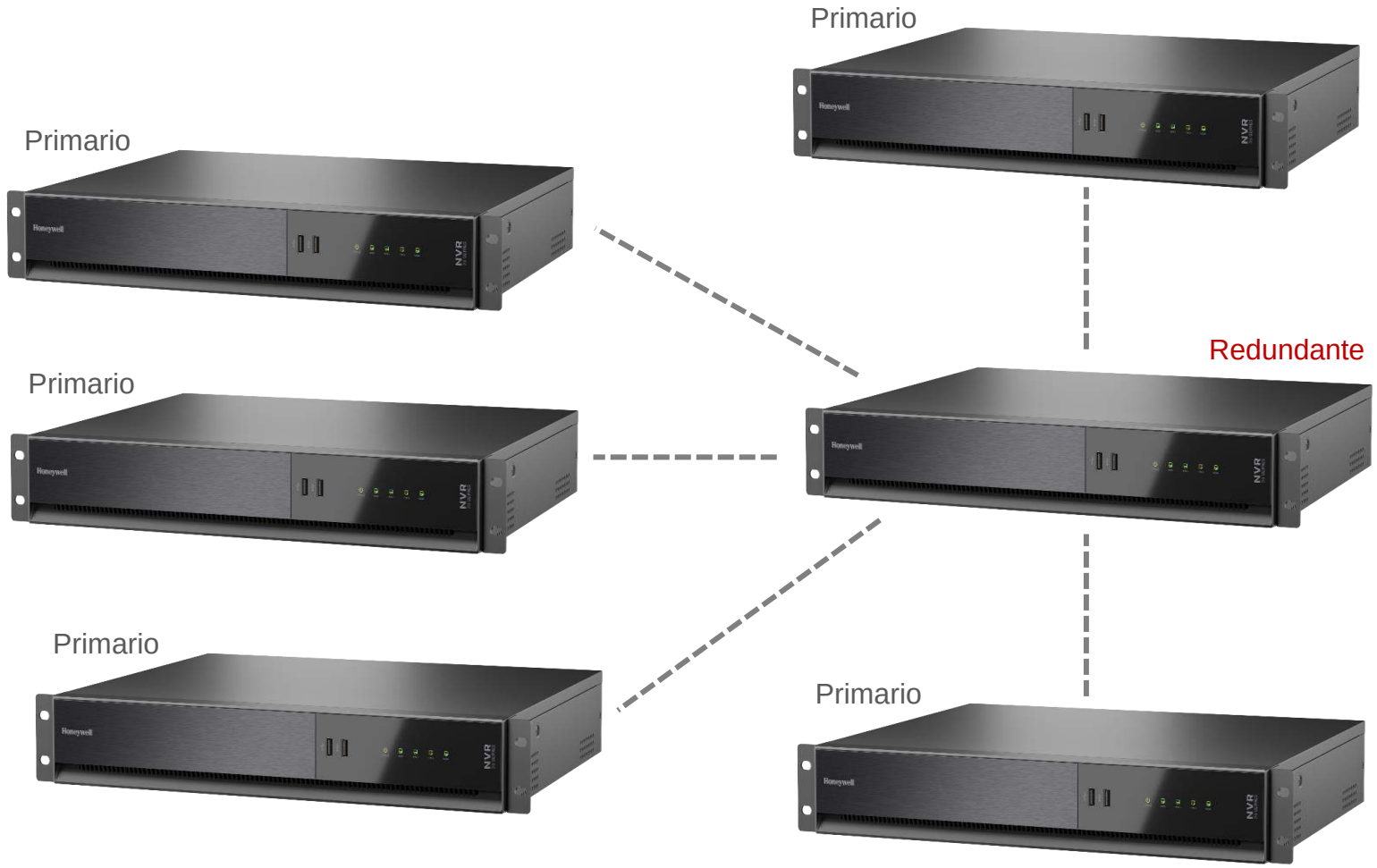
Cambio automático a un soporte de almacenamiento - Función FAILOVER

Los NVRs primarios se registran en el NVR redundante





El NVR redundante se hace cargo del primer NVR primario que falle



Ejemplo NVRs Serie 35 PRO

Rendimiento del NVR, gestión y grabación del sistema

RESOLUCIÓN

DÍAS DE ALMACENAMIENTO

DISCO DURO

	torage Calculator rev.: 2.0							
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

Nº DE CÁMARAS

RENDIMIENTO DEL NVR

ANCHO DE BANDA

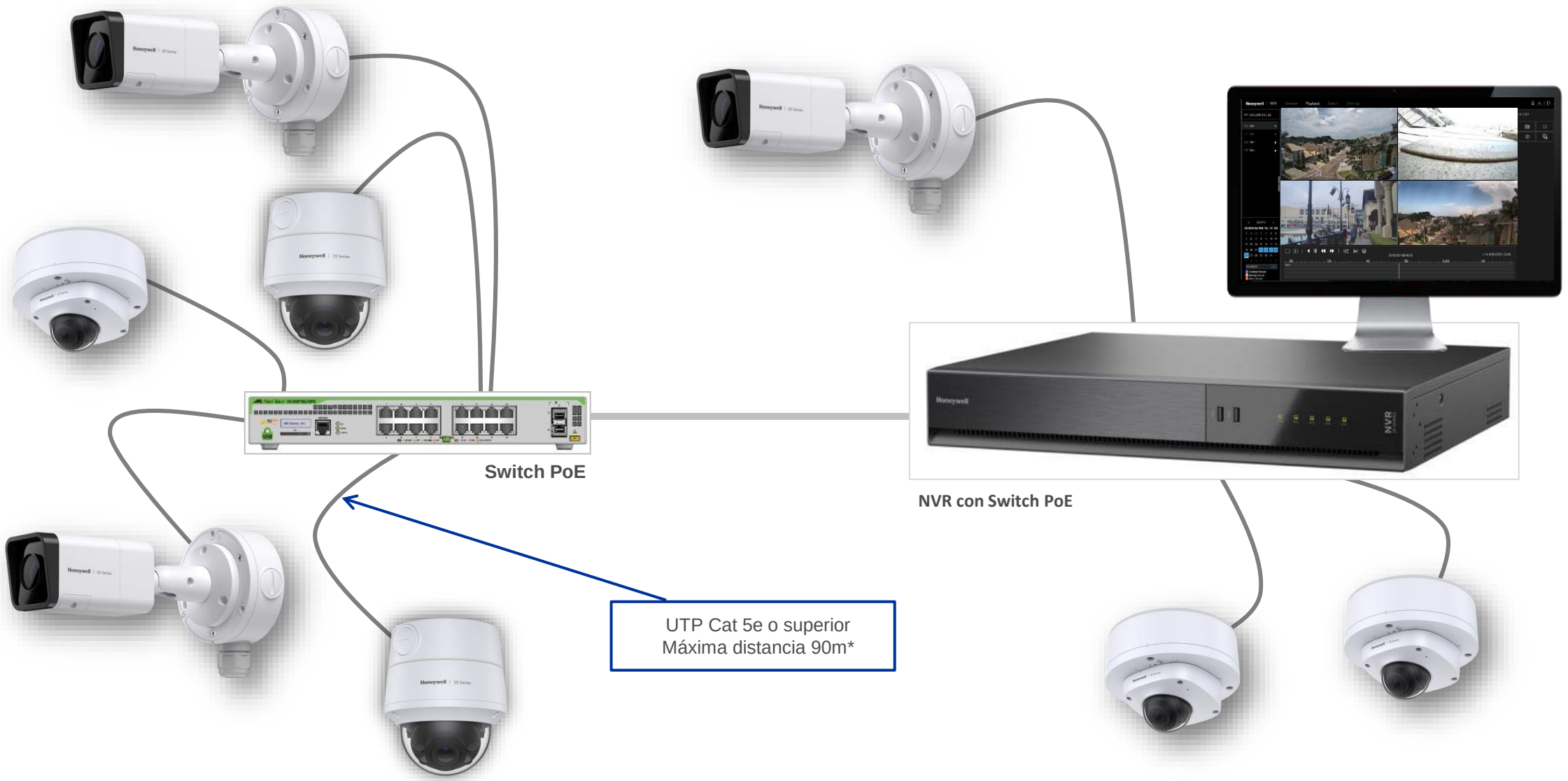
- **Garantizar** que el disco duro necesario en función a los días de grabación, el rendimiento del NVR y el ancho de banda requerido se adecuan a la especificación (Ejemplo de cálculo NVR ADPRO IFT)

UNE –EN 62676-1-1. Algunas cuestiones adicionales a tener en cuenta según Grado

Copias de Seguridad	1	2	3	4
Una copia de seguridad programada automáticamente de los datos de imagen de alarma				X
Una copia de seguridad de los datos de imagen de alarma por solicitud manual			X	X
La verificación de que se ha realizado con éxito la copia de seguridad de las imágenes			X	X

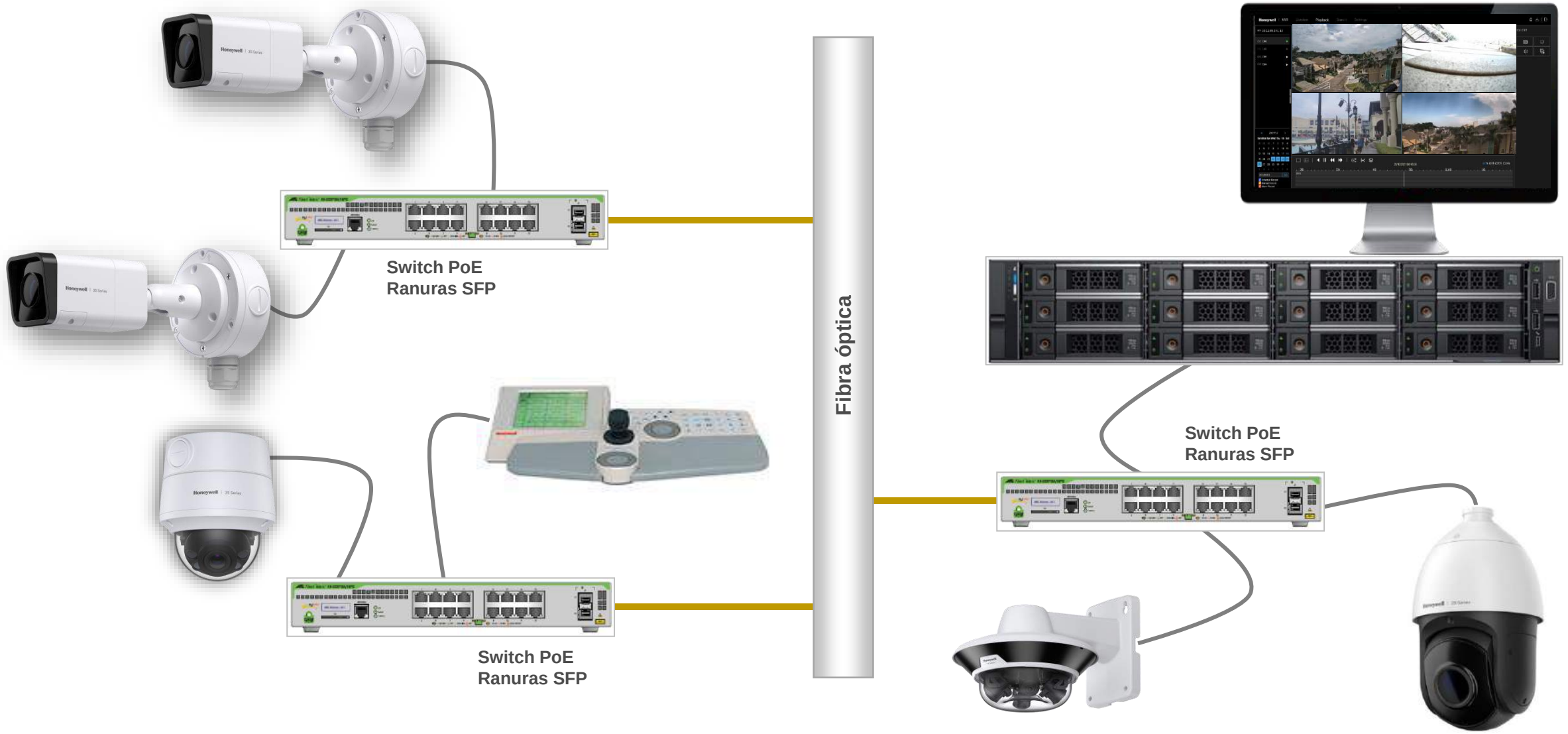
El sistema debe detectar	1	2	3	4
La pérdida de señal de vídeo		X	X	X
Si se deja de mostrar la totalidad del campo de visión especificado			X	X
El oscurecimiento o cegamiento deliberado de los dispositivos captadores de imagen			X	X
La sustitución de datos de vídeo a nivel de fuente de la imagen, interconexión o tratamiento				X
La reducción significativa del contraste de la imagen				X

Arquitectura de la propuesta, ejemplo 1

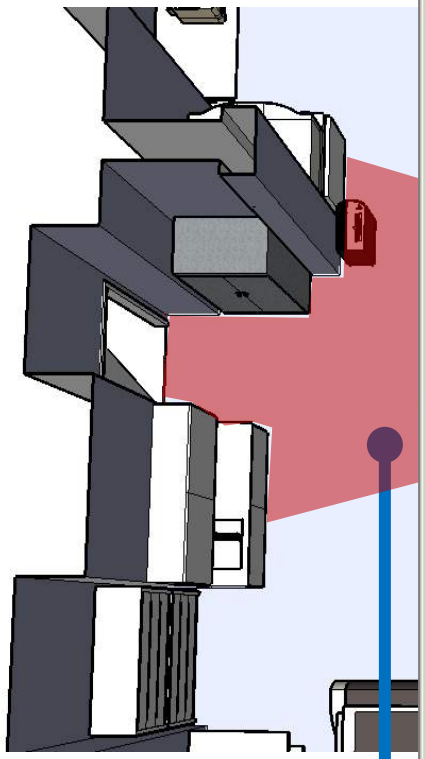


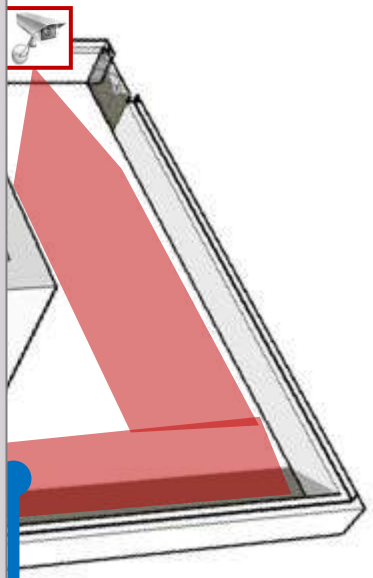
Determinar infraestructura de red en función a las distancias
* Si es necesario certificar la red de datos

Arquitectura de la propuesta, ejemplo 2



Análisis de vídeo





O ANÁLISIS:

undos de

saparece

onas

Opciones de gestión

Servicios Cloud para gestion y grabación de alarmas

Control local

Gestión mediante Apps

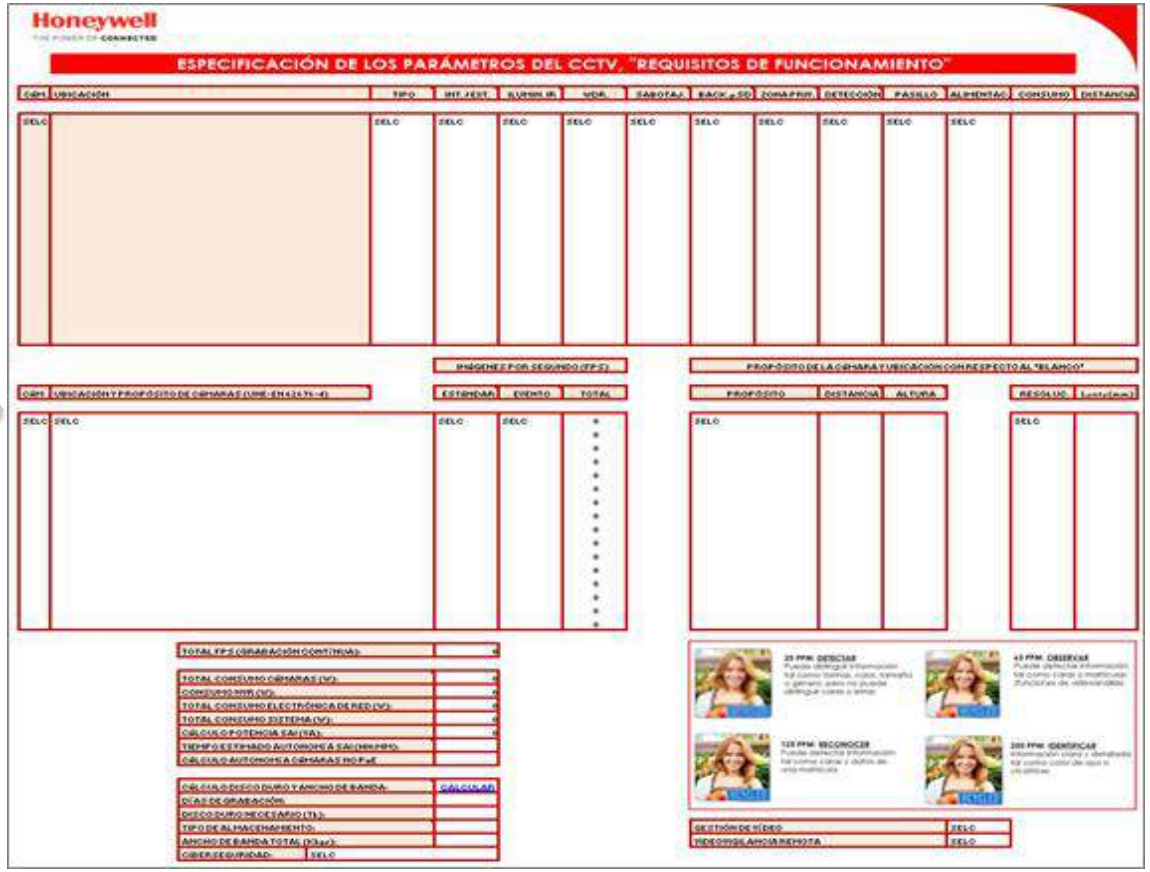
Acceso a través de WebServer (local / remoto)

Software de gestion del video VMS
Integración con otros sistemas

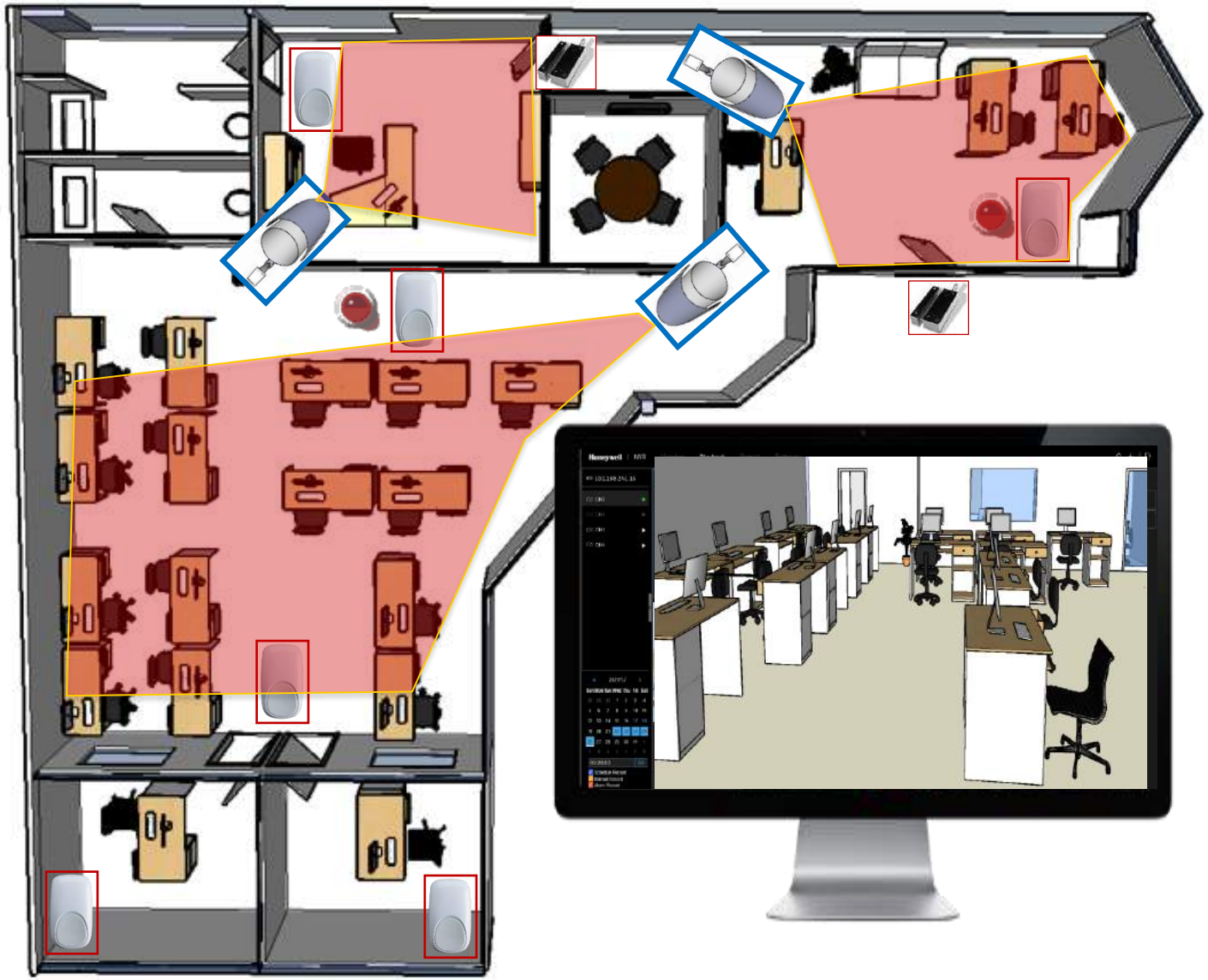
Documento “REQUISITOS DE FUNCIONAMIENTO”

- Al realizarse la propuesta de diseño, el propósito de la instalación de CCTV debe resumirse en un documento llamado **“Requisitos de funcionamiento”** (UNE-EN 62676), donde se establece lo que **el cliente espera de su sistema de videovigilancia.**

CONCEPTO	UNIDADES
A. SISTEMA DE CCTV IP.	
CÁMARA MINIDOMO IP 3 MPX Domo IP Honeywell Serie 35 3MP@25/30ips, H.265/H.264 ICR, 0,005 lux, Smart IR 50m Óptica motorizada de 2,7~13,5 mm WDR 120dB, 3D-DNR, ROI Ranura MicroSD, RJ45, Onvif, IP67, IK10, PoE, 3AXIS	40
CÁMARA BULLET IP 3MPX Cámara IP Honeywell Serie 35 3MP@25/30ips, H.265/H.264 ICR, 0,005 lux, Smart IR 60m Óptica motorizada de 2,7~13,5 mm WDR 120dB, 3D-DNR, ROI Ranura MicroSD, RJ45, Onvif, IP67, IK10, PoE	6
BASE CONEXIONES Caja de conexiones para cámaras Honeywell Serie 35 Aluminio fundido	46
GRABADOR NVR IP 32 CANALES NVR IP Honeywell Serie 35 de 32 canales H.265/H264 Grabación de hasta 8MP Ancho de banda de 320Mbps 2 salidas HDMI (4K+1080P), 1 salida VGA 1080P Reproducción sincronizada de 16 canales Audio bidireccional 6 entradas / 2 salidas de alarma Admite 4 HDD SATA 2 RJ45 Gigabit, 2 USB 2.0, 1 USB 3.0 220V CA, 16 puertos PoE+, 1U Conforme la NDAA	2



Verificación de alarmas, comentario acerca de la ubicación de las cámaras



Mantenimiento de los sistemas

Mantenimiento periódico de los sistemas de CCTV conforme a UNE EN 62676-4:2015

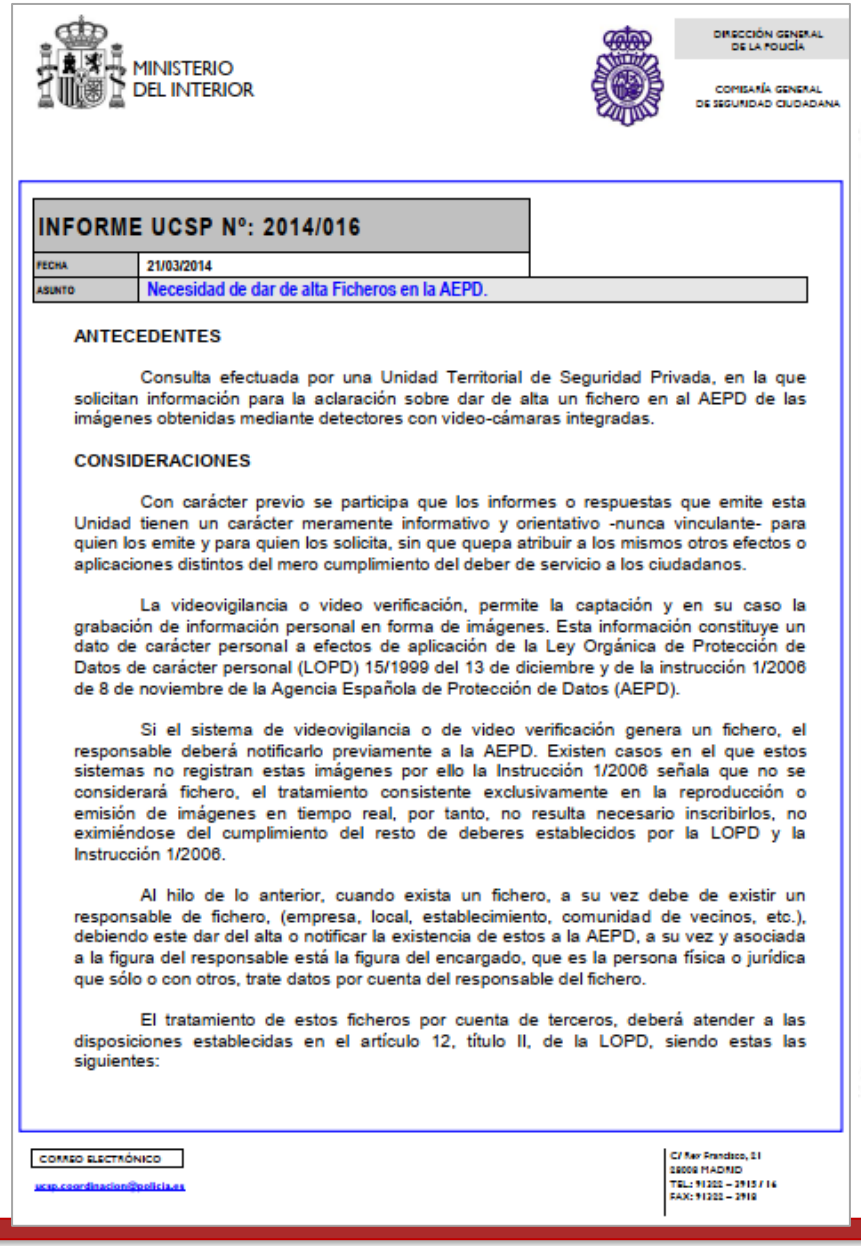
INSTALACIÓN:	FECHA:	

VERIFICACIÓN MANTENIMIENTO PRESENCIAL

EQUIPOS Y COMPROBACIONES A REALIZAR	UDS.	REALIZADO	OBSERVACIONES
INFORMACIÓN A RECABAR ANTES DE EMPEZAR LOS TRABAJOS DE MANTENIMIENTO • Establecer previamente con el cliente si ha habido cualquier problema con el sistema de CCTV desde la última visita de mantenimiento. • Examinar la documentación del sistema para ver si ha habido cualquier llamada al servicio o incidentes desde la última visita rutinaria. El técnico debe preguntar si ha habido algún cambio en el uso de las instalaciones, un cambio en los procedimientos de trabajo o un cambio de propietario. • El técnico debe asegurarse de que el cliente (o el representante del cliente) conoce todavía a fondo el funcionamiento del sistema de CCTV.		SELEC	
CÁMARAS DE CCTV • Verificar que el número y tipo de cámaras, incluyendo objetivos, están de acuerdo con lo que se indicó en la especificación o en cualquier modificación de la misma. • Verificar que los campos de visión están libres de obstrucciones. • Comprobar el estado de las fijaciones físicas. verificando que no haya aflojamiento o corrosión en soportes y fijaciones. • Comprobar las juntas y cierres herméticos de los equipos de exterior. • Búsquense las señales de condensación en las ventanas de las carcasas de las cámaras. Abriendo las cubiertas y carcasas para limpiar el interior cuando sea necesario. • Verificar que todas las funciones de cámara de control remoto y automático cumplen con la especificación: movimiento panorámico, inclinación, zoom, enfoque, presets, tours, limpiaparabrisas. • Verificar toma de alimentación de las cámaras y equipos de iluminación de apoyo si los hubiera. • Revisar condiciones de iluminación y equipos de iluminación de apoyo existentes (incorporados en la propia cámara o externos), verificando funcionamiento con condiciones de baja iluminación (a través del equipo de grabación si no hubiera otra forma). Estos eauipos deberán ser sustituídos según las frecuencias recomendadas por el fabricante.			
CÁMARA INTERIOR		SELEC	
CÁMARA EXTERIOR		SELEC	
DOMO PTZ INTERIOR		SELEC	
DOMO PTZ EXTERIOR		SELEC	
EQUIPO DE ILUMINACIÓN DE APOYO		SELEC	
• El funcionamiento de todas las interfaces con alarmas es satisfactoria, incluyendo la correcta activación por disparo de alarma. • En el caso de sistemas de análisis de vídeo, verificar que están funcionando de acuerdo con lo que se indicó y determinó en la especificación o en cualquier modificación de la misma, inluyéndose las actuaciones locales de alarma. • En el caso de equipos de alimentación de backup, producir fallo en la fuente de alimentación principal y verificar el correcto funcionamiento del sistema.			
EQUIPO DE GRABACIÓN		SELEC	
MONITOR		SELEC	
ANÁLISIS DE VÍDEO (CANALES)		SELEC	
OTROS EQUIPOS (VÍDEO ANALÓGICO): MULTIPLEXORES, DISTRIBUIDORES DE SEÑAL,...		SELEC	
SWITCHS		SELEC	
ALIMENTACIÓN DE BACKUP (FUENTE DE ALIMENTACIÓN CON BATERÍA DE RESPALDO, S.A.I.)		SELEC	
SERVICIO DE VIDEOVIGILANCIA REMOTA • Solicitar al operador de la C.R.A. que acceda al sistema y verifique el visionado de cada una de las cámaras. • Acceso a secuencias de video grabado de cada una de las cámaras. • En caso de sistemas de análisis de vídeo, activar los distintos canales y comprobar la recepción de las señales. • En caso actuaciones remotas sobre el sistema de videovigilancia, verificar su correcto funcionamiento.		SELEC	

https://www.aepd.es/areas-de-actuacion/videovigilancia

Consulta de alta de ficheros en la AEPD



MINISTERIO DEL INTERIOR

DIRECCIÓN GENERAL DE LA POLICÍA

COMISARÍA GENERAL DE SEGURIDAD CIUDADANA

INFORME UCSP Nº: 2014/016

FECHA	21/03/2014
ASUNTO	Necesidad de dar de alta Ficheros en la AEPD.

ANTECEDENTES

Consulta efectuada por una Unidad Territorial de Seguridad Privada, en la que solicitan información para la aclaración sobre dar de alta un fichero en al AEPD de las imágenes obtenidas mediante detectores con video-cámaras integradas.

CONSIDERACIONES

Con carácter previo se participa que los informes o respuestas que emite esta Unidad tienen un carácter meramente informativo y orientativo -nunca vinculante- para quien los emite y para quien los solicita, sin que quepa atribuir a los mismos otros efectos o aplicaciones distintos del mero cumplimiento del deber de servicio a los ciudadanos.

La videovigilancia o video verificación, permite la captación y en su caso la grabación de información personal en forma de imágenes. Esta información constituye un dato de carácter personal a efectos de aplicación de la Ley Orgánica de Protección de Datos de carácter personal (LOPD) 15/1999 del 13 de diciembre y de la instrucción 1/2006 de 8 de noviembre de la Agencia Española de Protección de Datos (AEPD).

Si el sistema de videovigilancia o de video verificación genera un fichero, el responsable deberá notificarlo previamente a la AEPD. Existen casos en el que estos sistemas no registran estas imágenes por ello la Instrucción 1/2006 señala que no se considerará fichero, el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real, por tanto, no resulta necesario inscribirlos, no eximiéndose del cumplimiento del resto de deberes establecidos por la LOPD y la Instrucción 1/2006.

Al hilo de lo anterior, cuando exista un fichero, a su vez debe de existir un responsable de fichero, (empresa, local, establecimiento, comunidad de vecinos, etc.), debiendo este dar del alta o notificar la existencia de estos a la AEPD, a su vez y asociada a la figura del responsable está la figura del encargado, que es la persona física o jurídica que sólo o con otros, trate datos por cuenta del responsable del fichero.

El tratamiento de estos ficheros por cuenta de terceros, deberá atender a las disposiciones establecidas en el artículo 12, título II, de la LOPD, siendo estas las siguientes:

CORREO ELECTRÓNICO

ucsp.coordinacion@policia.es

C/ Rey Francisco, 21
28008 MADRID
TEL.: 91322 – 2915 / 16
FAX: 91322 – 2918

1ª.- Con independencia de si se trata de la captura de imágenes secuenciales o de una videograbación, siempre que exista un almacenamiento de estas, existirá un fichero y como tal deberá de darse de alta en la AEPD, indicándose quién es el responsable y quien el encargado de su tratamiento, en el caso de existir tal figura.

2ª.- Para el tratamiento de imágenes por un tercero, deberá celebrarse un contrato entre el responsable del fichero y la persona que vaya a tratar estas imágenes, indicándose los preceptos anteriormente explicados.

3ª.- La instalación de un sistema de videovigilancia para la mera reproducción o emisión de imágenes en tiempo real, no conlleva la necesidad de inscribirse en la Agencia Española de Protección de Datos.

4ª.- Las empresas de seguridad autorizadas, singularmente aquellas con actividad de central receptora de alarmas, que tengan conectados equipos de detectores que presentan integradas una cámara, y utilicen los mismos para la verificación mediante video, o que los detectores de intrusión activen un subsistema de video o un video sensor, para la verificación de las señales de alarma, según lo establecido en la Orden Ministerial INT 316/2011, artículo 8, únicamente este proceso de verificación será válido, cuando el sistema registre un mínimo de una imagen del momento exacto de la alarma y dos imágenes posteriores, lo que lleva necesariamente a generar un fichero de imagen. Ficheros almacenados que en no pocas ocasiones se debe facilitar a la FCSE, cuando se trata de intrusiones reales o con capacidad identificativa del autor o autores. Lo que como ya se ha expresado, lleva a la obligación de dar de alta a dicho fichero en la AEPD, con indicación de quien es el responsable del mismo.

Principio de proporcionalidad

de Seguridad, y su Reglamento de desarrollo aprobado mediante Real Decreto 596/1999, de 16 de abril, la Ley 5/2014, de 4 de abril, de Seguridad Privada, o la Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte así como su reglamento de desarrollo aprobado mediante Real Decreto 203/2010, de 26 de febrero.

2.2 Proporcionalidad

2.2.1 Limitación de la finalidad

El RGPD recoge en su artículo 5 este principio, en virtud del cual, los datos personales será recogidos con fines determinados, explícitos y legítimos y no serán tratados ulteriormente de manera incompatible con dichos fines, de manera que los datos que sean objeto de tratamiento a través de la videovigilancia serán tratados para la finalidad que ha motivado la instalación de la misma y que está vinculada a garantizar la seguridad de personas, bienes e instalaciones.

2.2.2. Captación de imágenes de la vía pública

Como regla general, la captación de imágenes con fines de seguridad de la vía pública debe realizarse por las Fuerzas y Cuerpos de Seguridad.

Ya que les corresponde la prevención de hechos delictivos y la garantía de la seguridad en la citada vía pública, de conformidad con lo regulado por Ley Orgánica 4/1997, de 4 de agosto, y su Reglamento de desarrollo.

Sin embargo, sobre esta regla general es posible aplicar alguna excepción:

- En algunas ocasiones para la protección de espacios privados, donde se hayan instalado cámaras en fachadas o en el interior, puede ser necesario para garantizar la finalidad de seguridad la grabación de una porción de la vía pública, Es decir, las cámaras y videocámaras instaladas con fines de seguridad no podrán obtener imágenes de la vía pública salvo que resulte imprescindible para dicho fin, o resulte imposible evitarlo por razón de la ubicación de aquéllas. Por lo tanto, las cámaras podrían captar la porción mínimamente necesaria para la finalidad de seguridad que se pretende.
- Será posible la captación de la vía pública en una extensión superior cuando garantizar la seguridad de bienes o instalaciones estratégicas o de infraestr transporte.
- Gran parte de la actividad de los ciudadanos se desarrolla en espacios que público en general, como centros comerciales, restaurantes, lugares de ocio referimos a lugares a los que los ciudadanos pueden tener libre acceso aunq privada, en los que sus titulares utilizan los sistemas de videovigilancia para g de las personas e instalaciones.

2.2.3. Minimización de datos

Otro de los principios que recoge el RGPD en su artículo 5 es el principio de mini forma que los datos objeto de tratamiento sean adecuados, pertinentes y limitad fines para los que son tratados.

Además, existen espacios que por sus condiciones podría ser desproporcionado la utilización de la videovigilancia, en vestuarios, taquillas y zonas de descanso de trabajadores.

Por otra parte, el mencionado principio también se proyecta a través del número de cámaras que se pretenda utilizar así como el tipo de las mismas, ya que no es lo mismo la captación de imágenes a través de una cámara fija que la que se realiza mediante las denominadas `domo´, que permite grabaciones de 360 grados, o aquellas que son móviles.

Otra opción para aplicar este principio de minimización de datos es la posibilidad de utilizar las denominadas `máscaras de privacidad´, de tal forma que se evite captar y grabar imágenes excesivas.

- Valore si realmente es necesaria la instalación de la videovigilancia o si el fin perseguido se puede alcanzar de otra forma.
- Cuando realice la instalación, tenga en cuenta la proporcionalidad en función del número de cámaras, tipo de las mismas y la opción de utilizar "máscaras de privacidad".