COMISIÓN DE SEGURIDAD PRIVADA DE EXTREMADURA
JORNADAS DE CIBERSEGURIDAD

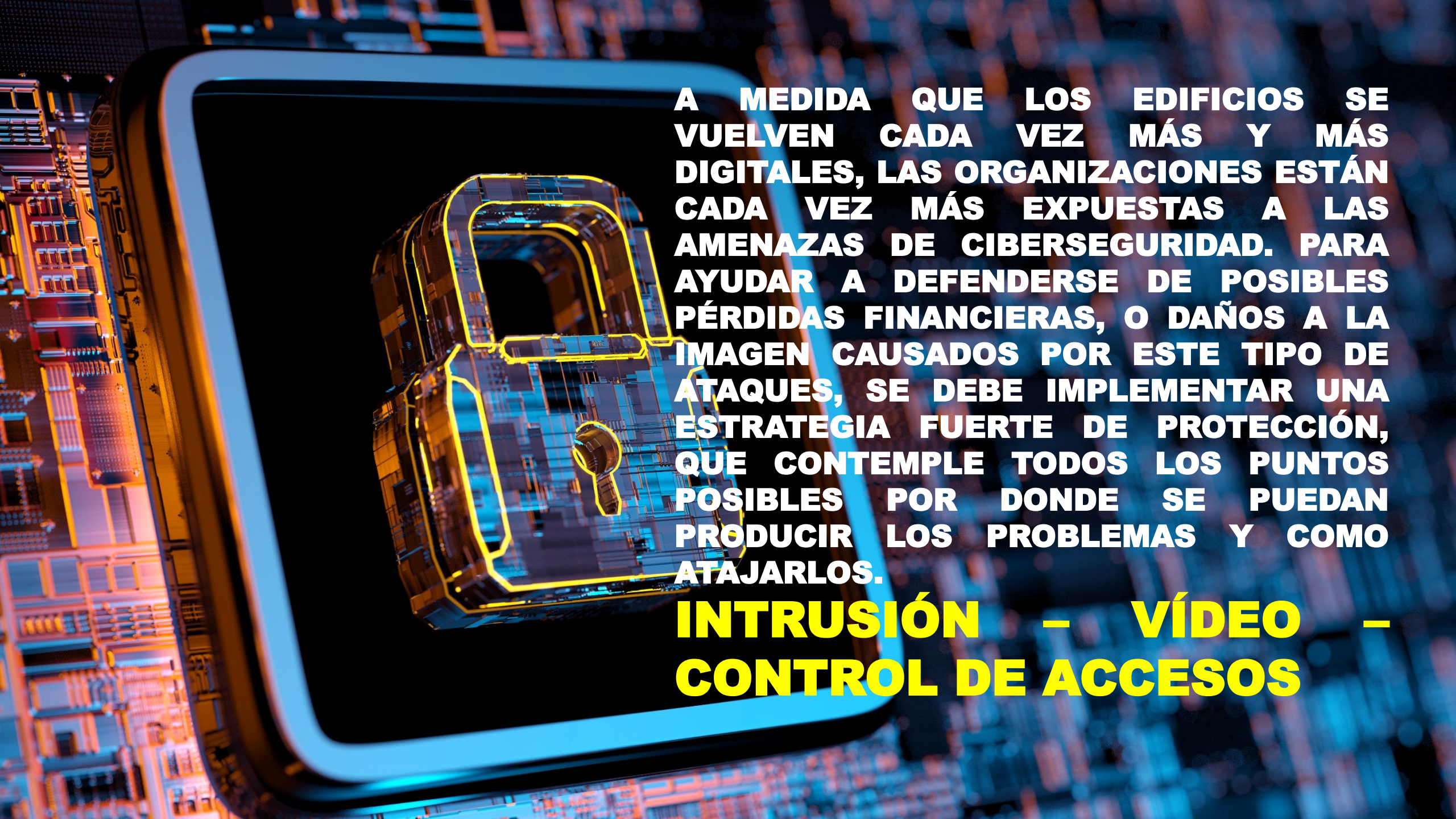
Diciembre 2022

CUESTIONES SOBRE CIBERSEGURIDAD

A TENER EN CUENTA EN LA ELECCIÓN DE EQUIPOS DE SEGURIDAD ELECTRÓNICA

Honeywell

Juan José Nadales Román
juan.jose.nadales@honeywell.com
616 792 016

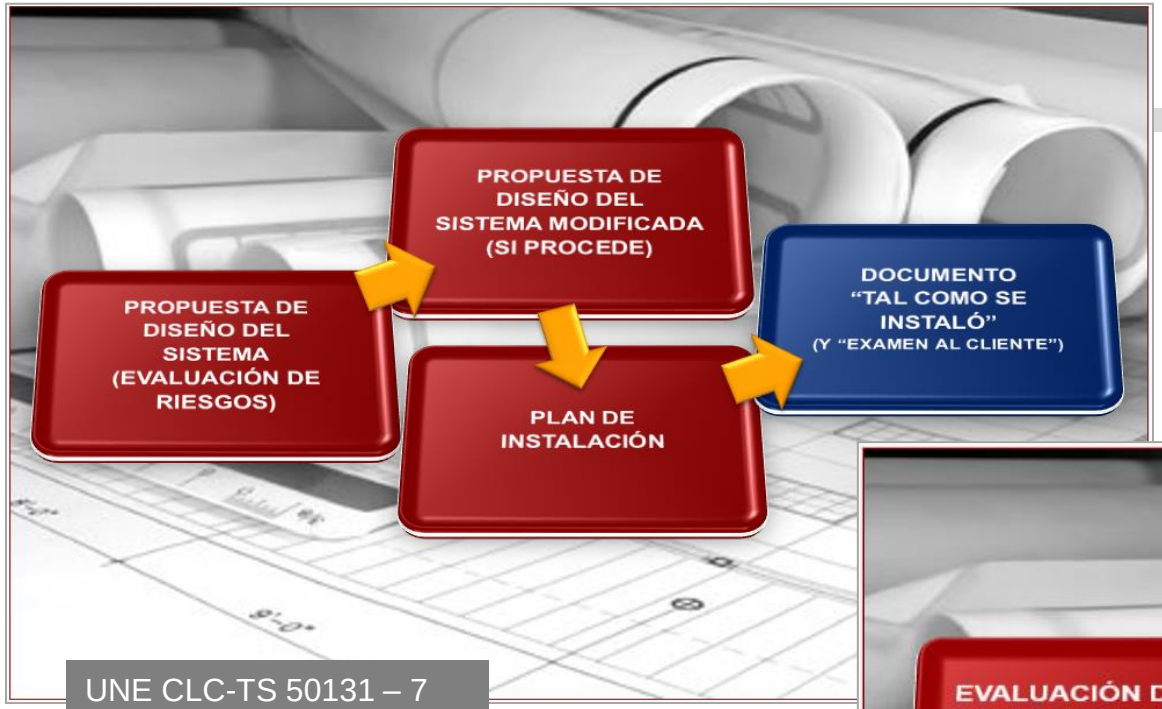


A MEDIDA QUE LOS EDIFICIOS SE VUELVEN CADA VEZ MÁS Y MÁS DIGITALES, LAS ORGANIZACIONES ESTÁN CADA VEZ MÁS EXPUESTAS A LAS AMENAZAS DE CIBERSEGURIDAD. PARA AYUDAR A DEFENDERSE DE POSIBLES PÉRDIDAS FINANCIERAS, O DAÑOS A LA IMAGEN CAUSADOS POR ESTE TIPO DE ATAQUES, SE DEBE IMPLEMENTAR UNA ESTRATEGIA FUERTE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

INTRUSIÓN – VÍDEO – CONTROL DE ACCESOS

PROTECCIÓN ANTE EL ATAQUE FÍSICO

DISEÑO DE INSTALACIONES DE SEGURIDAD



UNE CLC-TS 50131 – 7
(Sistemas contra intrusión)


BOLETÍN OFICIAL DEL ESTADO
Núm. 42 Viernes 18 de febrero de 2011 Sec. I. Pág. 18328

Tipo	Número	Año	Denominación
UNE-CLC/TS	50131-7	2005 V2	Sistemas de alarma. Sistemas de alarma de intrusión. Parte 7: Guía de aplicación.
UNE-EN	50132-1.	2010	Sistemas de alarma. Sistemas de vigilancia CCTV para uso en aplicaciones de seguridad. Parte 1: Requisitos del sistema.
UNE-EN	50132-2-1.	1998	Sistemas de alarma. Sistemas de vigilancia CCTV para uso en aplicaciones de seguridad. Parte 2-1: Cámaras en blanco y negro.
UNE-EN	50132-4-1.	2002	Sistemas de alarma. Sistemas de vigilancia CCTV para uso en aplicaciones de seguridad. Parte 4-1: Monitores en blanco y negro.
UNE-EN	50132-5.	2002	Sistemas de alarma. Sistemas de vigilancia CCTV para uso en aplicaciones de seguridad. Parte 5: Transmisión de vídeo.
UNE-EN	50132-7 CORR.	2004	Sistemas de alarma - Sistemas de vigilancia CCTV para uso en aplicaciones de seguridad. Parte 7: Guía de aplicación.
UNE-EN	50132-7.	1997	Sistemas de alarma. Sistemas de vigilancia CCTV para uso en aplicaciones de seguridad. Parte 7: Guía de aplicación.
UNE-EN	50133-1 CORR.	1998	Sistemas de alarma. Sistemas de control de accesos de uso en las aplicaciones de seguridad. Parte 1: Requisitos de los sistemas.
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	50133-1.	1998	Sistemas de alarma. Sistemas de control de accesos de uso en las aplicaciones de seguridad. Parte 1: Requisitos de los sistemas.
UNE-EN	50133-2-1.	2001	Sistemas de alarma. Sistemas de control de accesos de uso en las aplicaciones de seguridad. Parte 2-1: Requisitos generales de los componentes.
UNE-EN	50133-7.	2000	Sistemas de alarma. Sistemas de control de accesos de uso en las aplicaciones de seguridad. Parte 7: Guía de aplicación.
UNE-CLC/TS	50134-7.	2005	Sistemas de alarma. Sistemas de alarma social. Parte 7: Guía de aplicación.
UNE-EN	50134-1.	2003	Sistemas de alarma. Sistemas de alarma social. Parte 1: Requisitos del sistema.
UNE-EN	50134-2.	2000	Sistemas de alarma. Sistemas de alarma social. Parte 2: Dispositivos de activación.
UNE-EN	50134-3.	2002	Sistemas de alarma. Sistemas de alarma social. Parte 3: Unidad local y controlador.
UNE-EN	50134-5.	2005	Sistemas de alarma. Sistemas de alarma social. Parte 5: Interconexiones y comunicaciones.
UNE-EN	50136-1-1/A1	2002	Sistemas de alarma. Sistemas y equipos de transmisión de alarma. Parte 1-1: Requisitos generales para sistemas de transmisión de alarma.

UNE-EN 62676 – 4
(Sistemas de videovigilancia)

Contemplar el Ciberataque en los Análisis de Riesgos

CUESTIONES SOBRE CIBERSEGURIDAD

Sistemas de Videovigilancia

Honeywell

DISEÑO DE INSTALACIONES DE CCTV

EN BASE A ÓRDENES MINISTERIALES Y UNE-EN 62676:4

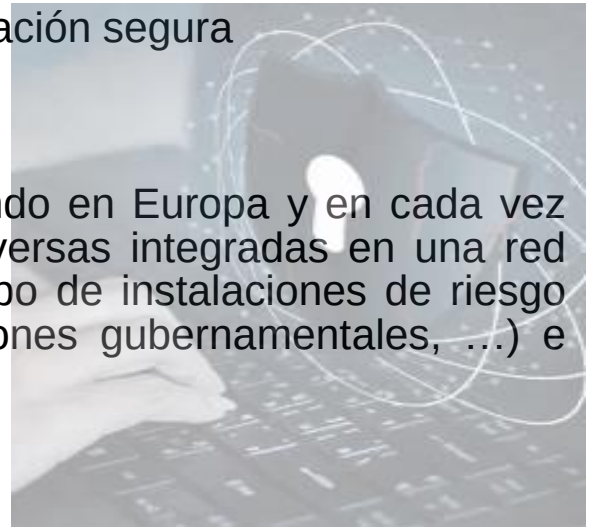
UBICACIÓN "BLANCO"	ALTO	MEDIO	BAJO
Pasillos	Observar - 6 fps	Observar - 6 fps	Observar - 2 fps
Cajero automático	Identificar, 12,5 fps	Identificar - 6 fps	Identificar - 6 fps
Zona de bar	Observar - 12,5 fps	Observar - 6 fps	Observar - 6 fps
Zonas de contenedores de basura	Reconocer - 6 fps	Observar - 6 fps	Observar - 6 fps
Aparcamiento, acceso de vehículos	VRN - 12,5 fps	VRN - 12,5 fps	VRN - 12,5 fps
	Observar + PTZ - 6 fps	Detectar + PTZ - 6 fps	Observar - 6 fps
	Reconocer - 6 fps	Observar - 6 fps	Observar - 2 fps
	Identificar, 12,5 fps	Identificar - 6 fps	Identificar - 6 fps
	Observar + PTZ - 12,5 fps	Observar + PTZ - 6 fps	Observar - 2 fps
es	Observar - 6 fps	Observar - 6 fps	Observar - 6 fps
	Reconocer - 6 fps	Observar - 6 fps	Observar - 6 fps
	Observar - 6 fps	Observar -	
	Identificar - 12,5 fps	Identificar -	
	Identificar - 12,5 fps	Identificar -	
	Observar + PTZ - 12,5 fps	Observar -	
	Reconocer - 12,5 fps	Observar -	
Artículos de alto valor	Reconocer - 12,5 fps	Reconocer	
Interior del ascensor	Reconocer - 6 fps	Reconocer	
Muelle de carga	Reconocer - 6 fps	Observar -	
Perímetro	Detectar - 2 fps	Detectar -	
Cabina de teléfono	Observar - 6 fps	Observar - 6 fps	Observar - 2 fps
Zona estéril	Detectar - 2 fps	Detectar - 2 fps	Detectar - 6 fps
Almacén	Reconocer - 12,5 fps	Observar - 6 fps	Observar - 6 fps
Parada de taxis	Observar + PTZ - 6 fps	Observar + PTZ - 6 fps	Observar - 6 fps
Cajas registradoras	Reconocer - 12,5 fps	Reconocer - 6 fps	Observar - 6 fps
Acceso a los baños	Reconocer - 6 fps	Observar - 6 fps	Observar - 2 fps

XO Storage Calculator rev.: 2.0						Results		
Cameras Recording (24/7)	Quantity	Image Resolution	Image Complexity and Motion	Number of Images Per Second	Days of online storage	Network data transfer	Storage capacity required (24/7 recording)	Storage Bandwidth
H.264	SET	SELECT	SELECT	SET	SET	Megabit/sec	Gigabyte	Megabyte/sec
Type 1	10	8Mpixel	Medium	25	15	158,40	25701,92	20,31
Type 2	0	CIF	Medium	0	0	0,00	0,00	0,00
Type 3	0	CIF	Medium	0	0	0,00	0,00	0,00
Type 4	0	CIF	Medium	0	0	0,00	0,00	0,00
Type 5	0	CIF	Medium	0	0	0,00	0,00	0,00
Type 6	0	CIF	Medium	0	0	0,00	0,00	0,00
Type 7	0	CIF	Medium	0	0	0,00	0,00	0,00
Type 8	0	CIF	Medium	0	0	0,00	0,00	0,00
Type 9	0	CIF	Medium	0	0	0,00	0,00	0,00
Type 10	0	CIF	Medium	0	0	0,00	0,00	0,00
Type 11	0	CIF	Medium	0	0	0,00	0,00	0,00
total:	10	Cameras			TOTAL:	158,40 Mbps (Max=150)	25701,92 GB	20,31 MBps

Propósito de las cámaras, gestión, grabación, opciones de backup, AEPD, …

PROTECCIÓN ANTE ATAQUES EXTERNOS

- La tecnología IP permite una videovigilancia eficaz y controlable para proteger tanto a las personas como a su información y propiedades, garantizando un funcionamiento contínuo. Así mismo puede crear el potencial de mayores beneficios en seguridad y protección para nuestra sociedad y evitar incidentes costosos.
- Sin embargo, la ciberseguridad de la tecnología IP ha experimentado el desafío de la transición y desarrollos tecnológicos, generando riesgos económicos y de seguridad potenciales.
- Es por ello que a la hora de la elección de estos equipos sea importante que dispongan de políticas de **Ciberseguridad** para evitar que estos y los datos no se copien, modifiquen o destruyan mediante accesos no deseados o ilegales:
  - ✓ Gestión de puestos de red, políticas de gestión de contraseñas, transmisiones seguras de datos, …
  - ✓ Cumplimiento de **PCI DSS**, Norma de Seguridad del sector de tarjetas de pago para prevenir el fraude y las infracciones de información
  - ✓ **Chipset FIPS**, estándar de encriptación
  - ✓ **AES256**, algoritmo para protección de datos clasificados.
  - ✓ **Encriptación TLS 1.2, bajo HTTPS**, protocolo criptográfico que permite una comunicación segura
  - ✓ **Encriptación local en tarjeta µSD**
  - ✓ Certificación **NDAA, Sección 889:**
    - ✓ Si bien atañe a instalaciones gubernamentales de EE.UU. Se está generalizando en Europa y en cada vez más sectores y mercados verticales, tanto donde se trata de instalaciones diversas integradas en una red corporativa (ej. banca, retail, distribución de combustibles, …) como en otro tipo de instalaciones de riesgo medio / alto (ej. hospitales, hoteles, industria, energías renovables, instalaciones gubernamentales, …) e infraestructuras críticas.



CUMPLIMIENTO DE NDAA, SECCIÓN 889

1. Determina la prohibición de la instalación de equipos de Videovigilancia y Comunicaciones que no la cumplan*, no impactando en otras áreas de la seguridad electrónica
2. No se puede instalar contenido ni materiales de empresas y subsidiarias no NDAA
3. Generalmente diseñados pensando en la Ciberseguridad
4. No todas las soluciones NDAA son Ciberseguras

* Ciertas compañías chinas y sus subsidiarias

PROTECCIÓN ANTE ATAQUES EXTERNOS

EJEMPLO NVR ADPRO Y CÁMARAS SERIE 35 HONEYWELL

NDAA Compliant

SECURE BY DEFAULT

PCI DSS COMPLIANT

FIPS 140-2 VALIDATED

HTTPS

HTTPS

Medidas de seguridad y encriptación segura de transmisión

SISTEMAS DE CCTV ¿CUMPLEN LOS REQUISITOS?

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 an
from any of the companies highlighted in NDAA 2019, Section 889. Toge
cameras they can be used to provide video systems compliant with NDA
ranges are well suited for SMB, entry-level enterprise and critical applicat
essential, such as government, utilities, premium commercial, campuses

NDAA 2019 Section 889 is focused on video surveillance and telecommu
impact other areas of security. Honeywell access control solutions are cy
components from banned suppliers, and are not addressed by NDAA 201
Watch, WINPAK and other access software and hardware can continue t
agencies or other businesses wishing to implement security solutions co
889.

Specific Honeywell products that can be used as part of NDAA Section 8
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

Cumplimientos por parte del fabricante

3/2/22, 9:55 AM HC35_5MIPC

nessus

Report generated by Nessus™

HC35_5MIPC
Tue, 01 Mar 2022 08:04:49 CST

TABLE OF CONTENTS

Vulnerabilities by Host
- 192.168.199.239

Vulnerabilities by Host

Collapse All | Expand All

192.168.199.239

0	0	0	0	32
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v2.0	Plugin	Name
			Remote Date Disclosure
			Errors
			urer Detection
			(per directory)
			col (HTTP) Information
			col (HTTP) Redirect Information
			nsport Security (STS)
			erface Forum (ONVIF) Protocol Detection
			formation Leakage
			andling False Positives
			ssed

228/HC35_5MIPC_summary.html

Evaluación de vulnerabilidades

SECURE BY DEFAULT, ALGUNAS CARACTERÍSTICAS

- Este estándar permite que la protección contra los ciberataques sea una de las principales características de los elementos que componen un sistema de videovigilancia.
- Los productos no tienen nombres de usuario ni contraseñas codificados.
- Los dispositivos incorporan un sistema de comprobación de contraseñas y no permiten contraseñas inseguras.
- No hay “puertas traseras” inseguras en los equipos.
- Los productos utilizan HTTPS por defecto para todas las comunicaciones con una interfaz basada en web.
- Deben tener Onvif desactivado en el arranque por defecto.
- Los fabricantes no pueden recuperar contraseñas perdidas u olvidadas de dispositivos.
- La cámara estará en estado de bloqueo en el primer arranque, requiriendo un proceso de inicio específico para empezar a trabajar.

CUESTIONES SOBRE CIBERSEGURIDAD

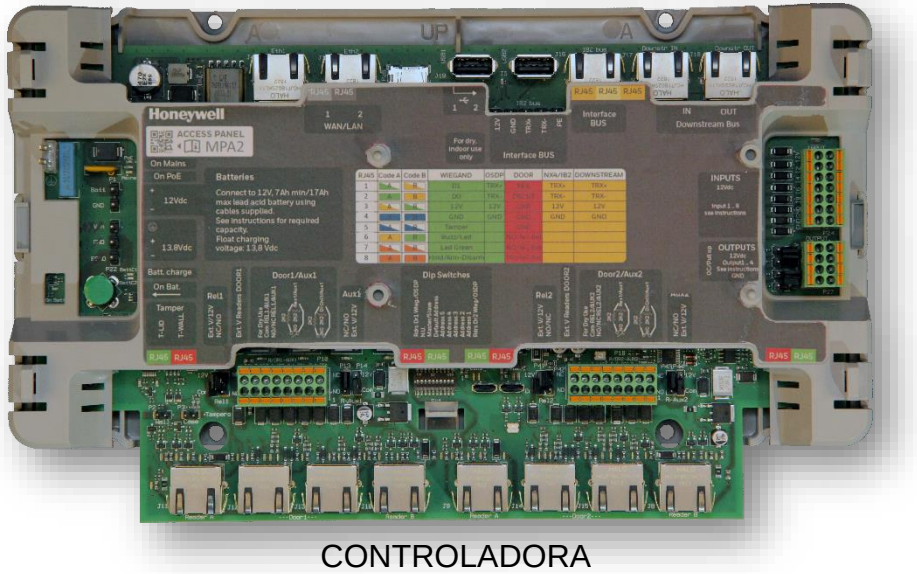
Sistemas de Control de Accesos

Honeywell

SEGURIDAD EN LAS COMUNICACIONES

LECTOR

01000001011110000110



CONTROLADORA

Wiegand

OSDP™

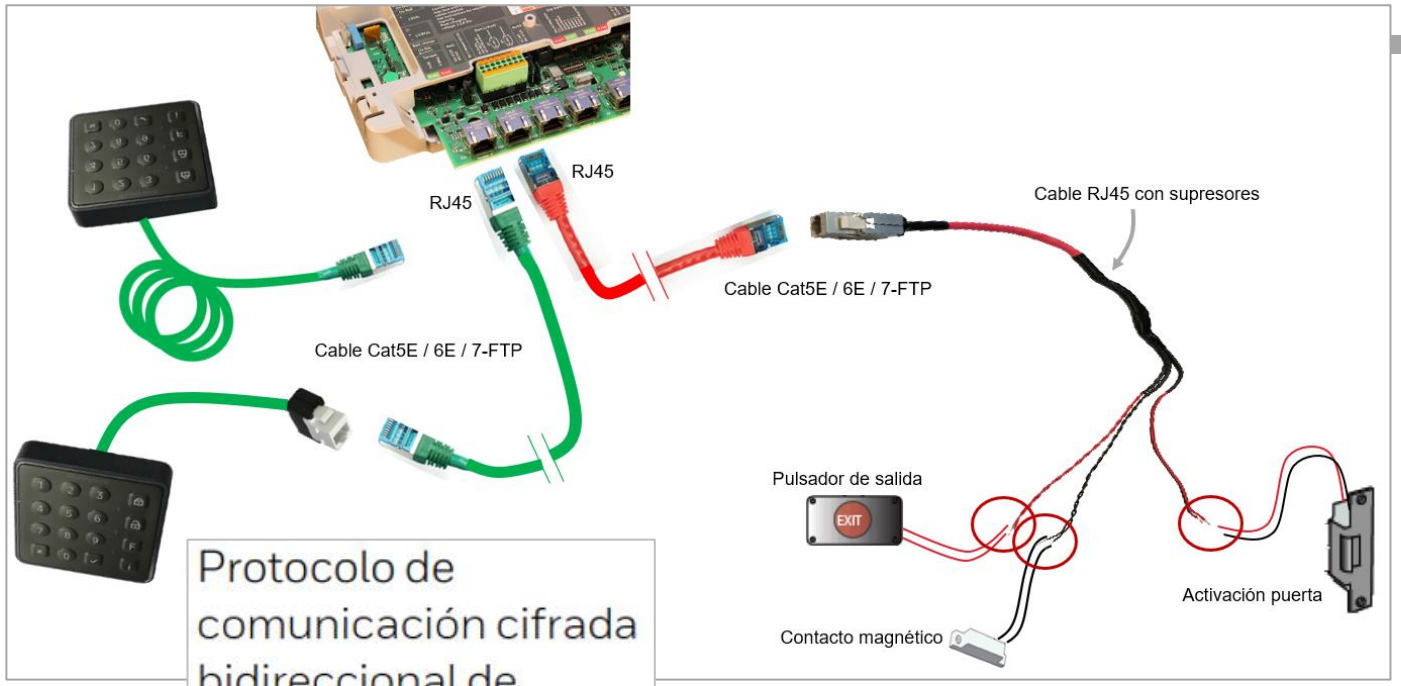
- Comunicación no encriptada
- Comunicación unidireccional
- 8 hilos para todas las funcionalidades
- Configuración lectores entrada/salida: una línea de cableado para cada uno

- Comunicación encriptada AES-128 y supervisada
- Comunicación bidireccional entre el panel y el lector
- 2 Hilos de alimentación + 2 de datos
- Configuración lectores entrada/salida: conectados en paralelo

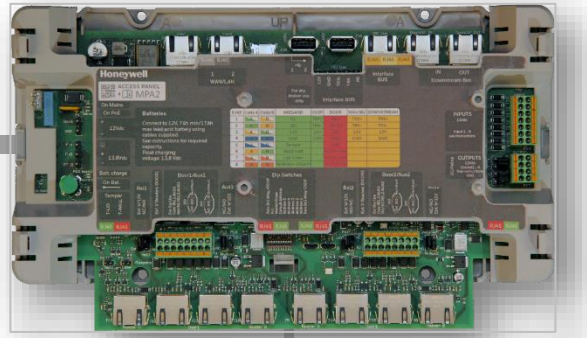
Lectores y Controladoras - Tecnología Wiegand Vs OSDP

PROTECCIÓN ANTE ATAQUES EXTERNOS

EJEMPLO MAXPRO ACCESS HONEYWELL



Protocolo de comunicación cifrada bidireccional de lector-panel AES de 128 bits (OSDP:V2).



Comunicación cifrada AES de 256 bits

Medidas de seguridad y encriptación segura de transmisión

PROTECCIÓN ANTE ATAQUES EXTERNOS

EJEMPLO MAXPRO ACCESS HONEYWELL CON CONEXIÓN A SERVICIOS CLOUD

Paneles MAXPRO Access

Lectores LuminAXS: LU45xxxx – OSDP

Tarjetas Honeywell

MPC Web cifrado punto a punto usando HTTPS, TLS 1.2

Comunicación bidireccional encriptada AES 128-bit entre los lectores y el panel

38 bits, tarjetas MiFare Desfire EV2, un único código de sitio y número de tarjeta

SERVICIOS CLOUD

Microsoft Azure

Instalador / Cliente

Medidas de seguridad y encriptación segura de transmisión

CUESTIONES SOBRE CIBERSEGURIDAD

Sistemas de contra Intrusión

Honeywell

SISTEMAS CONTRA INTRUSION

NORMAS DE OBLIGADO CUMPLIMIENTO

EN50131 – 1
Requisitos generales

EN50131 – 3
Paneles de control y periféricos

EN50131 – 5
Interconexiones

EN50131 – 6
Fuentes de alimentación

EN50131 – 2
Detectores de intrusión

EN50131 – 7
Guia de aplicación

EN50136
Comunicaciones

EN50131-5-1
Cableados

EN50131-5-3
Vía radio

EN50131-2-2
Infrarrojos pasivos

EN50131-2-4
Doble tecnología

EN50131-2-6
Contactos magnéticos

EN50131-2-7
Rotura de cristal

EN50131-2-8
Sensores de impacto

Sísmicos

Dispositivos de atraco

Detectores de exterior

SIN NORMA DE OBLIGADO CUMPLIMIENTO TODAVÍA

UNE-EN 50131-1:2008 / A3:2021

ANEXO C (INFORMATIVO)

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

Amenazas habituales a la seguridad cibernética

MÉTODOS DE ANÁLISIS DE RIESGOS

DETERMINAR GRADO DE SEGURIDAD DE LOS SISTEMAS

Honeywell
THE POWER OF CONNECTED

CÁLCULO DE NIVEL RIESGO Y GRADO DE SEGURIDAD - MÉTODO MOSLER

CRITERIO	SIGNIFICACIÓN	COEFICIENTE	Puntuación
FUNCIÓN (F)	Muy gravemente	5	Seleccione un valor
	Gravemente	4	
Los daños pueden alterar la actividad	Medianamente	3	
	Levemente	2	
	Muy Levemente	1	

CRITERIO	SIGNIFICACIÓN	COEFICIENTE	Puntuación
PROFUNDIDAD (P)	Muy Gravemente	5	Seleccione un valor
	Gravemente	4	
Los daños y efectos psicológicos pueden afectar a la imagen	Limitadamente	3	
	Levemente	2	
	Muy Levemente	1	

CRITERIO	SIGNIFICACIÓN	COEFICIENTE	Puntuación
EXTENSIÓN (E)	Internacional	5	Seleccione un valor
	Nacional	4	
	Regional	3	
El alcance de los daños puede ser de carácter	Local	2	
	Individual	1	

CRITERIO	SIGNIFICACIÓN	COEFICIENTE	Puntuación
VULNERABILIDAD (V)	Accesos autorizados habituales fuera de horario	10	Seleccione un valor
	Clientes externos	8	
	Empleados + Servicios + Visitas	6	
Perfil del ocupante	Empleados + Servicios	4	
	No aplica	0	

CRITERIO	SIGNIFICACIÓN	COEFICIENTE
SUSTITUCIÓN (S)	Muy difícilmente	
	Difícilmente	
	Sin mucha dificultad	
Los bienes pueden ser sustituídos	Fácilmente	
	Muy fácilmente	

CRITERIO	SIGNIFICACIÓN	COEFICIENTE
AGRESIÓN (A1)	Muy alta	
	Alta	
	Normal	
Probabilidad de que la amenaza se manifieste	Baja	
	Muy baja	

CRITERIO	SIGNIFICACIÓN	COEFICIENTE
AGRESIÓN (A2)	Recinto aislado	
	Zona industrial / residencial sin vigilancia	
	Zona industrial / residencial con vigilancia	
Ubicación geográfica	Extrarradio	
	Casco Urbano	

CRITERIO	SIGNIFICACIÓN	COEFICIENTE
AGRESIÓN (A3)	Población < 10.000 habitantes	
	Poblacion entre 10.000 y 25.000 habitantes	
Tipo de población	Población > 25.000 habitantes	
	Capital de provincia	

Carácter de la Amenaza	Cálculo del Carácter
"C" de carácter de la amenaza.	I = F x S = 0
"F" de función.	D = P x E = 0
"S" de sustitución.	C = I + D = 0
"P" de profundidad.	Probabilidad de Producirse
"E" de extensión.	P = A x V = 0
"I" de importancia del suceso.	
"D" de daños.	

Cálculo del Nivel de Riesgo	Valor ER	Nivel de Riesgo
	de 0 a 320	Muy Bajo
	de 321 a 640	Bajo
ER = C x P = 0	de 641 a 960	Normal
	de 961 a 1280	Alto
	más de 1281	Elevado

El Riesgo de que la Amenaza se produzca es:

Grado de Seguridad recomendado para la Instalación: Grad

Honeywell

ANÁLISIS Y EVALUACIÓN DEL RIESGO PARA INSTALACIONES DE SEGURIDAD

CRITERIO	SIGNIFICACIÓN	COEFICIENTE	Puntuación
PROBABILIDAD (P)	Ocurre con casi certeza, es la más probable que ocurra	10	10
	Puede ocurrir el 50% de las veces	6	
Mide el número de veces que puede presentarse el riesgo analizado	Es posible, pero poco usual	3	
	Remotamente posible	1	
	Concebible, aunque nunca ha ocurrido	0,5	
	Prácticamente imposible	0,1	

CRITERIO	SIGNIFICACIÓN	COEFICIENTE	Puntuación
EXPOSICIÓN (E)	Contínua (permanente)	10	3
	Frecuente (una vez al día)	6	
	Ocasional (una vez a la semana)	3	
Mide las veces que puede presentarse el agente dañino	Poco usual (una vez al mes)	2	
	Rara (unas pocas veces al año)	1	
	Muy rara (una vez al año)	0,5	

CLASIFICACIÓN DEL RIESGO
ENTRE 0 Y 20: ACEPTABLE
ENTRE 20 Y 70: POSIBLE
ENTRE 70 Y 200: CONSIDERABLE
ENTRE 200 Y 400: ALTO
ENTRE 400 Y 10.000: MUY ALTO

CRITERIO	SIGNIFICACIÓN	COEFICIENTE	Puntuación
CONSECUENCIA (C)	Catástrofe - dañar superiores a 1.500.000$	100	7
	Desastre - dañar entre 150.000 y 1.500.000$	40	
	Muy seria - dañar entre 75.000 y 150.000$	15	
Cuantifica en $ los daños y costes que pudieran producirse	Seria - dañar entre 15.000 y 75.000$	7	
	Importante - dañar entre 1.500 y 15.000$	3	
	Perceptible - dañar menores de 1.000$	1	

CÁLCULO DEL NIVEL DE RIESGO		
R = P x E x C		210
CLASIFICACIÓN DEL RIESGO	ALTO	
GRADO DE SEGURIDAD / NIVEL DE RIESGO	GRADO 3 / ALTO	
ACCIONES	MEDIDAS DE SEGURIDAD INMEDIATAS	

JUSTIFICACIÓN DE LAS ACCIONES CORRECTORAS

CRITERIO	SIGNIFICACIÓN	COEFICIENTE	Puntuación
COSTE DE LOS MEDIOS (CM)	Más de 75.300$	10	6
	Entre 75.300 y 37.650$	6	
	Entre 37.650 y 15.060$	4	
Determina el coste de las acciones correctoras	Entre 15.060 y 1.500$	3	
	Entre 1.500 y 150$	1	
	Menor de 150$	0,5	

CRITERIO	SIGNIFICACIÓN	COEFICIENTE	Puntuación
FACTOR DE CORRECIÓN (FC)	Elimina el 100% del riesgo	1	1
	Elimina entre un 100% y un 75%	2	
	Elimina entre un 75% y un 50%	3	
Mide la disminución del riesgo	Elimina entre un 50% y un 25%	4	
	Menor de un 25%	6	

NIVEL DE JUSTIFICACIÓN DE LAS ACCIONES CORRECTORAS
ENTRE 0 Y 10: NO SE JUSTIFICAN
ENTRE 10 Y 20: ZONA DE DUDAS, REVISAR PROYECTO
MÁS DE 20: LAS ACCIONES ESTÁN JUSTIFICADAS

CÁLCULO DEL NIVEL DE JUSTIFICACIÓN		
J = R / (CM x FC)		35
DECISIÓN	LAS ACCIONES CORRECTORAS ESTÁN JUSTIFICADAS	

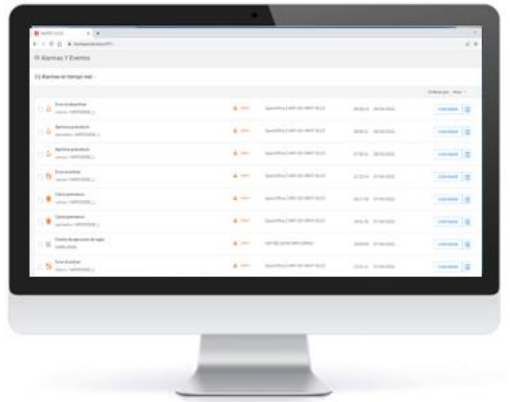
DISEÑO DE INSTALACIONES CONTRA INTRUSIÓN

EN BASE A ÓRDENES MINISTERIALES Y UNE-CLS/TS 50131-7

GESTIÓN DE USUARIO

COMUNICACIONES DE ALARMA A C.R.A.

- **Primaria y/o de backup (dependiendo de los equipos de notificación) – IP / GPRS LTE 4G**
- **Supervisión remota y permanente**



AUTONOMÍA DE FUNCIONAMIENTO

- **Determinar baterías y fuentes de alimentación auxiliares según grado requerido: 30 horas Grado 3 / 12 horas Grado 2**

DIFERENTES TECNOLOGÍAS DE DETECCIÓN

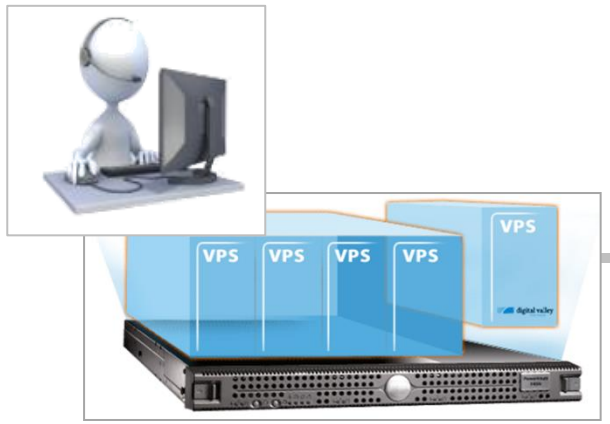
A CONSIDERAR	G1	G2	G3	G4
Puertas perimetrales	O	O	O/P	O/P
Ventanas		O	O/P	O/P
Otras aberturas		O	O/P	O/P
Paredes				P
Techos y tejados				P
Suelos				P
Sala	T	T	T	T
Alto riesgo			S	S

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

Gestión y transmisión de alarmas, alimentación, detección, …

PROTECCIÓN ANTE ATAQUES EXTERNOS
EJEMPLO MAXPRO INTRUSION HONEYWELL

ISOM, cifrado asimétrico punto a punto comprobación de certificacion bidireccional de clave pública / privada TLS 1.2



Certificado PKI emitido por Honeywell para desarrolladores de CRA,s (expira cada 2 años)

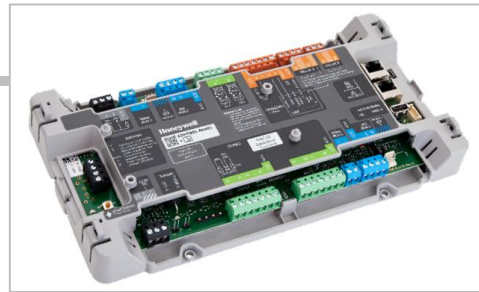
CENTRAL RECEPTORA DE ALARMAS

SERVICIOS CLOUD

MPC Web cifrado punto a punto usando HTTPS, TLS 1.2

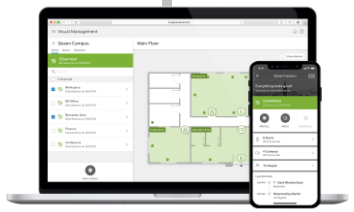
Microsoft Azure

Panel de intrusión



Clave pública/privada con Certificados de dispositivos IB2 unidireccionales validados

Periféricos



Instalador / Cliente

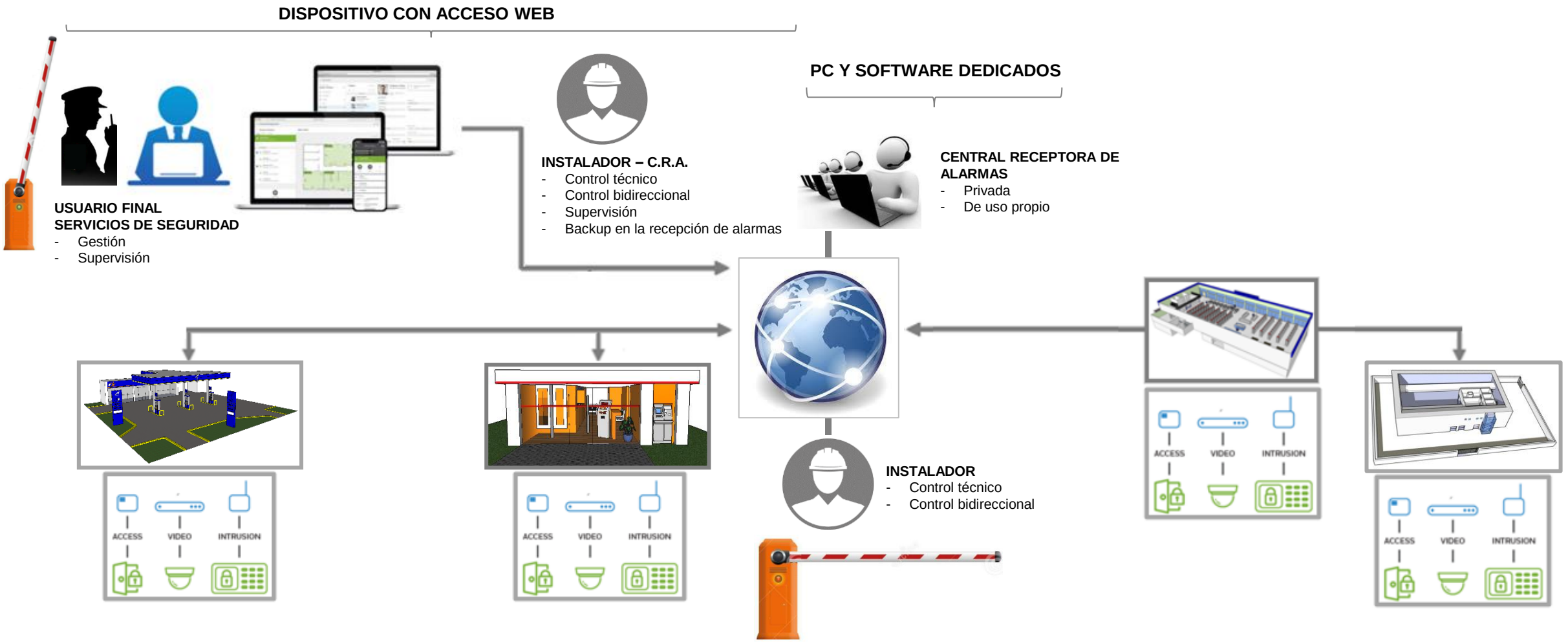
INSTALACIÓN

CUESTIONES SOBRE CIBERSEGURIDAD

Servicios Cloud

Honeywell

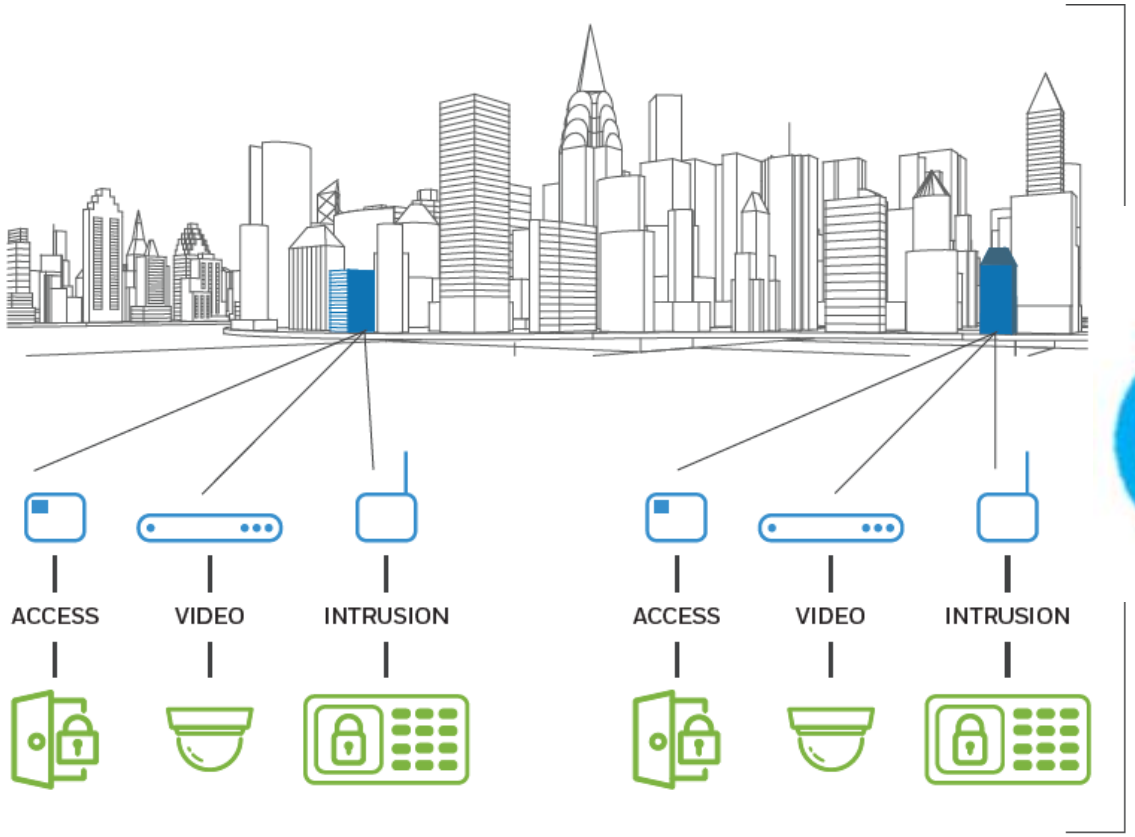
SERVICIOS CLOUD, OBJETIVO



Eliminar barreras en el control de los sistemas y obtener la máxima información

SERVICIOS CLOUD, OBJETIVO

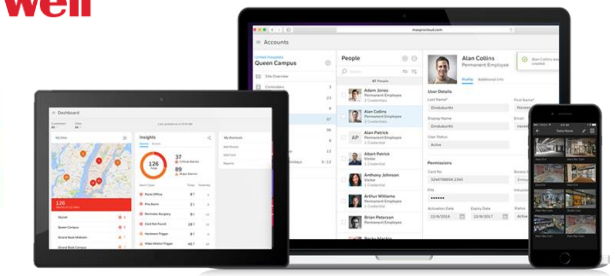
SERVICIOS DE VALOR AÑADIDO PARA USUARIOS FINALES Y EMPRESAS DE SEGURIDAD



Honeywell

MAXPRO Cloud

Microsoft Azure

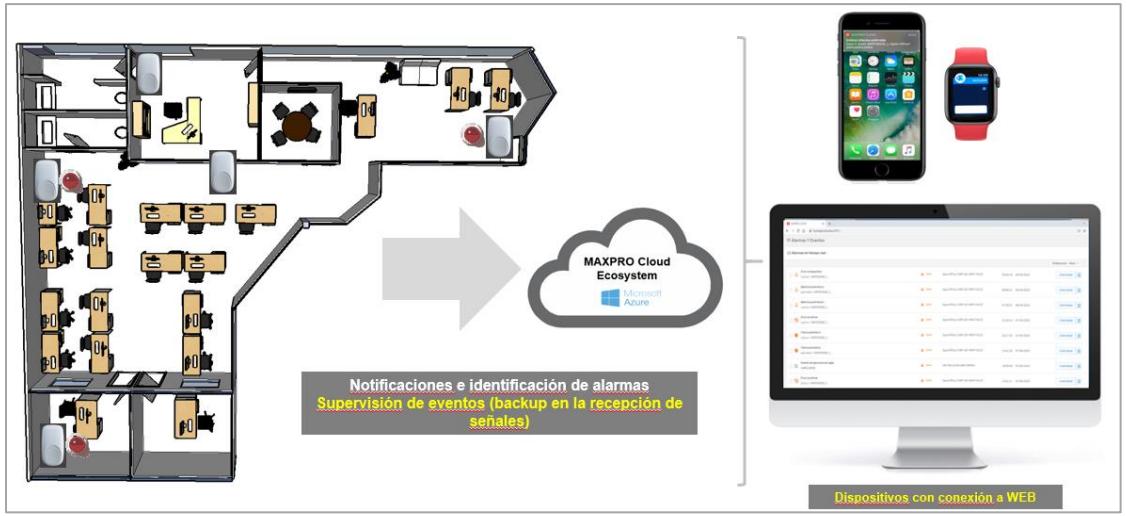


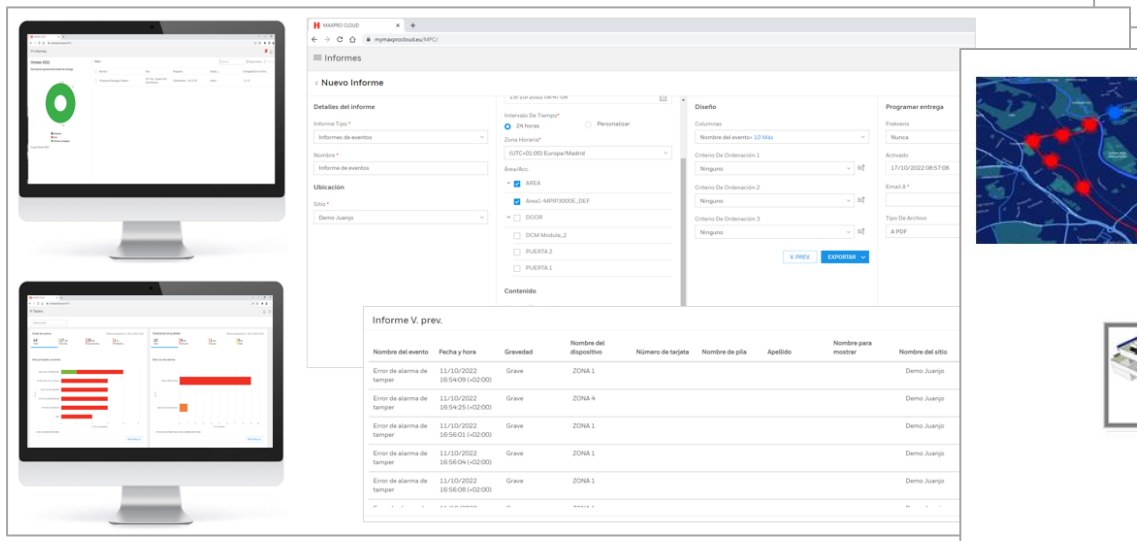
- **Toda la información de sus instalaciones en un solo lugar**
- **Acceda al Sistema desde cualquier sitio**
- **Gestión remota sencilla e intuitiva**
- **Mejor disponibidlidad de información y mayor nivel de seguridad**

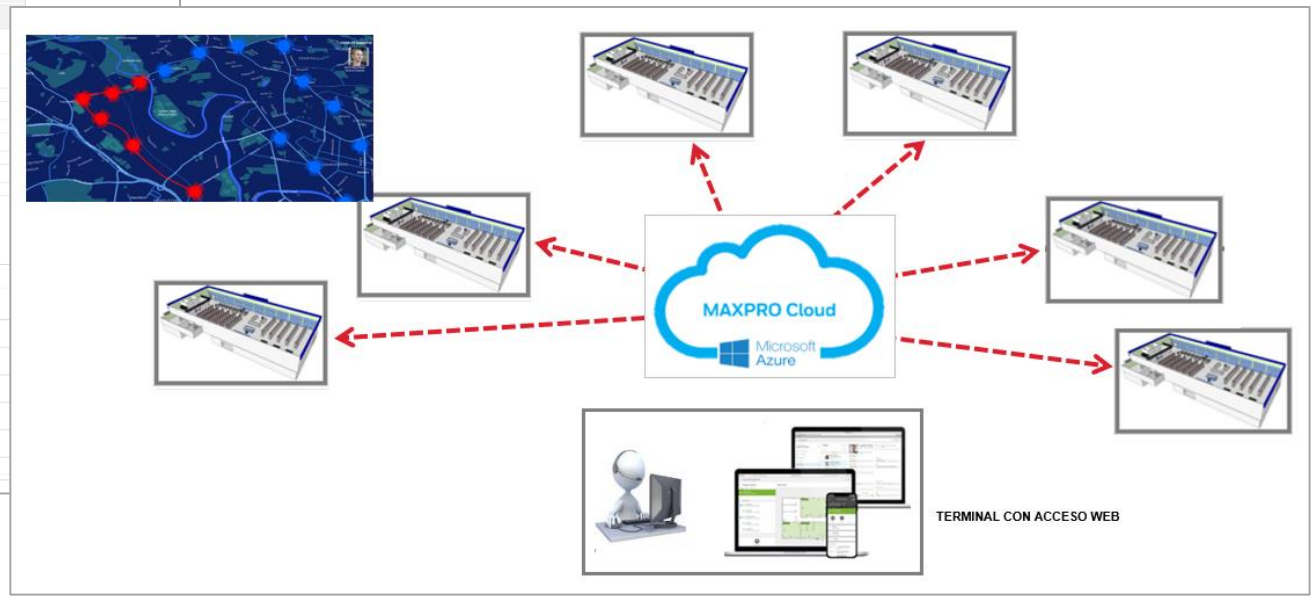
Industria | Retail | Sanidad | Banca | Ocio | Franquicias | Educación

SERVICIOS CLOUD

EJEMPLOS DE VALOR AÑADIDO PARA USUARIOS FINALES Y EMPRESAS DE SEGURIDAD

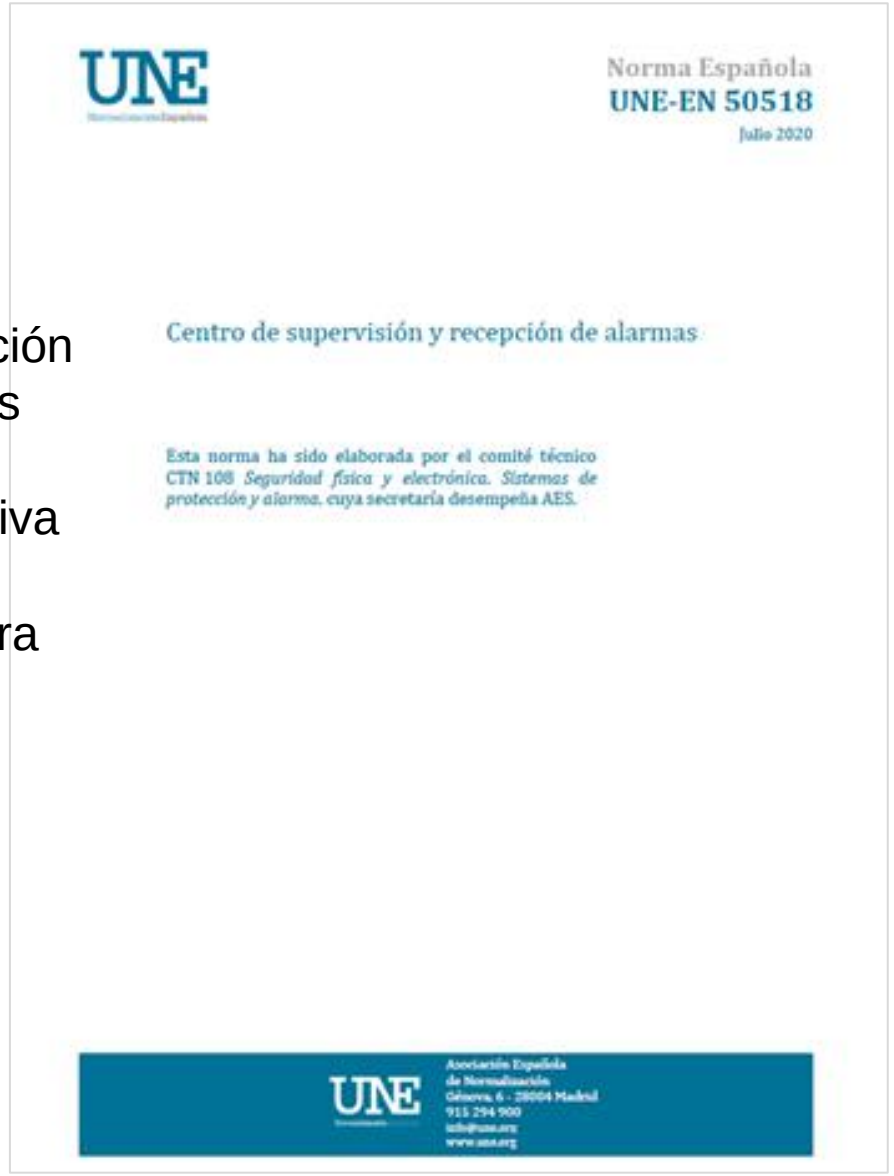






NORMA UNE EN 50518:2020

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


UNE

Norma Española
UNE-EN 50518
Julio 2020

Centro de supervisión y recepción de alarmas

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

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

CENTRALES RECEPTORAS DE ALARMAS

UNE-EN 50518:2020, DIAGRAMA DE CADENA DEL PROCESO TOTAL DE ALARMAS

INSTALACIONES (RIESGOS)

SISTEMAS CONTRA INTRUSIÓN
EN 50131-1: Requisitos del sistema
EN 50131-2: Detectores de intrusión
EN 50131-3: Equipos de control y señalización
EN 50131-4: Dispositivos de advertencia
EN 50131-7: Guía de aplicación. Diseño

SISTEMAS DE CCTV
VSS IEC 62676: Sistemas de videovigilancia para utilización en aplicaciones de seguridad

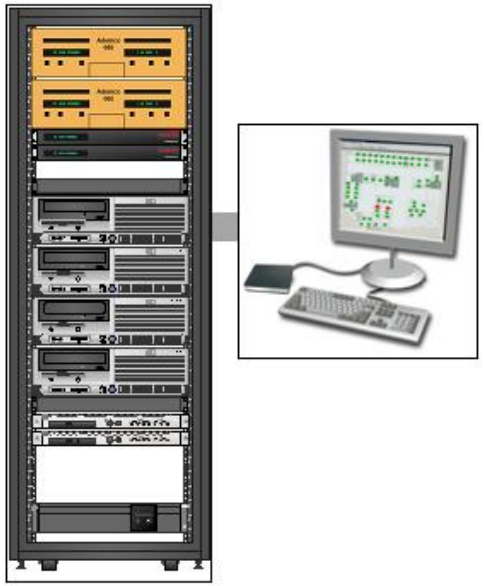
SISTEMAS CONTRA INCENDIOS
EN 54: Sistemas de detección y alarma de incendios

TRANSMISIÓN DE ALARMAS
EN 50136-2: Sistemas y equipos de transmisión de alarmas

TRANSMISIÓN DE MENSAJES DE FORMA SEGURA

CENTRO DE SUPERVISIÓN Y RECEPCIÓN DE ALARMAS

UNE EN 50518
ORDEN INT/316/2011
ORDEN INT/314/2011



RECEPCIÓN, VERIFICACIÓN Y TRANSMISIÓN

RESPUESTA

INTERVENCIÓN HUMANA:

- ✓ FUERZAS Y CUERPOS DE SEGURIDAD DEL ESTADO
- ✓ SERVICIOS DE SEGURIDAD PRIVADA
- ✓ TITULAR DE LA LLAVE DE ACCESO

ORDEN INT/316/211

FORMACIÓN PERSONAL C.R.A

INTERVENCIÓN NO HUMANA

- ✓ CONTROL BIDIRECCIONAL

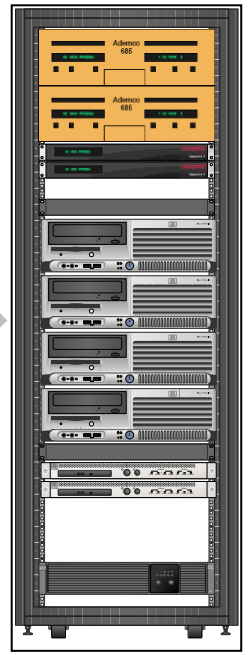
ORDEN INT/316/211

¿DEPENDENCIA DE LA NUBE?

CLIENTE FINAL
- Gestión de instalaciones
- Monitorización

INSTALADOR
- Control técnico
- Mantenimiento preventivo y predictivo

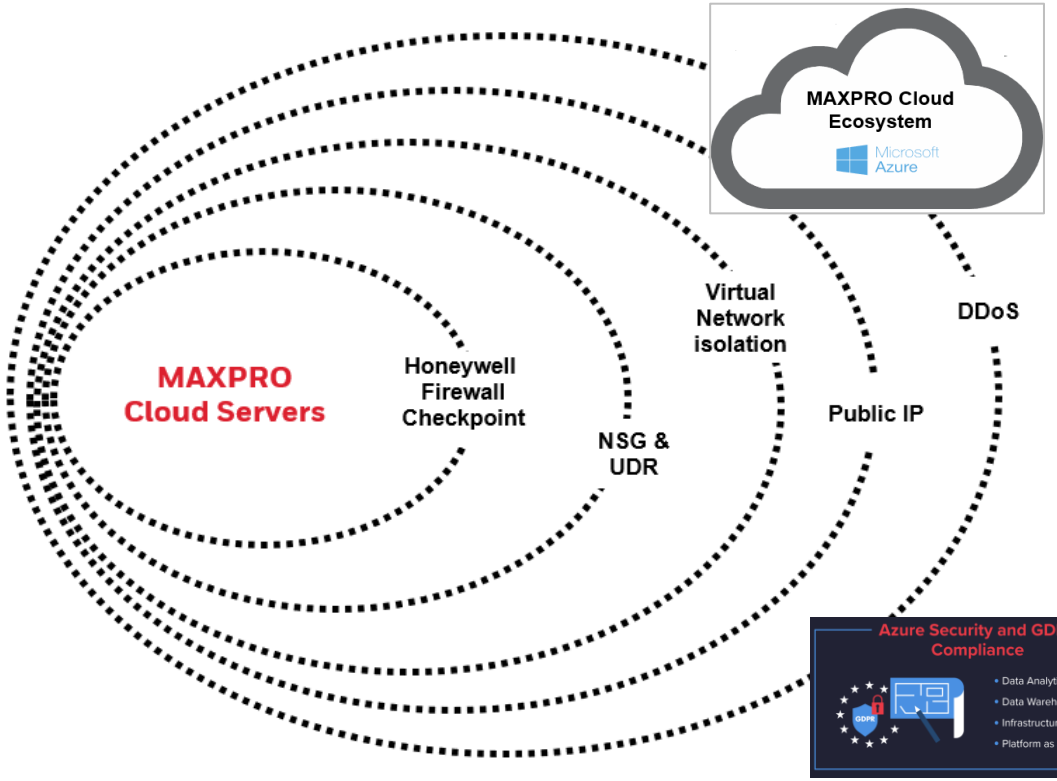
COMUNICACIONES A C.R.A
- **Privada**
- **De uso propio**
- **Primaria y de backup**



Funcionamiento local y comuniciones a C.R.A. totalmente independientes

EJEMPLO SOLUCIÓN MAXPRO® CLOUD

- Los servidores de MAXPRO Cloud (MPC) en la nube de Microsoft Azure están desplegados en una **red DMZ protegida contra ciberataques** mediante múltiples niveles de seguridad.
    - Protección DDoS, Sistemas de prevención y detección de intrusiones, reglas y políticas de cortafuegos.
- **Comunicación cifrada** entre los clientes/dispositivos web y el servidor MPC mediante el protocolo HTTPS.
- Todos los servidores están configurados con **certificados TLS 1.2, 256 bit AES y reforzados para una máxima seguridad**.
- El acceso remoto a los servidores se controla mediante certificados digitales con nombre y autenticación adicional basada en contraseña. **Todas las contraseñas están cifradas.**
- Todos los servidores están protegidos contra ataques de malware mediante un sistema de **detección y protección antimalware estándar del sector.**
- **Supervisión y alerta automatizadas en tiempo real de los incidentes de seguridad**, con un equipo de asistencia dedicado a su mitigación.
- **Active Directory**
- **Cumplimiento GDPR y Backup**, servidores en Europa: Datacenter en Irlanda y backup en Holanda



Actualizaciones automáticas de políticas de Ciberseguridad

Certification	Azure
CSA STAR Certification	✓
	✓
	✓
	✓
ISO 20000-1:2011	✓ (new)
ISO 22301:2012	✓
ISO 9001:2015	✓

Ciberseguridad – cumplimiento GDPR