JORNADA SOBRE VIGILANCIA Y SISTEMAS DE SEGURIDAD

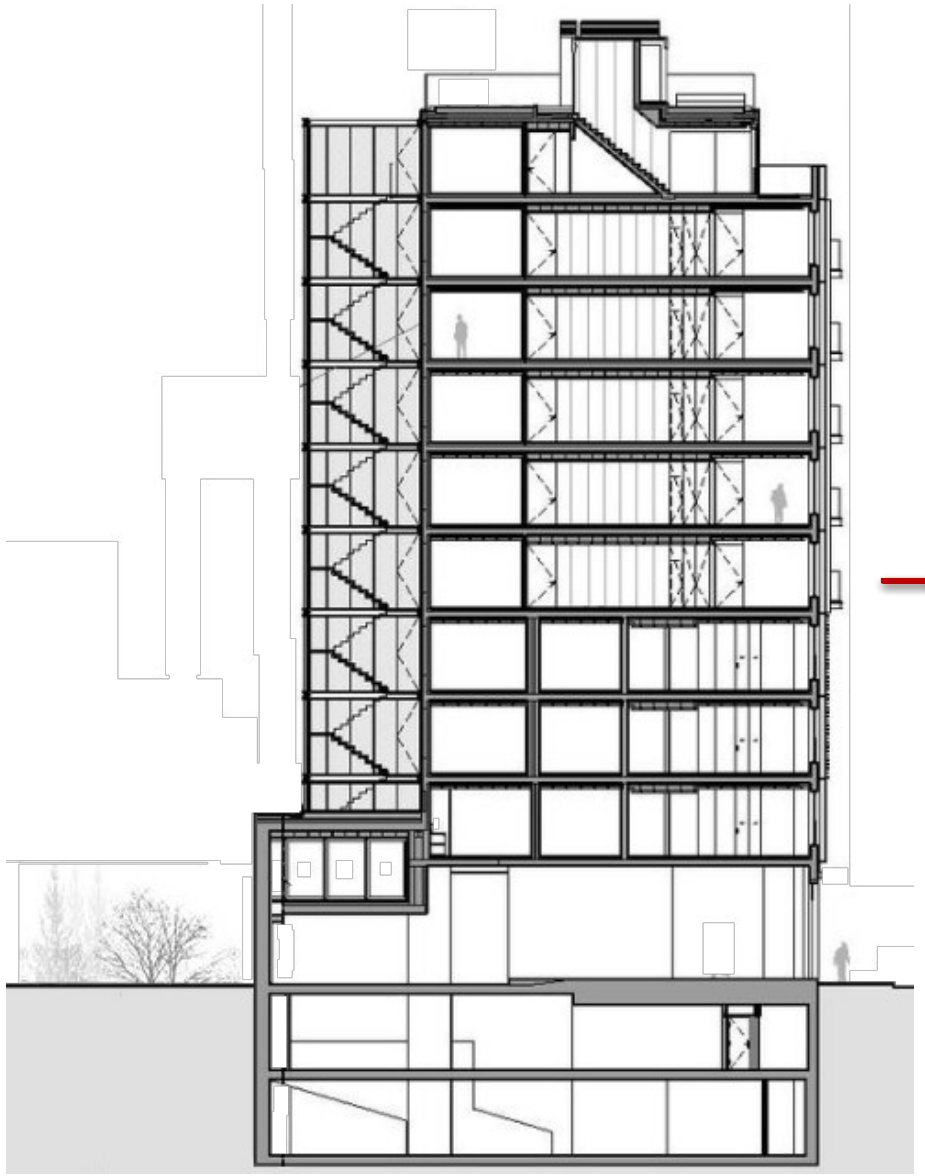
Badajoz, 27de Noviembre de 2024

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

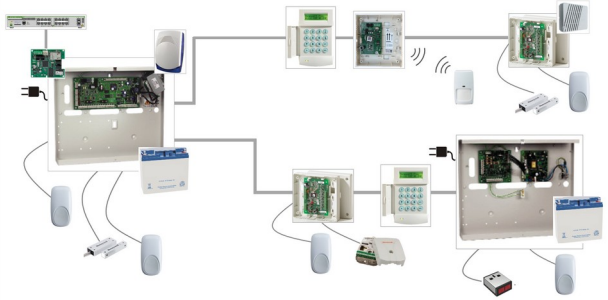
Introducción a la Directiva NIS2 relativa a medidas de Ciberseguridad

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

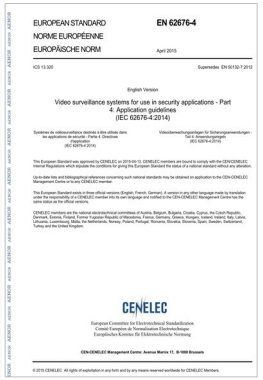
Normas UNE – EN de obligatorio cumplimiento para el diseño de sistemas



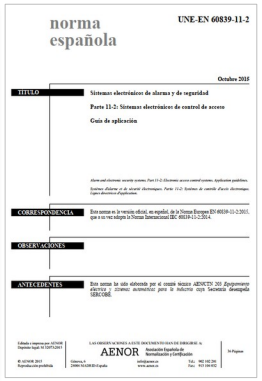
UNE-CLC/TS 50131-7: Contra Intrusión



UNE-EN 62676-47: Videovigilancia



UNE-EN 50398-11-2: Control de Accesos



Primer paso: análisis de riesgos – determinar el grado de seguridad

CONSECUENCIAS	PROBABILIDAD: MUY PROBABLE	PROBABLE	IMPROBABLE	ALTAMENTE IMPROBABLE
FATALIDAD	Grado 3	Grado 3	Grado 3	Grado 2
IMPORTANTES	Grado 3	Grado 3	Grado 2	Grado 2
LEVES	Grado 3	Grado 2	Grado 2	Grado 1
MUY LEVES	Grado 2	Grado 2	Grado 1	Grado 1

PROTECCIÓN ANTE EL ATAQUE FÍSICO

EL PAIS

Los Ciberataques alcanzan su máximo histórico: “no hay nadie a salvo”

Los ciberataques alcanzan su máximo histórico: “No hay nadie a salvo” | Tecnología | EL PAÍS (elpais.com)

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

HOSTELTUR

Los 8 tipos de ciberataques más habituales en hoteles en 2023

https://www.hosteltur.com/155703_los-8-tipos-de-ciberataques-mas-habituales-en-hoteles-en-2023.html

EL CONFIDENCIAL

Los Ciberataques golpean la eólica europea en pleno debate por cortar el gas ruso

https://www.elconfidencial.com/mercados/the-wall-street-journal/2022-04-26/el-sector-de-energia-eolica-europeo-victima-de-una-ola-de-ataques-ciberneticos_3414141/

DELOITE

Las ciberamenazas ponen en alerta a las universidades

https://www2.deloitte.com/es/es/pages/governance-risk-and-compliance/articles/ciberamenazas-alertan-universidades.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

IDRICA

La ciberseguridad, una prioridad para las gestoras de agua europeas

https://www.idrica.com/es/blog/ciberseguridad-gestoras-de-agua-europeas/

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/

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

TELEFONICA TECH

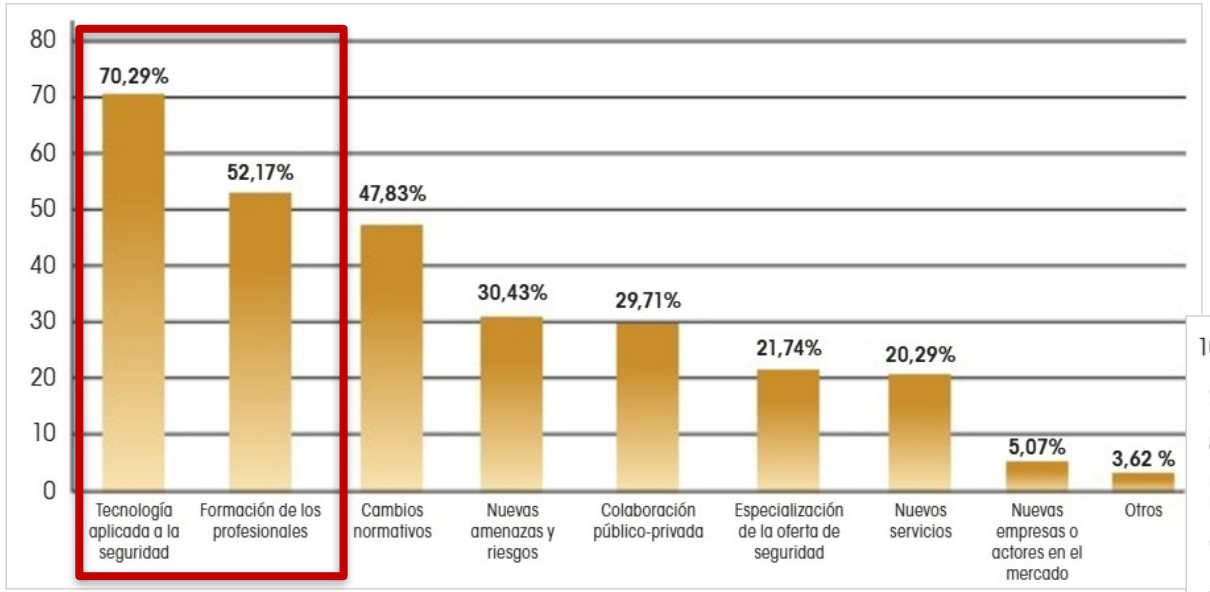
Consecuencias de un ciberataque en entornos industriales

https://telefonicatech.com/blog/consecuencias-de-un-ciberataque-en-entornos-industriales

Contemplar el Ciberataque en el análisis de riesgos y en la elección de los equipos (OT)

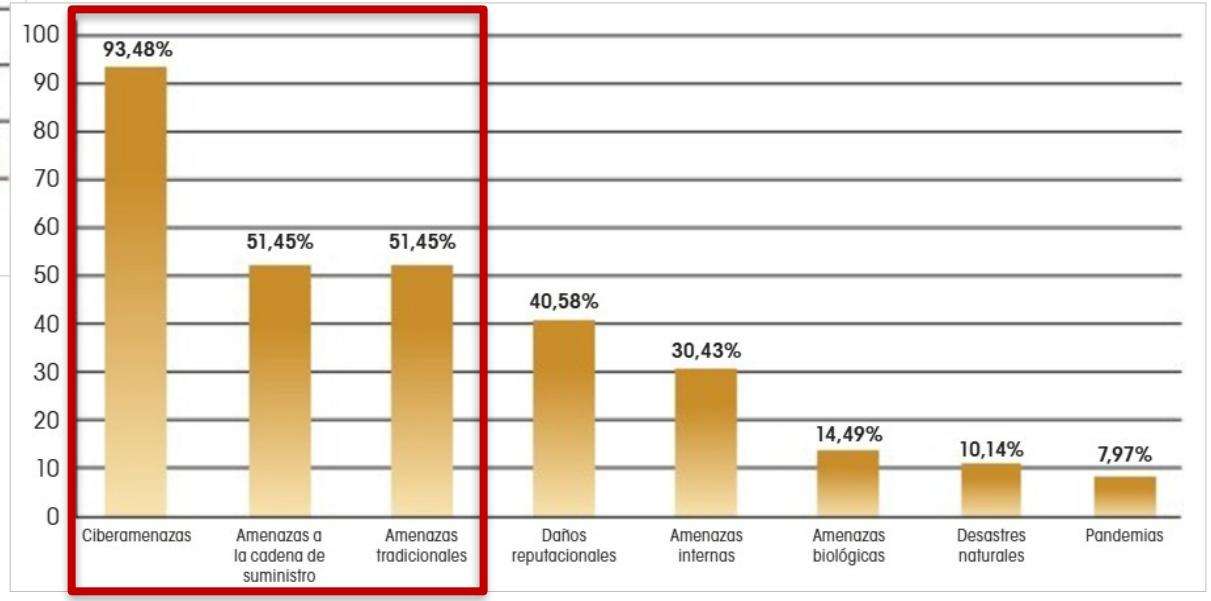
La Seguridad Privada en España hacia 2030 (encuesta año 2023)

Encuesta que ha recibido cerca de 500 respuestas de profesionales de la seguridad de diferentes perfiles



Factores que permitirán un mayor impulso y desarrollo de la Seguridad Privada de aquí a 2030

Las tres amenazas o riesgos que más preocupan a los responsables de seguridad de las empresas de cara al año 2030



FUENTE: SEGURITECNIA
https://www.seguritecnia.es/actualidad/seguridad-privada/estudio-sectorial-seguridad-privada-en-espana-hacia-2030_20230525.html

Directiva NIS2 relativa a medidas de Ciberseguridad, obligaciones

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 Ciberseguridad 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.

Directiva NIS2 relativa a medidas de Ciberseguridad, cronograma

6/07/2016 — Publicación Directiva (UE) 2016/1148

14/12/2022 — Publicación Directiva (UE) 2022/255

16/1/2023 — Inicio plazo transposición

17/10/2024 — Estados miembros deben adoptar y publicar medidas para cumplirla

17/1/2025 — La red de "Equipos de Respuesta a Incidentes Cibernéticos" evaluará los progresos realizados en materia de cooperación operativa

17/4/2025 — Estados miembros deben establecer una lista con las Entidades Esenciales e Importantes

17/10/2027 — Revisión de la directiva

Sectores involucrados

SECTORES DE ALTA CRITICIDAD Esenciales e Importantes

TRANSPORTE

Aéreo / Ferrocarril / Marítimo – Fluvial / Carretera

ENERGÍA

Electricidad / Gas / Crudo / Hidrógeno / Sistemas urbanos de calefacción y refrigeración

SALUD

Asistencia sanitaria / Farmacia

ESPACIO

AGUA POTABLE

AGUAS RESIDUALES

ADMINISTRACIÓN PÚBLICA

INFRAESTRUCTURAS DIGITALES

BANCA

MERCADOS FINANCIEROS

GESTIÓN DE SERVICIOS TIC

OTROS SECTORES CRÍTICOS Importantes

SERVICIOS POSTALES Y DE MENSAJERÍA

GESTIÓN DE RESÍDUOS

PROVEEDORES DIGITALES

Proveedores de mercado en línea / Proveedores de motores de búsqueda en línea / Proveedores de plataformas de servicios de redes sociales

QUÍMICAS

Producción, transformación y distribución de sustancias y mezclas químicas

ALIMENTACIÓN

Producción, transformación y distribución de alimentos

INVESTIGACIÓN

FABRICACIÓN

Fabricación de productos sanitarios y sanitarios para diagnóstico in vitro

Fabricación de equipos informáticos, electrónicos y ópticos

Fabricación de material eléctrico

Fabricación de maquinaria y equipamiento

Fabricación de vehículos de motor, remolques y semirremolques

Fabricación de otros equipos de transporte

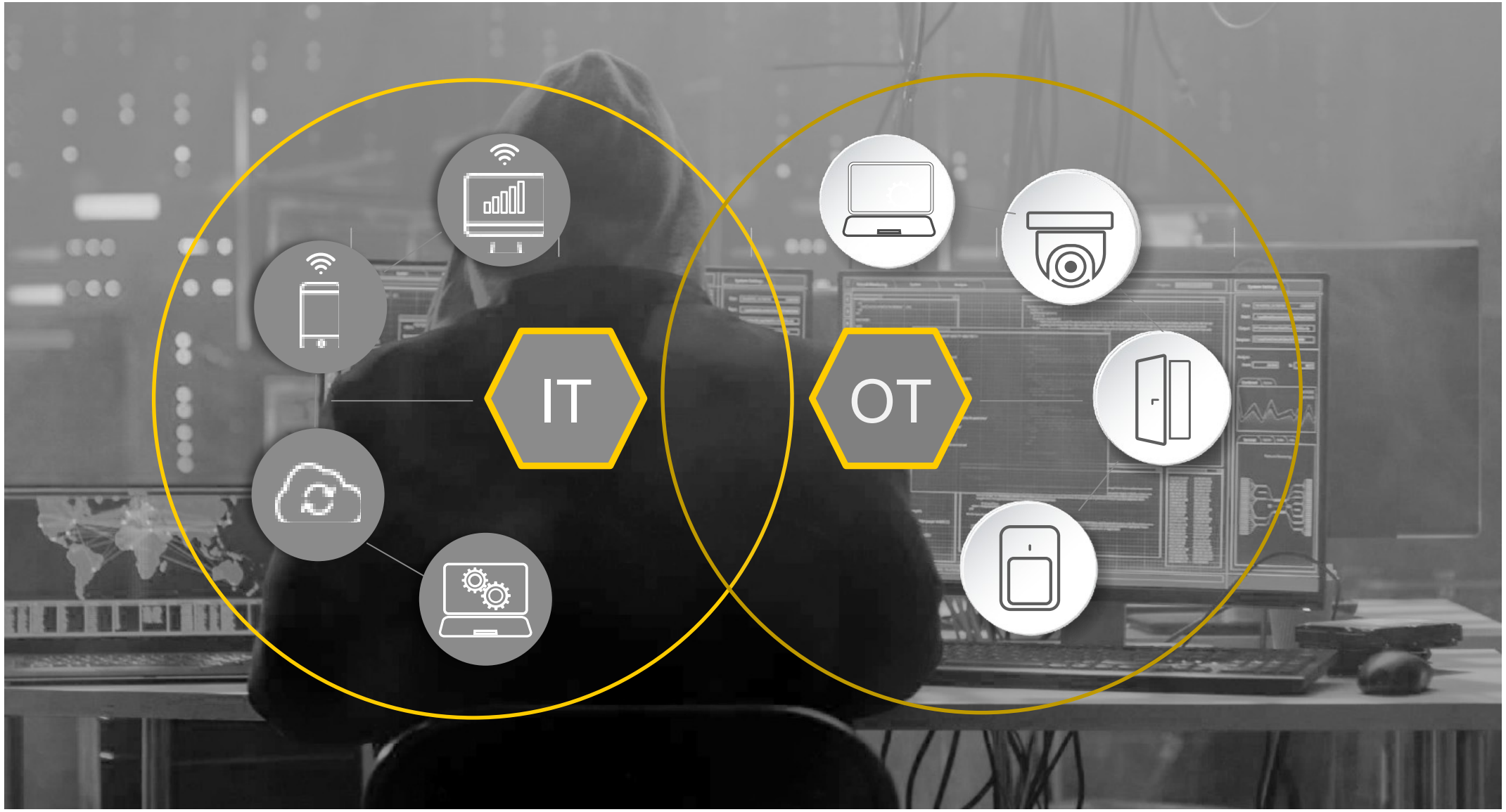
Acerca de los sectores de Alta Criticidad

	>=250 empleados y >50M€ facturac.	Entre 50 - 249 empleados y >10M€
ENERGÍA	EE	EI
TRANSPORTE	EE	EI
BANCA	EE	EI
MERCADOS FINANCIEROS	EE	EI
SALUD	EE	EI

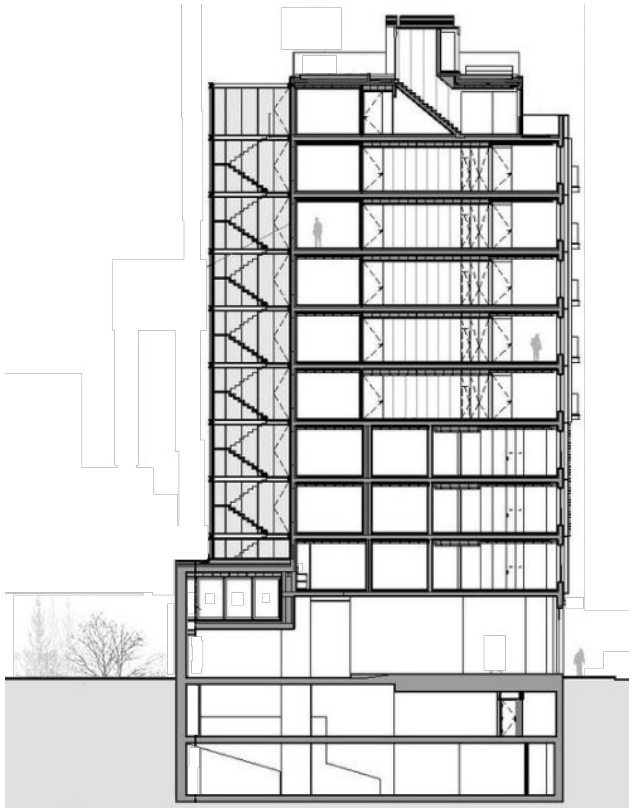
	>=250 empleados y >50M€ facturac.	Entre 50 - 249 empleados y >10M€
AGUA POTABLE	EE	EI
AGUAS RESIDUALES	EE	EI
INFRAESTRUCTURAS DIGITALES	EE	EE
GESTIÓN DE SERVICIOS TIC	EE	EI
ADMINISTRACIÓN PÚBLICA	EE	EE
ESPACIO	EE	EI

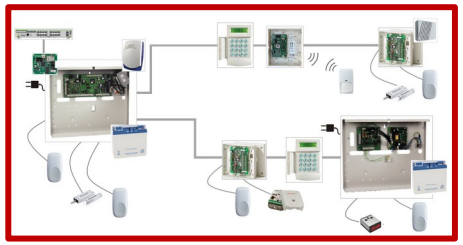
El resto de Sectores Críticos se mantienen como Entidades Importantes, independientemente del número de empleados y la facturación

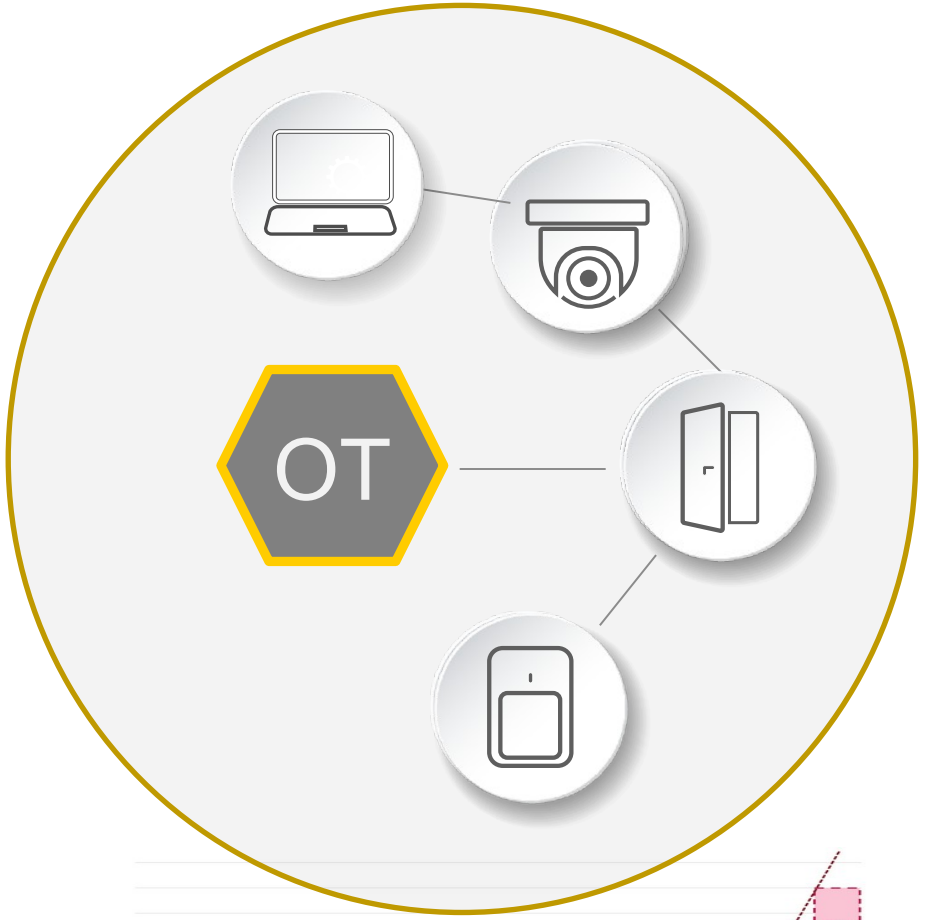
Tecnología de la Información Vs Tecnología Operativa

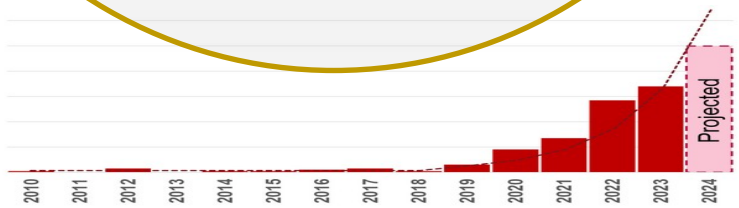


EN LA ELECCIÓN DE EQUIPOS, TENER EN CUENTA REQUERIMIENTOS ESPECÍFICOS PARA EL CUMPLIMIENTO DE NIS2



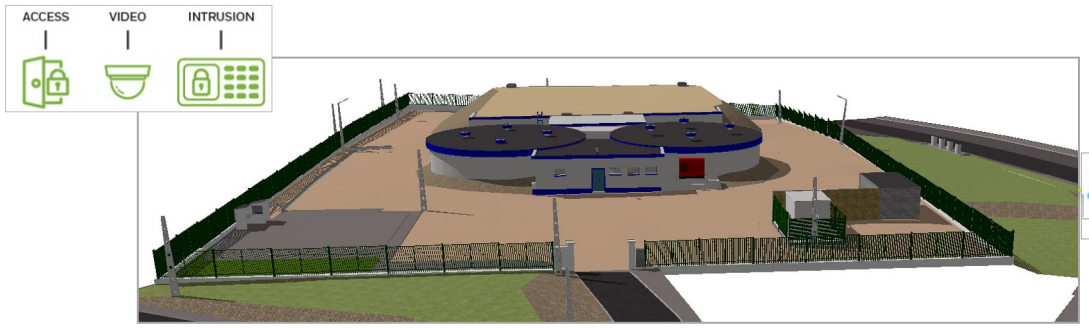


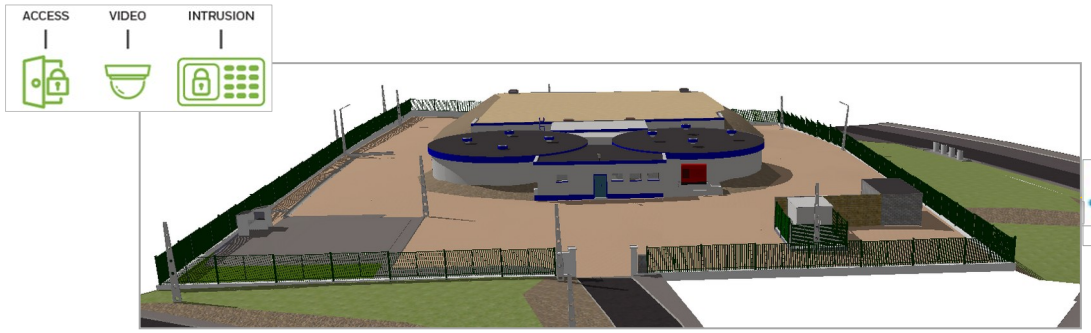




Evolución de los ataques con consecuencias físicas en OT
(Impacto económico – impacto reputacional)

Conexión de sistemas a red corporativa

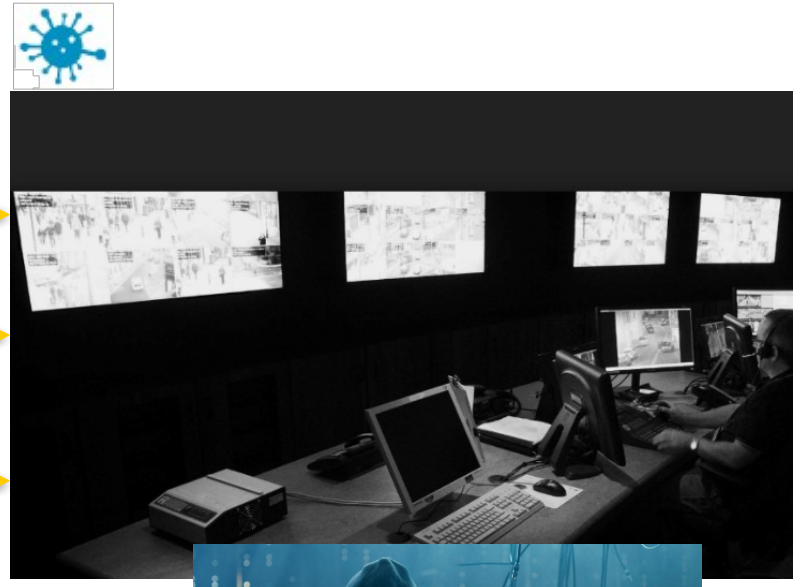




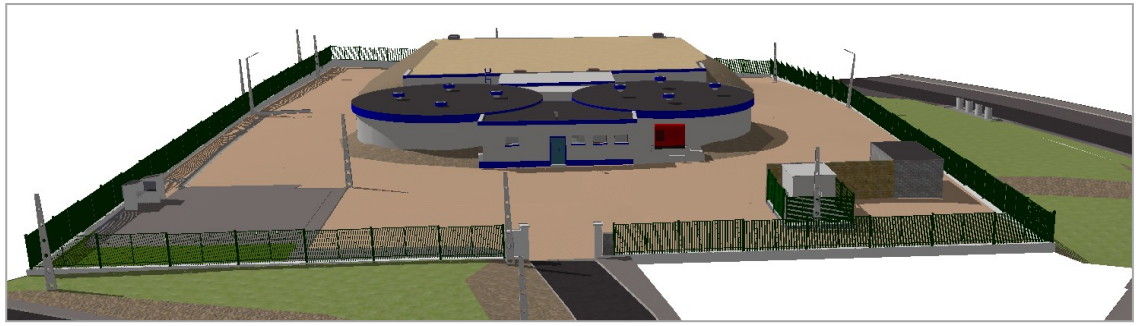
01000001011110000110

01000001011110000110

01000001011110000110



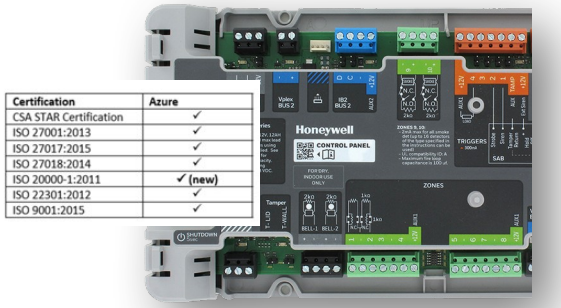
Algunas cuestiones a tener en cuenta en la elección de los equipos (Tecnología Operativa)



CCTV

- Doble tarjeta de red
- Cumplimiento NDAA
- Chipset TPM: cifra y almacena las claves de cifrado necesarias para el cifrado/descifrado de los intercambios de vídeo: datos, streaming y aplicaciones. Elimina las posibles puertas traseras de los NVR vinculadas a debilidades del software, dificultando la suplantación de agentes maliciosos:
  - Firmware firmado y encriptado
    - Encriptación de flujos de vídeo
    - Arranque Seguro
    - Derechos de acceso y conectividd Seguros
    - Encriptación HTTPS

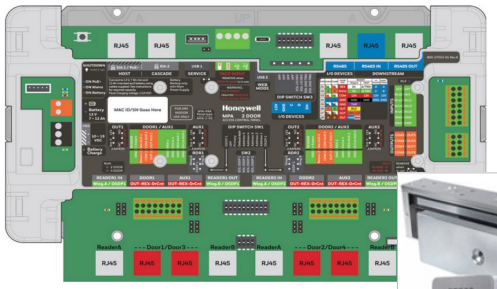
INTRUSIÓN



Certification	Azure
CSA STAR Certification	✓
ISO 27001:2013	✓
ISO 27017:2015	✓
ISO 27018:2014	✓
ISO 20000-1:2011	✓ (new)
ISO 22301:2012	✓
ISO 9001:2015	✓

- Bus de datos encriptado
- Comunicaciones encriptadas con Servicios Cloud
- Comunicaciones encriptadas con C.R.A.

CONTROL DE ACCESOS



- Cifrado de extremo a extremo
- Uso de tarjetas encriptadas (MIFARE Desfire EV2)
- Comunicación encriptada entre panel y lectores (OSDP)
- Autentición de doble o triple factor
- Control de accesos en modo transparente

Algunas cuestiones a tener en cuenta en la elección de los equipos (Tecnología Operativa)

EI – ENTIDAD IMPORTANTE
EE – ENTIDAD ESENCIAL
EC – ENTIDAD CRÍTICA

Directiva (UE) 2022/2555 y algunos ejemplos de Entidades

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

DIRECTIVAS

DIRECTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 14 de diciembre de 2022

relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2)

(Texto pertinente a efectos del EEE)

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 114,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de acto legislativo a los Parlamentos nacionales,

Visto el dictamen del Banco Central Europeo (1),

Visto el dictamen del Comité Económico y Social Europeo (2),

Previa consulta al Comité de las Regiones,

De conformidad con el procedimiento legislativo ordinario (3),

Considerando lo siguiente:

(1) El objetivo de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo (4) era desarrollar las capacidades en materia de ciberseguridad en toda la Unión, reducir las amenazas para los sistemas de redes y de información utilizados para prestar servicios esenciales en sectores fundamentales, y garantizar la continuidad de dichos servicios en caso de incidentes, contribuyendo así a la seguridad de la Unión y al funcionamiento eficaz de su economía y su sociedad.

(2) Desde la entrada en vigor de la Directiva (UE) 2016/1148 se han logrado considerables progresos en el incremento del nivel de ciberresiliencia de la Unión. La revisión de dicha Directiva ha demostrado que ha servido de catalizador del enfoque institucional y normativo relativo a la ciberseguridad en la Unión, preparando el cam cambio significativo de mentalidad. Con ella se ha logrado la realización de marcos nacionales de segu sistemas de redes y de información mediante la definición de estrategias nacionales de seguridad de lo redes y de información, el establecimiento de capacidades nacionales y la aplicación de medidas reg abarcan a las entidades y las infraestructuras esenciales determinadas por cada Estado miembro. A Directiva (UE) 2016/1148 ha propiciado la cooperación a nivel de la Unión mediante el establecimiento del Grupo de Cooperación y de la red de equipos de respuesta a incidentes de seguridad informática. A pesar de es revisión de la Directiva (UE) 2016/1148 ha puesto de manifiesto algunas deficiencias inherentes qu abordar eficazmente los retos actuales y emergentes en el ámbito de la ciberseguridad.

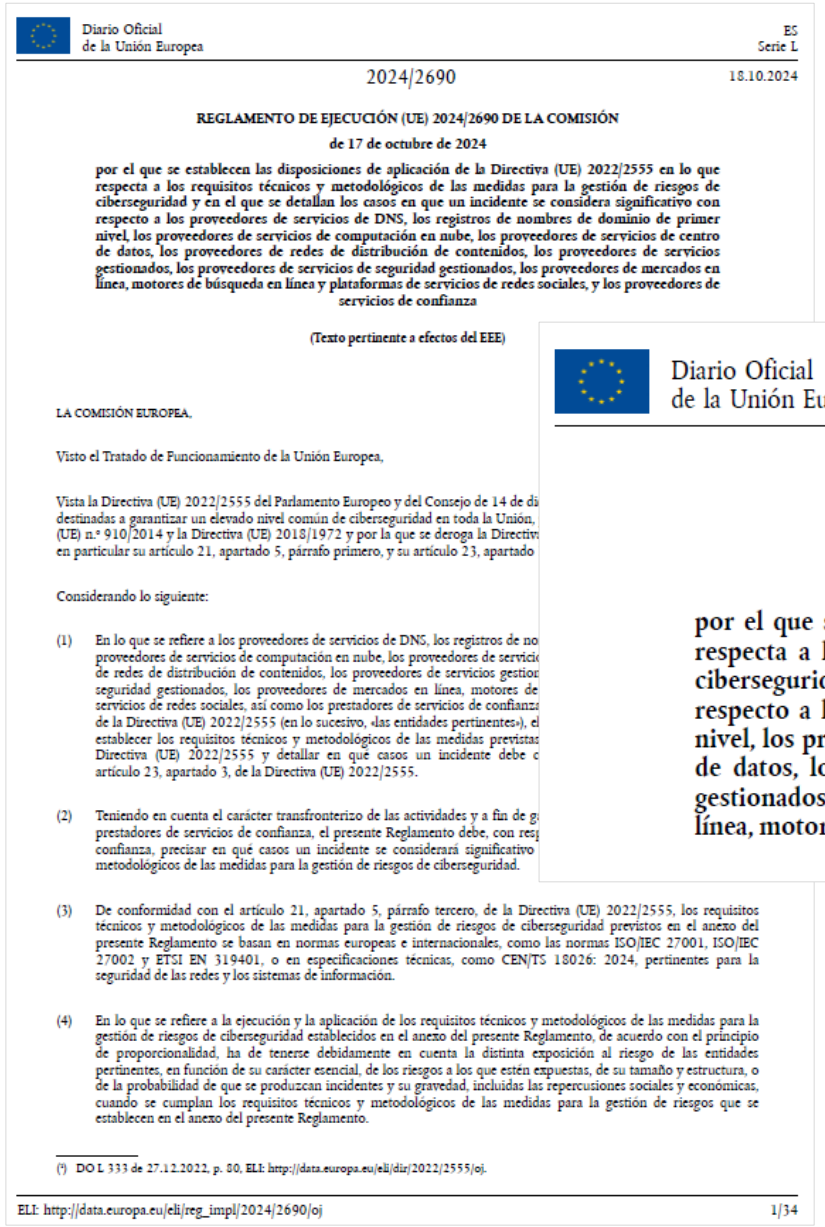
(3) Los sistemas de redes y de información se han convertido en un aspecto crucial del día a día gracias a la la transformación digital y la interconexión de la sociedad, también en los intercambios transfro evolución ha causado una expansión del panorama de las ciberamenazas, con la consiguiente aparici desafíos que requieren respuestas adaptadas, coordinadas e innovadoras en todos los Estados miembro la magnitud, la sofisticación, la frecuencia y los efectos de los incidentes van en aumento y represent amenaza para el funcionamiento de los sistemas de redes y de información. Como consecuencia

(1) DO C 233 de 16.6.2022, p. 22.
(2) DO C 286 de 16.7.2021, p. 170.
(3) Posición del Parlamento Europeo de 10 de noviembre de 2022 (pendiente de publicación en el Diario Oficial) y Decisi de 28 de noviembre de 2022.
(4) Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (DO L 194 de 19.7.2016, p. 1).

Sector	Subsector	Tipo de entidad
2. Transporte	a) Transporte aéreo	— Compañías aéreas, tal como se definen en el artículo 3, punto 4, del Reglamento (CE) n.º 300/2008 utilizadas con fines comerciales
		— Entidades gestoras de aeropuertos, tal como se definen en el artículo 2, punto 2, de la Directiva 2009/12/CE del Parlamento Europeo y del Consejo (6); aeropuertos, tal como se definen en el artículo 2, punto 1, de dicha Directiva, en particular los aeropuertos de la red básica enumerados en el anexo II, sección 2, del Reglamento (UE) n.º 1315/2013 del Parlamento Europeo y del Consejo (7); y entidades que explotan instalaciones anexas dentro de los recintos de los aeropuertos
		— Operadores de control de la gestión del tráfico que prestan servicios de control del tránsito aéreo, tal como se definen en el artículo 2, punto 1, del Reglamento (CE) n.º 549/2004 del Parlamento Europeo y del Consejo (8)
	b) Transporte por ferrocarril	— Administradores de infraestructuras, tal como se definen en el artículo 3, punto 2, de la Directiva 2012/34/UE del Parlamento Europeo y del Consejo (9)
		— Empresas ferroviarias, tal como se definen en el artículo 3, punto 1, de la Directiva 2012/34/UE, incluidos los explotadores de instalaciones de servicio, tal como se definen en el artículo 3, punto 12 de dicha Directiva
	c) Transporte marítimo y fluvial	— Empresas de transporte marítimo, fluvial y de cabotaje, tanto de pasajeros como de mercancías, tal como se definen para el transporte marítimo en el anexo I del Reglamento (CE) n.º 725/2004 del Parlamento Europeo y del Consejo (10), sin incluir los buques particulares explotados por esas empresas
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) — Entidades que fabrican productos farmacéuticos de base y especialidades farmacéuticas a que se refiere la sección C, división 21, de la NACE Rev. 2 — Entidades que fabrican productos sanitarios que se consideran esenciales en situaciones de emergencia de salud pública («lista de productos sanitarios esenciales durante la emergencia de salud pública») en el sentido del artículo 22 del Reglamento (UE) 2022/123 del Parlamento Europeo y del Consejo (21)
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)
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
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

Reglamento de ejecución 17 de Octubre de 2024

https://www.boe.es/doue/2024/2690/L00001-00034.pdf



Diario Oficial
de la Unión Europea

ES
Serie L

2024/2690

18.10.2024

REGLAMENTO DE EJECUCIÓN (UE) 2024/2690 DE LA COMISIÓN

de 17 de octubre de 2024

por el que se establecen las disposiciones de aplicación de la Directiva (UE) 2022/2555 en lo que respecta a los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad y en el que se detallan los casos en que un incidente se considera significativo con respecto a los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de servicios de computación en nube, los proveedores de servicios de centro de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados, los proveedores de servicios de seguridad gestionados, los proveedores de mercados en línea, motores de búsqueda en línea y plataformas de servicios de redes sociales, y los proveedores de servicios de confianza

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Vista la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de di
destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión,
(UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiv
en particular su artículo 21, apartado 5, párrafo primero, y su artículo 23, apartado

Considerando lo siguiente:

(1) En lo que se refiere a los proveedores de servicios de DNS, los registros de no
proveedores de servicios de computación en nube, los proveedores de servici
de redes de distribución de contenidos, los proveedores de servicios gestion
seguridad gestionados, los proveedores de mercados en línea, motores de
servicios de redes sociales, así como los prestadores de servicios de confianz
de la Directiva (UE) 2022/2555 (en lo sucesivo, «las entidades pertinentes»), el
establecer los requisitos técnicos y metodológicos de las medidas previstas
Directiva (UE) 2022/2555 y detallar en qué casos un incidente debe c
artículo 23, apartado 3, de la Directiva (UE) 2022/2555.

(2) Teniendo en cuenta el carácter transfronterizo de las actividades y a fin de g
prestadores de servicios de confianza, el presente Reglamento debe, con res
confianza, precisar en qué casos un incidente se considerará significativo
metodológicos de las medidas para la gestión de riesgos de ciberseguridad.

(3) De conformidad con el artículo 21, apartado 5, párrafo tercero, de la Directiva (UE) 2022/2555, los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad previstos en el anexo del presente Reglamento se basan en normas europeas e internacionales, como las normas ISO/IEC 27001, ISO/IEC 27002 y ETSI EN 319401, o en especificaciones técnicas, como CEN/TS 18026: 2024, pertinentes para la seguridad de las redes y los sistemas de información.

(4) En lo que se refiere a la ejecución y la aplicación de los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad establecidos en el anexo del presente Reglamento, de acuerdo con el principio de proporcionalidad, ha de tenerse debidamente en cuenta la distinta exposición al riesgo de las entidades pertinentes, en función de su carácter esencial, de los riesgos a los que estén expuestas, de su tamaño y estructura, o de la probabilidad de que se produzcan incidentes y su gravedad, incluidas las repercusiones sociales y económicas, cuando se cumplan los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos que se establecen en el anexo del presente Reglamento.

(1) DO L 333 de 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj.

ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj

1/34

Diario Oficial
de la Unión Europea

ES
Serie L

2024/2690

18.10.2024

REGLAMENTO DE EJECUCIÓN (UE) 2024/2690 DE LA COMISIÓN

de 17 de octubre de 2024

por el que se establecen las disposiciones de aplicación de la Directiva (UE) 2022/2555 en lo que respecta a los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad y en el que se detallan los casos en que un incidente se considera significativo con respecto a los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de servicios de computación en nube, los proveedores de servicios de centro de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados, los proveedores de servicios de seguridad gestionados, los proveedores de mercados en línea, motores de búsqueda en línea y plataformas de servicios de redes sociales, y los proveedores de servicios de confianza

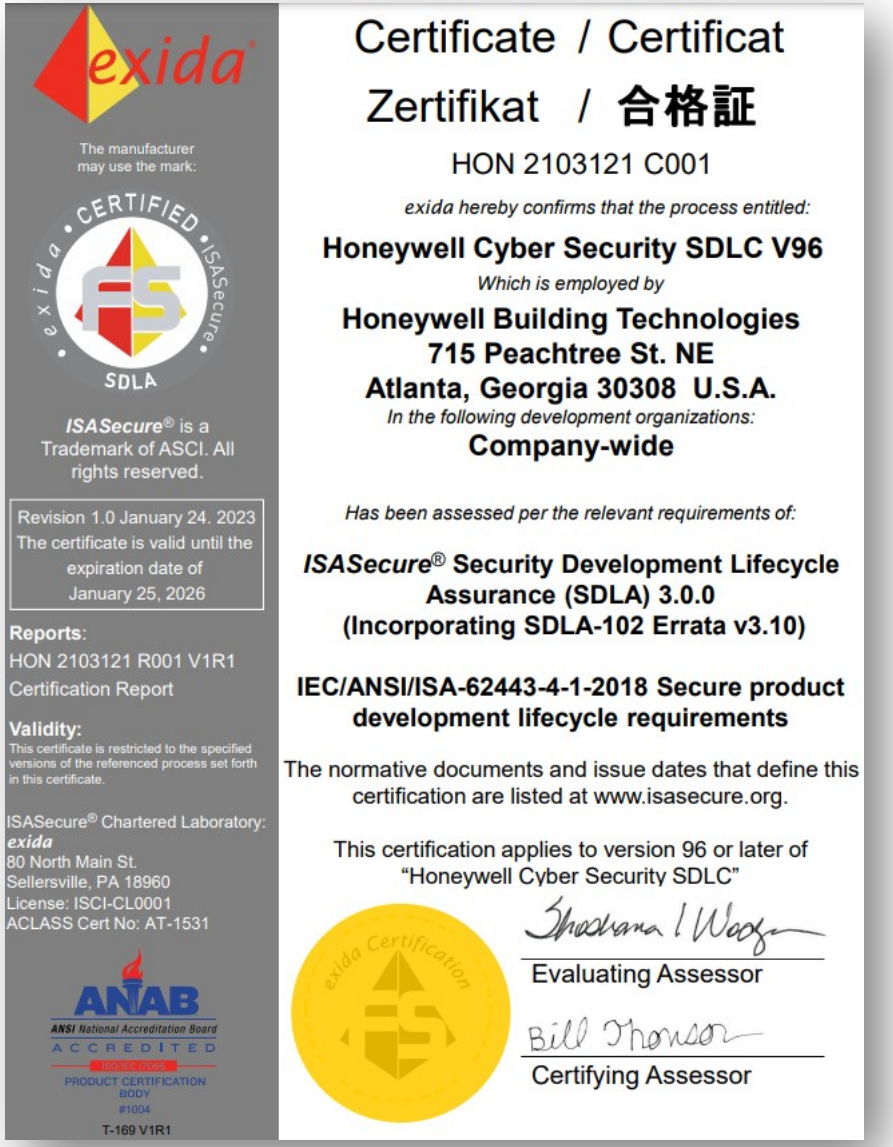
Honeywell | Commercial Security

Las diferentes gamas de productos de Honeywell Commercial Security ofrecen múltiples características y funcionalidades que pueden ayudar a las organizaciones a mejorar su ciberseguridad y facilitar el cumplimiento con la Directiva NIS2, tales como:

- Máxima seguridad gracias a coprocesadores criptográficos.
- Chipsets de cifrado integrados con certificación FIPS/TPM.
- Tipos de cifrado: TLS 1.2, AES 128/256 bits, cifrado punto a punto con OSDP V2, cifrado punto a punto del flujo de vídeo para protección perimetral.
- Conexión Ethernet cifrada y comunicaciones cifradas (HTTPS) con clientes web y App móviles.
- Autenticación multifactor y biometría para seguridad de TI, salas técnicas y de almacenamiento de datos.
- Informes de auditoría y cumplimiento.
- Lectores de control de accesos en modo transparente.
- Trazabilidad de activos de TI.

ISA SECURE SDLA CERTIFIED

- La serie de normas ISA/IEC 62443 define los requisitos y procesos para implantar y mantener sistemas de automatización y control industrial (IACS) electrónicamente seguros.
- La certificación ISA/IEC 62443-4-1 subraya el compromiso de seguir las mejores prácticas y normas en el desarrollo de productos seguros y Ciberresistentes. La implantación ofrece un importante nivel de garantía de que los productos desarrollados son resistentes a las Ciberamenazas.
- Honeywell es una de las 29 empresas que han obtenido esta certificación, lo que demuestra aún más su compromiso con la protección del mundo en el que trabajamos y vivimos.


exida

The manufacturer may use the mark:

exida CERTIFIED ISASecure SDLA

ISASecure® is a Trademark of ASCI. All rights reserved.

Revision 1.0 January 24. 2023
The certificate is valid until the expiration date of January 25, 2026

Reports:
HON 2103121 R001 V1R1
Certification Report

Validity:
This certificate is restricted to the specified versions of the referenced process set forth in this certificate.

ISASecure® Chartered Laboratory:
exida
80 North Main St.
Sellersville, PA 18960
License: ISCI-CL0001
ACLASS Cert No: AT-1531

ANAB
ANSI National Accreditation Board
ACCREDITED
ISO/IEC 17065
PRODUCT CERTIFICATION BODY
#1004

T-169 V1R1

Certificate / Certificat
Zertifikat / 合格証

HON 2103121 C001

exida hereby confirms that the process entitled:

Honeywell Cyber Security SDLC V96

Which is employed by

Honeywell Building Technologies
715 Peachtree St. NE
Atlanta, Georgia 30308 U.S.A.

In the following development organizations:

Company-wide

Has been assessed per the relevant requirements of:

***ISASecure*® Security Development Lifecycle Assurance (SDLA) 3.0.0**
(Incorporating SDLA-102 Errata v3.10)

IEC/ANSI/ISA-62443-4-1-2018 Secure product development lifecycle requirements

The normative documents and issue dates that define this certification are listed at www.isasecure.org.

This certification applies to version 96 or later of "Honeywell Cyber Security SDLC"

exida Certification

Evaluating Assessor

Certifying Assessor

Concepto Cloud según requerimientos NIS2

- ✓ **USUARIO FINAL**
- ✓ **SERVICIOS DE SEGURIDAD**
- ✓ **INSTALACIÓN Y MANTENIMIENTO**
- ✓ **CENTRAL RECEPTORA DE ALARMAS**

- Backup en la recepción y gestión de alarmas.
- **UNE-EN 50518:2020***, donde se establece que se requiere un plan de contingencia.

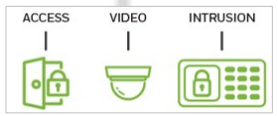
SERVICIOS CLOUD
CONTROL Y GESTIÓN A TRAVÉS DE SERVICIOS WEB

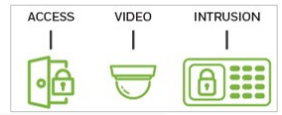
Líder en Ciberseguridad

Todos los datos, incluido el vídeo, con cifrado TLS 1.2+. Cifrado AES de 256 bits entre los paneles y el host
Cumplimiento GDPR

COMUNICACIONES CIFRADAS DE EXTREMO A EXTREMO

CENTRAL RECEPTORA DE ALARMAS EMPRESAS DE INSTALACÍÓN Y MANTENIMIENTO





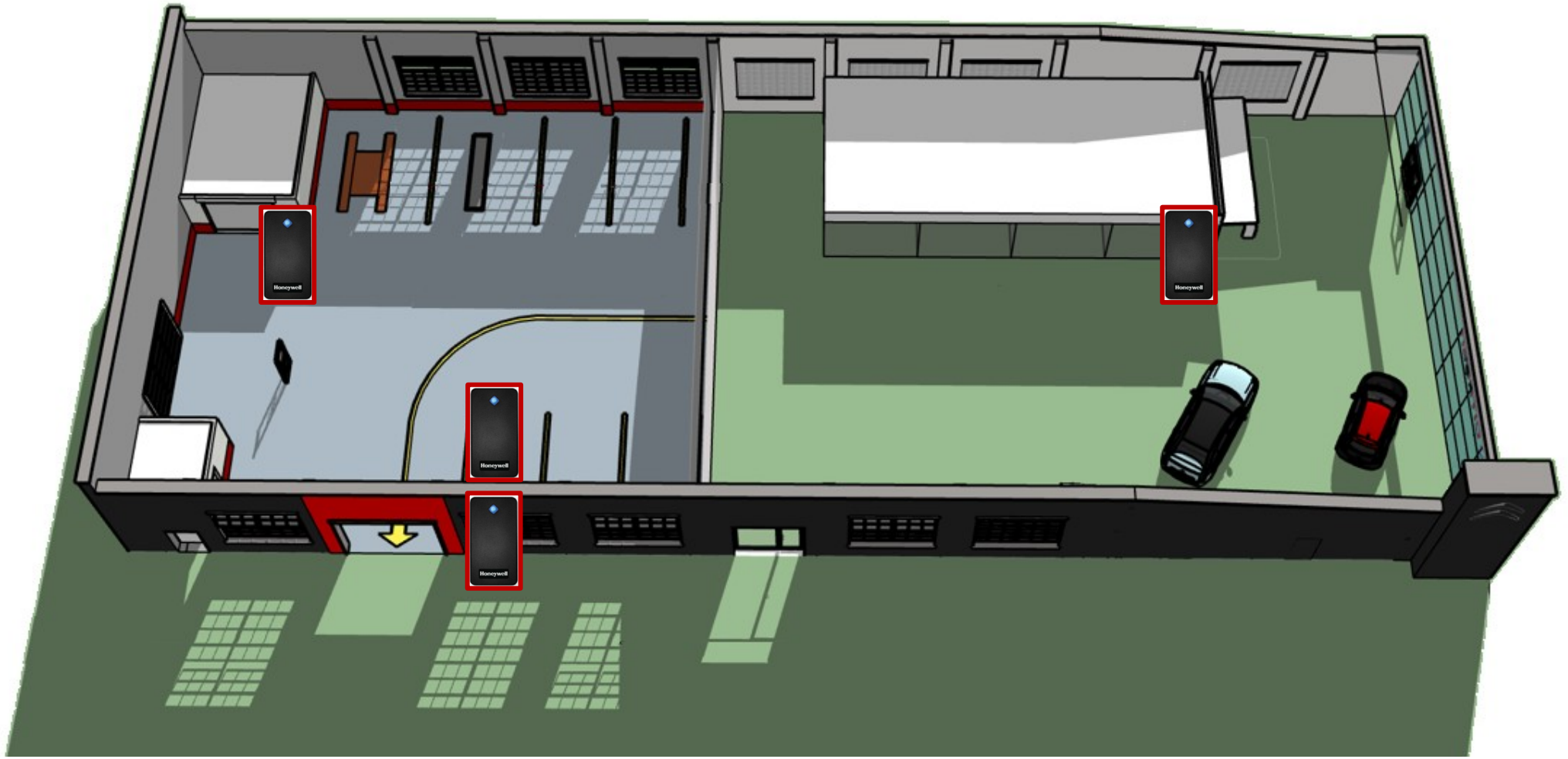
ACTUALIZACIONES AUTOMÁTICAS DE FIRMWARE:
NUEVAS FUNCIONES, MEJORAS EN CIBERSEGURIDAD, GARANTÍA DE QUE EL SOFTWARE Y EL FIRMWARE SE MANTIENEN ACTUALIZADOS

EJEMPLO CONTROL INSTALACIONES A TRAVÉS DE MAXPRO CLOUD

Honeywell

Introducción al diseño de sistemas de Control de Accesos

Ejemplo estudio de caso



Medidas de seguridad y encriptación segura de transmisión

X Proximidad (125Kz)

X Mifare Classic (13,56Mhz)

√ Mifare Desfire EV2 (13,56Mhz)

√ Mobile Credential NFC

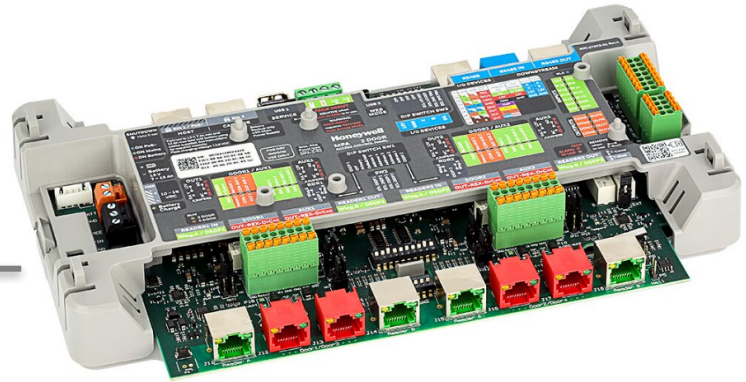
LECTORES – OPCIONES
(acerca de los lectores de proximidad)

PROX. 125Khz
WIEGAND

PROX.13,56Mhz
WIEGAND – OSDP

WIEGAND Vs OSDP:

0100000101111000000110



Wiegand

- **Comunicación no encriptada**
- **Comunicación unidireccional**
- 8 cables para todas las funciones
- Configuración lectores en entrada y salida: un cable para cada lector
- Comunicación saboteable si se acede al cableado

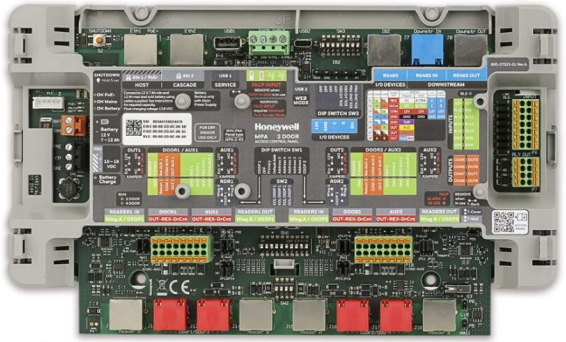
OSDP™

- **Comunicación encriptada AES-128 y supervisada**
- **Comunicación bidireccional** entre el lector y el panel (protección contra el sabotaje)
- 2 cables de alimentación + 2 de datos
- Configuración lectores en entrada y salida: conectados en paralelo

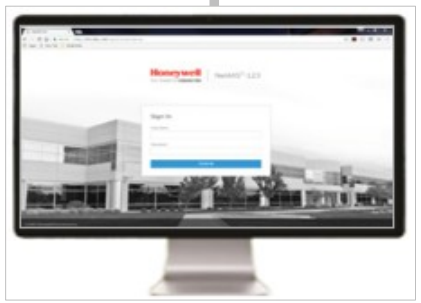
Medidas de seguridad y encriptación segura de transmisión

AES 128 bits (OSDP:V2)

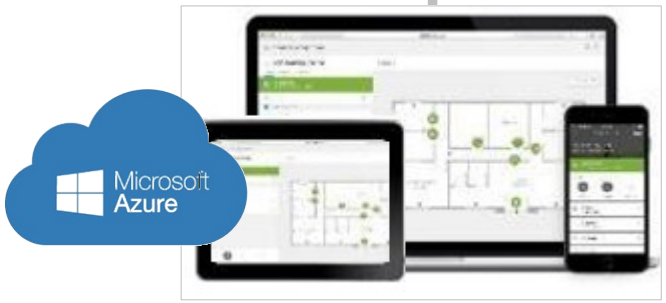
PANEL DE CONTROL DE ACCESOS



Comunicación cifrada AES de 256 bits



WEB SERVER



MAXPRO CLOUD

WINPAK
Software de Integración

EJEMPLO PANELES MAXPRO ACCESS

UNE – EN 60839-11-2. Grados de seguridad de los sistemas

- Los niveles de los grados de seguridad se determinan en función de los bienes que requieran protección y métodos de ataque utilizados por personas que intentan evitar el sistema de control de accesos.
  - Grado 1: Los bienes tiene un valor limitado y probablemente los adversarios abandonarán la idea del ataque cuando tengan que enfrentarse a una resistencia mínima.
  - Grado 2: Los bienes tiene un valor mayor y probablemente los adversarios abandonarán la idea de finalizar con éxito su acción cuando descubran que pueden ser detectados.
  - Grado 3: Los bienes tiene un alto valor y los adversarios pueden abandonar la idea de finalizar con éxito su acción cuando descubran que pueden ser identificados y capturados.
  - Grado 4: Los bienes tiene un valor muy alto y los adversarios pueden abandonar la idea de finalizar con éxito su acción cuando descubran que pueden ser identificados y capturados.

NIS2 DIRECTIVE COMPLIANT

Gado	1	2	3	4
Nivel de riesgo	Bajo	Bajo a medio	Medio a alto	Alto
Aplicación	Aspectos organizativos, protección de bienes de bajo valor	Aspectos organizativos, protección de bienes de valor bajo a medio	Aspectos organizativos, protección de bienes de valor medio a alto	Protección principalmente de bienes comerciales de muy alto valor o de infraestructuras críticas
Habilidades y conocimientos de los agresores	Escasos conocimientos y habilidades en relación con los sistemas de control de accesos. Desconocimiento de dispositivos de acceso electrónicos y de las tecnologías de la información. Escasos recursos económicos para llevar acabo ataques	Habilidades y conocimientos medios del sistema electrónico de control de accesos. Escasos conocimientos sobre dispositivos de acceso electrónicos y de las tecnologías de la información. Disponibilidad de recursos económicos bajos a medios para llevar a cabo ataques	Habilidades y conocimientos altos del sistema electrónico de control de accesos. Conocimientos medios sobre dispositivos de acceso electrónicos y de las tecnologías de la información. Disponibilidad de recursos económicos medios para llevar a cabo ataques	Habilidades y conocimientos muy altos del sistema electrónico de control de accesos. Conocimientos altos sobre dispositivos de acceso electrónicos y de las tecnologías de la información. Disponibilidad de recursos económicos altos para llevar a cabo ataques
Ejemplos	Hoteles	Oficinas comerciales, pequeños negocios	Sector industrial, administrativo y financiero	Zonas altamente sensibles (instalaciones militares, centros de gobierno, centros de I+D, zonas de producción críticas)

UNE – EN 60839-11-2. Guía de aplicación, disposición típica de los componentes

Gestión y conexión con otros sistemas

Puntos de acceso:
- Accionamientos
- Sensores

Unidad de control de acceso (ACU)

Alimentación (principal y de reserva)

Interfaz de usuario

Dispositivo de petición de salida (REX)
Opción LECTOR EN LA SALIDA

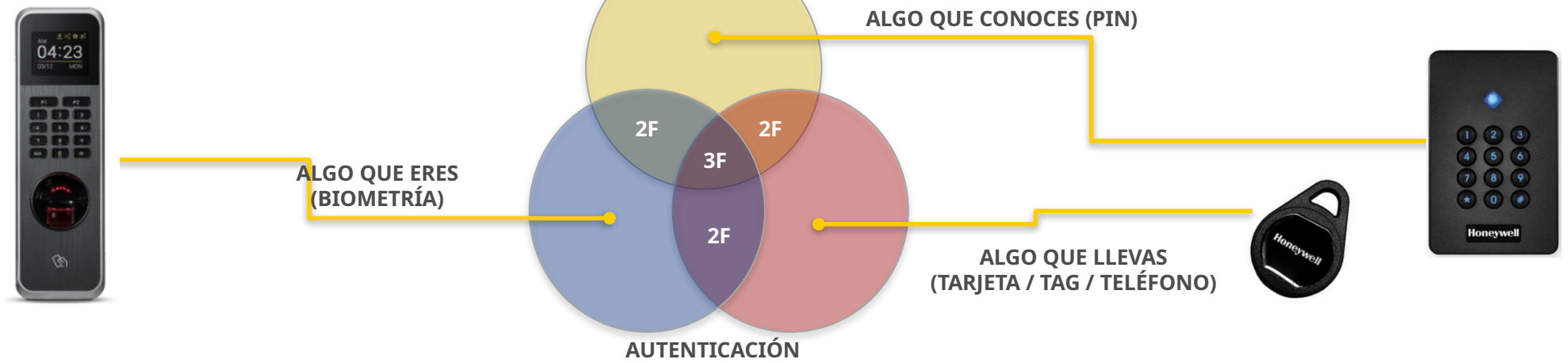
Modo de funcionamiento según grado

Grado	Modo funcionamiento	Tecnología Prox.
1	Sistema autónomo en el que la autenticación de credenciales y el control de la concesión de acceso es aplicable a una sola puerta. Se podrá utilizar código PIN o dispositivo de proximidad (tarjeta, TAG, teléfono)	Proximidad & Mifare Classics
2	Sistema on-line en el que todos los puntos de acceso están conectados a uno o varios controladores que registran los eventos y llevan a cabo el proceso de validación. Se podrá utlizar código PIN o dispositivo de proximidad (tarjeta, TAG, teléfono). Los eventos podrán ser recibidos, en tiempo real, en un software de monitorización.	Mifare Classic
3	Sistema on-line en el que todos los puntos de acceso están conectados a uno a varios controladores que registran los eventos y llevan a cabo el proceso de validación. Utilizando Autenticación de Doble Factor, o simple utilizando biometría. Los eventos podrán ser recibidos, en tiempo real, en un software de monitorización.	Mifare DESFIRE
4	Sistema on-line en el que todos los puntos de acceso están conectados a un controlador central que registra los eventos y lleva a cabo el proceso de validación. Utilizando Autenticación de Doble Factor (o más), uno de los cuales debería ser utilizando biometría. Los eventos podrán recibidos, en tiempo real, en un software de monitorización.	Mifare DESFIRE

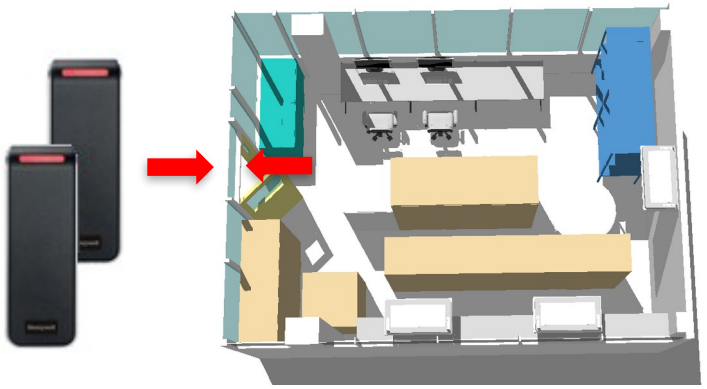
NIS2 DIRECTIVE COMPLIANT

Tecnología PROX: Proximidad - 125Khz / Mifare - 13,56Mhz

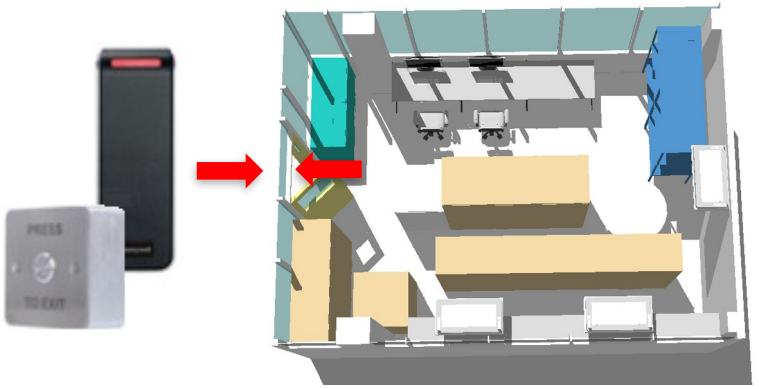
La calificación aplicada a cada punto puede aumentar con el tiempo en función de las necesidades. Ejemplo: lectura de tarjeta sólo durante las horas de oficina y tarjeta y código PIN fuera de horas.



Opciones para el control de una puerta



Lectores en entrada y salida



Lector en entrada, pulsador en salida

Requisitos de la interfaz del punto de acceso	Grado			
	1	2	3	4
Proporcionar control de acceso para entrada en una zona protegida	Obligatorio	Obligatorio	Obligatorio	Obligatorio
Proporcionar control de acceso para salida desde una zona protegida	Opcional	Obligatorio	Obligatorio	Obligatorio
Funciones de anti - retorno (antipassback)				
Anti - retorno blando	Opcional	Opcional	Opcional	Opcional
Anti - retorno duro	Opcional	Opcional	Obligatorio	Obligatorio

Anti-retorno: Se requiere validación del usuario a la hora de salir de una zona de seguridad controlada para ser capaz de volver a entrar y viceversa
Anti-retorno blando: Tras conceder acceso genera sólo una alerta tras la infracción de las normas anti-retorno
Anti-retorno duro: Genera una alerta y deniega el nuevo acceso a una credencial particular tras la infracción de las normas anti-retorno

Especificaciones para el control del punto de acceso

Uso de contacto magnético			
Grado 1	**Grado 2**	**Grado 3**	**Grado 4**
Opcional	Obligatorio		

Grado
1
2
3
4

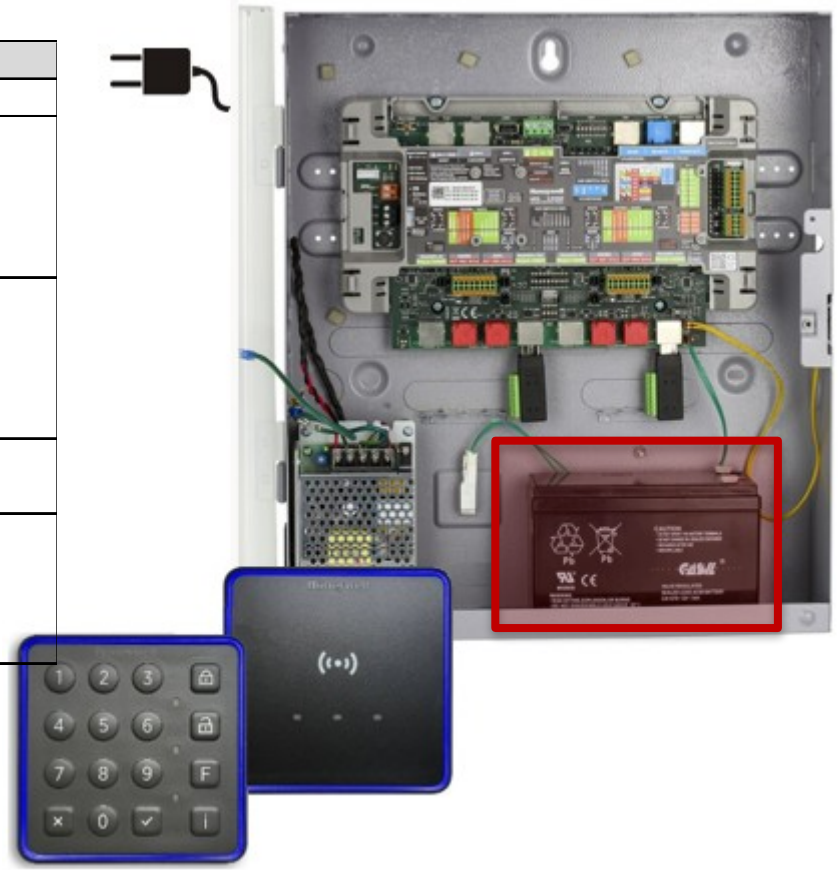
Fuerza de retención	
kN	**Kilos**
3kN	306
5kN	509
7kN	713
>=10kN	1020

Requisitos de alimentación eléctrica

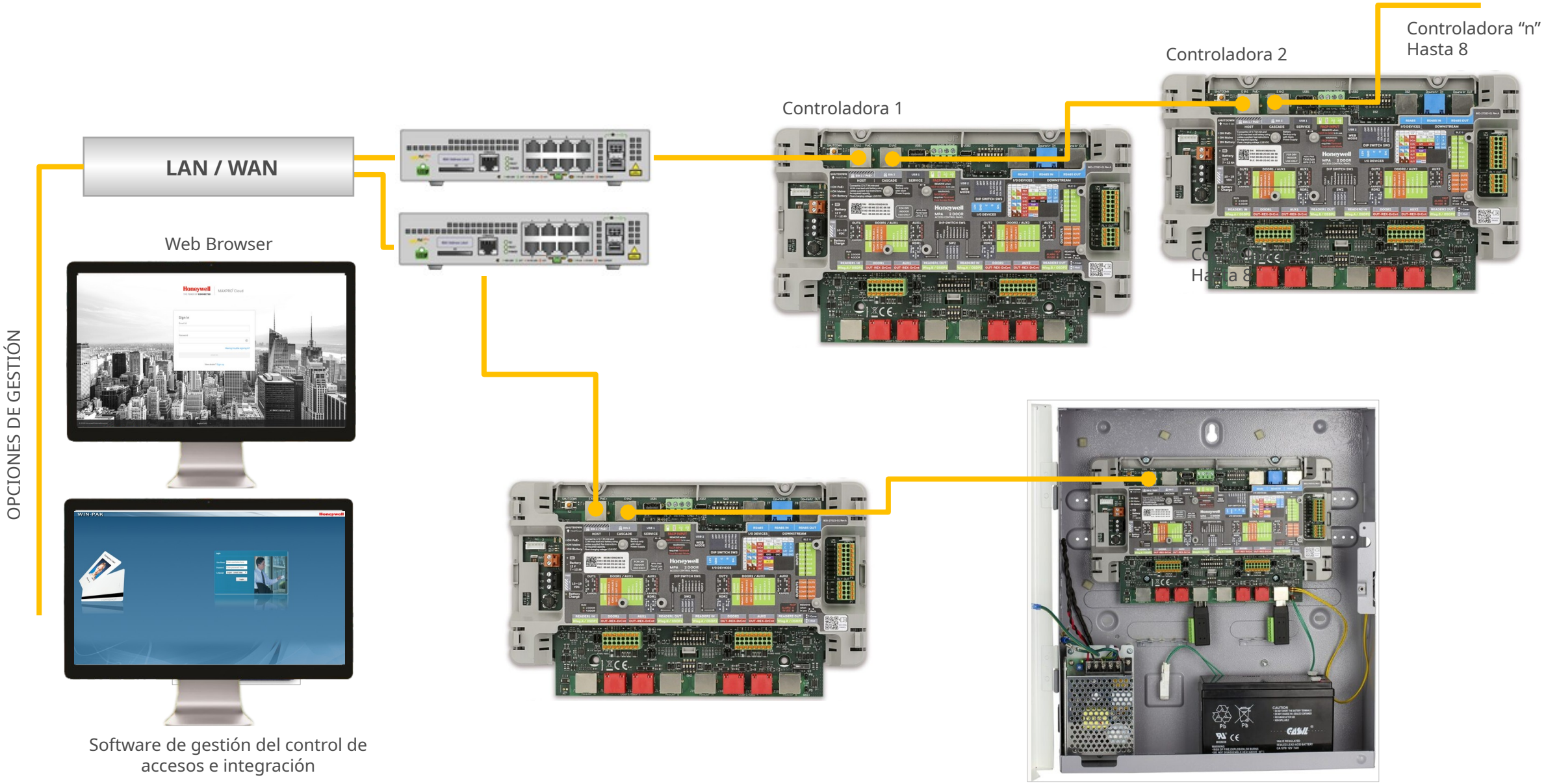
	Requisitos de alimentación eléctrica	Asignación de grado			
		1	2	3	4
1	La unidad de control de acceso debe disponer de fuente de enegía de reserva capaz de alimentar la unidad y sus accesorios en condición de plena carga especificada para el periodo de tiempo indicado. (Las condiciones de carga no incluyen la consola de supervisión o los actuadores del punto de acceso).	OP	OP	2 h	4 h
2	Tras un fallo prolongado de la fuente de alimentación primaria (se produjo un apagado del sistema) y el restablecimiento de la corriente, las baterías recargables se deben recargar al 80% de la capacidad asignada en un plazo de 14 horas y al 100% de la capacidad asignada en un plazo de 72 horas.	M	M	M	M
3	La perdida de la alimentación primaria o el restablecimiento no debe afectar negativamente al funcionamiento normal del sistema	OP	OP	M	M
4	Si se proporciona una fuente de energía de reserva deben adoptarse disposiciones para supervisar las siguientes condiciones: el nivel de baja tensión y ninguna batería presente (la anunciación común individual para ambas condiciones es aceptable	OP	OP	M	M

OP - Opcional / M - Obligatorio

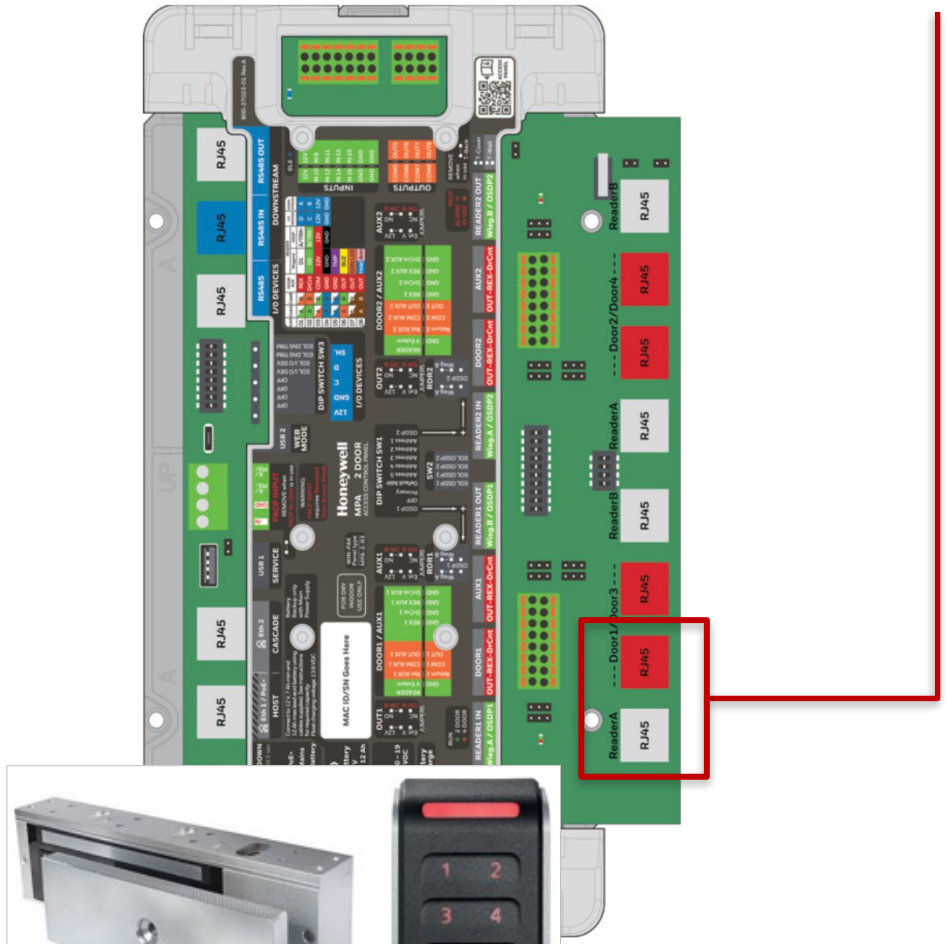
Controladora MAXPRO Access

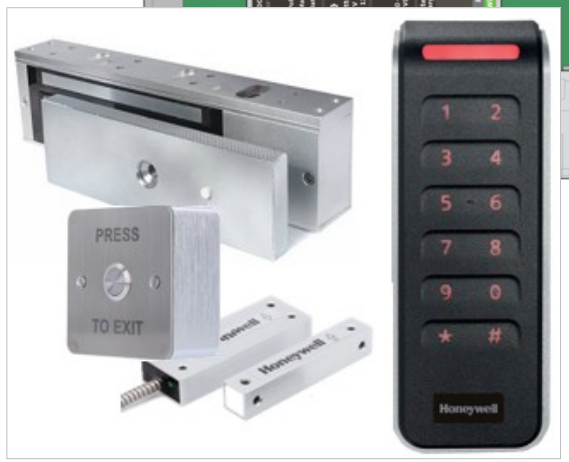


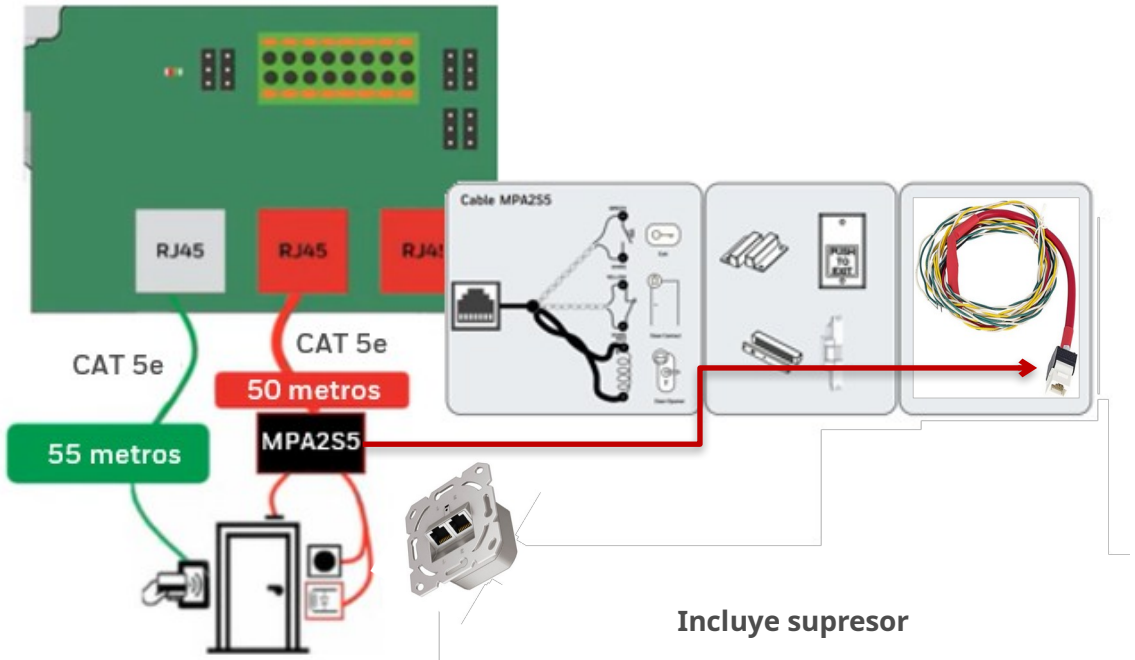
Requisitos de alimentación eléctrica



Ejemplo de cableado a especificar (MAXPRO Access)







Incluye supresor

Secc cable	Lector	Consumo dispositivo desbloqueo		
		200mA	375mA	500mA
AWG24	55	50	25	20
AWG23	70	60	32	25
AWG22	86	76	40	31
AWG20	142	121	64	49
AWG18	221	191	102	76

Distancias estimadas (metros)

Ejemplo de cableado a especificar (MAXPRO Access)