# CUADERNOS DE SEGURIDAD

Núm. 317 • DICIEMBRE 2016 • 10 euros

PUNTOSEGURIDAD.com

## Seguridad en museos y patrimonio

## Protección contra robo e intrusión

**ESPECIAL ADMINISTRADORES DE FINCAS**

# Cámara Wi-Fi doméstica Dahua

## Se activa con la aplicación Easy4ip

ISO 9001:2000


www.dahuasecurity.com

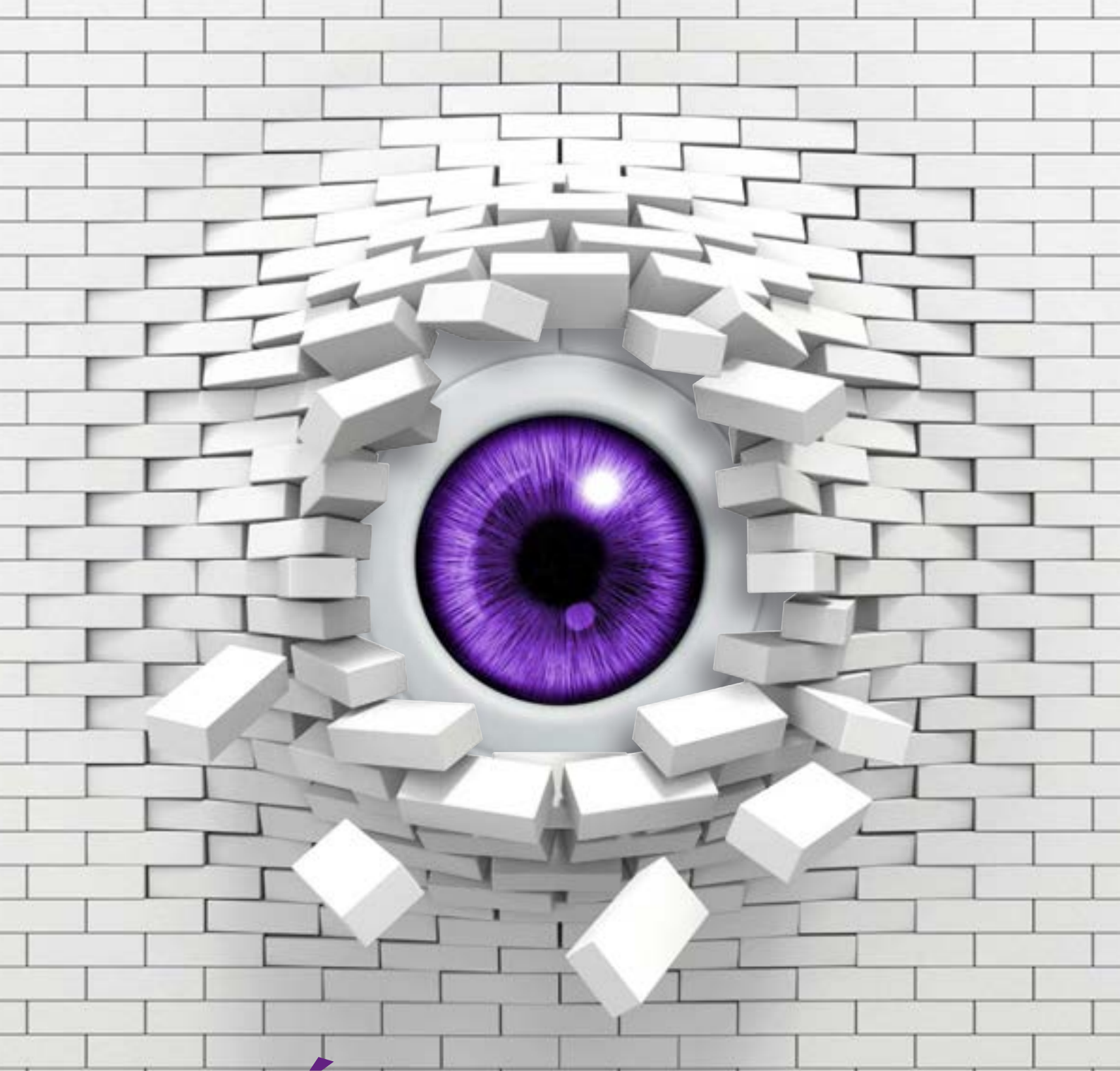
**DAHUA TECHNOLOGY CO., LTD.**

No.1199 Bin'an Road, Binjiang District, Hangzhou, China. 310053
Tel: +86-571-87688883 Fax: +86-571-87688815
Email: overseas@dahuatech.com
www.dahuasecurity com


España

Portugal

**DAHUA IBERIA**
Juan Esplandiú 15-1B-28007 Madrid, SPAIN
Tel: +34 917649862
Fax: +34 917649862



# ¿ESTÁS PREPARADO?

**CCIB**
Centro de Convenciones
Internacional de Barcelona

17 y 18 de mayo
BCN**2017**

www.securityforum.es

Security FORUM
International Security Conference & Exhibition

## EN 2017 PELDAÑO ORGANIZA TRES EVENTOS DE GRAN INTERÉS PARA EL SECTOR

# Experiencia y madurez

A poco más de dos semanas para que comience 2017, el sector de la Seguridad Privada despide este año con la inquietud e incertidumbre de saber si a lo largo de los próximos 365 días verá la luz el ansiado desarrollo reglamentario de la Ley de Seguridad Privada, Ley 5/2014 de 4 de abril. De nuevo estas páginas se hacen eco del esfuerzo y expectativas de un sector ante un reglamento del que depende y está en juego, en gran medida, el futuro de la Seguridad Privada.

Pero, de momento, ante un panorama económico que presenta ligeros síntomas de mejoría, y la composición de un nuevo gobierno, el sector debe demostrar, ahora más que nunca, que cuenta con la experiencia y la madurez suficiente para posicionarse y hacerse fuerte en los nuevos nichos de mercado que irán surgiendo.

Con estas premisas, y fiel a su compromiso con el sector, Peldaño, editora de la revista Cuadernos de Seguridad, organizará en 2017 tres eventos de gran interés para los profesionales de la Seguridad: por una parte, respondiendo a las necesidades y los retos a los que se enfrenta la figura del Jefe de Seguridad celebraremos el II Congreso Nacional de Jefes de Seguridad en esta ocasión en Barcelona. Un evento que cuenta con el respaldo de la Asociación de Jefes de Seguridad de España (AJSE), y que tiene entre sus objetivos analizar la figura de estos profesionales, así como sus futuras salidas profesionales dentro y fuera de las empresas en las que desarrollan su actividad.

En este final de año, también ponemos el punto de mira en Security Forum, donde el equipo de profesionales de Peldaño trabaja ya en su quinta edición, que se celebrará los días 17 y 18 de mayo en Barcelona, y que volverá a posicionarse como excepcional plataforma de networking, conocimiento, e innovador espacio que se adapta a las necesidades e inquietudes de los profesionales de la seguridad. El encuentro volverá a mostrar la oferta más selecta de servicios, equipos y sistemas de seguridad y, de forma paralela a la exposición, se desarrollará el Congreso Security Forum, desglosado en dos sesiones diferencias: Global Day y Ciber Day, que se convertirán en punto de reflexión donde reconocidos expertos debatirán y analizarán los nuevos riesgos y amenazas de un engorno global.

Y, por último, en otoño Bilbao será escenario de la tercera edición del Congreso de Seguridad en Euskadi, que servirá de punto de encuentro con los principales actores de la Seguridad en el País Vasco.

Citas imprescindibles para el sector, donde tendremos la oportunidad de compartir conocimiento con los profesionales y demostrar que, sobre los pilares de la madurez, la profesionalidad y el dinamismo, el sector está preparado para apostar por su reactivación y que, como siempre, contará con nuestro apoyo. ¡Felices Fiestas!

CUADERNOS DE SEGURIDAD

www.puntoseguridad.com

Nº 317 • DICIEMBRE 2016

Peldaño

Avda. del Manzanares, 196 • 28026 MADRID
**www.epeldano.com**

**Presidente:** Ignacio Rojas.
**Gerente:** Daniel R. Villarraso.
**Director de Desarrollo de Negocio:** Julio Ros.
**Directora de Contenidos:** Julia Benavides.
**Directora de Marketing:** Marta Hernández.
**Director de Producción:** Daniel R. del Castillo.
**Director de TI:** Raúl Alonso.
**Coordinación Técnica:** José Antonio Llorente.
**Jefa de Administración:** Anabel Lobato.

**Director Área de Seguridad:** Iván Rubio Sánchez.
**Redactora jefe de Seguridad:** Gemma G. Juanes.
**Redacción:** Arantza García, Marta Santamarina.
**Publicidad:** publi-seguridad@epeldano.com
Emilio Sánchez.
**Imagen y Diseño:** Eneko Rojas.
**Producción y Maquetación:** Miguel Fariñas, Débora Martín, Verónica Gil, Cristina Corchuelo.

**Distribución y suscripciones:**
Mar Sánchez y Laura López.
Horario: de 9,00 a 14,00 y de 15,00 a 18,00 horas)
Viernes: de 8,00 a 15,00 (suscripciones@epeldano.com)
**Redacción, administración y publicidad**
Avda. Manzanares, 196 - 28026 Madrid
Tel.: 91 476 80 00 - Fax: 91 476 60 57
Correo-e: cuadernosdeseguridad@epeldano.com

**Fotomecánica:** MARGEN, S. L.
**Impresión:** ROAL, S. L.
**Printed in Spain**
**Depósito Legal:** M-7303-1988
**ISNN:** 1698-4269
**Precio: 10 €.** Precio suscripción (un año, 11 núms.) 93 €, (dos años, 22 núms.) 165 € (España).





**EDICIONES PELDAÑO, S. A.**, TAMBIÉN EDITA:
Instalsec, Panorama Camping (profesional), Mab Hostelero, Hh Equipamiento Sociosanitario, TecnoHotel, Mab Oro, www.puntoseguridad.com




## 72 SEGURIDAD



## 89 C.S. ESTUVO ALLÍ



## 102 ACTUALIDAD



## 106 EQUIPOS Y SISTEMAS



# ENERO 2017 - Nº 318

# EN PORTADA

## EL SECTOR ANTE 2017: RETOS DE FUTURO

2017 arranca con perspectivas de mejora, a nivel general y, en particular, en el sector de la Seguridad Privada, pese a que aún espera ansioso el nuevo Reglamento de Seguridad Privada. ¿Qué deparará 2017 a la industria y al mercado del sector? ¿Se hará realidad por fin el desarrollo reglamentario de la Ley de Seguridad Privada? Muchos de los profesionales de la seguridad seguro que se han planteado a lo largo de 2016 éstas y otras muchas preguntas, así como qué pasará, en los primeros meses de 2017.

Por ello, en este primer número del año –un clásico ya de nuestra publicación– hemos querido pulsar la opinión de las asociaciones más representativas del sector que muestran su valoración sobre un tema de absoluta actualidad: el futuro del sector y el desarrollo reglamentario de la ley de Seguridad Privada. Unas pinceladas donde desvelan algunas de las claves de futuro para el sector.

Pixabay

Pixabay

## RPA´S Y SEGURIDAD

Analizar las novedades sobre la normativa actual referente al uso al uso de drones en España, así como exponer los retos y oportunidades que puede ofrecer al sector de la Seguridad Privada, serán algunos de los temas que se abordarán en el próximo número de Cuadernos de Seguridad en el que se dedicará una sección a este tema.

En el monográfico abordaremos un recorrido por la normativa de aplicación en determinados aspectos a esta nueva actividad, el uso y pilotaje de drones, que hoy en día está en auge.

Además, expertos en la materia analizarán a través de artículos y tribunas la tipología de drones, así como su aplicación para diferentes categorías, como es el caso en actividades de Seguridad Privada.

Igualmente, un tema a tener en cuenta es la protección de datos personales derivados del uso de RPAs.

Todos estos aspectos y muchos otros relacionados con el uso de drones en Seguridad Privada serán analizados.

**Como en cada número de nuestra revista CUADERNOS DE SEGURIDAD incluiremos las secciones habituales fijas: Actualidad, Cuadernos de Seguridad estuvo allí, Seguridad...**

# ÍNDICE DE EMPRESAS CITADAS EN ESTA EDICIÓN

| EMPRESA | PAG. | TELÉFONO | WEB |
|---|---|---|---|
| ARQUERO | 75,76 | 928092181 | sci-spain.com |
| HANWHA TECHWIN EUROPE | 106 | 916517507 | www.hanwha-security.eu |
| AXIS COMMUNICATIONS | 102 | 918034643 | www.axis.com |
| BOSCH SECURITY SYSTEMS | 98 | 902121497 | www.boschsecurity.es |
| BTV | 55,56 | 976108088 | www.btv.es |
| BUNKER | 106 | 913316313 | www.bunkerseguridad.es |
| CERRADURAS ISEO | 95 | 918843200 | www.iseo-iberica.eu |
| DAHUA | 2ª Cub, 3, 102 | 917649862 | www.dahuasecurity.com |
| DETNOV | 104 | 933716025 | www.detnov.com |
| DIID | 102 | 902565733 | www.diid.es |
| DORLET | 25 | 945298790 | www.dorlet.com |
| DORMAKABA | 23 | 917362480 | www.dormakaba.com |
| EL PARKING INTERNET | 37,58 | 923256051 | www.elparking.com |
| EVVA | 83 | 4318116501 | www.evva.com |
| FERRIMAX | 105 | 934601696 | www.ferrimax.es |
| GRUPO ESV | 52,60. | 916702071 | www.grupoesv.com |
| GRUPO VPS | 103 | 930047035 | www.vpsitex.es |
| HIKVISION | 4ª Cub,11,28,29 | 917371655 | www.hikvision.com |
| INNOTEC | 61 | 917281504 | www.innotecsystem.com |
| LEOPARD | 102 | | www.leopardperimeter.com |
| MOBOTIX | 32 | 911115824 | www.mobotix.com |
| MORSE WATCHMANS | 30,63 | 1159671567 | www.morsewatchmans.com |
| OPTEX | 87 | | www.optexiberia.com |
| PORTERALIA | 42 | 934358426 | www.porteralia.com |
| PYRONIX | 3ª Cub | 917371655 | www.pyronix.com |
| RISCO GROUP | 33 | 914902133 | www.riscogroup.es |
| SECURITAS DIRECT | 38,39 | 902195195 | www.securitasdirect.es |
| SECURITY FORUM | 4 | 914768000 | www.securityforum.es |
| SEGURIDAD INTEGRAL CANARIA | 71 | 902226047 | www.seguridadintegralcanaria.com |
| TECNOALARM | 68,69 | 936622417 | www.tecnoalarm.es |
| TECOSA | 15 | 915147500 | www.tecosa.es |
| TYCO IF & S | 40 | 916313999 | www.tyco.es |
| VANDERBILT | 104 | 911799770 | www.vanderbiltindustries.com |
| VISIOTECH | 27 | 911836285 | www.visiotech.com |
| VIVOTEK | 106 | 886282455282 | www.vivotek.com |

Datos de contacto de las empresas y entidades citadas en esta edición.


## ÍNDICE DE ANUNCIANTES

EL ENCUENTRO SE CELEBRARÁ EL 17 Y 18 DE MAYO EN BARCELONA

# Las empresas vuelven a apostar por **Security Forum 2017**

## El congreso Security Forum se desglosará en dos sesiones diferenciadas: Global Day y Ciber Day

A pocos días para que de comienzo 2017, la quinta edición de Security Forum sigue avanzando en su organización. Las empresas continúan reservando su espacio en el área de exposición, los Premios Security Forum empiezan a recibir trabajos, y el área de conferencias se desglosa en dos sesiones diferenciadas: Global Day y Ciber Day. Consolidado ya como un espacio de networking, esta nueva edición sigue apostando por la innovación y nuevos valores empresariales en el sector de la Seguridad.

A POCO más de cinco meses para su celebración Security Forum volverá a convertirse en un evento ágil, flexible y orientado a la innovación y desarrollo, que sigue respondiendo una edición más al espíritu emprendedor y audaz que caracteriza a las empresas y profesionales del sector de la Seguridad y que apuesta por reforzar el tejido empresarial de un sector en continua evolución, que demanda nuevos escenarios de plataformas de negocio e intercambio de conocimiento.

El encuentro contará de nuevo en esta edición con una zona de exposición, donde las empresas ya han comenzado a reservar su espacio, con áreas sobre CCTV, integración de sistemas, seguridad física, seguridad lógica, control de accesos, IP/REDES...; paneles de expertos, con charlas de transferencia tecnológica entre las empresas que aportan soluciones tecnológicas y los profesionales de la gestión, consultoría e instalación de sistemas; los Premios Security Forum 2017, galardones cuyo objetivo es promover la investigación, el desarrollo y la innovación de la industria de la Seguridad; así como un congreso que se convertirá en plataforma de conocimiento para analizar los cambios y gestionar ideas para transformarlas en oportunidades.

### Global Day y Ciber Day

Y respecto al congreso, cabe destacar que, una vez más, se desglosará en dos sesiones diferenciadas:

– **Global Day:** la primera jornada estará dedicada a la seguridad global. Los asistentes podrán descubrir desde una visión multidisciplinar temáticas como «Vigilados por defecto» o «La comunicación no verbal y análisis de conductas sospechosas como herramienta para el director de Seguridad».

– **Ciber Day:** la segunda jornada se centrará en la ciberseguridad. Temas como la figura del CISO o la coordinación estatal ante la Directiva NIS centrarán el debate de esta edición.

En la web www.securityforum.es se puede consultar la información actualizada sobre la próxima edición, así como el resumen de la edición de 2016. ●

### Ficha técnica

**Fechas:** 17 y 18 de mayo de 2017.

**Horario:** de 10:00 h a 18:30 h.

**Lugar:** Centro de Convenciones Internacional (CCIB). Pza de Willy Brandt, 11-14. de Barcelona.

**Periodicidad:** Anual.

**Carácter:** Exclusivamente profesional.

**Organiza:** Peldaño.

**Áreas de Exposición:**

- CCTV.
- Integración de sistemas.
- Seguridad lógica.
- Control de accesos.
- IP/redes.
- Protección contra robo e intrusión.
- Protección contra incendios.
- Ciberseguridad.

**Más información y contacto:**
**www.securityforum.es**
**info@securityforum.es**
**Tel.: 91 476 80 00**

HIKVISION


# DARKFIGHTER LITE
# ¿POR QUÉ CONFORMARSE CON BLANCO Y NEGRO?

En la oscuridad, los colores se difuminan hasta acabar en grises, pero para una seguridad eficaz es necesario entender todos los detalles de cada situación. Con la tecnología Darkfighter, en una situación urbana con un artista del grafiti actuando, no solo se distinguirá su silueta, sino que lucirá con tanto color y detalle como su creación en la pared.
Por muy tenue que sea la iluminación u oscura la escena, ningún color se escapa a la mirada de las cámaras Darkfighter de Hikvision.

**Hikvision Spain**
C/ Almazara, 9
28760 Tres Cantos (Madrid)
T +34 91 7371655
info.es@hikvision.com

www.hikvision.com

**MIGUEL ÁNGEL MOLINA.** DIRECTOR DE SEGURIDAD. MUSEO THYSSEN-BORNEMISZA. MADRID

# *«Aplicar el término "**alerta temprana**" es la clave para una **seguridad satisfactoria en los museos**»*

LAS nuevas tecnologías juegan hoy en día un papel clave, sobre todo en los museos, donde la seguridad debe estar siempre presente, pero de un modo discreto y que no interfiera en el visitante», explica a Cuadernos de Seguridad Miguel Ángel Molina, director de Seguridad del Museo Thyssen-Bornemisza, al tiempo que indica que entre los objetivos prioritarios que se marcó, tras su reciente incorporación al centro museístico, destaca la «actualización de los sistemas de seguridad para adaptarlos a la nueva amenaza global a la que nos enfrentamos todos, y especialmente los espacios públicos con gran concentración de visitantes».

**—¿Qué objetivos se planteó tras su reciente incorporación como director de Seguridad del Museo Thyssen-Bornemisza?**

—Los objetivos fueron varios, pero uno destacó especialmente entre otros, y es la actualización de los sistemas de seguridad para adaptarlos a la nueva amenaza global a la que nos enfrentamos todos, y especialmente los espacios públicos con gran concentración de visitantes. La amenaza yihadista, es nueva y nos obliga a adaptarnos a los nuevos retos, con nuevos sistemas de seguridad que generen una «alerta temprana», que permita articular los correspondientes protocolos de seguridad e intentar minimizar o neutralizar la posible agresión.

No se trata simplemente de incrementar los números de efectivos del personal de seguridad, sino de implantar el uso de nuevas tecnologías, y estrechar la colaboración con las FCS, puesto que ellos son los que están en la vanguardia de la lucha antiterrorista. Ante una amenaza de este tipo, todos los apoyos y colaboraciones son imprescindibles.

**—De manera general, ¿cómo se organiza la seguridad de una instalación museística como es el Museo Thyssen- Bornemisza donde este elemento es una de sus máximas prioridades?**

—Está formado por un director de Seguridad del que dependen los supervisores de Seguridad, los cuales son una pieza clave en la operatividad y maniobrabilidad del departamento y los cuales, a su vez, son delegados en Seguridad, por lo que reside en ellos la delegación del mando en ausencia del director de Seguridad.

Por otro lado, y no menos importantes, son los operadores de Consola que mantienen todo el soporte técnico e informático, así como operatividad de la CRA-UP (Central Receptora de Alarmas de Uso Propio) que dispone el museo, y son el enlace directo con el director de Seguridad, así como con las Fuerzas y Cuerpos de Seguridad. Éstos últimamente están realizando una labor muy eficaz en la coordinación y ejecución de los transportes de obras de arte, los cuales en la mayoría de los casos son escoltados por la Brigada Especial del Cuerpo Nacional de Policía.

Todo el personal anteriormente citado depende de la Fundación Thyssen-Bornemisma. Aparte y mediante concurso público, se contratan los servicios de seguridad con una empresa de seguri-

dad, en este caso CASESA, con Vigilantes de Seguridad, y a su vez coordinados por un supervisor de Seguridad de la empresa, que es el enlace directo de la misma con el director de Seguridad.

**—¿Tiene previsto el departamento de Seguridad del Museo Thyssen-Bornemisza llevar a cabo mejoras o ampliaciones de los medios y medidas de seguridad con que cuentan las instalaciones del centro museístico?**

—Sí, debido a las nuevas amenazas, hemos tenido que adaptar la seguridad física y electrónica. No es un proceso inmediato puesto que es complejo, no solo en el coste económico, sino en la integración en las instalaciones del museo, modificación de protocolos de seguridad, e instalaciones técnicas.

Se han instalado paneles detectores de metales, un elemento básico pero que también nos ha supuesto dificultades de integración para conseguir el equilibrio entre lo estético y lo funcional; esta problemática es habitual en el ámbito museístico y cualquier intervención tiene que buscar el mínimo impacto físico y visual en el visitante.

**—¿Qué papel juegan hoy en día las nuevas tecnologías a la hora de garantizar y mejorar la seguridad de los grandes centros museísticos?**

—Un papel clave, sobre todo en los museos, donde la seguridad debe estar siempre presente pero de un modo discreto y que no interfiera en el visitante. Las nuevas tecnologías digitales, sobre todo las cámaras IP, y la resolución que ofrecen, junto a las nuevas analíticas de vídeo nos permiten superar las barreras que ofrecían las anteriores tecnologías analógicas.

Se obtiene un mayor control en las salas de exposiciones, se detectan objetos abandonados, se localiza en cuestión de segundos a la persona que abandonó el objeto (voluntaria o involuntariamente), pudiendo así activar un protocolo u otro y evitando alarmas innecesarias.

Se delimitan zonas de acceso de un modo virtual, así como conteo de personas, pudiendo avisar directamente por el Centro de Control a los vigilantes.

Nos permiten la transcodificación dinámica, es decir, desde una tablet y de un modo encriptado y seguro conectar desde cualquier sitio al Centro de Control y sin que el ancho de banda sea una limitación. Visualizando las cámaras en HD y operando los domos y zooms.

Y otro tipo de aplicaciones que se irán implantando en posteriores fases.

**—En un mundo totalmente globalizado, ¿cómo han cambiado en los últimos años los riesgos y amenazas a los que tienen que hacer frente los responsables de Seguridad de los museos españoles?**

—Como comentaba anteriormente, lo riesgos y amenazas han cambiado muy rápido y de un modo muy radical. Tenemos que estudiar tecnologías y medios para implantarlos, cuando antes sólo se consideraba su implantación en infraestructuras críticas. El riesgo es tan imprevisible e indiscrimi-

nado que desde el punto de vista de una auditoría interna, son muchos los puntos a los que hacer frente. Lo que supone una actualización constante, el disponer de una plataforma digital, aunque resulta costosa en su implantación inicial, luego resulta interesante su flexibilidad y adaptación de nuevas tecnologías porque se trataría de instalar actualizaciones de software y buscar la interconectividad.

**—¿Cree que existe en la sociedad actual la concienciación de la necesidad de proteger y conservar el patrimonio cultural?**

—Sinceramente creo que sí, el patrimonio cultural es un legado histórico que no distingue entre banderas ni política, es común a todos, es nuestra historia y es un bien común a todos. A diario puedo observar cómo los visitantes asisten emocionados a las inauguraciones de las exposiciones temporales y también a visitar la permanente. Y salvo contadas excepciones las personas son muy respetuosas y conscientes de ello.

Siempre existirá un trabajo de concienciación a las nuevas generaciones y debe ser continuo y constante.

En este museo observamos con alegría la cantidad de institutos y colegios que nos visitan, de hecho, tenemos un área específica de educación para atender todas sus necesidades. Y nuestro lema, y que lo hace atractivo a este tipo de visitas, es «Un recorrido por la historia del arte», puesto que disponemos de obras de todas las épocas.

**—Bajo su punto de vista, ¿cree que los usuarios de las instalaciones museísticas y centros de arte valoran las medidas de seguridad implantadas o, por el contrario, se trata de un hecho que pasa desapercibido?**

—Buscamos siempre la integración de todos los elementos y el menor impacto visual, así como una mínima interferencia en el visitante. Pero sí que he observado en estos últimos meses una clara concienciación del visitante respecto a la seguridad, y de los mismos trabajadores del museo incluso. Nos suelen preguntar por los arcos detectores de metal, si están instalados o no, y claro no habían advertido su presencia al acceder al museo. Cuando luego se les explica se muestran satisfechos. Incluso llegan a aportar sugerencias.

Y por parte de la Dirección del museo también hay una clara concienciación sobre la seguridad, mostrando a este departamento de Seguridad todo su apoyo y colaboración. Y ante problemas que se plantean complejos formamos equipos entre las áreas afectadas para buscar su solución.

**—¿Cuáles considera que son las claves para una seguridad satisfactoria en este tipo de instalaciones?**

—La clave es aplicar el término «alerta temprana», en toda su extensión, tanto en medios físicos, técnicos como humanos. Hay que mentalizar a todo el personal de seguridad a la amenaza a la que nos enfrentamos y buscar un equilibrio entre atención y eficacia, estando siempre prevenido y nunca atemorizado. Si la amenaza se materializa, neutralizarla resultaría muy difícil y con riesgo de bajas. Por lo que la clave es adelantarse a los hechos, colaboración, información, inteligencia, son las fases que nos ayudarán a prevenir esos riesgos y ataques.

**—¿Cuáles son las prioridades de seguridad para el responsable de Seguridad de una instalación como el Museo Thyssen-Bornemisza?**

—Las prioridades son varias, pero evidentemente la prioridad máxima son las vidas de las personas, tanto visitantes como trabajadores, así como las obras de arte aquí expuestas, puesto que de producirse un incendio o inundación, la pérdida sería irrecuperable.

También se están reforzando y actualizando los Planes de Evacuación de Obras de Arte ante Catástrofes o Emergencias. En colaboración con el Ministerio de Educación, Cultura y Deporte, así como con la UME Unidad Militar de Emergencias. Son medidas que no buscamos generar alarma, pero debemos estar preparados ante cualquier contingencia que se pueda producir, y contar con protocolos y colaboraciones que presten apoyo desde el exterior. ●

*Texto: Gemma G. Juanes.*
*Fotos: Museo Thyssen-Bornemisza*

# Siveillance SiteIQ WA

## Sistema de Mando y Control para protección de Infraestructuras Críticas

Siveillance SiteIQ WA permite la Gestión Integral de múltiples sensores de seguridad (Radar, AIS, vídeo inteligente, vallas y defensas activas...).

Genera alarmas globales independientes del sensor que las haya detectado.

Supervisa toda la instalación en una pantalla única.

No requiere la atención permanente del operador.

Visualización georreferenciada en 3D.

Manejo y configuración sencillos.

TECOSA

Telecomunicación,
Electrónica y Conmutación S.A.
Grupo Siemens

w w w . t e c o s a . e s

**JOSÉ RAMÓN LÓPEZ PERAL.** DIRECTOR DE SEGURIDAD DEL INSTITUT VALENCIÀ D´ART MODERN. IVAM. VALENCIA.

# *«No se pueden tratar de forma lineal todas las **exposiciones**, para cada una de ellas se deben adaptar **medidas concretas para asegurarla**»*

EL IVAM cuenta con todas las medidas necesarias para garantizar la seguridad de las personas, el patrimonio y el propio edificio», explica José Ramón López Peral, director de Seguridad del IVAM, quien además señala que el departamento de Seguridad intenta mantener, optimizar y mejorar todos los medios físicos, técnicos y personales «que nos ayudan a cumplir con la labor establecida para este departamento: evitar los daños por fuego, robo y vandalismo, entre otros».

**—Para empezar, ¿podría ofrecernos datos concretos del Museo: número de trabajadores, número de visitas anuales, exposiciones...?**

—En el año 2015, un total de 107.624 personas visitaron el IVAM, un aumento de casi un 48% respecto al año anterior. Estas cifras han sido posibles con la mitad del presupuesto que tenía el IVAM hace cinco años, que ha pasado de 10.5 millones de euros a los 5.6 millones de euros actuales. El museo está llevando a cabo una política de puertas abiertas que ha tenido como consecuencia la apertura del IVAM al público, la apertura a las instituciones y la apertura a nuevos servicios. El IVAM ha mantenido la calidad expositiva sin que la merma del presupuesto le haya afectado.

**—A grandes rasgos, ¿cómo se organiza la seguridad de una instalación museística como es el Instituto Valenciano de Arte Moderno (IVAM), donde este elemento es una de sus máximas prioridades? ¿Cuál es la estructura e infraestructura actual del Área de Seguridad del IVAM?**

—El departamento está organizado jerárquicamente desde el área de Administración, con un director de Seguridad perteneciente a la plantilla y unos responsables Jefes de Equipo de la empresa de seguridad, junto a un servicio de vigilantes de salas de exposición y los vigilantes del Centro de Control.

La coordinación con los diversos departamentos del museo se realiza de forma diaria, atención al público, registro, conservación, mantenimiento, etc., puesto que es indispensable esta interrelación para el funcionamiento del departamento de Seguridad de forma eficaz en sus cometidos, sin interferir en el normal funcionamiento del museo. El arte moderno lleva consigo la dificultad del tipo de obras, tamaños, formas y materiales; no se puede tratar de forma lineal todas las exposiciones. Para cada una de ellas se deben adaptar medidas concretas para asegurarla, intentando interferir lo menos posible en la obra o exposición.

**—De manera general, ¿con qué medios y me-**

**didas de seguridad cuentan las instalaciones del Instituto Valenciano de Arte Moderno?**

—Sin entrar en detalles por motivos de la propia seguridad, el IVAM cuenta con todas las medidas necesarias para garantizar la seguridad de las personas, el patrimonio y el propio edificio. El departamento de Seguridad intenta mantener, optimizar y mejorar todos los medios físicos, técnicos y personales que nos ayudan a cumplir con la labor establecida para este departamento: evitar los daños por fuego, robo y vandalismo, entre otros.

**—¿Qué papel juega la tecnología a la hora de garantizar y mejorar la seguridad de los grandes centros museísticos como es el IVAM?**

Todos los elementos que componen la seguridad del IVAM son gestionados desde un Centro de Control, el auténtico cerebro que controla y gestiona los diversos sistemas de seguridad, CCTV, central de incendio, central de alarmas de intrusión y robo, vídeo grabadores, teléfonos y emisoras de radiofrecuencia durante las 24h. del día.

**—¿Cree que en los últimos años han cambiado los riesgos y amenazas a los que tienen que hacer frente los responsables de Seguridad de los museos españoles?**

—Creo que los riesgos y amenazas pueden ser de dos tipos: las fijas (robo, incendio, fenómenos naturales...), y otras variables que dependen del entorno social de donde proceden (terrorismo físico o tecnológico). Evidentemente, las tecnologías han cambiado y es necesario adaptar los medios de protección y el personal de seguridad a estas nuevas tecnologías, minimizando riesgos y amenazas, es necesario un continuo reciclaje del conocimiento y capacitación del personal que trabaja en la seguridad de un museo, tal y como sucede para todos los profesionales de distintos sectores.

**—¿Cree que existe en la sociedad actual la concienciación de la necesidad de proteger y conservar el patrimonio cultural?**

—La conservación del patrimonio es directamente proporcional al nivel de educación y formación de una sociedad. En el caso de España, este nivel ha aumentado de forma muy visible en las últimas décadas y este hecho ha facilitado su comprensión, estudio y disfrute.

**—Bajo su punto de vista, ¿cree que los usuarios de las instalaciones museísticas y centros de arte valoran las medidas de seguridad implantadas o, por el contrario, se trata de un hecho que pasa desapercibido?**

—La finalidad de las medidas de seguridad en un museo tiene como objetivo asegurar los bienes y las personas, pero no es menos cierto que deben hacer que el público se sienta lo más cómodo posible en su visita. Las funciones del departamento de Seguridad de un museo deben realizarse con discreción, sin dar una sensación molesta a los visitantes, discretos pero visibles. Bajo esta perspectiva, creo que el público en general las acepta y las valora satisfactoriamente

**—¿Cuáles considera que son las claves para una seguridad satisfactoria en este tipo de instalaciones?**

—El mantenimiento de las instalaciones y su adaptación a las nuevas tecnologías, junto con la formación del personal de seguridad en cuanto a emergencias, el conocimiento de sus cometidos dentro del plan de autoprotección del edificio, el conocimiento de los medios que utilizan, y algo que desde mi punto de vista es fundamental para desarrollar todos los cometidos: la participación e implicación del personal de seguridad del museo en los programas de formación.

**—¿Cuáles son las prioridades de seguridad para el responsable de Seguridad de una instalación como el IVAM?**

—No existe una prioridad única: todas nuestras funciones son igual de importantes y necesarias para garantizar la seguridad del museo. ●

*Texto: Gemma G. Juanes.*
*Fotos: IVAM*

**LUIS BARRIOS RINCÓN.** JEFE DEL ÁREA DE SEGURIDAD. MUSEO NACIONAL CENTRO DE ARTE REINA SOFÍA. MADRID

# «Incidimos mucho en la **seguridad global** para dar respuesta a posibles imprevistos»

PARA nosotros es prioritario prever las circunstancias que puedan poner en peligro la vida y la salud de las personas, tanto visitantes como trabajadores, así como las que atentan contra la integridad de las obras y del propio edificio», explica Luis Barrios Rincón, jefe del Área de Seguridad del Museo Nacional Centro de Arte Reina Sofía, quien además señala durante la entrevista cómo se organiza la seguridad de una instalación museística, así como las claves para conseguir una seguridad satisfactoria.

Museo Nacional Centro de Arte Reina Sofía
Vista de la fachada del Edificio Sabatini
Fotografía: Joaquín Cortés/Román Lores

**—Para empezar, ¿podría ofrecernos datos concretos del Museo: número de trabajadores, número de visitas anuales, exposiciones...?**

—El Museo Reina Sofía cuenta con, aproximadamente, uno 500 trabajadores; de ellos una parte importante desarrolla su labor en el área de Seguridad. En cuanto a la evolución de las visitas, hemos comprobado que se está produciendo un incremento que se mantiene en los últimos años. En concreto el pasado año, 3.249.591 personas visitaron los distintos espacios del Museo, incluidos los palacios de Velázquez y Cristal. El Reina Sofía organiza a lo largo del año, una media de 12 exposiciones, pero además, el visitante que se acerca al Museo no sólo puede contemplar muestras temporales, sino su colección permanente, con el Guernica como núcleo central, así como disfrutar de las numerosas actividades que se desarrollan en él: ciclos de cine, seminarios, conferencias, performances, conciertos, etc.

**—A grandes rasgos, ¿cómo se organiza la seguridad de una instalación museística como es el Museo Nacional Centro de Arte Reina Sofía, donde este elemento es una de sus máximas prioridades?**

—Contamos con un conjunto de medios humanos, físicos y técnicos, conjugados con una serie de medidas organizativas. En cuanto a los primeros, el Museo cuenta con dos colectivos, uno encuadrado en lo que se denomina Seguridad Privada, que se encarga fundamentalmente del control de accesos, seguridad interior y Centro de Control, y el personal de Control de Sala, que tiene encomendada la función de velar por la integridad de las obras expuestas en los distintos espacios durante el horario de apertura del Museo al público. Junto a los medios físicos puestos al servicio de la seguridad, destacan los técnicos: Sísmicos, magnéticos, volumétricos, barreras de rayos infrarrojos, CCTV, escáneres, etc.

Por supuesto que el Museo dispone de medidas organizativas de carácter general y otras más específicas, entre las que citaría los Protocolos de Actuación y Comunicación con las Fuerzas y Cuerpos de Seguridad, Bomberos, etc.

**—De manera general, ¿con qué medios y medidas de seguridad cuentan las instalaciones del Museo Nacional Centro de Arte Reina Sofía?**

—Con el elemento imprescindible que es el personal de seguridad, y con todas y cada una de las herramientas que la tecnología punta más avanzada nos ofrece.

**—¿Cree que en los últimos años han cambiado los riesgos y amenazas a los que tienen que hacer frente los responsables de Seguridad de los museos españoles?**

—A la hora de planificar las estrategias a seguir para lograr el mayor nivel posible

de seguridad se tienen en cuenta todos los riesgos presentes y futuros, intentando prever el mayor número de hipotéticas circunstancias adversas, aunque hay que decir que el riesgo 0 no existe. Incidimos mucho en la seguridad global para dar respuesta a posibles imprevistos. Se trata de dotarnos del personal necesario (seguridad humana), los medios técnicos (instalaciones y sistemas de seguridad electrónicos, activos y pasivos), para llegar a un equilibrio entre la prevención y la protección. En concreto se está trabajando en un Plan de Protección de Colecciones ante Emergencias, en cuyo desarrollo están implicados diversos departamentos del Museo (Restauración, Colecciones, Exposiciones, Arquitectura, Registro de Obras de Arte, etc.).

**—¿Cree que existe en la sociedad actual la concienciación de la necesidad de proteger y conservar el patrimonio cultural?**

—Creo que se ha evolucionado bastante en este terreno y que fruto de la enorme labor de divulgación que se ha desarrollado en los últimos años, haciendo hincapié en la importancia de la conservación y defensa de nuestro patrimonio, la gente es cada vez más sensible y está mejor informada. En general la población es bastante respetuosa y eso se nota en la visita y en la aceptación de determinadas normas que, si bien a veces pueden parecer innecesarias o molestas, contribuyen precisamente a eso, a proteger al máximo el patrimonio.

**Museo Nacional Centro de Arte Reina Sofía**
Edificio Nouvel. Patio central
Fotografía: Joaquín Cortés/Román Lores

**—Bajo su punto de vista, ¿cree que los usuarios de las instalaciones museísticas y centros de arte valoran las medidas de seguridad implantadas o, por el contrario, se trata de un hecho que pasa desapercibido?**

—Creo que, en general, se valoran y respetan.

**—¿Cuáles considera que son las claves para una seguridad satisfactoria en este tipo de instalaciones?**

—El intentar cubrir todos los posibles riesgos que puedan existir de cara a la conservación de las obras, tanto las expuestas como las que se encuentran en los almacenes, pero también la seguridad de los visitantes, adoptando las medidas que permitan todo ello. Además de disponer de medios técnicos que ayuden a incrementar la seguridad, es imprescindible la formación del personal implicado directamente e indirectamente en la seguridad del Museo. También hay que intentar adoptar el mayor número de medidas de seguridad que resulten eficaces en todos los terrenos, sin que el visitante se sienta abrumado, lo que le permitirá disfrutar de la visita con normalidad.

**—¿Cuáles son las prioridades de seguridad para el responsable de Seguridad de una instalación como el Museo Nacional Centro de Arte Reina Sofía?**

—Para nosotros es prioritario prever las circunstancias que puedan poner en peligro la vida y la salud de las personas, tanto visitantes como trabajadores, así como las que atentan contra la integridad de las obras y del propio edificio. ●

***MARCEL BROODTHAERS. Una retrospectiva.*** Vista de sala
***MARCEL BROODTHAERS. A retrospective.*** Exhibition room
Museo Nacional Centro de Arte Reina Sofía, 2016
Fotografía/Photography: Joaquín Cortés/Román Lores

*Texto: Gemma G. Juanes.*
*Fotos: Museo Reina Sofía*

**JUAN JOSÉ PINTADO GARCÍA.** JEFE DEL DEPARTAMENTO DE SEGURIDAD. MUSEU NACIONAL D´ART DE CATALUNYA

# *«El departamento de Seguridad es **pieza indispensable** en cualquier museo de envergadura **para protegerlo adecuadamente**»*

NO cabe duda que una de las mayores amenazas de nuestro tiempo, no solo en instituciones museísticas, sino en cualquier actividad empresarial, política o de cualquier sector, son las ciberamenazas o ataques virtuales, de ahí la importancia que tiene dentro de la estructura de un museo de relevancia, el departamento de Informática coordinado con el departamento de Seguridad». Así lo asegura Juan José Pintado García, jefe del departamento de Seguridad del Museu Nacional d´ART de Catalunya, quien analiza para Cuadernos de Seguridad los elementos fundamentales a la hora de plantear una seguridad integral en un museo, así como los pilares sobre los que debe asentarse la seguridad en este tipo de instalaciones.

**—¿Cómo ha variado la seguridad, en cuanto a logística y estrategia, en los grandes centros museísticos como es el caso del Museu Nacional d´ART de Catalunya?**

—Cuando me hice cargo de la seguridad del museo, concretamente en el año 2002, éste como tal ya disponía de un departamento de Seguridad registrado en el Ministerio del Interior y en el Departament d'Interior de la Generalitat. Esto demuestra que por parte de mi antecesor y la dirección del museo en aquellos momentos tenían claro, que como mínimo, el futuro de la seguridad del fondo museístico y de la institución pasaba por la creación del departamento de Seguridad, pieza indispensable en cualquier institución museística de envergadura para protegerlo adecuadamente. Tuve la oportunidad de coincidir con una reforma total del edificio y participé tanto en el proyecto arquitectónico como en el artístico en el apartado de instalaciones de seguridad.

El reto más importante era adaptar y consolidar este edificio histórico y singular a las necesidades de ingeniería actuales, tanto energéticas como de seguridad. Para ello toda actuación debía de ser coordinada través de una dirección facultativa en la que todos los departamentos implicados exponíamos nuestras necesidades. En el caso del departamento de Seguridad teníamos clara una estrategia de seguridad, no mirar al pasado sino al futuro. Para ello intenté asesorarme al máximo, a nivel de ingenierías y de las experiencias de otras instituciones museísticas, hasta que optamos por una decisión que en

el futuro no significara un problema integrar cualquier sistema actualizado. Actualmente, transcurridos estos años, la tecnología ha evolucionado mucho y en concreto el cambio de la tecnología analógica a digital, estamos precisamente en este estadio, aprovechado la infraestructura ya incorporada a través de red, para migrar el sistema a digital.

**—En un mundo globalizado, donde somos objeto de ciberamenazas y ataques virtuales, ¿están los museos expuestos a estos nuevos tipos de riesgos y amenazas? ¿Están preparados los centros museísticos para hacer frente a estos riesgos?**

—No cabe duda que una de las mayores amenazas de nuestro tiempo, no solo en instituciones museísticas, sino en cualquier actividad empresarial, política o de cualquier sector, son las ciberamenazas o ataques virtuales, de ahí la importancia que tiene dentro de la estructura de un museo de relevancia, el departamento de Informática coordinado con el departamento de Seguridad.

Nuestras instituciones como todos sabemos están dentro de plataformas o programas en las que están la mayoría de museos para disponer de la máxima información sobre sus fondos artísticos, las cuales sirven para estudiar, prestar y difundir los conocimientos de éstos. Esta plataforma o programa informático requiere de unos niveles de seguridad en la red importantes. Nuestro departamento junto al de informática trabaja en equipo para dar respuesta a cualquier incidencia que afecte a la institución.

**—¿Cuáles considera que son actualmente los elementos fundamentales a la hora de plantear una seguridad integral y convergente en un centro museístico?**

—La optimización de todos los recursos de los cuales se dispone. Cuando nos referimos a optimizar, estamos hablando de la necesidad de equilibrar estos recursos con la respuesta adecuada a cualquier alarma o evento. En mi institución disponemos de la instalación de sistemas electrónicos de seguridad de Intrusión, Control de Accesos, CCTV, Detección y Extinción de Incendios, todos gestionados desde un centro de control en el edificio; la respuesta a cualquier incidencia que nos puedan comunicar éstos, debe de ser realizada por la vigilancia de seguridad. La importancia está en que la respuesta por parte del servicio de vigilancia sea eficaz y rápida, no sirve de nada disponer de un sistema muy bien dotado, si no tiene una respuesta adecuada. En los museos hay público, personal que trabaja, mobiliario, fondo artístico, documentación, investigación, etc., para que el ciudadano pueda disfrutar de ello, se requiere de los medios suficientes para su protección.

**—¿Cree que los grandes centros museísticos siguen apostando actualmente, pese a la situación de incertidumbre económica y política, por la inversión en seguridad?**

—En concreto nosotros como museo nacional tenemos un órgano rector representado en un patronato por 50% Generalitat de Catalunya, 25% Ayuntamiento de Barcelona y 25% Ministerio de Cultura del Estado. Esto significa que estamos a expensas de la dotación presupuestaria que nos viene por parte de estas administraciones. No cabe duda que la incertidumbre económica y política tienen mucha incidencia, prueba de ello es que en los últimos 5 años nuestro presupuesto se ha visto reducido en un 25%.

Como departamento de Seguridad hemos optimizado todos nuestros recursos presupuestarios, sin que ello signifique bajar niveles de seguridad, sobre todo aprovechando a través de concursos de licitación, con todas las ventajas que te ofrecen las mejoras de los mismos, conjugar en lo posible la falta de inversión.

**—Con una visión de futuro, ¿cómo imagina el futuro de la seguridad en los museos donde los grandes avances tecnológicos serán los protagonistas?**

—Un departamento de Seguridad ha de estar siempre investigando las posibilidades de mejorar tecnológicamente

su instalación aprovechando las novedades que te ofrece el mercado. Nuestra instalación de CCTV está efectuando un paso determinante a la conexión digital. Ésta es nuestra apuesta más importante de cara al futuro. En la medida que los museos dispongan de una red para la conexión a través de IP, veremos incrementada esa protección del patrimonio a través de sistemas que te darán más información y precisión sobre las posibles amenazas. Creo que sí, los avances tecnológicos serán protagonistas, esta dimensión del paso del sistema de conexión analógica a la digital nos dará muchas más posibilidades de cara al futuro de los museos, te ofrecerán mejor y más información sobre la incidencia en las obras y en el control, pero no en la respuesta; ésta sigue siendo esencialmente humana (el Vigilante de Seguridad). Importante su formación y su aptitud.

**—¿Cree que hoy en día las empresas responden adecuadamente a las necesidades de seguridad de los centros museísticos?**

—Por lo que llevo observando, cuando las empresas a nivel comercial te vienen a ofrecer sus productos, miran que éstos que sirvan para otros sectores, se pueden adaptar a tus necesidades como institución museística. Las obras de arte para su protección directa requieren de sistemas que en la mayoría de ocasiones son muy específicos, y en muchos casos de adaptación al medio donde se encuentran éstas. Hay pocas empresas que se dediquen de forma específica y única a la comercialización de sistemas para la protección directa del patrimonio. Todas te ofrecen el producto generalizado para diferentes sectores para que lo apliques en la protección del patrimonio, a veces es aplicable y otras no. Como departamento hemos de racionalizar e investigar si el producto que adquirimos cubre las necesidades de protección que nosotros exigimos.

**—¿Cuáles son los pilares sobre los que debe asentarse hoy en día la seguridad de un museo?**

—Es básico que todo el personal que trabaja en una institución museística asuma que la aportación que está haciendo laboralmente es determinante para que futuras generaciones se encuentren el patrimonio igual o mejor que como nos lo dejaron nuestros antecesores. Por tanto, no ha de ser únicamente el personal destinado a seguridad el responsable de la protección del patrimonio, sino que tanto a nivel de información, como del cumplimiento de los protocolos de seguridad, colaboren de forma efectiva el personal que trabaja (restauradores, conservadores, documentación y registro, mantenimiento, administrativos, etc).

Otro de los pilares básicos de seguridad de un museo es disponer de un departamento de Seguridad, sobre todo dependiendo de volumen y valor del fondo. Al frente del mismo ha de haber un director de Seguridad, que será la persona que se encargará de que todo el personal laboral a través de una formación asuma esa responsabilidad de la que hablamos. La figura del director de Seguridad también es la que se va encargar de diseñar y coordinar toda la seguridad integral dentro de la institución, por medio de la instalación de sistemas electrónicos (activos y pasivos) y la vigilancia humana de seguridad.

Otro pilar básico es también la formación del personal tanto de seguridad como de otros departamentos implicados en planes de autoprotección y planes de seguridad. Es importante tener claro cómo han de reaccionar delante de posibles amenazas. ●

*Texto: Gemma G. Juanes.*
*Fotos: MNAC*

# El acceso inteligente

**El socio de confianza que aporta soluciones de acceso innovadoras y seguras en todo el mundo**

Le ofrecemos un servicio completo que incluye desde el asesoramiento en su proyecto hasta la implementación y el correspondiente servicio posventa.

**dorma+kaba**
María Tubau 4
28050 Madrid
España

T: +34 91 736 21 10

www.dormakaba.com

dormakaba

**JESÚS ALCANTARILLA DÍAZ.** PRESIDENTE DE PROTECTURI

# **Decálogo** para los nuevos retos de la **protección del patrimonio cultural**

SIEMPRE he entendido que la seguridad de una institución cultural es un ejemplo patente, y tantas veces imperceptible, de transversalidad organizativa. Los profesionales de la protección deberían de estar presentes desde el diseño de la infraestructura, para proyectar el programa de seguridad integral adecuado y proporcional a los bienes, las personas y el programa de usos de los diferentes ámbitos del equipamiento.

Para aportar mi grano de arena a esta labor, he querido embarcarme en la elaboración de una propuesta de decálogo, y como tal incompleto, de lo que serían algunos de los factores que concretan y explican nuestra labor y nuestra misión como responsables de la protección del patrimonio cultural. Pero antes de presentarlo, quiero plantear unas cuestiones previas.

PROTECTURI, desde su fundación, se marcó la prioridad de mediar entre los diferentes agentes involucrados en la protección del patrimonio para generar espacios de diálogo.

Estábamos convencidos de que ese contacto sería fructífero, y que requeriría, por parte de los responsables de la protección de:

1. Sistematización de los contenidos.
2. Pedagogía con los fines.

Sistematizamos nuestra experiencia sectorial redactando el Sistema de Gestión de la Protección del Patrimonio Cultural. Un recurso que está al alcance de los diferentes agentes del patrimonio cultural. Su desarrollo, contextualizador y técnico, permite conocer qué efectos tiene sobre una organización la adopción de una cultura de la seguridad adecuada para cada centro.

Implícitamente, a ningún profesional se le escapa las consecuencias de una actitud mecanizada que no valore, diariamente, los efectos que sobre su organización tienen los contextos internos y externos.

El responsable de Seguridad, a similitud del dios Jano de la mitología romana, es el responsable de las «puertas» del equipamiento. Como él, mira hacia el interior, pero como bifronte, también mira hacia el exterior. Quizás sea una de las metáforas, uno de los mitos, que mejor represente la misión de la dirección de seguridad. Esa doble mirada, que integra los contextos internos y externos de la institución, hace que nuestra labor se difumine a los ojos de quien desconoce ese enfoque múltiple.

Dadas las circunstancias socioeconómicas globales y el impacto del desarrollo tecnológico, el binomio actitud y mentalidad se convierte en un factor determinante para proteger los bienes y las personas. Este quizás sea uno de los principios que definen, no sólo la calidad, sino la viabilidad de un programa de seguridad de cualquier centro cultural.

Quienes nos hacemos cargo de la dirección de la seguridad de una institución cultural, debemos tener un conocimiento transversal de nuestra organización. Sólo así podremos diseñar un modelo de protección ad hoc a las necesidades reales del mismo.

Caer en la tentación de ser, o atrincherarse en ser, exclusivamente un

«técnico» en seguridad, sería, a mi parecer, no sólo contraproducente, sino un riesgo inaudito. Entre otros argumentos, porque los ámbitos de actuación son muy amplios y el desarrollo tecnológico experimenta un ritmo exponencial.

Un responsable de Seguridad además de ser un experto que debe prepararse de manera constante, estar atento a los cambios y ser minucioso en los procesos, creo que debe ser un mediador. Alguien capaz de conocer los entornos que pueden afectar la realidad de su centro, para establecer las conexiones y las redes que beneficien la cultura de la seguridad del patrimonio y mediar con el resto de agentes. Más adelante abundaré en esta idea.

Otro de los factores que considero esencial en nuestro quehacer profesional es la pedagogía. Nuestra agenda sectorial debe incorporar un enfoque pedagógico, interno y externo, de una conceptualización contemporánea de la seguridad en entornos culturales. Sólo así podremos hacer comprender las necesidades organizativas que reclama ese futuro en el que ya estamos viviendo. Tenemos que ser didactas, no sólo de la labor que realizamos, sino de la misión encomendada, de los objetivos específicos, y de qué supone un programa de seguridad en un sistema complejo como es un museo o cualquier otra institución cultural.

Será así como podremos lograr que el resto de agentes implicados en la «conservación» del patrimonio cultural sean conscientes de que la seguridad no es una batería de medidas y recursos, sino que, esencialmente, es planteamiento estratégico de prevención transversal e integral.

Como he mencionado con anterioridad, considero que, más allá de las responsabilidades técnicas y organizativas inherentes a sus funciones, el director de Seguridad debe ser un mediador con gran parte de los agentes externos del centro.

Brevemente, destacaría dos de ellas.

La primera mediación la realiza con las instituciones públicas y con las Fuerzas y Cuerpos de Seguridad Pública. La globalización y la tecnología, entre otros factores, han hecho emerger riesgos y amenazas que sólo pueden ser atendidos desde una colaboración basada en la confianza y la confidencialidad.

Prueba de ello es la participación de PROTECTURI en las mesas de trabajo para la confección de sugerencias e ideas enfocadas en la protección del patrimonio cultural, tanto en la ley 5/2014, como en el reglamento que se está «cocinando». Nos tranquiliza en lo referente a los procesos de mejora, integrando el concepto de seguridad integral patrimonial.

La segunda mediación se da con las organizaciones que proveen de servicios y recursos, humanos y técnicos, a la institución. Si algo define a un museo es ser un espacio de múltiples y dinámicas realidades. Algunas de ellas imprevisibles, atendiendo a la participación del público. El responsable de Seguridad debe, con las empresas proveedoras, establecer una relación de continuidad y seguimiento. Debe ayudar a los responsables organizativos y técnicos de las mismas a que entiendan, e interioricen, los valores añadidos de ofrecer sus servicios en una organización cultural. Esta realidad dinámica sólo será correspondida con un programa óptimo si el departamento de Seguridad transforma su papel de cliente en un traductor-mediador de la realidad del museo.

Para finalizar, quisiera esbozar un «decálogo» de lo que considero que debe significar a los profesionales y responsables de la prevención, protección y salvaguarda del patrimonio cultural en los entornos profesionales emergentes.

El director de Seguridad debe:

1. Conocer sus obligaciones y responsabilidades, las genéricas de su cargo y responsabilidades, y las específicas del centro.

2. Interiorizar el binomio actitud-mentalidad como una directriz en todas sus actuaciones.

3. Asumir que la seguridad al 100 x 100 no existe y transferirlo al resto de la organización.

4. Perseverar para disponer de los conocimientos, los recursos y las medidas adecuadas para alcanzar las cuotas más altas de eficacia y eficiencia en cada una de las situaciones.

5. Promover una cultura de la seguridad específica, e intrínseca, para la seguridad de sus entornos profesionales.

6. Responsabilizarse de su ámbito de actuación como factor vertebrador de la institución, para que la seguridad sea percibida como factor prioritario garante del adecuado desarrollo de los colectivos humanos que trabajan o visitan la institución y la protección de los bienes.

7. Crear una red de colaboración, interna y externa, que proyecte y coopere en dar respuesta a los retos, sus riesgos, sus amenazas y sus vulnerabilidades.

8. Mediar para integrar a los diferentes agentes del sistema y maximizar sus potencialidades.

9. Colaborar en la generación de un entorno de datos masivos (Big Data).

10. Transformar los datos en conocimiento e inteligencia como principales recursos para el programa de seguridad integral, generador de confianza y tranquilidad profesional y social.

Y como última consideración desearía que los profesionales que nos dedicamos a la protección del patrimonio cultural hiciésemos nuestro el lema «unus pro ómnibus, omnes pro uno», es decir «uno para todos y todos para uno», con toda humildad ante la complejidad de los entornos en los que actuamos.

Agradecer a Cuadernos de Seguridad esta nueva oportunidad para poder escribir y compartir una batería de reflexiones, que tienen la voluntad de sumar para multiplicar en este trabajo diario de velar por la protección del patrimonio cultural. ●

Fotos: *Protecturi*

safire

# IP CÁMARAS

## ADVANCE SERIES

- Mayor Resolución 2Mp & 4 Mp
- WDR Real (120 dB)
- H.264/H.264+
- Audio, Alarmas, PoE, Slot SD
- Video Content Analytics

ONVIF

Distribuidores oficiales:

www.jmsystems.es

Avantech Electronics
www.avantech.info

VISIOTECH
www.visiotech.es

SAFIRE
www.safirecctv.com
info@safirecctv.com

**ROBERTO OTERO.** TECHNICAL MANAGER DE HIKVISION SPAIN


# Pyronix & Hikvision

**Hikvision planea aplicar la experiencia y el know-how de Pyronix en sistemas de intrusión, en el desarrollo de nuevos avances y productos innovadores para el mercado de la seguridad**

EN mayo de 2016 Hikvision adquirió la compañía inglesa Pyronix, especializada en productos para la protección contra la intrusión. Fundada en 1986, Pyronix cuenta con múltiples patentes para sus diseños y tecnologías, y ha ganado numerosos premios por la innovación de sus productos y soluciones.

Con esta compra, Hikvision planea aplicar la experiencia y el know-how de Pyronix en sistemas de intrusión, en el desarrollo de nuevos avances y productos innovadores para el mercado de la seguridad, uniendo las tecnologías de videovigilancia e intrusión.

Hikvision ha creado un departamento de desarrollo para Intrusión con más de 500 ingenieros, que junto con la colaboración del departamento de I+D de Pyronix, están ya diseñando la nueva revolución en el mercado de la seguridad.

Hikvision ha iniciado la comercialización de los productos y soluciones de Pyronix, entre los que se encuentran paneles de intrusión cableados de Grado 2 y 3, centrales vía radio de Grado 2, y una amplia gama de detectores de interior y exterior, tanto cableados como vía radio.

Dentro de los detectores de exterior destacan los XDH10TT-AM.

## XDH10TT-AM – Detección de exterior de alta seguridad

El detector de exterior para montaje en pared, XDH10TT-AM, exhibe la innovación, la fiabilidad y la calidad con la que Pyronix ha construido su reputación. Es un detector cableado el cual combina una serie de tecnologías avanzadas y consolidadas que mantienen un alto rendimiento incluso en las condiciones más extremas.

Ideal tanto para instalaciones residenciales como comerciales, cuenta con Tecnología de Triple-Detección, combinando dos sensores PIR con un sensor de microondas, y está construido dentro de una nueva y mejorada carcasa de plástico, que hace la instalación y configuración aún más rápida y sencilla.

**Altura de instalación y alcance de detección**

El detector XDH10TT-AM proporciona una cobertura volumétrica de 10m en ambas lentes. El alcance del detector se determina mediante una combinación de las tres tecnologías de detección (Rango de Triple Detección).

En el modo de instalación a 2,4m (lente 5, rango de 10m), el detector se instala a una altura de 2,4m para proporcionar cobertura volumétrica, con inmunidad contra animales de hasta 10kg (esta es la configuración predeterminada de fábrica).

**Tecnología**

La Lógica de Triple Señal de Detección con la que cuenta el XDH10TT-AM mejora notablemente su estabilidad, ya que detecta la presencia de un ser humano en base al análisis avanzado de las tres tecnologías de detección. Esto significa que las tres tecnologías deben ser activadas para provocar una alarma.

Gracias a las múltiples frecuencias del microondas, el XD también proporciona una instalación flexible, minimizando los efectos de colisión entre microondas. Con cada frecuencia indicada con una etiqueta de color diferente, se pueden instalar múltiples detectores próximos entre sí.

La Compensación Digital de la Temperatura permite que el detector XD se autoajuste para mantener el rango de detección en entornos cambiantes, mientras que la tecnología de Eliminación de Oscilaciones de la Vegetación está dirigida a mantener el detector estable cuando está instalado cerca de vegetación, como árboles.

El XDH10TT-AM también utiliza otra serie de contrastadas tecnologías patentadas por Pyronix, incluyendo la tecnología IFT (Independent Floating Thresholds) con Umbrales Variables Independientes. Estos permiten al detector ajustar automáticamente los umbrales de disparo de alarma, filtrando las interferencias causadas por perturbaciones tales como iluminación, pequeños objetos que caen, insectos, lluvia, nieve y otros.

También cuenta con la tecnología patentada de Triple Anti-Masking, que ofrece protección contra el enmascaramiento tanto para los detectores PIR como para el microondas. Esta tecnología crea una burbuja protectora de anti-enmascaramiento delante del detector, que es ajustable de 0 a 1m. Una vez que la burbuja protectora ha sido atravesada y cualquier tecnología está enmascarada por sustancias como aerosoles, lacas, papel, cinta adhesiva o cajas de cartón, el XD activará el relé de anti-enmascaramiento destinado para ello. El XD también tiene filtros de ultravioleta resistentes para protegerlo contra la fuerte radiación ultravioleta a gran altura o al nivel del mar.

Con Ópticas Selladas Impermeables, la fijación de la lente del XD ha sido diseñada para sujetar firmemente la lente en su lugar y crear una cámara medioambiental estable entre ella y el sensor PIR. La junta de goma en la lente y la junta de espuma en el sensor PIR se utilizan como un sellador adicional contra todas las condiciones climáticas y la humedad. Además, la cámara sellada del sensor de PIR protege los sensores de PIR de una potencial infestación de insectos, así como del movimiento interno del aire.

**Otras características**

Tradicionalmente, una prueba de paseo en el exterior puede ser difícil y llevar mucho tiempo, teniendo que volver a consultar a la central o confiar en ver los LED de alarma a distancia. El detector XD incorpora un Zumbador de Prueba de Paseo que reduce drásticamente este proceso, emitiendo un pitido para indicar una activación de alarma. Esto permite una prueba de paseo rápida y sencilla durante el proceso de instalación, junto con una indicación audible de una presencia dentro del área de detección (si es necesario). El zumbador se puede desactivar si no es necesario.

El XDH10TT-AM también tiene un soporte opcional con tamper, que permite ocultar los cables por dentro del soporte, facilitando la instalación y aportando una mayor seguridad. El soporte también se mueve 45 grados a izquierda y derecha para permitir una total cobertura del área de hasta 90 grados.

El XD se suministra con dos rejillas de enmascaramiento (fijas y adaptables), que se pueden utilizar para tapar zonas a cubrir por los sensores PIR según sea necesario, sobre todo cuando se utiliza junto con los soportes opcionales.

Con el XDH10TT-AM Pyronix prosigue su historia de 30 años de innovación y mejora continua, creando el detector de exterior más adaptable y robusto. ●

> «El detector de exterior para montaje en pared, XDH10TT-AM, exhibe la innovación, la fiabilidad y la calidad con la que Pyronix ha construido su reputación. »

Fotos: *Hikvision*

Contactos de empresas, p. 9.

**FERNANDO PIRES.** VICEPRESIDENTE DE VENTAS Y MARKETING. MORSE WATCHMANS

# Diseño ergonómico del **sistema de gestión de llaves**

## Ofrece beneficios prácticos

DESDE el siglo XVIII, se ha estudiado el lugar de trabajo en relación con el trabajador. En el siglo XXI, el principio se sigue estudiando, pero ahora bajo un nombre más amplio: ergonomía. La palabra ergonomía proviene de la palabra griega ergos (trabajo) y nomos (leyes naturales). En un lugar de trabajo ergonómico, las tareas y las herramientas están diseñadas en función de las capacidades y las limitaciones individuales, para que las personas puedan hacer sus tareas con mayor confort y conveniencia, sin lesionarse. En un sentido más amplio, la ergonomía puede aplicarse para optimizar sistemas de mayor envergadura, como gestión de recursos, diseño de trabajo, interfaces humano-máquina, etc., dentro de la organización (de allí el término «ergonomía organizacional»).

Cuando nuestra compañía se estaba abriendo camino en la industria de la seguridad con un sistema de gestión y control de llaves automatizado, la ergonomía era fundamental para su diseño. Estudiamos la manera en que las personas de todo tipo usarían el dispositivo para asegurarnos de que la pantalla tuviera la posición correcta para que se pueda ver bien, que el acceso con llave fuera rápido y no estuviera obstruido y, cuando se instalaban dos o más gabinetes, que las aperturas de las puertas fuesen uniformes.

## Seguridad, facilidad de uso...

Estos hallazgos particulares, junto con muchas otras pruebas y estudios, se usaron para desarrollar un sistema de control de llaves que abarcara cuatro principios fundamentales del diseño ergonómico: seguridad, facilidad de uso, productividad/rendimiento y estética. Luego están los beneficios propios de los sistemas de control de llaves inteligentes, que se ajustan a esos principios de diseño ergonómico.

**Seguridad:** está de más decir que si las llaves se guardan en el lugar equivocado y los bienes se extravían, la seguridad del individuo puede verse comprometida. Para ello, el diseño de un gabinete resistente al vandalismo ayuda al personal de seguridad a garantizar que las llaves importantes estén seguras y protegidas del acceso no autorizado, mientras que los anillos de bloqueo de acero inoxidable refuerzan la seguridad de las llaves, ya que evitan el uso indebido. El diseño se complementa con un sistema de alarma incorporado, que suena si se intenta violar la seguridad del gabinete o si se ingresan códigos incorrectos reiteradamente. El acceso a los gabinetes y a las llaves individuales está controlado en todo momento, y absolutamente todas las llaves están registradas. Cuando hay conexión en red, un firewall y tecnología de encriptación AES256 para el intercambio de datos entre el gabinete y el servidor ayudan a proteger el sistema y los bienes de la organización.

**Facilidad de uso:** desde el pun-

to de vista físico, los gabinetes con llaves de seguridad están diseñados para ofrecer la flexibilidad necesaria para su instalación en prácticamente cualquier altura que permita al usuario alcanzarlos y utilizarlos con facilidad. Una consola inclinada proporciona un ángulo de visión natural, y permite pasar fácilmente la tarjeta por el lector o usar el sistema de identificación de huellas digitales para acceder al gabinete. Una vez abierto el gabinete, la ubicación de la llave solicitada se ilumina para que el usuario pueda identificarla fácilmente. Las pantallas táctiles más grandes y las indicaciones de voz ayudan a que la interacción sea más rápida y conveniente, y permiten mejorar la productividad.

**Productividad / Rendimiento:** las llaves están sujetas a un llavero que tiene un microchip de identificación y un anillo de bloqueo de acero inoxidable. El llavero de seguridad entra en la ranura para llaves del gabinete y registra automáticamente toda actividad de acceso. No hay que pasar más tiempo registrando la actividad con las llaves manualmente. Los datos registrados permiten a los usuarios autorizados determinar con más facilidad quién sacó las llaves y cuándo debe devolverlas; además, las alertas por correo electrónico o mensaje de texto simplifican la gestión aún más, ya que avisan si una llave no se devolvió o cuándo se devolvió. Sin duda que los sistemas de inventario de llaves con tecnología de seguimiento integrada pueden ayudar a evitar que se pierdan las llaves y reducir puntos vulnerables (además del tiempo perdido y la frustración del usuario).

> «Los datos registrados permiten a los usuarios autorizados determinar con más facilidad quién sacó las llaves y cuándo debe devolverlas»

**Estética:** el gabinete, con diseño estéticamente agradable y pantalla de la ubicación organizada de las llaves, es mucho más atractivo que un casillero de llaves desordenado. Los gabinetes están diseñados de manera tal que pueden instalarse de forma horizontal o vertical; además, el usuario tiene la posibilidad de instalar múltiples unidades a la perfección para mantener una apariencia profesional. En el diseño también se tuvo en cuenta el mantenimiento del sistema, el cual puede hacerse con interrupciones mínimas y sin tener que desarmar la unidad.

Estos beneficios de los sistemas de inventario de llaves, y muchos otros, son acumulativos, lo cual ayuda a simplificar la vida a los usuarios, respaldar las actividades de la compañía y reducir el riesgo de pérdidas. Todas estas son buenas noticias para las empresas; ¿quién dijo que el buen diseño no puede ir de la mano con el buen precio? ●

Fotos: *Morse Watchmans*

Contactos de empresas, p. 9.

**ALFREDO GUTIÉRREZ.** BUSINESS DEVELOPMENT MANAGER PARA IBERIA. MOBOTIX AG

# Sistemas de **última tecnología**

## Protección eficaz del patrimonio artístico

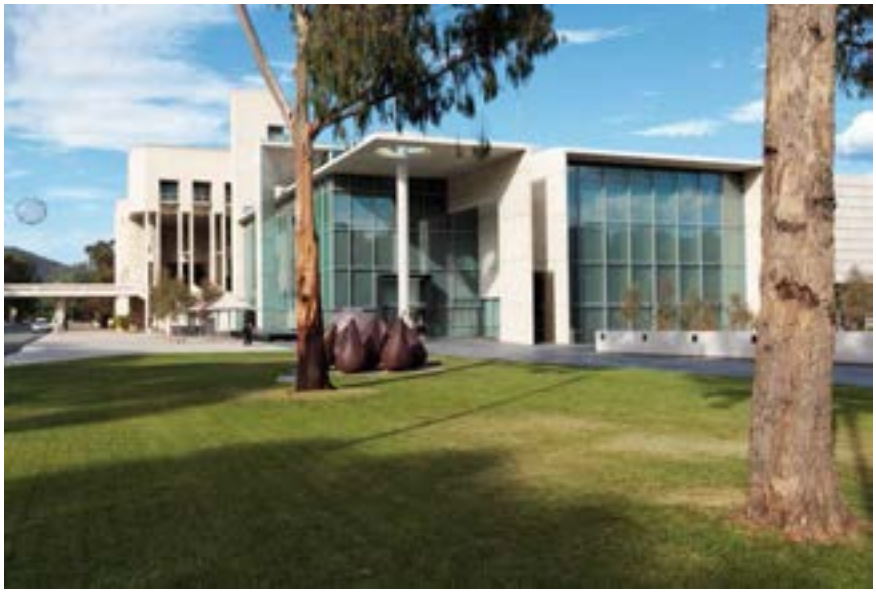
TODO patrimonio artístico, ya sea público o privado, precisa un grado de seguridad acorde al valor de los bienes que se encuentran en su interior. Al hablar de valor no solo nos referimos al económico, pues cada una de las obras alberga un significado especial con connotaciones tradicionales, emocionales o religiosas.

Los museos son instituciones públicas o privadas que cumplen con unas funciones sociales y culturales imprescindibles para la historia o la pedagogía y que resultan transcendentales para la humanidad. No obstante, y pese a que su custodia nos concierne en cierta medida a todos, en diversas ocasiones las pérdidas, daños y deterioros que se han producido en estos lugares han sido irreparables.

### Peligros y riesgos a tener en cuenta

Debido a su permanente exposición, pueden ocurrir innumerables altercados en el interior de estos lugares. Por un lado, es necesario prestar atención a la gran afluencia de visitantes que se congrega en las distintas salas en un mismo tiempo. Continuamente el personal debe estar alerta para que ninguna obra sea manoseada, para que no se tomen fotografías con flash que los puedan deteriorar, o simplemente para que no suceda nada fuera de los patrones establecidos.

También es interesante contar con algún sistema que tenga la capacidad de registrar datos acerca del aforo diario, con el objetivo de realizar estudios que aporten información útil a la institución.



Por otro lado, es realmente importante asegurar la protección cuando el museo se encuentra cerrado al público. El valioso material que atesoran convierte estos espacios en una magnífica oportunidad para los intrusos.

Partiendo de esta base, se necesitan una serie de herramientas que proporcionen la seguridad demandada y que cumplan con los requisitos que exigen estos emplazamientos.

### Sistemas especializados

Pese a que lo habitual es disponer de personal cualificado encargado de mantener el control y proteger todas las estancias, lo ideal es que exista un sistema de videovigilancia capaz de complementar la labor física de los vigilantes.

De hecho, este fue el motivo por el que el director general de la Galería de Arte de Australia vio la necesidad de contactar con nosotros con el propósito de solventar esta carencia. «Para poder llevar a cabo este tipo de vigilancia de forma efectiva, tenemos que poder monitorizar todo el espacio de la galería en tiempo real durante el horario de apertura, y tener acceso a grabaciones de calidad fáciles de manipular fuera de este horario», explica el director de Seguridad de la Galería de Arte de Australia.

riscogroup.es

RISCO GROUP

Smart Home

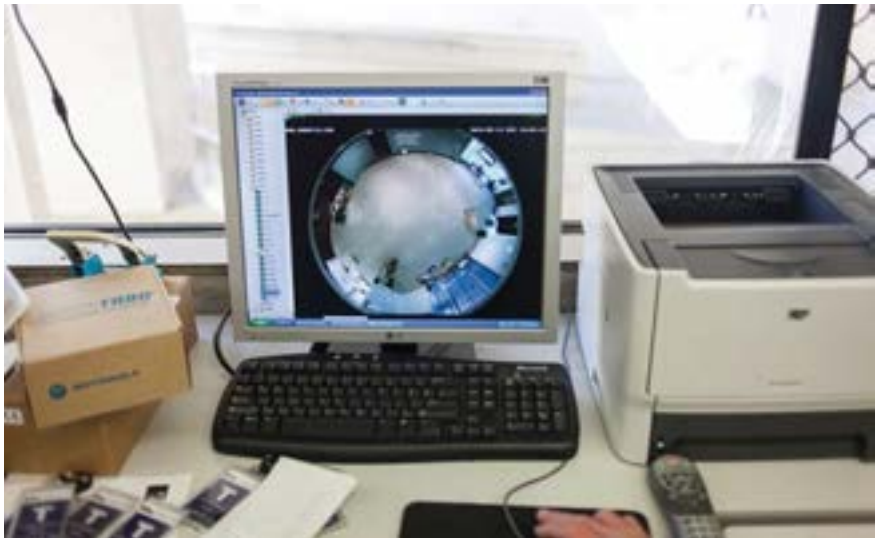
# Smart Home de RISCO, tu Elección Inteligente

## Seguridad y Gestión del Hogar total

Haz la elección INTELIGENTE y mantente a la vanguardia de las últimas tecnologías en el mercado de soluciones de seguridad ofreciendo Smart Home de RISCO. Puedes ofrecer más a tus clientes con una solución profesional de seguridad que combina la vídeo vigilancia con la gestión energética, el acceso inteligente y los dispositivos del hogar conectados – todo ello gestionado desde una única e intuitiva aplicación.

Smart Home de RISCO es la opción más inteligente para un estilo de vida moderno y simplificado ofreciendo comodidad y tranquilidad.

**RISCO Group Iberia** | riscogroup.es | Tel.: 91 490 21 33 | e-mail: sales-es@riscogroup.com



En estos espacios es imprescindible que la solución de videovigilancia con la que se cuenta disponga de cámaras IP de alta resolución, para tener imágenes claras que permitan ver en detalle y que, en caso de incidente, se pueda reconocer cualquier objeto o persona con precisión.

Por otro lado, sería interesante contar con sistemas de detección térmica que permitiesen grabar en malas condiciones lumínicas y generasen alarmas automáticas definidas por límites o rangos de temperaturas, lo que resulta funcional para detectar fuentes de calor o posibles incendios. Igualmente es significativo que propicien un análisis de movimiento inteligente que ignore determinados patrones de movimiento.

> «La seguridad de un museo requiere especial atención y un sistema acorde a las necesidades que implícitamente lleva consigo»

También es recomendable contar con tecnología panorámica 360º con el propósito de registrar un amplio espacio y cubrir absolutamente toda la sala. Característica muy importante, teniendo en cuenta la amplitud de cada una de las estancias y la multitud de personas en cada una de ellas.

Dado que son espacios dedicados a las artes visuales, es importante que el sistema que se instale no llame la atención y tenga un diseño compacto, elegante y discreto. Se trata de que los visitantes puedan sentirse seguros sin tener que estar intimidados.

Otro requisito indispensable un software inteligente que detecte el movimiento e ignore todo tipo de interferencias, a la vez que proporcione una gestión de alarma fiable. Un sistema que avise al personal de seguridad en caso de intrusión y active automáticamente un mensaje por megafonía para intimidar a visitantes no deseados.

Por último, como hemos nombrado anteriormente, es bastante útil que el software de la cámara, además de cumplir con las funciones propias de la seguridad, disponga de un sistema de conteo de personas, así como análisis de comportamiento, basándonos en unos parámetros que establezcamos como la velocidad o la dirección. Este tipo de herramientas facilitaría estadísticas con datos de los visitantes, permitirá optimizar la planificación del personal y proporcionaría el estudio del comportamiento de las personas ante una obra o una exposición.

Como hemos visto, la seguridad de un museo requiere especial atención y un sistema acorde a las necesidades que implícitamente lleva consigo. Haciendo un repaso, un buen sistema de seguridad para estos espacios debería contar con una solución de videovigilancia de cámaras IP de alta resolución, que alguna cámara cuente con tecnología panorámica 360º y alguna con detección térmica, un software inteligente que detecte el movimiento y avise al personal de vigilancia, así como una herramienta que contabilice a los visitantes y genere información útil para la institución. ●

Fotos: *Mobotix*

Contactos de empresas, p. 9.

# ESPECIAL
## ADMINISTRADORES DE FINCAS

- **Soluciones y sistemas**
- **Nuevas tecnologías para la seguridad residencial**

CONTROL DE ACCESOS | PROTECCIÓN CONTRA INCENDIOS | CCTV | ALARMAS
PROTECCIÓN CONTRA ROBO | COMUNICACIONES | SERVICIOS AUXILIARES

**MANUELA JULIA MARTÍNEZ TORRES.** PRESIDENTA DEL COLEGIO PROFESIONAL DE ADMINISTRADORES DE FINCAS DE MADRID (CAFMADRID)

# *«**Colaboramos** con la **Policía, Bomberos...** para trasladar a las comunidades las **medidas a tomar** y evitar la inseguridad»*

**CASI dos años después desde su nombramiento como presidenta del Colegio Profesional de Administradores de Fincas de Madrid (CAFMadrid), ¿que valoración haría de esta primera etapa al frente de la institución?**

—La valoración es muy positiva cuando tu equipo de Gobierno, el personal y los compañeros de profesión agradecen la labor que estás desarrollando, aportan ideas y se suman a proyectos que son de interés para todo el colectivo.

**—¿Cuáles son los principales retos del Colegio Profesional de Administradores de Fincas de Madrid (CAFMadrid) de cara al próximo año?**

—Posicionar la Institución ante los Organismos Públicos y hacer valer ante los dirigentes políticos la importancia de la gestión patrimonial que desarrollan los administradores de fincas colegiados, porque movemos casi el 4% del P.I.B.

**—El administrador de fincas se ve obligado a conocer temas muy diversos para poder desempeñar bien su función, ¿en materia de Seguridad cree que requiere algún tipo de formación o asesoramiento específico?**

—Toda información y formación es poca, y estamos encantados de coordinar las actuaciones formativas con profesionales de otros sectores. No quiero la información cuando se publica, solicito a todas las empresas y/o asociaciones que me anticipen la Normativa o Reglamento que se va a implantar, a fin de tener información de primera mano y tener preparados a nuestros clientes cuando llegue el momento, tomando medidas preventivas en los presupuestos de las Comunidades de Propietarios para que les afecte económicamente en la menor medida posible. Aquí es donde nos diferenciamos los profesionales cualificados.


**—¿Se percibe un interés especial de los administradores por preservar la seguridad de sus viviendas? ¿Cuáles son los temas que más les preocupan?**

—Si nos referimos a nuestras viviendas, tan preocupados como las de nuestros clientes, de hecho, estamos colaborando con la Policía Municipal, Nacional y Bomberos para trasladar a las Comunidades de Propietarios las medidas cautelares que se deben tomar y evitar la inseguridad.

Ahora mismo, el tema de mayor interés es el control de acceso al edificio, cambiando los porteros automáticos por vídeo-porteros y las llaves convencionales por llaves de seguridad. Una vez que ya disponen de estos medios, se suelen implantar los Circuitos Cerrados de TV.

**—La intrusión, el robo, el vandalismo, la posibilidad de incendios, los conflictos derivados a veces de una mala convivencia, son algunos de los factores más preocupantes en la seguridad residencial. En su opi-**

**nión, ¿cuáles son los puntos más vulnerables, las necesidades más importantes de un inmueble en materia de seguridad?**

—Algunos de los mencionados se contradicen entre ellos y generan un problema de inseguridad en el edificio, por ejemplo: para dar seguridad a la finca y evitar que la gente pernoctara o se escondiese en el último tramo de la escalera, ha sido muy habitual instalar verjas o cancelas que impidan esta circunstancia, pero dicha actuación se contradice con la normativa de incendios. ¿Cómo podríamos resolver esta circunstancia? En algunos casos se salva colocando una llave cerca de la cancela bajo cristal de fácil rotura, pero no lo considero suficiente.

Otro problema que preocupa es la ocupación ilegal de las viviendas cerradas y la poca actuación que tienen al respecto las autoridades.

**—¿Considera adecuada la oferta del mercado en cuanto a soluciones para la seguridad domiciliaria? ¿Qué echa de menos en ese aspecto?**

—Existe una oferta adecuada pero genérica, tendría que ser más moldeable tanto en necesidad como en la parte económica. Ahí es donde tendríamos que trabajar en conjunto la empresa proponente y los administradores de fincas colegiados.


**—¿Qué oferta formativa ofrece el CAFMadrid a los administradores de fincas en general, y de manera particular, en el ámbito de la seguridad?**

—Hasta ahora nos hemos centrado en el cumplimiento de la normativa en lo que afecta a la instalación de cámaras y/o CCTV, así como en definir las diferentes figuras en la subcontratación del servicio de vigilancia (auxiliares, vigilantes…). ●

Texto: Gemma G. Juanes.
Fotos: CAFMadrid

**JOSÉ IGNACIO JIMÉNEZ DEL CASTILLO.** DIRECTOR DE RELACIONES INSTITUCIONALES. SECURITAS DIRECT

# Vigías

**Sentimos la responsabilidad de seguir mejorando, de ayudar a proteger a nuestros clientes, y al mismo tiempo queremos continuar con la mejora de nuestros procesos, para minimizar las falsas alarmas**

LA gran mayoría de los saltos de alarma que llegan a una central receptora son falsos: un error al desconectar el equipo, un usuario que no encuentra la llave o se equivoca con el código, una cortina que se mueve, un perro que no se está quieto…

Por eso es especialmente importante que los operadores de una CRA permanezcan muy concentrados para cuando llega el salto de alarma real. Los operadores son gente muy preparada, que deben verificar qué situación está teniendo lugar a partir de sonidos, imágenes y señales que no siempre son evidentes. A eso hay que añadir que viven situaciones de tensión, y que a pesar de ello deben actuar con rapidez, precisión y contundencia. La profesionalidad de estas personas está fuera de toda duda, y su buen hacer es la base de la tranquilidad que sienten nuestros más de 800.000 clientes.

## Mejora continua de nuestros procedimientos

Nos sentimos orgullosos de la mejora continua de nuestros procedimientos. Como en todo proceso humano, no existe la infalibilidad, y en ocasiones se producen falsos avisos. Trabajamos intensamente para reducir el número de falsas alarmas, y aunque queda camino por recorrer, estamos satisfechos con la línea que estamos siguiendo.

Tenemos clara nuestra misión. Cuando nos preguntan si nos dedicamos a luchar contra el crimen, nosotros matizamos: ayudamos a luchar contra el crimen, tratamos de ser los ojos de las Fuerzas y Cuerpos de Seguridad, de vigilar esos rincones a los que ellos no pueden llegar. Y a partir de ahí, damos aviso en tiempo y forma. Nosotros avisamos y ellos actúan.

Esa sí es nuestra misión, la de vigías, y la CRA juega un papel crucial en ello. Sentimos la responsabilidad de seguir mejorando, de ayudar a proteger a nuestros clientes, y al mismo tiempo queremos continuar con la mejora de nuestros procesos, para minimizar las falsas alarmas, porque somos conscientes de que consumen recursos públicos que pueden ser necesarios en otras situaciones de emergencia.

No es un equilibrio fácil, pero vamos a seguir trabajando en ello. ●

Contactos de empresas, p. 9.

# La central de Alarmas más grande de Europa

**Nº1 en Alarmas con verificación por imagen**

Presencia en 14 países de Europa y Latinoamérica con más de 2 millones de clientes satisfechos.

**Central de Alarmas Líder en España**

Más de 850.000 clientes en España.
Más de 700 vigilantes de Acuda para garantizar una intervención inmediata.

**4.000 profesionales pendientes de usted**

Le protegen 24 horas al día los 365 días del año.
Tiempo medio de respuesta 27 segundos (2015).

## Líderes en seguridad.
## Referencia en tecnología y usabilidad en alarmas.

Verisure Smart Alarm de Securitas Direct cumple con las demandas más exigentes en materia de protección, tanto para su hogar como para su negocio.


902 432 431
www.securitasdirect.es

RNSP: 2737

Nº1 en alarmas

SECURITAS Direct

**JOSÉ GONZÁLEZ OSMA.** DIRECTOR DE SERVICIOS Y RESIDENCIAL DE TYCO IF&S

# La seguridad y el **hogar digital**

CONSEGUIR un hogar seguro sigue siendo una necesidad elemental para proteger lo que más queremos. Sin embargo, nuestras necesidades evolucionan y se transforman con el paso de los años gracias a la continua innovación de las tecnologías. La aparición del internet de las cosas y de la domótica han dado lugar al hogar conectado, permitiéndonos controlar y gestionar desde cualquier lugar los diversos dispositivos que tenemos en la vivienda, haciendo más fácil y cómodo nuestro día a día. El hogar digital ha dado un vuelco a la manera de relacionarnos con nuestro propio entorno, consiguiendo abrir un amplio abanico de posibilidades. El reto actual de la seguridad consiste en adaptarse a estas nuevas necesidades.

El hogar digital ya es una realidad en España. Según los datos del estudio «Hogar Inteligente y Conectado en España 2016» realizado por Tyco, más de la mitad (51%) de los españoles cuenta ya con dispositivos inteligentes y conectados en su hogar. Mientras que la gran mayoría de los españoles (82%) tiene previsto instalar tecnologías relacionadas con el hogar digital en un futuro cercano, principalmente sistemas de iluminación (51%) y electrodomésticos inteligentes (55%).

Este mismo estudio nos muestra lo que un hogar conectado debe proporcionar. La búsqueda del confort es una de ellas, la domótica es capaz de convertir las tareas relacionadas con la ejecución manual de dispositivos -como la climatización, el control de las luces y electrodomésticos- en procesos automatizados que podemos controlar con un solo click desde nuestro móvil. Otro punto sería la innovación, cada vez se demandan más viviendas con los últimos equipamientos tecnológicos que nos permiten ahorrar poco a poco, tiempo y costes mediante acciones del día a día, como el control de la luz de manera remota, regulando y temporizando la temperatura del hogar o pudiendo controlar el consumo de aparatos electrónicos. Aunque es la seguridad y protección del hogar lo que sigue siendo el principal aliciente para la adopción de la domótica y las ventajas que posibilita tener un hogar conectado.

En el mercado ya existen soluciones que permiten un control completo del hogar desde cualquier dispositivo móvil. Permitiendo controlar de forma remota todos los dispositivos conectados a la red eléctrica. En este contexto, Tyco ha sido pionero en el desarrollo del hogar digital en España, con el

lanzamiento de Tyco Interactive Security, una solución que incorpora funcionalidades de control y gestión de los recursos energéticos y de confort al sistema de seguridad y alarma en el hogar o negocio, aprovechando el desarrollo de los teléfonos inteligentes.

Entre las funcionalidades que incluyen las soluciones de domótica y seguridad, destacan:

**• Visualización en vivo de la vivienda o del negocio a través de cámaras IP.** Esta función permite ver en cualquier momento y desde cualquier lugar, lo que está sucediendo en la vivienda o el negocio. El usuario puede acceder a las cámaras desde su teléfono móvil, tablet o PC y gestionar o almacenar los vídeos en la nube (video on-demand). El sistema garantiza además la total privacidad del hogar o negocio, ya que sólo el usuario tiene acceso a estas cámaras.

**• Automatización de dispositivos:** Permite controlar de forma remota todos los dispositivos conectados a la red eléctrica. De esta forma es posible encender o apagar luces, electrodomésticos, etc. desde el teléfono móvil. Esto permite también simular la presencia en el domicilio gracias a la creación de patrones de iluminación.

**• Gestión remota del sistema de alarma,** pudiendo conectar y desconectar total o parcialmente el sistema y los distintos elementos de nuestra vivienda, a través de tablets y teléfonos inteligentes.

**• Control de la calefacción y ahorro energético.** Las nuevas soluciones de domótica permiten encender y apagar dispositivos eléctricos y programar el termostato de la calefacción a distancia, permitiendo así gestionar mejor el consumo y aprovechar al máximo los recursos energéticos.


**• Creación de escenarios adaptados al estilo de vida del usuario.** Con objeto de mejorar la habitabilidad, la solución de Tyco permite decirle a la casa cómo quiere que se comporte cuando está o no está habitada.

Un aspecto clave de cualquier solución de seguridad para el hogar debe ser la conexión constante a la Central Receptora de Alarmas (CRA), ya que es el único modo de garantizar la protección del hogar durante las 24 horas. Además de gestionar las alarmas de los sistemas anti-intrusión, la CRA debe ser capaz de monitorizar de forma remota instalaciones, edificios y comunidades de vecinos utilizando los equipos de vídeo instalados. Establece comunicación directa con el abonado, proporcionando mayor seguridad y confianza en caso de intrusión. Los profesionales de la CRA comprueban cada aviso a través de un proceso de vídeo verificación de la alerta, avisando directamente a las Fuerzas del Orden en caso de confirmarse la incidencia.


El desarrollo de un sistema inteligente que se adapte a la actividad del usuario ha conseguido proporcionar mejoras en las capacidades de control, confort y eficiencia de los dispositivos del hogar. Pero por encima de todo está consiguiendo mejorar la seguridad y la habitabilidad de la vivienda, que sigue siendo la mayor preocupación de los españoles. Por lo que podemos afirmar sin miedo a equivocarnos, que un hogar nunca será inteligente si no te ofrece toda la tranquilidad y comodidad que necesitas. ●

Fotos: *Tyco IF&S*

Contactos de empresas, p. 9.

**CARLOS ALONSO.** MARKETING Y VENTAS. PORTERALIA

# **Videoportero conectado** o IOT (Internet de las Cosas)

Si nos preguntamos qué es un Dispositivo Conectado o IOT, Internet de las Cosas, la respuesta es que nos referimos a aquellos aparatos que conectados a Internet adquieren un valor añadido en términos de funcionamiento, información, uso o interacción con su entorno.

La empresa Legrand dispone del programa ELIOT, que es una fusión entre EL (Electricidad) e IOT (Internet de las Cosas), y que comprende todos los dispositivos que tienen conectividad.

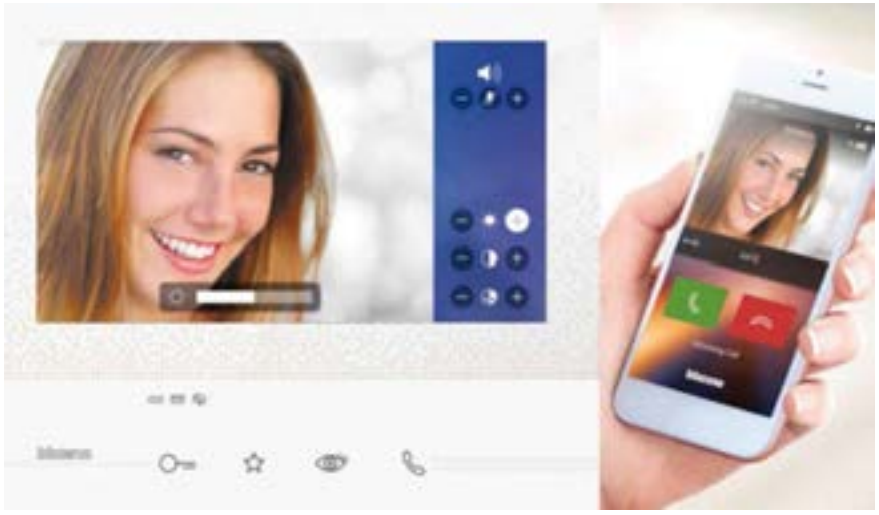
La necesidad de disponer de dispositivos conectados es creciente en el sector de los edificios, y más para las personas que tienen alguna discapacidad. Y son estos dispositivos los que van a formar parte de las soluciones que necesitan las personas discapacitadas para poder interactuar con sus viviendas a través de sus Smartphones.

En el año 2014 había 14.000 millones de dispositivos conectados y, según Cisco, se espera que en el año 2020 esa cifra crezca hasta los 50.000 millones. Los dispositivos conectados aportan valor a los usuarios ya que pueden automatizar procesos que les facilitan la vida.

## Monitor Bticino Classe 300X13E

El Monitor Bticino Classe 300X13E dispone de una pantalla de 7" y de teclas de función directa táctiles. Además incorpora el Bucle Inductivo para las personas que llevan prótesis auditivas.

Con el Monitor Bticino Classe 300 X13E ya puedes estar conectado y conseguir aumentar la seguridad y la accesibilidad a personas con discapacidad. Una vez que ya tienes tu instalación TEGUI o Bticino de 2 hilos no polarizados puedes conectar el monitor a la WIFI de tu vivienda, descargar la App «Door Entry», y recibir las llamadas en tu Smartphone que disponga de Sistema Android o IOS.



Básicamente podremos contestar desde nuestro Smartphone las llamadas que se produzcan en la placa de la calle, contestar, ver quién es y accionar el abrepuertas desde cualquier lugar, siempre que haya cobertura 3G o 4G, o estemos con Wifi.

También podremos hacer una autovigilancia y ver la cámara de la Placa de la calle.

Abrir la cerradura de manera remota.

Llamar directamente a casa con la función de intercomunicación.

Activar diferentes accesorios que podamos tener en la instalación: Cámaras de CCTV, activación de luces, calefacción, riego, etc.

El Monitor Bticino Classe 300 X13E va a facilitar la vida a todas las personas con discapacidad. ●

Contactos de empresas, p. 9.

**JOSÉ MIGUEL ÁNGEL OLLEROS.** DIRECTOR DE SEGURIDAD PRIVADA/ESPECIALIZADO EN PREVENCIÓN DEL DELITO RESIDENCIAL

# Diez mandamientos en **la seguridad residencial**

COMO consultor especializado en seguridad contra el delito, quiero aportaros algunas reflexiones que pueden hacer cambiar vuestro actual paradigma de la seguridad y prevención contra el robo residencial.

## Primero, ser conscientes de la realidad

**Pocos recursos del Gobierno de turno.**

La delincuencia es una inevitable característica de la civilización, que además va en aumento en la medida que aumentan las desigualdades sociales y la migración hacia los núcleos urbanos.

Las Fuerzas y Cuerpos de Seguridad del Estado tienen limitaciones de recursos para poder atender a la avalancha de actos delictivos y que, en los próximos años, los respectivos gobiernos nacionales o locales deberán decidir las prioridades: gamberrismo de bandas, tráfico de drogas, extorsiones, agresiones físicas, violaciones, secuestros, crímenes, terrorismo,… robos en viviendas.

No hay recursos para todos los delitos y mucho menos para la prevención del delito, de tal forma que la seguridad residencial pasará poco a poco a ser una responsabilidad de seguridad privada que cada ciudadano deberá contratar de forma individualizada, al igual que ahora se contrata su sanidad privada.

Crisis, aumento de desigualdades, pocos recursos policiales, propietarios aceptando mercado de segunda mano sin importar proveniencia, compra de sistemas fast security, viviendas fáciles de entrar y salir… terreno abonado para la delincuencia.

## Segundo, conocer tu prioridad

**¿Qué es lo más importante que guardas en tu hogar?**

Es un principio básico de reflexión para determinar la inversión en sistemas de seguridad.

Si solo se tiene objetos de valor económico, quizás «no merezca la pena una alta inversión», puesto que un buen seguro y un sistema de alarma puede cubrir el riesgo.

Para mi, lo más importante que guardo en mi hogar es la suma de mi familia, los enseres sentimentales y mi estabilidad emocional de no sentirme violado en mi intimidad… Trato de evitar los ya conocidos síntomas de la víctima: sentimientos de rabia, miedo, paranoia, ansiedad, estrés… que perduran en el tiempo y no creo que las coberturas de un seguro cubran mi pérdida.

Para mi, lo más importante es que no entren!

## Tercero, tener un enfoque inteligente

**Conocer al delincuente**

El delincuente es una persona racional y por lo tanto toma decisiones racionales. El delincuente no quiere ser visto y no quiere ser detenido, por lo tanto su objetivo es la facilidad y rapidez para entrar y salir de una vivienda. No importa tanto el botín como la facilidad del acceso.

**Disuasión y prevención contra el robo residencial**

La mayoría de las personas que han sido víctimas de un robo, no esperaban serlo, e incluso se sorprenden porque se consideran a si mismos «personas anónimas» sin dinero, ni joyas en su vivienda, como para ser interesante para un delincuente.

¿Cómo sabe el ladrón que no tienes joyas, ni dinero en casa? la respuesta es sencilla: no lo sabe!

Existe la falsa creencia de que el delincuente analiza el botín esperado, para robar en una vivienda… seguro que es así en ciertos casos VIP –menos de un 10% del total de los robos– pero en el resto, el otro 90%, el delincuente analiza la facilidad de acceso y no el botín puesto que ya presupone que algo encontrará, bien en efectivo o en enseres, que puedan venderse en el mercado de segunda mano (muy activo con la crisis que ya dura desde 2007).

**¡Olvidar ya! este falso mito, que tanto daño nos ha hecho!**

Pensar que nunca seremos víctimas de un robo porque vivimos de forma humilde. Precisamente los propietarios de alto poder adquisitivo son cada vez menos accesibles para el delincuente común y los clanes familiares, debido a la cantidad de medidas técnicas y disuasorias que ya aplican.

## Cuarto, evitar los Fast Security Systems

**¿Qué son los Fast Security Systems?**

En España, estamos ante la eclosión de la seguridad rápida, fácil y económica.

Fast Security es sinónimo de rápido, precio bajo, no tengo tiempo, así mismo me vale, de momento me apaño... Y un sinfín de justificaciones que el comprador se hace, fruto de su manifiesta inexperiencia en seguridad y con la complicidad de los vendedores altamente incentivados por las comisiones de venta.


El cliente adquiere un producto o servicio supuestamente atractivo y económico en el origen del contrato pero con alta obsolescencia, cautividad, baja efectividad para su seguridad y no tan económico con el paso del tiempo.

El resultado son cientos de miles de viviendas con multitud de carencias técnicas y de usabilidad, cautividades de años y de costoso mantenimiento o actualización.

–Fast Security– un viaje muy peligroso del propietario hacia lo desconocido, que agradece el delincuente.

## Quinto, seguridad en capas separadas

**Las capas separadas dificultan la intrusión.**

*Disuasión*

Solo se consigue con resistencia física como puertas, rejas, persianas, cerraduras, muros, y cristales. La resistencia física obliga a gastar más tiempo en romper la resistencia, llevar más y mejores herramientas de ataque (pesan y se notan), obliga a realizar más ruido y a tener suficiente fuerza física para golpear y golpear hasta romper.

*Detección anticipada del ataque*

Se aplica al perímetro de la vivienda, bien sea el jardín de un chalet o la terraza de un segundo piso o ático. Es eficaz combinar electrónica del detector con resistencia física de la persiana o de la cerradura y lo que llamamos respuesta vinculada, es decir, que si detecto un intruso que la persiana se baje, que encienda luces, que me avise al móvil, etcétera.

Para que la detección anticipada sea eficaz no hay que volver a caer en el Fast

Security System que ofrecen las empresas de sistema de alarmas y que se basan en un simple detector electrónico.

*Protección interior*

En base a una puerta de seguridad en una habitación que genere un espacio de refugio durante el tiempo que esperamos a la policía, normalmente 20-30 minutos en ciudades y 40-60 minutos en poblaciones rurales o aisladas.

También ayuda una caja fuerte de 100 kg de peso para dificultar que el delincuente la traslade fácilmente y obligarle a abrirla in situ, lo cual le obliga a llevar más herramientas diferentes y gastar más tiempo.

*Detección y verificación de la intrusión.*

Se trata del sistema de alarma. Los kits autoinstalables sirven para otras cosas pero no para impedir un robo. Tampoco sirven los kits Fast Security que ofrecen las grandes compañías de seguridad que todos conocemos.

Los sistemas tienen que tener zonas diferenciadas (interior y exterior), tienen que ser bidireccionales, certificados en grado 2, tienen que ofrecer sistema pulling de máximo 5 minutos, los detectores deben ser anti masking e incoporar cámara para vídeo verificación (no confundir con foto verificación). Por supuesto, su centralita debe comunicar de forma redundante (cable ADSL al router y vía radio GPRS, 3G,…).

## Sexto, lo primero es lo primero

**Resistencia física.**

Recordar que hablamos de viviendas y no de edificios. Las viviendas no tienen otras medidas de seguridad y no suelen tener vigilantes de seguridad armados.

Así pues, necesitamos una puerta de alta seguridad como primera medida, y después, decidir según el presupuesto, y lo que comentaba en el punto quinto (anterior).

La inmediatez de la información (detección anticipada) y la demora de la intrusión, son innegociables. El resto de bondades de la propuesta del vendedor, son bienvenidas pero secundarias.

## Séptimo, pensar en la obsolescencia

**¿Coste bajo y baja durabilidad?**

En seguridad no existen las gangas, ni las ofertas. Los sistemas profesionales tienen su precio establecido y los instaladores también lo tienen, así que cuidado con compras que en pocos meses o años quedan obsoletas y por lo tanto hay que volver a gastar dinero.

Yo realizo innumerables consultorías de seguridad en viviendas y veo barba-

ridades en viviendas recién entregadas; puertas con certificaciones de hace 10 años, llaves sin protocolos de seguridad, sistemas de alarma sin pulling de 5 minutos, cristales estándar, puertas correderas que puedes forzar con la mano y poco esfuerzo, etc.

En seguridad, tan importante es ¿qué sistema compras? como ¿a quién se lo compras? y ¿quién lo instala?

## Octavo, saber qué necesito

**¿Te auto recetas o contratas a un consultor especializado?**

Para adquirir un producto o servicio de seguridad que perdure en el tiempo y que se ajuste a lo que realmente se necesita, debe existir un diagnóstico previo a la compra, realizado a través de un proceso disciplinado de descubrimiento, evaluación y solución.

Este diagnóstico, debe ser realizado por un experto o especialista –bien formado– en alguna especialidad de la seguridad: física, electrónica, lógica, y «su receta» debe permitir a los propietarios poder decidir en qué establecimiento adquirir «la medicina» o aplicar «el tratamiento».

Cada vivienda es una patología diferente porque, aunque comparte vecindad con la vivienda de al lado, existen importantes diferencias en hábitos de vida, perfil familiar, valor del patrimonio guardado, sentimiento de inseguridad personal…

No hay que confundir la atención que nos ofrecen en un establecimiento generalista, de bricolaje con una consultoría profesional. Tampoco hay que confundir a un vendedor de una marca con un consultor independiente.


## Noveno, evitar el error de bulto

**El delincuente es completamente estúpido**

Pensar que el delincuente es completamente estúpido y que un simple cartel o la mera instalación de un simple sistema de alarma va a engañarle o disuadirle del intento de robo.

Os recuerdo que son profesionales en su actividad y están bien entrenados… Trabajan cada día al igual que vosotros!

## Décimo, que no entren!

**No olvidar la prioridad**

En viviendas, la prioridad es que no entren y para esto debemos tener resistencia física, después detección anticipada, después sistema de alarma y por último cajas fuerte y habitación refugio.

Elegir bien al establecimiento.

Y nunca, nunca, nunca, comprar un sistema de seguridad sin una evaluación profesional previa. ●

TECNIFUEGO-AESPI

# Instalar **detección en las viviendas** salva vidas

DE nuevo la tragedia por incendio en vivienda. Dos personas fallecieron recientemente en el incendio de su vivienda en L'Hospitalet de Llobregat: una anciana de 84 años y su hijo de 59. El incendio se originó de madrugada en la habitación que ocupaba la anciana.

Desde TECNIFUEGO-AESPI se alerta de la circunstancia que más se repite en los incendios: muerte de un anciano y de madrugada, y se apunta a la necesidad de instalar detectores de incendio en las viviendas, como sucede en Francia donde es obligatorio tener detector en el hogar. El argumento es simple y está probado, la instalación de un simple detector de incendio, puede alertar del mismo y permitir a las personas que están durmiendo escapar de las llamas.

**Consejos para evitar incendios en la vivienda:**

- Las estufas pueden originar un incendio.Manténgalas alejadas (como mínimo un metro) de otros objetos: cortinas, ropa puesta a secar, etc.
- No deje velas encendidas sin vigilancia.
- Mantenga las cerillas y los encendedores fuera del alcance de los niños.
- Antes de salir de casa o de acostarse, apague todos los aparatos que puedan originar un incendio (estufas, fogones, etc.), velas, y cierre las llaves de paso del gas.
- Desconecte las planchas de pelo o de ropa después de su uso. Y cuando las esté utilizando, colóquelas sobre superficies no inflamables.
- No conecte varios aparatos en un solo enchufe múltiple y mantenga en buen estado la instalación eléctrica.
- No utilice aparatos de ningún tipo en mal estado (estufas, cocinas, neveras, etc.).
- No fume en la cama y no tire las colillas en cualquier sitio. Asegúrese de apagarlas.
- Instale detectores de incendios.
- Tenga a mano un extintor de incendio.

**Qué hacer si se produce un incendio**

- Avise al teléfono de emergencias 112.
- Corte la corriente eléctrica y la entrada de gas.
- Conozca la ubicación de extintores caseros y su manejo.
- Intente apagar el fuego sólo si es pequeño y se puede controlar.
- Si intenta apagarlo, debe situarse entre el fuego y la vía de escape.
- No utilice agua:
  - Cuando pueda alcanzar instalaciones eléctricas.
  - Cuando el incendio es de líquidos inflamables (aceite, gasolina, etc.).
- Si no puede apagarlo, no corra riesgos inútiles, busque un lugar seguro y abandone la zona.
- Al abandonar el lugar incendiado:
  - Cierre las puertas al salir.
  - Gatee si hubiera humo.
  - No empuje a otros afectados.
- No utilice los ascensores como vía de evacuación.
- Si la escalera está llena de humo manténgase en su vivienda.
- En caso de no poder abandonar la vivienda por el fuego:
  - Enciérrese en una habitación.
  - Tape las ranuras de la puerta, preferiblemente con trapos mojados para evitar que entre humo.
  - Hágase ver por la ventana.

Para más información: www.tecnifuego-aespi.org ●

**JON MICHELENA.** DIRECTOR GENERAL DE CEPREVEN

# Prevención: Formar, informar y concienciar a la sociedad

CON la llegada del otoño, mi querida amiga Gemma, redactora jefe de esta revista, tiene por costumbre solicitarme un escrito para el número de diciembre. Siempre me hace ilusión tener la oportunidad de difundir los principios básicos de la prevención y poder concienciar a alguna persona más sobre los riesgos asociados a los incendios en los hogares. Además, por qué no decirlo, su petición ayuda a mantener mi ego en unos niveles razonables, por lo que, invariablemente, acepto gustoso la encomienda.

Antes de empezar a redactar un artículo, tengo por costumbre releer aquellos que he preparado en años anteriores sobre el mismo tema, para evitar que mi memoria me juegue una mala pasada y acabe escribiendo un artículo similar. Hoy, cumplido este hábito, me he dado cuenta de que cualquiera de ellos sería válido y estaría tristemente vigente.

Y digo tristemente porque la situación no mejora y siguen produciéndose incendios en viviendas y en edificios residenciales de forma sistemática; en los últimos años siguen presentándose unos ratios de víctimas que lamentablemente no presentan una tendencia a la baja. Según los datos elaborados por Tecnifuego-Aespi, en el año 2015, último del que se disponen de cifras sobre víctimas en incendios domésticos, el número de fallecidos fue de 112, en 2014 murieron 116 personas, y en 2013 fueron 110. Otras fuentes, como la Fundación Mapfre y APTB dan un número mayor de víctimas, el motivo es la falta de un método de recogida uniforme de datos que permita la elaboración de unas estadísticas homogéneas y fiables. Aun así, las estadísticas nos demuestran que, inexorablemente, pierden la vida por causa de incendios 10 personas al mes. Este año no parece que vaya a distinguirse de sus predecesores. Solo los titulares de los incendios domésticos con repercusión mediática acaecidos durante el mes de octubre ocuparían una extensión mucho mayor que la del presente artículo.

Trabajar con estadísticas tiene el riesgo de distanciarse del problema y verlo todo desde un punto de vista matemático. Si en enero mueren 10 personas y al mes siguiente fallecen 9, nos demostrarán con gráficas y fórmulas que ha fallecido una persona menos, cuando la realidad es que han fallecido 9 más, todas ellas con nombre y apellidos.

Si cotejamos las muertes por incendio con las que ocurren en accidentes de tráfico son mucho menores, sobre el 6%, lo que puede justificar las campañas de concienciación que sobre los diferentes aspectos de la seguridad vial se vienen desarrollando desde hace décadas. La comparación fría y numérica con las víctimas de violencia de género ofrece unos resultados equiparables, siendo algo mayores las provocadas por los incendios. En seguridad vial las campañas han dado su resultado, las relacionadas con la violencia de género están en todos los medios y cuentan con el apoyo de toda la socie-

dad… ¿Y las de prevención de incendios? Simplemente son anecdóticas y de pequeño alcance. Existen algunos ayuntamientos que distribuyen carteles entre los vecinos, otros colocan detectores a personas mayores, pero sin llegar a articular una gran campaña de ámbito nacional.

Deberíamos consultar a psicólogos y a otros analistas del comportamiento humano para saber por qué la sociedad no reacciona de una forma más visceral ante los incendios domésticos y las víctimas que causan. Parece que el incendio es una fatalidad contra la que no se puede luchar, como si fuese un movimiento sísmico que llega sin avisar y contra el que no se puede hacer nada. Pero no es así, los incendios pueden prevenirse, deben prevenirse. Solo son necesarios unos conocimientos mínimos y un poco de sentido común para aplicarlos. La gran mayoría de incendios en las viviendas son consecuencias de despistes, imprudencias o de malas prácticas; fumadores, fuentes de calor, aparatos mal mantenidos, sobrecargas de la instalación eléctrica, mal uso de materiales combustibles e inflamables… Éstas son las principales causas objetivas, pero sobre ellas planea otra, mucho más subjetiva, que es la falta del concepto del riesgo. En infinidad de ocasiones, cuando los prevencionistas ponemos de manifiesto una de estas situaciones, por lo general obtenemos una respuesta del tipo «siempre lo he hecho así y nunca pasa nada».

Pero llega el invierno, estación en la que se concentran la mitad de las muertes anuales, y podremos comprobar en las noticias que sí, que los incendios ocurren y que en ellos pierden la vida personas como yo y como tú, querido lector.

**¿Qué podemos hacer?**

La primera opción es sencilla y barata: conformarnos con la situación, al fin y al cabo no es tan mala, en Francia, por ejemplo, tienen más de 800 muertos al año…

La segunda opción, reclamada por muchos, es legislar. Obligar a instalar detectores, obligar a reforzar la protección pasiva de las viviendas. En un país en el que somos especialistas en obtener papeles que dicen que cumplimos con todo, no parece la opción más eficiente.

La tercera, a mi juicio la única viable, es formar, informar y concienciar a la sociedad del riesgo asociado a los incendios.Todos los niños deberían aprender a utilizar un extintor, a apagar una sartén ardiendo, las empresas deberían hacer lo mismo con sus empleados, más allá de las habituales presentaciones tediosas que sobre el tema y para salir del paso, se estilan en nuestro país.

Únicamente cuando todos estemos convencidos que en cualquier momento podemos ser víctimas de un incendio, nos preocuparemos de aprender a prevenirlos y, por si acaso, saber cómo controlarlos y extinguirlos.

Para finalizar, animo a todas las personas que lo deseen a visionar el vídeo que ha preparado Cepreven para aprender a manejar un extintor portátil (www.cepreven.com). ●


> «Cuando todos estemos convencidos que en cualquier momento podemos ser víctimas de un incendio, nos preocuparemos de aprender a prevenirlos»

INFORME ELABORADO POR UNESPA SOBRE «LOS ROBOS EN HOGARES EN ESPAÑA»

# Los robos en viviendas son más frecuentes en el litoral mediterráneo y en Madrid

## Los ladrones prefieren actuar en los meses de invierno y en agosto

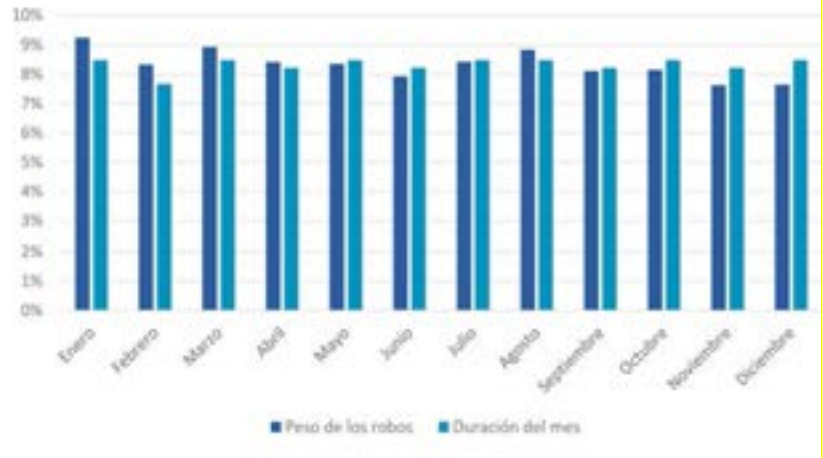
EL invierno es temporada alta de robos en hogares. Los meses de enero, febrero y marzo son los preferidos por los ladrones para actuar y, por tanto, son los que presentan una mayor propensión a presenciar asaltos a viviendas. A estos se suma agosto, un mes igualmente proclive a acoger incidentes. Esta es una de las conclusiones del informe «Los robos en los hogares en España» elaborado por UNESPA. Otra de las conclusiones del trabajo es que las provincias donde se dan robos con mayor asiduidad son las que conforman la costa mediterránea. En concreto, llama la atención la situación de Tarragona y Murcia. Más allá del litoral, destaca Madrid por la frecuencia de incidentes.

El estudio forma parte de la nueva edición de la Memoria social del seguro, una publicación que, cada año, realiza la Asociación Empresarial del Seguro. En la elaboración del trabajo se han tomado como referencia 80.000 robos padecidos por un parque de 10 millones de residencias aseguradas y distribuidas por toda España.

Los resultados del informe revelan que los ladrones operan durante todo el año. De hecho, en contra de la creencia popular, su actuación no se intensifica apenas en los periodos estivales. Así lo demuestra el hecho de que los meses de frío son más problemáticos que los de calor –con la salvedad de agosto, que sí presenta un índice de incidentes superior a los días que abarca dicho mes en el año–. En contraste, el otoño es la estación con menos asaltos a viviendas. Esta dinámica pone de manifiesto que muchas veces los delincuentes asaltan segundas residencias. Unos inmuebles que, por definición, presentan índices de ocupación más bajos en la época laboral que en los periodos vacacionales.

La estacionalidad de los robos diverge algo cuando lo que se mide no es la frecuencia de los asaltos, sino su gravedad. Por gravedad se entiende la relación entre el coste del siniestro y el capital asegurado de la póliza. Es decir, aquello que es susceptible de ser robado. El informe de UNESPA considera un robo grave en caso de que el valor de lo potencialmente sustraíble (lo asegurado) y lo efectivamente sustraído (lo robado) se acerquen. Independiente de si el valor sea elevado o bajo en términos absolutos. Bajo este prisma, pues, queda claro que di-

*Tabla/Gráfico 1. Distribución del número de robos por meses.*




Fuente: Elaboración propia

ciembre, enero y agosto son, en este orden, los meses que presentan los robos más llamativos.

La jornada del año en que los robos fueron más graves fue el Día de Reyes (6 de enero). Entre tanto, la jornada en la que ocurrieron incidentes que conllevaron el pago de indemnizaciones más bajas en relación con lo asegurado fue el 15 de julio.

(**Ver Tabla/Gráfico 1.** Distribución del número de robos por meses, y **Gráfico 2.** Gravedad media de robos en hogares por meses del año)

La información recabada por UNESPA permite realizar un análisis territorial de los robos en los hogares. Una revisión de dichos robos que sólo se fijara en el número de incidentes provocaría que las poblaciones más grandes de España aparecieran como las más problemáticas, por el simple hecho de que albergan más población y, por extensión, más viviendas. Para evitar este efecto, en lugar de tomar como referencia el número total de asaltos, el estudio que figura en la Memoria social del seguro 2015 relaciona el número de incidentes con el tamaño del parque de viviendas aseguradoras en tal o cual lugar.

## Análisis territorial de los datos

El análisis territorial de los datos deja constancia de que, como se ha avanzado más arriba, las provincias del litoral mediterráneo son las más propensas a presenciar robos en relación con el número de viviendas aseguradas. Entre los puestos de cabeza se sitúan Tarragona, donde es un 65,72% más probable que una vivienda sufra un asalto que en el conjunto del país, y Murcia (44,28%). Entre medias se cuelan Madrid (56,06%) y Toledo (36,52%), en segunda y cuarta posición, seguidas inmediatamente del resto de provincias del Levante. Se da la circunstancia de que las provincias costeras albergan una gran cantidad de segundas residencias de uso, principalmente, estival. Este hecho concuerda con la existencia de un mayor número de robos en invierno.


Fuente: Elaboración propia

> «Los siniestros más caros se dan en Toledo, Gerona, Barcelona, Murcia, Baleares, Orense y Guadalajara»

En el extremo opuesto, las provincias españolas donde es más infrecuente sufrir un robo en casa son Navarra (–66,34%, respecto del conjunto de España), Orense (–65,12%) y Palencia (–63,91%). Todas ellas son, a su vez, provincias de interior.

El mapa varía si, en lugar de la frecuencia, se mide la intensidad de los robos. En este caso, los asaltos más graves se dan en Orense. Aunque ahí ocurran pocos percances, los datos muestran que en dicha provincia un asalto suele ser un 82,41% más grave que en el conjunto de España. Le siguen en importancia Murcia (72,33%), Almería (58,41%) y Teruel (40,78%).

El informe «Los robos en los hogares en España» también da cuenta del coste medio de los siniestros que sufren las viviendas. En concreto, los datos muestran que los robos tienen un coste superior a los 1.500 euros en Murcia, Cataluña, Baleares y Castilla-La Mancha. Las comunidades autónomas donde el robo típico es menos grave son Aragón y Asturias. Ahí, las pérdidas provocadas por un asalto no llegan a los 1.000 euros.

Cuando este análisis se efectúa por provincias, a la cabeza se encuentran Toledo, Gerona, Barcelona, Murcia, Baleares, Orense y Guadalajara. En estos siete casos, el coste medio de los robos supera los 1.500 euros. Los robos más modestos se dan, en cambio, en Palencia, Asturias, Lugo, Álava, Zaragoza, Ávila, Ciudad Real, Jaén, Cuenca y Las Palmas de Gran Canaria. En cada una de estas 10 provincias los asaltos tienen un coste medio inferior a los 1.000 euros. ●

Fotos: UNESPA

**Nota: España actúa como referencia de base. Los datos en rojo expresan una tasa de gravedad de robo mayor a la del conjunto del país y los datos en azul expresan una tasa de gravedad de robo menor.**

Contactos de empresas, p. 9.

**JOSÉ MARÍA LAZARENO MARTÍNEZ.** DIRECTOR COMERCIAL DE GRUPO ESV

# *Videovigilancia activa protocolizada: comunidades videovigiladas 24h en tiempo real*

**—De cara a nuevos proyectos para 2017, ¿cuáles son las últimas novedades o servicios que ofrecen ustedes?**

—En el Grupo ESV estamos continuamente buscando nuevas soluciones y nuevos servicios que nos permitan dar un mejor servicio a nuestros clientes y diferenciarnos de nuestra competencia, que en este sector es muy dura.

Por eso hemos dejado definitivamente atrás la tradicional estructura en la que las empresas realizan una instalación de cámaras, de control de accesos o incluso de alarmas, y luego se limitan a realizar una, dos o tres visitas anuales para mantenimiento. ¿Y durante ese tiempo, qué ocurre si falla una cámara?

Nuestro Centro de Gestión de Alarmas (CGA) está dotado de una serie de herramientas de software y hardware que nos permiten realizar acciones preventivas a nuestros clientes.

De esta manera, la gestión íntegra de las comunidades que instalamos, al igual que ocurre con las naves industriales, por ejemplo, se realiza de manera remota.

Actualmente ofrecemos a nuestros clientes los siguientes servicios en remoto, entre otros:

• Gestión de los sistemas de vídeo, con detección de averías en grabadores o cámaras.

• Rondas preventivas diarias realizadas desde nuestro Centro gestor.


• Rondas protocolizadas, en las cuales podemos interaccionar con la instalación, detectando incidencias tales como una puerta que se ha quedado abierta, una luz encendida, una caldera que no funciona, etc., sobre las cuales actuamos.

• Gestión remota de controles de accesos, con apertura de puertas en remoto, baja de tarjetas o mandos perdidos en el mismo momento de la notificación 24x7.

• Gestión de puertas forzadas o accesos no permitidos a cuartos de la comunidad.

• Informes al administrador de la situación de la instalación, con aviso inmediato a FSE.

• Seguimiento de tarjetas perdidas o robadas.

• Sistemas de socorro SOS mediante puntos de vídeo-comunicación con El Centro de Control 24x7, para apoyo ante cualquier eventualidad o peligro en garajes o portales.

• Sistema de control de accesos de vehículos con lectura de matrículas, con sistema de matrículas blancas y negras para aviso a policía.

• Etc.

Pero esto no es todo. La seguridad es un mundo muy dinámico y siempre hay que estar intentando ofrecer nuevas prestaciones a los clientes. Para este año tenemos 2 nuevos servicios en preparación que serán una revolución dentro del sector. Pero de esto mejor hablamos en unos meses.

**—¿Cuál es la evolución que ustedes esperan del mercado?**

—Como ocurre en otros sectores, el futuro de la seguridad pasa por la gestión en remoto de las instalaciones.

En Grupo ESV creemos que el futuro de las empresas de seguridad pasa por dejar de ser meros instaladores de sistemas de seguridad y tramitadores de alarmas en caso de que se produzcan intrusiones, para pasar a ser empresas que realmente gestionen en tiempo real la seguridad de los clientes. Empresas capaces de prever y anticiparse a cualquier intrusión y, en su caso, actuar con iniciativa propia y no solo ser meros tramitadores para avisar a las FCS.

Por ello nuestra Central Receptora de Alarmas (CRA) ha pasado a ser un Centro de Gestión de Alarmas (CGA).

¿Cuál es la diferencia? Hace apenas unas semanas ofrecimos una interesante ponencia dentro del foro de las II Jornadas de Centrales Receptoras de Alarmas en el cual expusimos esta nueva tendencia del mercado en la que somos pioneros.

El futuro de las CRA,s ha de pasar por este cambio. Todas las centrales que se empeñen en mantenerse como una mera receptora de alarmas, por muy importante que sean, quedarán fuera del mercado en unos pocos años.

Durante años las mejoras que se han obtenido en el sector han venido reflejadas en métodos de trasmisión de las alarmas más seguras, equipos que verifican las alarmas de una manera más segura, etc. Por supuesto todas estas mejoras son no solo necesarias sino imprescindibles. Pero claramente insuficientes si no se combinan con acciones preventivas como rondas de vídeo, acción directa sobre puertas e interruptores, etc.

**—¿Esto es válido también para la seguridad en comunidades de propietarios?**

—Más que en ningún otro mercado. Solo hay que pensar que las instalaciones en una comunidad son lo que nosotros llamamos instalaciones desasistidas. Es decir son instalaciones en las que en el propio edificio no hay un responsable que las gestione.

Cuando se hace una instalación en una empresa, el gerente o alguien en quien delega es quien visualiza las cámaras, quien crea o anula tarjetas, en definitiva existe una persona que interacciona todos los días con el sistema, y por lo tanto lo conoce y nos puede indicar si algo falla. En una comunidad no es así y no hay nadie que esté pendiente del funcionamiento diario. Por esto se hace imprescindible que sea la empresa mantenedora quien gestione 24 horas al día, de manera remota, la instalación.

Así se puede controlar el sistema, saber en el momento cuando algo falla, interaccionar con el sistema dando de baja una tarjeta, abriendo una puerta a un vecino que no puede pasar, respondiendo ante una petición de ayuda y llamando a una ambulancia o a bomberos, llamando al servicio técnico cuando se rompe una puerta, etc.

Desde el Grupo ESV pensamos que hoy en día cualquier empresa de seguridad que no de estos servicios no presta a la comunidad un servicio suficiente, y seguramente acabarán por quedarse obsoletos y desaparecer.

**—Entonces, ¿conectar las instalaciones de la Comunidad a una Central Receptora es importante?**

—Es fundamental para dar un buen servicio. Pero además debemos añadir que es muy importante que la Central Receptora o Central de Gestión de Alarmas sea propiedad de la propia empresa instaladora y mantenedora.

La subcontratación de servicios de Central Receptora, como realizan la práctica totalidad de empresas de nuestra competencia en Comunidades de propietarios es un error. Una cortina de humo para intentar vender unos servicios que realmente no son efectivos. ¿Por qué?. Es de cajón. Cuando se contratan unos servicios con una receptora externa ocurre que nos tenemos que adecuar a los servicios que esa receptora está capacitada para dar, tanto a nivel técnico como operativo. Cada cambio o mejora en el servicio es un triunfo, y siempre estamos en manos de un tercero que es quien da el servicio, normalmente anteponiendo en caso de necesidad el servicio a sus propios clientes.

El hecho de disponer de un Centro de Gestión de Alarmas (CGA) propio nos permite poder diseñar los servicios que queremos dar al cliente según criterios de calidad, y luego realizar en la CGA los cambios necesarios, tanto materiales como humanos. Además nos

permite poder abordar directamente cualquier eventualidad o incidencia no prevista de una manera adecuada.

En definitiva nos permite poder garantizar que damos el servicio que necesita el cliente y, además, que en cualquier circunstancia podemos reaccionar de la manera más adecuada dentro de la estrategia de beneficio de nuestro cliente.

Todas las acciones quedan dentro de la empresa. El cliente nunca oirá eso de que «eso es cosa de la receptora que actúa según esos protocolos» o «consultare si podemos darle ese servicio».

día desde nuestro Centro de Gestión de Alarmas (CGA)

ESVISION está diseñado para que sea fácil de adquirir por una comunidad, sin necesidad de derramas, puesto que se comercializa como un servicio de pago por cuotas.

ESVISION se compone de dos ramas que se complementan entre ellas:

• ESVISION Cámaras. Es un sistema de videovigilancia compuesto por grabadores digitales tríbidos de última generación y cámaras de alta resolución que permite tener un control visual de las instalaciones. Todo el sistema se protege con un SAI y queda ubicado en un armario de seguridad para evitar su manipulación no autorizada. Todo el sistema se controla en tiempo real desde nuestra CGA, realizando Rondas Automáticas y Rondas Protocolizadas. ESVISION es actualmente el único sistema del mercado diseñado para comunidades y que ofrece servicios como la actuación directa tanto ante delitos como ante incidentes menores en las instalaciones, tales como encontrar una puerta de un garaje abierta por la noche o un cristal roto en un portal.

> «La vigilancia de la comunidad se realiza a través de la nube, de una manera precisa y detallada»

**—¿Qué soluciones aporta su empresa para satisfacer la creciente demanda de seguridd en las comunidades de vecinos?**

—El Grupo ESV ha diseñado el producto ESVISION para dar solución a la seguridad de las comunidades de vecinos. Es un producto especialmente diseñado para las necesidades de este tipo de clientes, cuya principal característica es que todo el sistema está gestionado on line las 24 horas del


• ESVISION Accesos. Es un sistema que gestiona los accesos a la comunidad en tiempo real, tanto en los garajes como en portales o en cuartos comunes o trasteros. Las tarjetas de seguridad que sustituyen a las peligrosas llaves permiten, en conexión directa con nuestra CGA, ser desactivas en cualquier momento del día o de la noche si han sido robadas o perdidas. Además, el servicio 24x7 permite otras actividades de valor añadido como poder abrir una puerta en remoto si un vecino lo requiere o dar aviso o incluso actuar directamente si, por ejemplo, una puerta ha quedado abierta.

Pero ESVISION no solo se queda en estos dos módulos. Actualmente existen ya varios productos «satélite», instalados como complemento del producto central como pueden ser por ejemplo:

• ESVISION Matrículas. Es un acceso controlado a los garajes mediante la lectura de las matrículas, olvidando las llaves magnéticas, los mandos y cualquier elemento de apertura.

• ESVSION Trasteros. Una solución definitiva para proteger los trasteros combinando un control de accesos con un potente emisor de niebla, que se activa en caso de una apertura forzada sin uso de las claves o tarjetas autorizadas que lleva la estancia de niebla e impide de cualquier tipo de robo

• ESVISION SOS. Una solución IP de Vídeo-Comunicadores que permiten en cualquier momento y mediante la sola pulsación de un botón, establecer contacto visual con nuestra CGA para solicitar cualquier tipo de ayuda.

Y estos módulos son solo el principio de una gran familia ESVISION que irá creciendo cada año para dar cada vez una solución más amplia a cualquier comunidad de vecinos. ●

Texto: Gemma G. Juanes.
Fotos: GrupoESV

Contactos de empresas, p. 9.

btv
desde 1962

Líderes en fabricación de **Seguridad Física** desde **1962**

www.btv.es
btv@btv.es

# Alta Seguridad

*Certificadas para empresas que requieran las más altas medidas de seguridad*

Cartago

Armero Athenas

Athenas

Luxor

Alexandria

# Ignífugas

*Resistencia al robo y al fuego*

Solid

Vulcano

Ignis

FABRICACIÓN NACIONAL 100 %

# Sobreponer y Empotrar

*Protección y funcionalidad para todo tipo de hogares y negocios*


Cuarzo


Rubí


Zafiro


Depósito

**EVA VILLAVERDE.** DIRECTORA GENERAL DE BTV

# «Calidad, tradición, seguridad y respeto son parte de nuestros valores como empresa»

**CUÁLES son los principales valores que definen a BTV como empresa?**

—Desde BTV tenemos un objetivo fundamental: conseguir una experiencia superior a través de nuestros productos y servicios mediante la excelencia empresarial. Calidad, tradición, servicio, seguridad, respeto, entre otros, son parte de nuestros valores como empresa.

Podemos destacar varios:

- Servir a nuestros clientes retándonos continuamente para alcanzar los máximos niveles de calidad en nuestros productos y servicios.
- Compromiso con una sólida ética laboral, integridad y honestidad, así como con el cumplimiento de la legislación aplicable y los principios, políticas y estándares de BTV SL.
- Compromiso con prácticas empresariales medioambientalmente sostenibles, que protejan a las generaciones futuras.
- Relaciones personales basadas en la confianza y en el respeto mutuo.

**—¿Cuál ha sido su evolución dentro del sector de la Seguridad?**

—Desde que en los años 80 BTV emprende una política de diversificación de producto, la Caja Fuerte, hasta día de hoy, no para de crecer mediante la innovación y actualización de sus productos.

Ya en los inicios incorporamos el sistema de cerradura electrónico y nuestro departamento de I+D+i mejoró la sofisticación tecnológica de las cajas. Pronto nos dirigimos también hacia el sector comercial y, muy especialmente, al hotelero.

En los años 90 comenzó nuestra expansión territorial y lo que empezó siendo un pequeño negocio familiar se ha convertido 50 años después en una empresa que vende en el exterior y cuenta con filiales en México y China. Las aplicaciones del laboratorio de investigación en sistemas de cerradura electrónica digital para cajas fuertes, nos han convertido en uno de los fabricantes más innovadores y dinámicos a nivel internacional.

**—¿Qué productos y soluciones ofrece para el mercado residencial?**

—En BTV, 1.500 buzones al día salen de nuestras fábricas: alrededor de 80 series distintas y unos 700 modelos, en catálogo.

Disponemos de un servicio casi «a la carta» por la extensa gama en materiales (plástico, PVC o metalizados); instalación (exterior e interior); individuales o de urbanización; amplia gama de terminaciones y diversos tamaños.

Los buzones se complementan con productos para vestir las áreas comunes

de las urbanizaciones y edificios, como paneles porta-anuncios, papeleras, bandejas para publicidad, cerraduras para puertas, botiquines, etc.

**—¿Cuál ha sido el rasgo característico en su sector que más ha cambiado en estos últimos años?**

—Las demandas del mercado de incorporar a los fabricados las nuevas tecnologías, para su aplicación en las aperturas y cierres de las Cajas Fuertes. Comunicación entre las cajas y el cliente: Por IP, wifi, bluetooth, etc.

**—¿Sus productos han evolucionado a la par que ha crecido el sector digital?**

—Hemos aplicado la innovación incorporando las nuevas tecnologías a nuestros productos.

Para ello BTV, ha apostado claramente por dar a sus fabricados, un valor añadido, que empieza desde la inversión en «Máquinas herramientas de última generación» llevadas desde el departamento Técnico. Este departamento cuenta con más de 10 ingenieros, que desarrollan la optimización de los productos a fabricar, desde programas diseñados específicamente para la obtención de mayor rendimiento y calidad de producto terminado.

**—¿Son partidarios de la adaptación de estas nuevas tecnologías a su sector?**

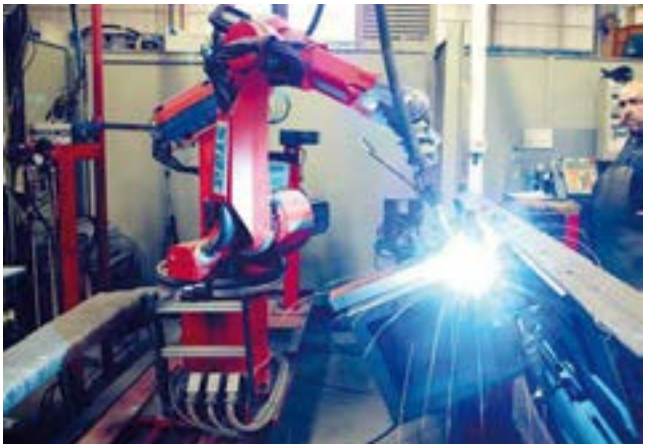
—«Sí» con rotundidad, hay que adaptarse a la nueva ola que arrastra el mundo de las Nuevas Tecnologías. Un ejemplo de ello es la gestión electrónica del efectivo, para los distintos sectores: Retail, Alimentación, Estaciones de Servicio… Eso sí, sin dejar de dar soluciones a las personas que siguen prefiriendo soluciones más sencillas, como por ejemplo con cerraduras de «solo llave».

**—Tanto en el campo de nuevos productos o en el campo de mejoras de los ya fabricados, ¿ha habido grandes avances?**

—Los avances pasan por una concepción en la seguridad de incorporar cada vez más obstáculos al ladrón. Se trata de añadir barreras, que validamos con nuestras propias pruebas de ensayo, así como en laboratorios acreditados para ello, antes de «salir a la venta».

**—¿Cuáles son exactamente esos avances?**

—Desde el departamento de I + D y junto con universidades pioneras en estudios de materiales, se realizan estudios de mejora de componentes (calidad de los aceros a emplear, cerraduras de última generación, materiales de alta resistencia a los ataques…) Nos centramos también en conseguir diseños atractivos y novedosos para el cliente final (acabados de colores, manetas de apertura de diseño innovador, etc).



**—¿En qué nuevas líneas está trabajando?**

—En la división de Alta Seguridad estamos ampliando la gama PREMIUM: con cajas Fuerte de GRADO III- IV y V, Certificadas por AENOR y ECBS, con una amplísima referencia en dimensiones y formas de aperturas, incorporando al mercado, las distintas soluciones y requisitos que piden desde el Ministerio del Interior. Junto a estas cajas, la variedad de producto personalizado crece continuamente: cajas para la gestión de efectivo, armeros de usos específicos, casilleros bancarios, etc.

En la división de Hotel: soluciones de equipamiento interno de la habitación del hotel: Cajas fuertes motorizadas, con diseño innovador y prestaciones de comunicación remota; minibares silenciosos y de bajo consumo; complementos para el baño y áreas comunes.

En la división doméstica y de ferretería, las gamas crecen tanto en cajas ligeras como de ocultación. También en buzones de distintas terminaciones y acabados especiales, para composiciones de montaje según los requisitos de los clientes finales.

**—¿Qué elementos diferenciales presenta con respecto a su competencia?**

—Desde la Dirección de la empresa BTV, se ha apostado claramente por la inversión en una doble vertiente: en personal netamente cualificado y con formación empresarial, así como en recursos productivos en forma de maquinaria y sistemas informáticos de última generación. El objetivo es mantener el precio más atractivo del mercado que nos ha caracterizado siempre, junto con producto de calidad y prestaciones exquisitas. Por último, un servicio de entrega y posventa extrarápido y con cobertura completa en todo el territorio, lo que garantiza tranquilidad a nuestros clientes más exigentes. ●

Contactos de empresas, p. 9.

**ENRIQUE DOMÍNGUEZ.** FUNDADOR DE ELPARKING INTERNET

# *«Con **Parkingdoor** se puede gestionar el acceso al garaje de forma cómoda y segura, sin utilizar mandos o llaves»*

La tecnología Parkingdoor se compone de un dispositivo inteligente instalado en la puerta del garaje y una aplicación con la que se puede controlar la apertura del parking desde prácticamente cualquier teléfono o reloj inteligente», explica Enrique Domínguez, fundador de ElParking Internet, quien ideó este innovador dispositivo al comprobar lo incómodo que resultaba «llevar el mando del garaje a cuestas, y me di cuenta de lo cómodo que sería poder abrir el garaje con el móvil, en lugar de depender de mandos y llaves físicas». En esta entrevista analiza de manera detallada las características y funcionamiento del dispositivo.

**—¿Qué es Parkingdoor?**

—Parkingdoor es un sistema que permite abrir la puerta del parking desde el teléfono móvil.

La tecnología Parkingdoor se compone de un dispositivo inteligente instalado en la puerta del garaje, y una aplicación con la que se puede controlar la apertura del parking desde prácticamente cualquier teléfono o reloj inteligente.

Con el sistema Parkingdoor se puede gestionar el acceso a los garajes de forma cómoda y segura, sin necesidad de utilizar mandos, llaves o tarjetas.

**—¿Cómo surgió la idea de ponerla en marcha?**

—Como en otros muchos casos, la idea surgió de la propia experiencia de mí, fundador de Parkingdoor. Me parecía bastante incómodo tener que llevar el mando del garaje a cuestas y me di cuenta de lo cómodo que sería poder abrir el garaje con el móvil, en lugar de depender de mandos y llaves físicas.

Desde la idea inicial, pensada para un uso personal, se evolucionó a un sistema completo de control seguro de accesos al garaje, tanto para el mercado residencial como para el comercial.

Parkingdoor comenzó su andadura con un equipo de 4 personas y, en la actualidad, ya cuenta con una plantilla de 30 trabajadores, repartidos entre las oficinas de Madrid (departamento de ventas, soporte y operaciones) y Salamanca (equipo técnico, diseño y marketing).

**—¿Cómo funciona el dispositivo Parkingdoor?**

—El dispositivo Parkingdoor se instala sobre el sistema de apertura con el que cuente el garaje y abre o cierra la puerta cuando conecta vía Bluetooth con un móvil o reloj inteligentes que tenga instalada la aplicación, y cuando el usuario esté autorizado para acceder al aparcamiento.

La persona propietaria o administradora del garaje puede activar y desactivar el acceso de otras personas al parking, en cualquier momento y en tiempo real, sin tener que preocuparse de prestar mandos o llaves físicas.

**—¿Qué se necesita para poder usarlo?**

—Sólo es necesario disponer del dispositivo Parkingdoor instalado en el garaje e instalar la aplicación en el móvil, disponible para smartphones Android y para iPhone.

**—¿Qué ventajas aporta la solución para los usuarios de garajes en materia de seguridad principalmente?**

—Al ser una plataforma basada en tecnología en la nube, permite gestionar el acceso al aparcamiento desde cualquier ordenador y desde el móvil en tiempo real. Así, el administrador puede permitir que los propietarios de las plazas entren al garaje y además usar el sistema para conceder accesos temporales a inquilinos, proveedores o servicios de mantenimiento sin necesidad de darles llaves o mandos que puedan copiar.

«El sistema es compatible con casi la totalidad de los automatismos de apertura para aparcamientos del mercado, tanto en uso residencial como empresarial»

Parkingdoor usa un robusto encriptado en sus comunicaciones usando estándares abiertos y públicos, la misma tecnología de seguridad en comunicaciones usada por las instituciones financieras para su banca electrónica. Se aplica seguridad a dos niveles, a nivel de protocolo y a nivel de aplicación, para asegurar que sólo los usuarios autorizados puedan tener acceso al garaje.

**—¿Cuáles son los elementos diferenciales con respecto a otras soluciones?**

—Además de ofrecer un nivel de seguridad elevado en las conexiones entre el dispositivo Parkingdoor y el móvil, que evita la interceptación y copia de la señal, Parkingdoor tiene ventajas respecto a otras soluciones.

El sistema es compatible con casi la totalidad de los automatismos de apertura para aparcamientos del mercado tanto en uso residencial como empresarial. Su instalación no requiere de ningún tipo de obra ni anula las llaves, tarjeta o mandos del sistema, con lo que es posible tener un sistema de respaldo físico.

Parkingdoor es quizás la solución más asequible del mercado para un control de accesos seguro, inteligente y en tiempo real. ●

**Fotos:**
**ElParking Internet**

Contactos de empresas, p. 9.

Grupo ESV

# ESVISION
vigilancia inteligente

ACUERDO DE COLABORACIÓN
CAFMadrid Colegio Profesional Administradores Fincas | Administrador Fincas Colegiado

## LÍDERES EN INSTALACIÓN DE CÁMARAS Y CONTROL DE ACCESOS EN COMUNIDADES


## ESTAMOS SIEMPRE VIGILANDO

CENTRAL RECEPTORA DE ALARMAS (CRA)

INSTALACIONES Y MANTENIMIENTO DE SIST. DE SEGURIDAD

CÁMARAS DE VIGILANCIA

CONTROL DE ACCESOS

VIGILANTES DE SEGURIDAD

SERVICIOS DE ACUDA

CONSERJES-AUXILIARES



**Instalación y equipos sin coste***

**VISITA NUESTRA WEB**

esvisionseguridad.com
**Oferta ESVision ONE**

Oferta válida hasta el **30 junio de 2017** o hasta completar las **150 primeras instalaciones**

**Rondas de videovigilancia real** mediante CRA propia | **Control de accesos** gestionados 24h

**PIDA INFORMACIÓN EN**
**91 670 20 71**
info@esvisionseguridad.com
**esvisionseguridad.com**

* Incluye instalación hasta 100 metros de cableado

ASESORAMIENTO PARA EL CUMPLIMIENTO DE LA LEY DE SEGURIDAD PRIVADA, NUEVAS NORMATIVAS Y LA LEY LOPD 15/1999 DE PROTECCIÓN DE DATOS

PDM
Empresa instaladora de sistemas de seguridad autorizada por la D.G.P. nº 1484

ESV
Empresa de seguridad autorizada por la D.G.S.E. nº 1762

Grupo ESV
grupoesv.com

SEDE CENTRAL:
Cincel, 13. Pol. Ind. Santa Ana
28522 RIVAS VACIAMADRID (MADRID)
Tel: 902 38 40 42 Fax: 91 670 20 91
grupoesv@grupoesv.com

ISO 9001 BUREAU VERITAS Certification
ISO 14001 BUREAU VERITAS Certification

**JOSECHU MIGOYA ELDUAYEN.** INNOTEC SYSTEM

# Fraude bancario, el juego del ratón y el gato

**Una técnica de defensa muy utilizada por nuestros equipos es el uso de códigos trampa avanzados (trapcode) que se ocultan en los sitios web de las entidades bancarias, y que recogen información de todas las peticiones recibidas para que sean correladas y analizadas por los servicios de gestión de incidentes**

Suplantación de identidad (corporativa o de usuarios), malware y troyanos, correos fraudulentos, black markets, phishing, pharming, abusos de marca..., son numerosos los vectores de ataque con los que los ciberdelincuentes intentan estafar y obtener un importante botín a los clientes del sector bancario. Ante esta situación, las entidades deben apostar por una detección proactiva, que permita la monitorización de sus redes y equipos, el análisis de sitios web fraudulentos y, sobre todo, una capacidad absoluta para evolucionar al ritmo de los atacantes e, incluso, anticiparse a sus acciones.

La historia del fraude bancario ha sido el juego del ratón y el gato: según se añaden capas de seguridad a los procesos, los atacantes buscan nuevas formas de saltárselos y, según los atacantes encuentran nuevos métodos de ataque, las entidades implementan nuevas estrategias para repelerlos.

El objetivo de estas entidades es doble: por un lado ofrecer al cliente la misma seguridad al operar por Internet (bien sea desde un ordenador, un portátil o un Smartphone), que personándose en una sucursal bancaria; y, por otro, asegurar que las operaciones son realizadas por usuarios legítimos sin interferencias o intervenciones maliciosas.

## Medidas tradicionales frente al fraude

Un ejemplo concreto de esta evolución lo encontramos en la identificación de los usuarios. Inicialmente se proporcionaba unas claves de acceso (usuario/contraseña) que tenían que introducir al acceder al sistema.

Al aparecer el malware (programas maliciosos) de tipo keylogger, que registra las pulsaciones de los usuarios, se

empezaron a implementar teclados virtuales que permiten introducir parte de la clave pulsando en la pantalla sin que sea registrada por el teclado. Posteriormente surgieron variantes que capturaban, además del teclado, la pantalla del usuario.

La respuesta de las entidades financieras fue la introducción de un «doble factor» (o «segundo factor») de seguridad en las operaciones más delicadas. Este se basa en la aportación de dos credenciales de diferente naturaleza:

- **Algo que sabes:** credenciales de acceso o pregunta de seguridad.
- **Algo que tienes:** valor de una tarjeta de coordenadas, DNI electrónico o SMS.
- **Algo que eres:** uso de sistema biométrico que permite validar tu persona como la huella dactilar, la voz o el iris del ojo.

Además, muchas de las entidades bancarias han aumentado la seguridad, incluyendo también soluciones de OTP (One-Time Password) en las que se pide un valor aleatorio que el cliente recibe por otra vía, por ejemplo, un mensaje SMS. Este tipo de sistemas son bastante efectivos pero, aún y así, los atacantes han rizado el rizo creando malware que modifica la página del banco al ser visitada, invitando a los usuarios a instalarse en su dispositivo una aplicación móvil para recibir algún supuesto servicio, cuando en realidad roban los OTP que envía el banco.

Este tipo de malware, conocido como troyanos bancarios, lleva entre nosotros mucho tiempo, siendo los más famosos Zeus y sus variantes. Estos programas maliciosos, una vez que infectan a un cliente, se inyectan en el navegador monitorizando las páginas que visitan de forma que, cuando se conecte a ciertos sitios web, modifican su contenido. De esta forma pueden robar las credenciales, mostrar mensajes que engañen al usuario o pedir otros


datos. Las modificaciones para cada entidad se encuentran en un fichero de configuración que se descarga de Internet, lo que permite afectar a varios bancos con una sola infección y mantener actualizado el fraude.

## Conociendo a la víctima, ingeniería social

En nuestro servicio de antifraude, se han llegado a detectar incidentes donde un ordenador es infectado con un malware, de tipo spyware, que espía durante mucho tiempo el comportamiento del cliente, accediendo a sus correos electrónicos, historial de navegación , acceso a redes sociales, etc. y, por tanto, llegando a conocer casi al completo su vida.

Incluso, se detectó el caso de una persona que, para agilizar sus trámites, se ponía en contacto con el director de la sucursal por correo electrónico y realizaba transferencias por altos importes. Para tener más seguridad, se ponía en copia al gestor o al departamento financiero de la empresa. Los atacantes espiaron durante meses a esa persona y después enviaron un correo electrónico al director de la sucursal, solicitando una transferencia a una cuenta bancaria controlada por ellos. El correo imitaba perfectamente la forma de escribir utilizada en otros mensajes, incluida la firma y poniendo en copia al gestor para dar mayor veracidad a la petición. ¿Quién podría sospechar? Por suerte, en este caso, al no ser una transferencia nacional, como todas las anteriores, el director de la oficina se puso en contacto por teléfono para ratificar la información y la transferencia nunca llegó a realizarse.

Otro de los casos que hemos investigado de ingeniería social (cada vez más común), es el de una víctima que recibía una llamada desde fuera de España en la que alguien, que se identificaba como trabajador de Microsoft, le informaba de que su ordenador personal estaba comprometido con «un virus». A continuación, se le decía que, dentro del servicio ofrecido al adquirir una licencia de Windows, ellos mismos se encargarían de proceder a la limpie-

za del ordenador. Para ello solicitaban la instalación de una aplicación de control remoto, así como los datos de las cuentas bancarias habituales para validar que no estaban comprometidas. Por si fuese poco, indicaban que para arreglar el equipo necesitaban tres horas durante las cuales se debía ignorar cualquier llamada que recibiese que no fuese de ellos, así como cualquier SMS o acercarse al ordenador. De lo contrario, los «otros delincuentes» podrían llamar fingiendo ser del banco e inventarse que estaban realizando alguna transferencia.

Desgraciadamente, en esta ocasión, los delincuentes sí lograron su objetivo.

## Defensa proactiva

Ante esta situación, las entidades bancarias han reaccionado utilizando nuevas técnicas de detección con diferentes tecnologías.

Una de ellas es el uso de la esteganografía; es decir, ocultar información en ficheros legítimos sin que sea visible para un posible intruso. De este modo, cuando un atacante se descarga una web para manipularla y hacer posteriormente phishing (una copia de la imagen del portal para fines fraudulentos), también se descargan ciertos ficheros, por ejemplo, imágenes, que contienen información identificativa de la conexión. Cuando el Phishing es activado, se puede obtener un rastro que localice al atacante a través de esta información.

Otro ejemplo, muy utilizado por nuestro equipo, es el uso de códigos trampa avanzados (trapcode) que se ocultan en los sitios web de las entidades bancarias y que recogen información de todas las peticiones recibidas para que sean correladas y analizadas por los servicios de gestión de incidentes.

La confección de listas blancas de marcas y dominios, el análisis de sitios web fraudulentos o el bloqueo de navegadores web son otras de las técnicas fundamentales a la hora de luchar contra este tipo de fraude.

No obstante, y a pesar de que se van incluyendo nuevas medidas de seguridad que hacen más difícil los fraudes y extorsiones, siempre existen nuevas posibilidades de que los delincuentes lleven a cabo sus actividades. Por lo tanto, es preciso seguir trabajando en actualizar las medidas de protección y concienciar a los usuarios de las amenazas existentes dado que, al final, muchos de los ataques son llevados a cabo abusando de su confianza, ingenuidad y desconocimiento. ●

*Fotos: Innotec System*

Contactos de empresas, p. 9.

**MARÍA JOSÉ DE LA CALLE.** COFUNDADORA, DIRECTORA DE COMUNICACIÓN & ANALISTA SENIOR DE ITTI. MJDELACALLE@ITTRENDSINSTITUTE.ORG

# Cómo la «casa inteligente» desvela nuestras vidas

El título del artículo es un remedo de otro cuyo título es «Cómo los modernos dispositivos desvelan nuestras vidas»[1], centrado en la falta de [ciber]seguridad de dispositivos de uso cotidiano a los que hoy día se ha dotado de funciones propias de un ordenador y de conectividad a Internet. Dispositivos como frigoríficos, termostatos, «vigilabebés», televisores, cámaras de vigilancia, cerraduras «inteligentes», etc., los cuales, por medio de un chip, pueden recoger, procesar, enviar y recibir datos, y actuar con y sin intervención humana.

SE ha demostrado que dichos objetos conectados son muy vulnerables, no sólo por los resultados de las investigaciones que expone el artículo mencionado, sino por otras anteriores o por ataques ya acaecidos. No hay más que escribir en un buscador, por ejemplo, «vulnerabilidades IoT», para encontrar gran cantidad de información, como el estudio realizado por HP en 2014 sobre el tema.

Según el blog «Segu-Info»[2], que comentaba dicho estudio, se encontró una media de 25 vulnerabilidades en cada dispositivo examinado –cámaras web, termostatos, tomas de alimentación remota, alarmas, cerraduras, etc.–, lo que los hace estar expuestos a ataques. El fácil acceso a cualquiera de ellos, manipulables a distancia, no sólo podría servir para modificar datos o comportamientos del propio dispositivo, sino para hacer de puerta de acceso a otros dispositivos teóricamente más protegidos con los que estuvieran conectados, como ordenadores o teléfonos.


## Botnets, Mirai y Dyn

La falta de protección de estos objetos hace que sea fácil introducir en ellos malware por personas no autorizadas, con el fin de tomar control sobre ellos y ordenar acciones cuando quieran. De esta manera los atacantes forman una red de dispositivos a sus órdenes. Esta red es lo que se conoce como «botnet», red de dispositivos comprometidos.

Hasta ahora, las botnet estaban fundamentalmente formadas por ordenadores personales, a los que se han ido uniendo teléfonos, tabletas, y en el momento actual cualquier objeto más simple conectado, mucho más sencillo de controlar que los anteriores. Estos objetos vienen con una configuración de fábrica, incluidas las contraseñas, las cuales, en muchos casos, como el de los routers, están publicadas en Internet por fabricante y modelo; en otros, están recopiladas en diccionarios utilizados para perpetrar ataques con herramientas de forma automática.

Incluso hay dispositivos para los cuales entre las recomendaciones del fabricante está la de no cambiar la contraseña, ya que podría dejar de funcionar correctamente, o también que esta acción sea realmente difícil para llevarla a cabo por los propios usuarios.[3]

El pasado 21 de octubre se produjo un ataque de denegación de servicio distribuido o DDoS (Distributed Denial of Service) contra la empresa Dyn, utilizando para ello un malware –«Mirai»– para comprometer miles de dispositivos de la IoT. Dyn es un proveedor de DNS's. El DNS –Domain Name System– es una tabla que relaciona la dirección digital –dirección IP, una serie de ceros y unos– donde reside una página, con su nombre o URL (Uniform Resource Locator) –ej. www.twitter.com–, que es la forma acostumbrada al navegar o buscar una página.

Ese ataque, citando el blog de «Kaspersky Lab»[4] se produjo por medio de una botnet de miles de dispositivos conectados (IoT), lanzando tantas peticiones a la vez a los servidores de la empresa –1,2 terabits/sg– que los colapsaron.

La consecuencia fue que no se pudo acceder durante unas horas a las web correspondientes a las URL's de empresas (muchas muy grandes) registradas en servidores de Dyn. Más de 80 grandes websites y servicios en-línea quedaron inaccesibles, como si se hubiera ejecutado un ataque sobre todas ellas a la vez, y no estuvieran accesibles. ¡Y no lo estaban! No se podía encontrar la dirección IP de las url's correspondientes, ya que el servidor de DNS no podía responder.

Entre las páginas afectadas figuraban Netflix, PayPal, Sony PlayStation, y, tampoco se podía tweetear, porque también Twitter era un cliente de Dyn.

Siguiendo con el mismo post del blog de «Kaspersky Lab» citado, «Mirai» ya se utilizó en el mes de septiembre de este año para lanzar un ataque sobre el blog[5] del periodista de seguridad Brian Krebs, colapsando el servidor con peticiones de 665 gigabits/sg procedentes de 380.000 dispositivos zombis.

Freepik.

Poco después del ataque, se publicó el código fuente de «Mirai», provocando que el número de bots aumentara. El ataque a Dyn ocurrió en menos de un mes después.

El pasado 14 de octubre y unos días antes del ataque a Dyn, el «Department of Homeland Security» de los EEUU publicó una alerta[6] sobre «Mirai» y sobre los peligros de los ataques DDoS por botnets de dispositivos de la IoT. La alerta también preveía posibles ataques futuros. Concretamente «Mirai» se apoya en dispositivos de la IoT, tal como routers de los hogares, cámaras con IP y aparatos de vídeo.

El éxito de los ataques DDoS sólo depende de lanzar solicitudes suficientes para colapsar la capacidad de los servidores atacados, es decir, el ancho de banda. Cuanto más ancho de banda más peticiones a la vez se necesitan, o lo que es lo mismo, más dispositivos. Pero su número no parece que vaya a ser un problema con la IoT, con la que se puede contar con billones de dispositivos conectados para hacer una botnet, o unir varias de las ya existentes.

## La «casa inteligente»

Se puede definir como un edificio en el cual hay una red domótica que abarca comunicaciones, seguridad, iluminación, climatización, aparatos de música, televisión, puertas, y cualquier objeto al que se le haya dotado de un chip y pueda proporcionar alguna función en el hogar.

Estos objetos, conectados a Internet, pueden ser manejados a distancia por otros dispositivos y/o por un ordenador, teléfono o tableta, con o sin intervención humana, pueden enviar alertas, e incluso, pueden hablar, caso de «Echo»[7] de Amazon. Este dispositi-

vo con su interfaz de voz «Alexa», responde preguntas como si de una «Wikipedia» parlante se tratara, proporciona información sobre la previsión meteorológica u horarios de eventos locales; además, es un reproductor de música, y puede controlar niveles de luz o termostatos.

«La importancia de la seguridad de la IoT en general, y de los dispositivos inteligentes para los hogares en particular se torna vital»

«Echo» siempre está escuchando las conversaciones por si se dice «Alexa», en cuyo caso tiene que responder. En la casa hay otros aparatos que también están a la escucha, como el televisor cuyo mando se ha sustituido por la voz.

Para la seguridad en la casa hay cámaras, que estarán conectadas o desconectadas según los requerimientos de los habitantes de la vivienda. Las puertas de la calle o del garaje se abrirán cuando detecten a alguien o algo, como el coche, que tenga permiso para entrar, bien por alguna señal enviada por algún otro dispositivo, por reconocimiento facial o por la voz.

Todas estas funciones se apoyan, como ya se ha dicho, en chips que constituyen pequeños ordenadores con sus mismas necesidades de seguridad pero sin las medidas que sus homólogos más tradicionales, los ordenadores o los teléfonos, ya tienen. Y todos estos aparatos están en el hogar.

Ya se ha apuntado que cualquiera puede fácilmente acceder a los «objetos inteligentes» que conforman el «hogar inteligente», con lo cual la confidencialidad y la integridad de los datos que recogen, procesan y comunican están en entredicho. Son datos que se pueden robar, divulgar o vender; y el software se puede manipular.


Freepik.

Un escenario podría ser el siguiente: se podría modificar el software de la cerradura para dejar pasar a un intruso. La cerradura conectada con las cámaras de vigilancia, las indica que todo es correcto y no se activa la alarma. El intruso previamente ha recogido datos de las costumbres de los habitantes de la casa gracias a los objetos de escucha y a las cámaras.

La ingeniería social[8], técnicas psico-sociológicas para obtener ilegítimamente información de terceros, nunca fue tan sencilla. El intruso puede anticipar que no haya nadie en casa o que quien esté no le vaya a suponer un problema.

Según «Help Net Security»[9] en un artículo del 19 de septiembre pasado, parece que hay un alarmante incremento de «ransomware» (extorsión basada en la amenaza del cese de un servicio tecnológico), en televisores inteligentes y en cámaras conectadas, ataques de inyección de código y amenazas de «día-cero», así como muchas vulnerabilidades en protocolos de comunicación para el «hogar inteligente».

Esta falta de seguridad que puede servir para recoger datos sobre todo lo que ocurre en el hogar, espacio que es considerado eminentemente privado, es lo que constituye una preocupación especial en la seguridad de la información en general.

Teniendo en cuenta que los objetos «escuchan» y «ven», la información disponible no son sólo datos acerca de la temperatura de la casa o del nivel de iluminación deseada, es información sobre lo que dicen y hacen las personas que la habitan, sus costumbres y sus gustos, información personal e íntima que expone la vida de sus habitantes a ojos y oídos no deseados.

## Conclusión

La importancia de la seguridad de la IoT en general, y de los dispositivos inteligentes para los hogares en particular se torna vital. Por una parte, la inseguridad de estos dispositivos los hace muy apetecibles para ser utilizados para actividades no deseadas. Y teniendo en cuenta su gran número, su potencia de ataque es extraordinaria, pudiendo inhabilitar parte de Internet actuando sólo sobre unos cuantos servidores –ataque a Dyn–. Por otra, puede hacer de nuestros hogares un lugar inseguro y vigilado.

¿Tienen los ciudadanos que ser expertos en ciberseguridad para tener su casa segura?

El número 315 de «Cuadernos de Seguridad», del pasado mes de octubre, contiene una entrevista a Miguel Ángel Abad, Jefe del Servicio de Seguridad del Centro Nacional para la Protección de Infraestructuras Críticas o CNPIC. En ella Abad opinaba lo siguiente:

«...pongo en duda que los usuarios deban convertirse en expertos en ciberseguridad. A nivel personal opino que la ciberseguridad debe evolucionar hacia sistemas transparentes para el usuario final».

A los ciudadanos no se les debería convencer de que son ellos responsables de que sus dispositivos sean seguros. Son los fabricantes los que deben proporcionar dispositivos seguros, e instalarlos en los hogares de forma segura, haciéndose responsables de los posibles fallos que puedan tener, análogamente a otros cualesquiera fallos físicos de funcionamiento.

Pero corresponde a la sociedad civil, a los ciudadanos, las asociaciones, los partidos políticos, los colegios profesionales crear un estado de opinión que fuerce a los políticos a un necesario esfuerzo regulador. Y mientras tanto, no estaría de más mantenerse informado


sobre lo que puede traernos un empacho de tecnología, dejándonos embaucar por lo atractivo de lo que nos aporta, sin considerar que podemos estar (y estamos) metiendo el caballo de troya en el dormitorio de nuestros bebés, en el coche automático o en la «termomix». ●

## REFERENCIAS

[1].- Mirko Zorz (9 de mayo, 2016). «Internet of Fail: How modern devices expose our lives». HelpnetSecurity. url [a 30-10-2016] https://www.helpnetsecurity.com/2016/05/09/internet-of-fail/

[2].- «Segu-Info» (5 de agosto, 2014) «Internet of Things: un promedio de 25 vulnerabilidades por dispositivo». url [a 30-10-2016] http://blog.segu-info.com.ar/2014/08/internet-of-things-un-promedio-de-25.html

[3].- Brian Krebs (16 de octubre, 2016) «Who Makes the IoT Things Under Attack?» KrebsOnSecurity. url [a 30-10-2016] https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/

[4].- Kate Kochetkova (26 de octubre, 2016) «How to not break the Internet». Kaspersky-lab. url [a 30-10-2016] https://blog.kaspersky.com/attack-on-dyn-explained/13325/

[5].- Brian Krebs (16 de septiembre, 2016) «KrebsOnSecurity Hit With Record DDoS». KrebsOnSecurity. url [a 30-10-2016] https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

[6].- «Heightened DDoS Threat Posed by Mirai and Other Botnets» (14 de octubre, 2016). DHS. url [a 30-10-2016] https://www.us-cert.gov/ncas/alerts/TA16-288A

[7].- url [a 30-10-2016] https://www.amazon.com/Amazon-Echo-Bluetooth-Speaker-with-WiFi-Alexa/dp/B00X4WHP5E

[8].- url [a 30-10-2016] https://es.wikipedia.org/wiki/Ingeniería_social_%28seguridad_informática%29

[9].- «Connected devices riddled with badly-coded APIs, poor encryption (9 de septiembre, 2016) «Help Net Security» url [a 30-10-2016] https://www.helpnetsecurity.com/2016/09/19/connected-devices-insecurity/

# UTS

## La nueva generación de unidades de control y visualización


Tecnoalarm
HI-TECHNOLOGY & DESIGN
WORLDWIDE FROM ITALY

Videoalarm

www.tecnoalarm.com

# Las innovadoras consolas UTS: Uso complementario con los sistemas anti-intrusión de Tecnoalarm y posibilidad de integración con sistemas de vídeovigilancia CCTV

## UTS V4 y V8

4 u 8 entradas de vídeo para cámaras de vigilancia analógicas estándar 960H
Visualización de los “live streams” asociada a alarma de programa, alarma de zona, conexión y/o activación de telecomando
Asociación a un total de 4 eventos

## UTS C

Pantalla TFT 7” capacitiva, síntesis vocal y gestión plurilingüe
Gestión de hasta 32 programas

## UTS 4.3 PROX

Pantalla TFT 4.3” capacitiva, síntesis vocal, interfaz usuario interactiva e intuitiva
Gestión de hasta 15 programas

*Compatible con los sistemas de alarma TP8-28, TP8-28 GSM, TP10-42, TP8-88, TP20-440*
*Un plug-in que permite la gestión de planos está disponible para las UTS V4, UTS V8 y UTS C.*

Tecnoalarm ESPAÑA

c/Vapor 18 (Pol. Ind. El Regas)
08850 Gavá - Barcelona (España) - tel. +34936622417
tecnoalarm@tecnoalarm.es - www.tecnoalarm.com

INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE)

# El sector de la Ciberseguridad demandará 825.000 profesionales especializados hasta 2025

El sector de la ciberseguridad crece en España a un ritmo del 12% anual y emplea a 42.500 profesionales, constituyendo uno de los ámbitos tecnológicos de mayor proyección nacional e internacional para la industria, además de convertirse en un sector con enormes expectativas de empleo. El aumento de ciberataques, y la proliferación de nuevas amenazas con un grado de sofisticación elevado y creciente, conducen a la necesidad de incorporar profesionales expertos en ciberseguridad para cubrir puestos de trabajo especializados en distintos tipos de organizaciones.

ESTE diagnóstico de déficit de perfiles especialistas en ciberseguridad hace prever que la Unión Europea tendrá una necesidad de incorporar en la próxima década en torno a los 825.000 empleos cualificados en este sector.

España es consciente de esta situación y, por ello, se hace necesario el impulso de actuaciones que contribuyan a contrarrestar la brecha entre oferta y demanda de talento, y la adopción de medidas que estimulen la generación, identificación, captación, retención y gestión del mismo.

Desde el Instituto Nacional de Ciberseguridad (INCIBE), organismo dependiente del Ministerio de Industria, Energía y Turismo, se ha realizado un trabajo previo de estudio de la situación en España, que ha concluido en la elaboración de un documento que se ha definido como Punto de Partida al Modelo de Gestión y Seguimiento del Talento en Ciberseguridad en España. Para su elaboración, se ha contado con la visión de los principales actores del mercado de la ciberseguridad: industria, sector académico e investigador, Administración y el propio colectivo de talento. Fruto de este trabajo, se han identificado un total de catorce actuaciones que persiguen promover el talento en ciberseguridad.

## Análisis del mercado del talento en ciberseguridad

INCIBE ha contado con la colaboración de los sectores industrial, profesional y académico-investigador. En el documento se muestra un análisis preliminar del mercado del talento en ciberseguridad en España, incluyendo una descripción del escenario actual, así como los limitadores y potenciadores del mismo. En base a dicho diagnóstico, se proponen una serie de líneas generales de actuación (algunas de ellas ya puestas en marcha por INCIBE), para conocer mejor las necesidades y demandas del mercado y como una forma de paliar la carencia de profesionales suficientemente cualificados. ●

*Foto: Pixabay*

# *Líderes en Seguridad*

**Seguridad Integral Canaria** es referente de seguridad. Un complejo sistema tecnológico y humano, perfectamente sincronizado para hacer que su confianza y tranquilidad esté más que garantizada. Seguridad Integral Canaria dispone de una preparada plantilla de vigilantes de seguridad con todos los recursos necesarios para desarrollar las labores más efectivas en materia de seguridad y vigilancia, haciendo de esta empresa la elección más acertada cuando se habla de protección eficaz.

Vigilancia y Protección de Bienes e Instalaciones | Transportes de Seguridad | Ingeniería y Sistemas de Seguridad | Servicio Acuda | Central Receptora de Alarmas

ISO 9001 ISO 14001 OHSAS 18001

**T 902 226 047**

DGSE: 2562

www.seguridadintegralcanaria.com

**JORGE SALGUEIRO RODRÍGUEZ.** PRESIDENTE EJECUTIVO DE AECRA. JURISTA-ABOGADO Y VOCAL EXPERTO EN LA COMISIÓN NACIONAL DE SEGURIDAD PRIVADA

# Aproximación a las políticas de **cumplimiento normativo**

## El Compliance Officer en la Seguridad Privada

La tendencia legislativa existente, tanto nacional como internacional, apuesta por el buen gobierno corporativo, la transparencia y la necesidad de implantar controles para luchar contra el fraude y la comisión de delitos; se trata del Corporate Compliance.

LLEVAMOS años conviviendo con términos como el Buen Gobierno Corporativo o la «Responsabilidad Social de las Empresas», que se han ido incorporando en la práctica en los Códigos Éticos empresariales, pero recientemente se están haciendo aún mayor eco en el panorama empresarial y legal actual, debido a la irrupción de la reforma del Código Penal L.O. 1/2015 de 30 de marzo, que entró en vigor el 1 de julio de 2015, respecto de la responsabilidad penal de las personas jurídicas, al constituir los Códigos Éticos, uno de los requisitos esenciales en los Compliance Program, para que las organizaciones puedan beneficiarse de la exención de la responsabilidad penal.

Aunque el entorno normativo afecta el desarrollo de cualquier actividad empresarial, es cierto que aumenta su criticidad para las Empresas de Seguridad autorizadas que, por operar en un mercado regulado, su modelo de negocio está íntimamente relacionado con el cumplimiento de determinado bloque normativo.

Vigilar el cumplimiento normativo resulta cada vez más complejo a causa de la gran cantidad de normas jurídicas que afectan a la actividad empresarial de las empresas de seguridad, su creciente complejidad y rápida evolución.

Esta función de cumplimiento ha afectado primero al mercado de la Seguridad Privada y se ha vinculado a determinados bloques normativos. Sin embargo, actualmente se reconoce que el cometido de dicha función es más amplio y que no es patrimonio exclusivo de las empresas de seguridad.

El cumplimiento normativo ha sido una función y tarea tratada en múltiples textos reconocidos internacionalmente antes de ser introducido en nuestro Derecho Patrio con la reforma reciente del Código Penal del año 2015.

Un ejemplo de entorno sectorial de cumplimiento voluntario lo promovió AECRA como Asociación en el año 2008, al proponer en la actividad de gestión de alarmas, un modelo de norma auto impuesta a nuestros miembros y colaboradores, como esfuerzo por desarrollar buenas prácticas y promover una forma ética de hacer negocios. Este modelo de entorno de cumplimiento implicaba asumir un deber de respeto y vigilancia en relación con su contenido, cayendo así dentro del ámbito de cumplimiento. Fueron cinco los elementos fundamentales que pueden facilitar el alcance del objetivo de cumplimiento que planteaba por ejemplo AECRA: A) declaración de valores fundamentales. B) patrones de conducta. C) cumplimiento obligado. D) comunicación. E) salvaguardias.

Destacar por otro lado, en lo que puede constituir un entorno de cumplimiento obligatorio, las notas de subordinación y complementariedad de la Seguridad Privada respecto de la Seguridad Pública y nuestra Constitución.

Así se establece e impone en la normativa de Seguridad Privada un especial deber de cumplimiento para las empresas de seguridad, implicando que todas las actividad, servicios, funciones, medidas, recursos y personas tienen que ser puestas a disposición de las Fuerzas y Cuerpos de Seguridad, cuando las mismas tienen que proteger el libre ejercicio de los derechos y liber-

tades, y garantizar la seguridad ciudadana en el artículo 104 de la CE.

Por consiguiente dicha exigencia y circunstancia tendría que haber provocado desde hace muchos años, que las empresas de seguridad hubieran incorporado equipos humanos altamente especializados en el conocimiento y cumplimiento de las normas de Seguridad Privada.

Significar además que el concepto «cumplimiento» o «compliance» se utiliza con diferentes significados y aparece recogido en distintos tipos de normas.

Tal y como se afirma en la Norma ISO 19600 por la que se contempla las Directrices del Compliance se establece: «Compliance es el resultado de que una organización cumpla con sus obligaciones, y se hace sostenible introduciéndola en la cultura de la organización y en el comportamiento y en la actitud de las personas que trabajan en ella. Mientras mantenga su independencia, es preferible que la gestión de compliance esté integrada con los procesos de gestión de finanzas, riesgos, calidad, medio ambiente y salud y seguridad, y en sus requisitos y procedimientos operacionales».

De forma general tengo que indicar que en cualquier organización empresarial, surgen plantearse muchas preguntas a la hora de implantar una función o política de Compliance o cumplimiento normativo, ya que debe contar con el apoyo de la alta dirección, seleccionar un adecuado Compliance Officer, actuar con criterios de independencia, pero alineado al negocio, y debe ser transversal en la organización empresarial. No ignoro que nuestros entornos normativos son cada vez más que dinámicos, siendo necesario poder asumir materias o normativas con cada vez menor esfuerzo, y que además el mismo sea sostenible.

En lo que se refiere al ámbito normativo regulatorio de la Seguridad Privada establecemos como punto de partida que sus normas son de derecho positivo, de cumplimiento obligado por vía coercitiva (hard law).

Para comprender el carácter coercitivo de sus normas debemos tener en cuenta lo dispuesto en el Preámbulo de la Ley 5/2014 de Seguridad Privada de 4 de abril, respecto del modelo de Seguridad Privada cuando se afirma literalmente en dicho texto legal:

«En la relación especial que mantiene la Seguridad Privada con las Fuerzas y Cuerpos de Seguridad, auténticos garantes del sistema de libertades y derechos que constitucionalmente protegen, se hace necesario avanzar en fórmulas jurídicas que reconozcan el papel auxiliar y especialmente colaborador desempeñado por la Seguridad Privada, de forma que, además de integrar funcionalmente sus capacidades en el sistema público de seguridad, les haga partícipes de la información que resulte necesaria para el mejor cumplimiento de sus deberes.

En resumen, puede decirse que el conjunto de los cambios propuestos en la nueva ley... profundiza decididamente en el actual modelo español de Seguridad Privada (complementaria, subordinada, colaboradora y controlada por la Seguridad Pública), apostando por su papel preventivo en beneficio de la seguridad general... ».

Las amenazas que se derivan para las empresas y personal de Seguridad del incumplimiento de obligaciones legales y contractuales impuestas, se incrementan de forma especial particularmente por las empresas de seguridad de inicio, a los efectos de disponer de un mapa de riesgos de cumplimiento normativo completo, así como de un sistema de gestión que permita identificarlos, valorarlos y gestionarlos de forma adecuada.

Este nivel de sensibilización de las empresas de seguridad con esta materia es lógico, por cuanto el incumplimiento de tales regulaciones les puede reportar sanciones administrativas significativas o incluso la intervención o paralización de su actividad por parte del órgano regulador correspondiente, a través en ultima instancia de la cancelación de la inscripción como empresa de seguridad para el desarrollo de actividades de Seguridad Privada.

Esta circunstancia en un mercado regulado como el de la Seguridad Privada debiera haberse producido un mayor desarrollo en el control de los riesgos legales así entendido, dando lugar a las figuras del Chief Compliance Officer (CCO), como persona física encargada de vigilar el cumplimiento estricto del marco regulatorio de la/s actividad/es de la Seguridad Privada en la prestación de sus servicios frente a ámbitos privados objeto de protección, así como de determinadas políticas o procedimientos internos (normalmente relacionados con el marco regulatorio de la seguridad privada y seguridad ciudadana).

Sin embargo, extrañamente el sector de la Seguridad Privada ha vivido ajeno a dicha realidad compleja hasta que se produce la modificación reciente del Codigo Penal Español primero en el año 2010, y recientemente en el año 2015 a través del articulo 31 bis en lo que se refiere a la responsabilidad penal de la empresa.

Nuestro Código Penal establece como eximente de la responsabilidad de la empresa, entre ellas las empresas de seguridad, la implantación de un modelo de organización y gestión idóneo para prevenir delitos, estableciendo además que un órgano de la misma (la llamada función de cumplimiento normativo representada por el compliance officer) debe ejecutar las pertinentes funciones de supervisión, vigilancia y control a tal fin.

Como consecuencia de lo anterior, una pregunta a formularnos sería: ¿quién podría ostentar y representar dicha figura de compliance officer en la empresa de seguridad?.

Si acudimos al artículo 22 de la reciente Ley 5/2014 de 4 de abril de Seguridad Privada se hace mención a la figura de representantes legales en las empresas de Seguridad Privada, definiéndose como tal en su apartado 1 «todo aquel que asuma o realice las tareas de dirección, administración, gestión y representación, o cualquiera de ellas, en nombre de aquéllas». Y añade dicho artículo en su apartado 3: «Los representantes legales de las empresas de Seguridad Privada serán responsables del cumplimiento de las obligaciones generales impuestas a las mismas por el artículo anterior».

De dicha definición expuesta y como luego veremos del estatuto del compliance officer, parece que debiéramos identificar el representante legal con dicha figura, dado que nadie mejor que el representante legal como máximo personal de Seguridad Privada, el que mejor conoce la estructura y actividades de las empresas de seguridad, sus riesgos y amenazas.

Desde luego, que el compliance officer como personal de Seguridad Privada, que hemos relacionado con la figura del representante legal contemplado en el artículo 22 de la Ley 5/2014 de Seguridad Privada, por sus funciones y responsabilidades impuestas en la normativa de Seguridad Privada quien debe conocer en profundidad las exigencias, no ya del Código Penal y la interpretación que del mismo hacen jueces y fiscales, sino también el marco regulatorio aplicable a las actividades y servicios de Seguridad Privada.

Por último quiero resaltar que dicho representante legal asumiendo la función de compliance officer, entiendo que es quien mejor sabe interpretar los estándares internacionales que existen de la materia al respecto, y cómo aplicarlos en los procedimientos y especialmente los controles que debe implantar en la empresa.

Pero es que además, resalto que este representante legal identificado como compliance officer debe ser suficientemente hábil como para sustraerse a su posición en la propia empresa, y ser capaz de verla desde fuera y bajo una perspectiva crítica, todo ello con el fin de evitar posibles sesgos corporativos (conscientes o inconscientes).

Lo que puede parecer una labor de supervisión del modelo la podemos convertir en una tarea sumamente compleja, que entraña además un riesgo de derivación de responsabilidad para el propio profesional, que ya la tendría asumida por la normativa de Seguridad Privada en el artículo 22 de la Ley de Seguridad como representante legal.

Este representante legal sometido como es lógico en las sociedades mercantiles a la labor de supervisión de los órganos y directivos de la empresa, nos conduce a una importante realidad consistente en que el consejo de administración no tiene los conocimientos necesarios para supervisar íntegramente la función de compliance officer o representante legal de la empresa de seguridad; sin embargo, no le exime de su obligación de supervisar al compliance officer.

Visto desde esta segunda perspectiva parece recomendable acudir a la auditoría y certificación del modelo de prevención que se tiene implantado en la empresa por parte de un tercero independiente resulta, sin lugar a dudas, y utilizando las palabras de la propia Ley, «una medida precisa para la buena dirección y el control de la sociedad» tal y como se hizo eco la Fiscalía General del Estado en su famosa Circular 1/2016 sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del código penal efectuada por ley orgánica 1/2015.

Se puede concluir, por tanto, que la certificación por un tercero independiente de los modelos de prevención penal tendrá relevancia a la hora de valorar el compromiso de la compañía con la cultura de cumplimiento, además de salvaguardar las obligaciones de supervisión que tienen tanto el órgano de compliance respecto del modelo implantado, como el propio consejo de administración respecto del funcionamiento de su órgano de compliance.

En este sentido AECRA como Asociación de Profesionales está trabajando y colaborando en un futuro modelo de Certificación del Compliance Office. Sobre esta cuestión y funciones del compliance officer trataré en futuros artículos. ●

*Fotos: Archivo/ Pixabay*

# Plataforma de seguridad CORPORATIVA

Casos de éxito en sectores de defensa, sanidad, banca, retail, administración pública, logística e industria.

Plataforma abierta de seguridad con amplio catálogo de productos integrados.

Solución de gestión para centros de control de seguridad y centrales receptoras de alarma corporativas.

Integración natural dentro del ecosistema de tecnologías de información.

ARQUERO
SISTEMA CORPORATIVO

928 092 181 ■ info@arquero.es ■ www.arquero.es

ARQUERO SISTEMA CORPORATIVO

# Plataformas PSIM

## ARQ-MILESTONE es la solución para la integración total en Milestone de centrales de intrusión, sensores perimetrales y paneles de incendio

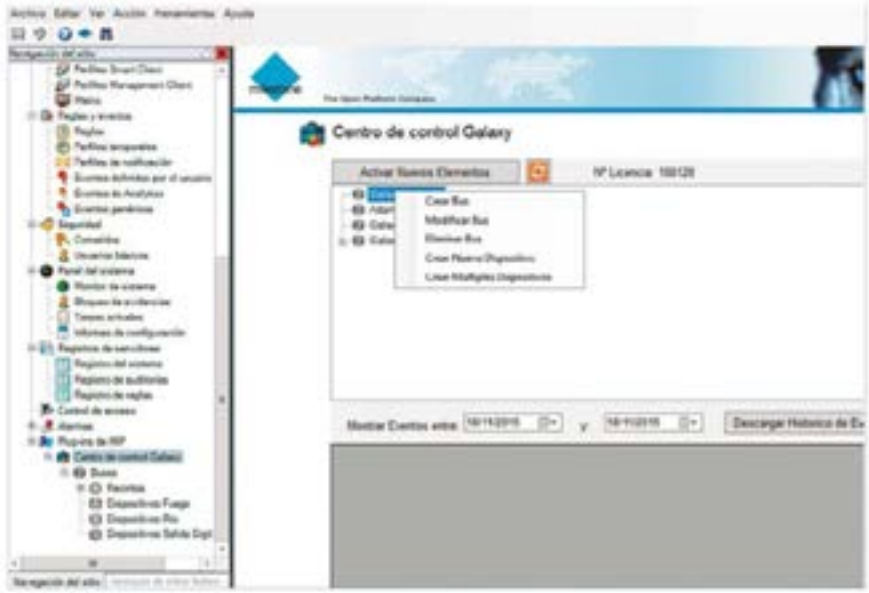
Los sistemas de seguridad física están convergiendo a la integración en plataformas multifabricante (lo que, por sus siglas en inglés, se denominan PSIM). Mientras que plataformas como Milestone tienen una gran historia en la integración de vídeo, otras como Arquero se han especializado en la integración e interoperación del resto de los sistemas (intrusión, incendio, control de accesos, gestión de visitas,...).

LA plataforma Arquero integra actualmente a la mayor parte de los principales equipos de intrusión e incendios.

Dispone para todos los fabricantes de unas capacidades básicas (armar, desarmar, anular, reconocer incendio,...) y, según el fabricante, con algunas capacidades avanzadas propias de cada equipo (activar sirenas, disparar la evacuación,...).

La operación y monitorización de todos los equipos es independiente de las peculiaridades de cada fabricante. Para el operador y para el administrador no existe diferencia entre una marca u otra a la hora de ejecutar comandos u obtener información del sistema.

Cuando lo que se integra son sensores sin «central de intrusión» como perimetrales, detección de movimiento o analítica de vídeo, Arquero aporta la capacidad de agrupar las señales en «grupos» para su armado y desarmado, y permite anular y restaurar cada una de las señales. De esta manera aporta, de una forma sencilla, la funcionalidad de central de intrusión.




## Integración en Milestone

Todos estos fabricantes y todas estas capacidades se encuentran disponibles en la plataforma Milestone a través de un nuevo plug-in desarrollado por Servicios de Consultoría Independiente (propietaria de la marca Arquero Sistema Corporativo®).

ARQ-MILESTONE es la solución para la integración total en Milestone de centrales de intrusión, sensores perimetrales y paneles de incendio. La total integración en Milestone permite la gestión en el Management de la configuración de los equipos y explotación de los históricos, mientras que el Smart Client permite la visualización y operación en tiempo real.

Una interfaz sencilla y potente permite la creación de centrales y elementos de detección, tanto de forma individual como en «proceso de lotes», simplificando la tarea y ahorrando tiempo.

Los históricos se pueden obtener mediante filtros que permiten seleccionar la información que se desea, permitiendo su exportación.

Al basar la integración en el kernel de la plataforma Arquero, la fiabilidad y estabilidad han sido contrastadas du-

rante más de quince años en cientos de instalaciones. En intrusión, proyectos emblemáticos como las cerca de seiscientas instalaciones de Telefónica Colombia, y en incendio la instalación nuclear CIEMAT y el Aeropuerto de Palma, avalan este nuevo producto.

## Representación gráfica

Los elementos integrados en los equipos pueden visualizarse en los planos, pudiendo llevar a cabo acciones sobre los mismos. De una forma simple, los operadores gestionan en un mismo entorno gráfico las cámaras, los paneles y centrales, y los sensores y detectores.

Todos los elementos supervisados pueden representarse en los planos con todos sus estados posibles. Tanto desde el árbol de elementos como desde los planos se pueden ejecutar todas las acciones que cada tipo de elemento permite.

## Integración en el ecosistema Milestone

Todas las operaciones permitidas sobre los elementos están también disponibles como acciones, que pueden asociarse fácilmente a eventos y a cualquier tipo de condiciones contempladas dentro del entorno de Milestone mediante la configuración de reglas. Ante una alarma de intrusión, por ejemplo, se pueden activar salidas digitales de la misma central o de otra distinta para encender las luces de la zona.

Todos los eventos recibidos de los equipos monitorizados se traducen en eventos internos de Milestone para que puedan ser capturados y procesados por otros módulos. Esto permite, por ejemplo, ejecutar el preset y activar el vídeo de las cámaras adecuadas a la incidencia.

## Operación simultánea Arquero y Milestone

En aquellas instalaciones donde se requiera la integración de otros sistemas como control de accesos, gestión de visitas, control de horarios, señales técnicas, gestión de rondas, CRA,…, las aplicaciones Milestone (Smart Client y Management) pueden convivir con aplicaciones nativas de la plataforma Arquero.

Todos los eventos y actividades de los operadores (armar, anular,…) de los sistemas de intrusión e incendio se pueden ejecutar de forma indiferenciada en cualquier aplicación y sus resultados se visualizan en ambas plataformas. La operación y monitorización del resto de los sistemas se realiza desde la plataforma Arquero. Las cámaras de vídeos así como las grabaciones pueden visualizarse también desde Arquero.

Esta dualidad es una ventaja cuando los operadores de seguridad, que gestionan vídeo, intrusión e incendio, son independientes de los responsables del control de accesos y de visitas y de recursos humanos.

Resumen de características:

• Monitorización y control de centrales de intrusión, sistemas perimetrales, paneles de incendio y analíticas de vídeo.

• Múltiples fabricantes y equipos integrados.

• Número ilimitado de equipos (limitación según licencia de uso)

• Elementos supervisados: panel, sensores de intrusión, sensores de incendio, particiones, salidas digitales, módulos remotos, comunicación con paneles, cámaras y motores de analítica.

• Operaciones básicas: armar, armar forzado, desarmar, anular zona, restaurar zona, activar salida digital y desactivar salida digital.

• Información recibida: armado, desarmado, alarma, zona anulada, zona restaurada, tamper, masking, pérdida de comunicaciones con el panel, activación y desactivación de salida digital, apertura y cierre de zonas.

• Representación esquemática en árbol y representación en los planos.

• Generación de eventos milestone que se pueden usar para las reglas de visualización de cámaras y otras acciones.

• Ejecución de cualquier acción (armar, desarmar,…) desde reglas Milestone.

• Visualización en el Smart Client de los eventos recibidos durante el funcionamiento del software.

• Visualización, filtrado y exportación de histórico de eventos desde el Management.

• Aplicación de cambios (creación de nuevas zonas, cambio de parámetros,...) en caliente sin necesidad de reinicio. ●

*Fotos: Arquero*

Contactos de empresas, p. 9.

**XAVIER HERRERO.** JEFE DE ESTUDIOS DE SEGURIDAD PRIVADA. IDFO-UGT

# Certificados de **profesionalidad de seguridad privada**

El Institut per al Desenvolupament de la Formació i l'Ocupació (IDFO) nace con la misión de ayudar a los trabajadores/as de Catalunya y sus empresas a mejorar permanentemente su cualificación profesional. Fue creado en 1993 por la UGT de Catalunya como una fundación privada sin ánimo de lucro y desde entonces hemos estado junto al mercado laboral sin perder de vista nuestra misión.

EL año 2002 IDFO se acredita en Barcelona para impartir cursos de formación para personal de Seguridad Privada. Posteriormente acredita sus sedes en Girona, Reus (Tarragona), Lleida, Mataró y Cornellà de Llobregat (Barcelona), formando durante estos años miles de profesionales dentro del ámbito de la Seguridad Privada.

Su labor en pro de la formación en Seguridad Privada durante estos años ha hecho que sea merecedor de diversas menciones honoríficas por parte de la Dirección General de la Policía Nacional.

## Certificados de profesionalidad de Seguridad Privada

El año 2015 IDFO fue el primer centro en obtener la autorización del Servei d'Ocupació de Catalunya del Departament de Treball de la Generalitat de Catalunya para impartir el Certificado de Profesionalidad de Vigilancia, Seguridad Privada y Protección de Personas.

Esta oportunidad nos ha permitido organizar con éxito los primeros dos cursos de esta especialidad en las instalaciones de IDFO-UGT en Cornellà de Llobregat (Barcelona)

Los Certificados de Profesionalidad, se regulan por el Real Decreto 34/2008, de 18 de enero, y constituyen el instrumento de acreditación oficial de las cualificaciones profesionales del Catálogo Nacional de Cualificaciones Profesionales en el ámbito de la administración laboral.

Estos certificados tienen carácter oficial, son expedidos por el Servicio de Empleo Público Estatal (SEPE) y los órganos competentes de las Comunidades Autónomas, y acreditan que el alumno ha adquirido las competencias profesionales que le capacitan para desarrollar una actividad laboral concreta.

El Certificado de Profesionalidad de Vigilancia, Seguridad Privada y Protección de Personas, así como el de Vigilancia, Seguridad Privada y Protección de Explosivos, de 330 y 350 horas de duración, respectivamente, han significado un cambio de paradigma en la formación del personal de Seguridad Privada.

Ambos certificados vienen recogidos en el Real Decreto 548/2014, de 27 de junio del Ministerio de Trabajo y Seguridad Social, por el cual se establecen los certificados de profesionalidad de la familia profesional de seguridad y medio ambiente.

Por otra parte, La Ley 5/2014 de 5 de abril, de Seguridad Privada, recoge en su artículo 29 los certificados de profesionalidad como formación suficiente para habilitar el personal de Seguridad Privada.

Entre las principales dificultades que nos hemos encontrado al ejecutar los certificados de profesionalidad, cabe destacar la necesidad de reestructurar el contenido del curso para adaptarse a las nuevas unidades formativas del programa, y principalmente, la dificultad para disponer de formadores que cumplan los requisitos que exigen los certificados de profesionalidad. Me consta que estas dificultades son comunes a los centros que han impartido el certificado de profesionalidad en otras comunidades autónomas.

Los fuertes requisitos que tiene que reunir el centro de formación para poder impartir los certificados de profesionalidad tanto a nivel de instalaciones como de material para realizar las prácticas de comunicaciones, primeros auxilios, sistemas de detección, defensa personal, conducción de vehículos, etc., son una garantía de que estos centros autorizados han realizado una apuesta muy importante para profesionalizar la formación en Seguridad Privada, que repercute en una mejora de la calidad formativa.

En los últimos años, probablemente debido a diversos factores como pueden ser la disminución de los requisitos de acceso para habilitarse como centro de formación de personal de Seguridad Privada, la crisis económica que ha sufrido nuestro país y la dudosa ética de unos pocos, hemos asistido a la apertura de algunos centros de formación, (una minoría, por supuesto, pero no por ello deja de ser relevante) que no han ofrecido la calidad formativa que requiere el sector.

La exigencia por normativa del certificado de profesionalidad de que todos los alumnos para acceder al curso tengan que cumplir de inicio los requisitos para ser vigilantes de seguridad privada, conjuntamente con las pruebas de selección que se han pasado, como test de personalidad entre otros, sin duda han elevado el nivel de los aspirantes. A modo de ejemplo, entre los alumnos hemos contado con un detective privado y una diplomada en enfermería. No me cabe ninguna duda que hemos formado profesionales que en los próximos años van a desarrollar sus puestos en Seguridad Privada con solvencia y profesionalidad.


Los certificados de profesionalidad amplían los contenidos respecto al curso tradicional de Aspirante a Vigilante de Seguridad de 180 horas de duración, dando relevancia a nuevas formas de delincuencia que sufre nuestra sociedad actual y profundizando en materias como los sistemas de detección.

A mi entender, un aspecto muy positivo para los aspirantes como por las empresas de seguridad es la agilización en el proceso de habilitación de los aspirantes, al no tener los alumnos que presentarse a las convocatorias que hace la Policía Nacional. En el

año 2016 únicamente se han realizado cuatro convocatorias de examen para Vigilantes de Seguridad, Vigilantes de Explosivos y Escoltas Privados, lo cual ha ralentizado el proceso de habilitación de los aspirantes respecto a los anteriores años.

El hecho de que los alumnos de los certificados de profesionalidad no necesitan presentarse a las pruebas convocadas por Policía Nacional podría comportar suspicacias iniciales; es ahí donde los centros de formación deben estar a la altura, demostrar su grado responsabilidad y profesionalidad. Sin duda, se trata de un reto para los centros de formación; el rigor y la exigencia tienen que ser máximos para garantizar un grado de conocimientos y actitudes adecuadas para la incorporación de los alumnos al sector de la Seguridad Privada.

El curso requiere por normativa de una evaluación continuada con pruebas parciales y finales por cada unidad formativa y módulo, así como una asistencia presencial obligatoria; esto ha comportado que en esta primera experiencia un 20% de alumnos no han superado todas las pruebas y por tanto no han logrado la titulación. Sin ninguna duda, se trata del curso más intenso y completo que hemos impartido en toda nuestra trayectoria de formación en el ámbito de la Seguridad Privada.

Estos requerimientos están siempre tutelados desde el Departament de Treball de la Generalitat de Catalunya, en concreto desde el Servei d'Ocupació de Catalunya.

Un elemento diferenciador a destacar del certificado de profesionalidad es que las cuarenta horas de prácticas no laborales que los alumnos realizan, ha venido a paliar una deficiencia histórica donde los aspirantes hasta ahora no podían tener ningún contacto real con los Servicios de Seguridad Privada hasta que no se incorporaban al mercado laboral. Sin duda, las prácticas han sido un valor añadido para su incorporación al sector, que los alumnos han valorado muy positivamente y las empresas agradecerán.

A este respecto, en IDFO valoramos de forma muy positiva la buena predisposición de las empresas líderes del sector como Ilunion Seguridad y Prosegur para garantizar que las prácticas se realizan de forma correcta en servicios relevantes en Cataluña, como el Aeropuerto de El Prat, hospitales de primer nivel, o recintos patrimoniales históricos, donde los alumnos pueden adquirir unos conocimientos prácticos de primera mano acompañando a profesionales habilitados durante las tareas propias de los Servicios de Seguridad Privada.

Por otro lado, ha sido clave la inestimable colaboración y asesoramiento del Servei de Seguretat Privada del Departament d'Interior i de la Unitat Central de Seguretat Privada de Mossos d'Esquadra, a la hora de organizar las prácticas, de forma que no se produjera ninguna intromisión dentro del sector ni se diera lugar a ninguna confusión, dado que hablamos de un proyecto innovador y pionero en Cataluña. La comunicación ha sido continua y muy satisfactoria.

También queremos destacar la labor de la Unidad Provincial de Seguridad Privada de Policía Nacional de Barcelona, asesorándonos a la hora de informar a los alumnos de los trámites y la documentación necesarios para habilitarse.

Estos certificados son el presente, el futuro más inmediato y la antesala de una futura formación profesional en la familia de Seguridad Privada.

Ha llegado el momento de que la Seguridad Privada se desprenda de determinados complejos, que afronte nuevos retos y oportunidades que sin duda se le presentarán.

La Seguridad Pública tiene que ir de la mano de la Seguridad Privada, necesita una Seguridad Privada respetada, profesional, con una formación completa y con una continua adaptación a las nuevas formas de delincuencia de nuestra sociedad.

«No disfrutaremos de la seguridad sin desarrollo, no disfrutaremos del desarrollo sin seguridad, y no disfrutaremos ninguna de las dos sin respeto por los derechos humanos», Kofi Annan. ●

**ANTONIO GALÁN PENALVA.** CONSULTOR DE SEGURIDAD CONTRA INCENDIOS

# Comportamiento al fuego de los **paneles sándwich metálicos** de núcleo aislante

En la actualidad, los paneles sándwich metálicos con núcleo aislante se emplean de manera generalizada en muchos ámbitos constructivos debido a sus propiedades físicas y aislantes.
Los paneles sándwich son instalados en espacios interiores (compartimentando sectores de incendios, salas blancas, salas de procesado de alimentos, etc.), así como en espacios exteriores en cerramientos de cubiertas y fachadas.

AL ser un producto muy empleado especialmente en la industria alimentaria, se ha visto involucrado en incendios de diferente índole. Por ello, en este artículo se van a presentar los diversos aspectos que deben conocerse para reducir el riesgo de propagación del incendio en los recintos en los que se emplean los paneles sándwich. ***(Figura 1)***

## Núcleos aislante empleados

Actualmente en España, los paneles sándwich metálicos suelen presentarse principalmente con un núcleo de poliuretano o bien de lana de roca. Otros tipos de núcleos aislantes disponibles podrían ser el poliestireno y la espuma fenólica, más usados en otros países pero menos frecuentes en nuestro país. Cada núcleo aislante proporcionará al panel unas propiedades específicas que afectarán a sus prestaciones, incluyendo por supuesto el comportamiento al fuego. Por tanto, es básico conocer los factores que influyen en el comportamiento al fuego de un panel, ya que no solo depende del núcleo aislante seleccionado.

**Figura 1. Ejemplo de almacenamiento en la industria alimentaria realizado con paneles sándwich.**

## Paneles sándwich de Poliuretano

Primeramente conviene aclarar que el aislamiento de poliuretano presenta diferentes tipos de productos tales como el poliuretano proyectado, la plancha de poliuretano y el panel sándwich. Cada tipo de producto presenta unas características específicas y por tanto un comportamiento al fuego diferente.

Con respecto al panel sándwich, además del núcleo de poliuretano es posible emplear un núcleo aislante de poliisocianurato. Este núcleo aislante es una variación de la espuma de poliuretano, como consecuencia de una mayor cantidad de isocianato en los productos precursores para la formación de la espuma rígida de poliuretano. Este aumento de isocianato proporciona unas mayores prestaciones en el comportamiento al fuego. A pesar de este cambio, ambos tipos de núcleos aislantes son del mismo tipo, tal y como se explica en la norma para el marcado CE de paneles sándwiches metálicos (UNE-EN 14509).

| Tipo de panel sándwich | Euroclases habituales | | | | | | |
|---|---|---|---|---|---|---|---|
| | A1 | A2 | B | C | D | E | F |
| Lana mineral | | A2-s1,d0 | | | | | |
| Poliuretano | | | B-s1,d0<br>B-s2,d0<br>B-s3,d0 | C-s3,d0 | | | |

**Tabla 1. Euroclases habituales de los paneles sándwich.**

Este tipo de paneles está formado por un núcleo aislante (poliuretano o poliisocianurato) recubierto por ambos lados por una lámina fina metálica. Normalmente se emplea acero prelacado o recubrimientos plásticos, siendo también posible el uso de aluminio o cobre. La lámina metálica suele presentarse con unos espesores comprendidos entre 0,5 y 0,6 mm.

## Paneles sándwich de Lana de Roca

El aislamiento con lana mineral puede presentar diferentes productos en función del uso que se precise. Ejemplos de esta gama de productos serían las coquillas con/sin revestimiento, los paneles con/sin revestimiento, la lana mineral desnuda y los paneles sándwich. Al igual que el aislamiento de poliuretano, cada tipo de producto presentará unas características específicas y por tanto un comportamiento al fuego diferente.

Centrándonos en el panel sándwich, éste está formado por un núcleo aislante de lana de roca recubierto por ambas caras por un adhesivo que servirá para unir una lámina fina metálica.

Con respecto a los recubrimientos metálicos, es aplicable todo lo indicado para el tipo de panel sándwich anterior.

## Exigencias reglamentarias en España y Marcado CE

Los paneles sándwich metálicos disponen de una norma de producto para el marcado CE que es la UNE-EN 14509:2014 «Paneles sándwich aislantes autoportantes de doble cara metálica. Productos hechos en fábrica. Especificaciones». No todos los paneles sándwich están cubiertos por esta norma. Un ejemplo sería los paneles con caras perforadas, los cuales están excluidos expresamente por dicha norma.

A día de hoy, es obligatorio el marcado CE de los paneles cubiertos por esta norma de acuerdo con la nueva versión de 2014, ya que el periodo de coexistencia con la versión anterior finalizó en agosto de 2015.

Es importante resaltar que el cumplimiento con el anexo ZA de la norma para el marcado CE de un producto no implica el cumplimiento con la legislación nacional. El marcado CE solamente indica que el producto cumple con los requisitos mínimos para circular por Europa libremente.

A nivel nacional, el Código Técnico de la Edificación (CTE DB SI) y el Reglamento de Seguridad contra Incendios en Establecimientos Industriales (RSCIEI) regulan el comportamiento frente al fuego que como mínimo deben cumplir los paneles sándwich para poder ser instalados en un determinado recinto.

Desde el punto de vista de reacción al fuego, en el CTE DB SI, las exigencias varían entre una euroclase B-s1,d0 hasta C-s2,d0 para recintos interiores y un rango comprendido entre B-s3,d2 y C-s3,d2 para exteriores. En el caso de cubiertas, se exige una clase Broof(t1). Por el contrario en el RSCIEI, es suficiente con disponer de una euroclase C-s3,d0.

Las clasificaciones habituales que presentan los paneles sándwich se muestran en la ***Tabla 1***.

Como se puede apreciar en la tabla, ninguna de las euroclases habituales de los paneles sándwich presenta caída de partículas inflamadas.

Para obtener las euroclases anteriores, los paneles sándwich tienen que ser ensayados y clasificados según los criterios mostrados en la norma de clasificación UNE-EN 13501-1:2007+A1:2010 «Clasificación en función del comportamiento frente al fuego de los productos de construcción y elementos para la edificación. Parte 1: Clasificación a partir de datos obtenidos en ensayos de reacción al fuego».

## Ensayos aplicables

Los paneles sándwich con núcleos de lana mineral deben ser ensayados de acuerdo a la norma UNE-EN 13823:2012 «Ensayo del SBI (Single Burning Item)» y con la norma UNE-EN ISO 1716 «Ensayo de la bomba calorimétrica».

Para el caso de los paneles de poliuretano, deben ensayarse de acuerdo a la norma UNE-EN 13823:2012 «Ensayo del SBI (Single Burning Item)» y el ensayo según la norma UNE-EN ISO 11925-2:2011 (Ensayo del Pequeño Quemador).

Además, los paneles sándwich de lana mineral presentan un comportamiento de resistencia que proporciona a este tipo de paneles unas clasificaciones de hasta EI 240. De hecho, este tipo de paneles se emplean de manera frecuente como elementos compartimentadores. Algunos tipos de paneles sándwich de poliuretano pueden llegar a alcanzar clasificaciones de hasta EI 60.

A la hora de manejar los resultados y clasificaciones de ensayo de los paneles sándwich, hay que saber que éstos corresponden con el comportamiento de las muestras de ensayo de un producto, bajo unas condiciones particulares de ensayo y que por ello no pretenden constituir el único criterio de valoración del riesgo potencial de incendio que puede conllevar el uso de un panel.

## Causas habituales de incendios en instalaciones con paneles sándwich

En el pasado, este elemento constructivo se ha visto involucrado en numerosos incendios sucedidos principalmente en la industria alimentaria. Esto ha sido debido a 3 factores principalmente:

- Alta combustibilidad de los productos almacenados.
- Los primeros diseños de paneles no disponían de clasificación de reacción al fuego.
- Mala concepción de la seguridad contra incendios.

Este tipo de incendios se caracteriza por no tener una incidencia muy alta pero cuando se producen ocasionan unas pérdidas económicas y materiales elevadas. Los focos más habituales de incendios en instalaciones donde se emplean paneles sándwich entre otros pueden ser los trabajos en caliente incontrolados, escombros en la base de los hornos, colillas desechadas en los almacenes de envasado, depósitos de aceite en filtros encendidos por una chispa, mantenimiento inadecuado de freidoras, equipamiento eléctrico dentro de zonas frigoríficas (área de iluminación, cables, cargador de baterías), cuadros de distribución de energía eléctrica, incendios intencionados, etc.

## Consideraciones sobre su uso

El comportamiento frente al fuego de este tipo de productos no solamente depende del núcleo aislante, sino hay otros factores que afectan de manera muy significativa en el comportamiento de un panel en caso de incendio. Es-

tos factores son el tipo de espuma empleada y su calidad, la homogeneidad del aislante dentro del panel (sin burbujas de aire), el tipo de junta practicada en el panel, el método de fijación y montaje, el espesor chapa metálica y la cantidad de adhesivo empleado (solo paneles de lana mineral).

Además y con respecto al diseño de las instalaciones con paneles sándwich, los errores más habituales que suelen presentarse son la ausencia de sistemas de control de temperatura y evacuación de humos (SCTEH), ausencia de compartimentación (muros cortafuegos) o muros cortafuegos que no son efectivos por estar perforados sin el tratamiento adecuado; también ausencia de rociadores, grandes espacios sin muros cortafuegos, mala ejecución del equipamiento eléctrico, ensamblaje inapropiado de paneles y las sustituciones parciales de panel.

## Comportamiento al fuego

En caso de incendio, los paneles sándwich primeramente experimentarán la liberación de gases en los extremos del panel. Si el incendio sigue progresando, la unión entre la chapa metálica y el material aislante se debilitará llegando a incluso a desprenderse si la chapa no está fijada correctamente. Este será un punto muy importante para ambos tipos de paneles, ya que una caída de la lámina metálica, podría afectar a los servicios de extinción. Este efecto será mucho más relevante en los puntos singulares del panel (esquinas, cumbreras, etc).

A medida que el incendio evoluciona, el poliuretano será afectado por el calor y las llamas. La evolución será mucho más rápida si en el interior del panel hubiera cavidades de aire, ya que éstas favorecerían la propagación del incendio al interior del panel. La superficie del poliuretano se irá carbonizando a medida que avanza el incendio. El grado de carbonización dependerá de la formulación de la espuma.

La fase en la que se podría intentar minimizar los efectos del incendio por parte de los servicios de extinción sería la fase pre-flashover. En dicha fase, se ha comprobado que ambos tipos de paneles cuando se exponen a temperaturas inferiores a 400ºC producen gases de pirolisis. El peligro potencial de formación de una mezcla inflamable en la capa de humo se encuentra por encima del rango de temperatura a la que los servicios de extinción trabajan en un incendio.

La presencia de aditivos combustibles en paneles sándwich metálicos (sintéticos y lana mineral) puede, en algunos casos, y sobre todo después del pre-flashover aumentar la intensidad del fuego.

Finalmente, la pérdida de masa real debido a la pirólisis de los núcleos sintéticos y los núcleos de lana mineral no difiere mucho hasta 300 ºC. La pérdida de masa de los paneles poliuretano es exponencial y comienza a perder una cantidad significativa de su masa alrededor de 300ºC, mientras que los paneles de poliisocianurato y lana de roca tienen una temperatura de pirólisis inferior y muestran una tendencia más lineal.

## Conclusiones

1. La seguridad contra incendios no se puede basar solamente en la clasificación de reacción al fuego. Se tienen que tener en cuenta las medidas de protección activa y pasiva, así como su correcto funcionamiento.

2. El mantenimiento y revisión de los medios de protección activa y pasiva debe ser realizado por personal cualificado.

3. Seguir siempre el procedimiento de fijación y montaje descrito en los informes de ensayo, así como las indicaciones del fabricante. Si no se respetan las condiciones descritas en los informes de ensayo, clasificación y EXAP (Extended Applications), el panel no dispondrá de clasificación de fuego. ●

## Bibliografía


UNE-EN 14509:2014. «Paneles sándwich aislantes autoportantes de doble cara metálica. Productos hechos en fábrica. Especificaciones».

Fire behaviour of sandwich panel core materials in the pre-flashover phase. Ing.A.W. Giunta d'Albani. Brandweer and University of Technology Eindhoven.

Código Técnico de la Edificación. CTE DB SI. (Junio 2016).

Reglamento de Seguridad contra Incendios en Establecimientos Industriales. (RSCIEI). (2004).

Sandwich elements as room-closing Wall and roof components. (VdS 2244 EN:2006)

Specifications for the protection of cold areas. (VdS 2032:2008).

UNE-EN 13501-1:2007+A1:2010. «Clasificación en función del comportamiento frente al fuego de los productos de construcción y elementos para la edificación. Parte 1: Clasificación a partir de datos obtenidos en ensayos de reacción al fuego».

UNE-EN 13823:2012. «Ensayos de reacción al fuego de productos de construcción. Productos de construcción, excluyendo revestimientos de suelos, expuestos al ataque térmico provocado por un único objeto ardiendo. (Ensayo del SBI)».

UNE-EN ISO 1716:2011. «Ensayos de reacción al fuego de productos. Determinación del calor bruto de combustión (valor calorífico). (ISO 1716:2010)».

UNE-EN ISO 11925-2:2011. «Ensayos de reacción al fuego de los materiales de construcción. Inflamabilidad de los productos de construcción cuando se someten a la acción directa de la llama. Parte 2: Ensayo con una fuente de llama única. (ISO 11925-2:2010)».

PROTECCIÓN CONTRA INCENDIOS, DEBATE DE EXPERTOS EN SEVILLA

# Retos ante la «alarma» de incendio

## Mesa de Debate organizada por Tecnifuego-Aespi

Retos ante la «Alarma» de Incendio, ha sido el título de la mesa redonda, organizada por el Comité de Detección de Tecnifuego-Aespi, que ha reunido a un nutrido número de expertos en el Colegio de Aparejadores y Arquitectos Técnicos de Sevilla.

La presentación de la jornada, en la que ha colaborado la Junta de Andalucía y el Ayuntamiento de Sevilla, corrió a cargo de Ramón F. Becerra, del Colegio de Aparejadores, y Antonio Tortosa, vicepresidente de Tecnifuego-Aespi. Durante su intervención, Tortosa comentó que «Hay que prestar especial atención a la detección y alarma de incendios, ya que son instalaciones que solo deben entrar en funcionamiento en caso de emergencia, y por tanto su instalación y mantenimiento son las piezas angulares de su eficacia para dar la alarma ante un conato de incendio». Destacó, además, el compromiso de la Asociación con la calidad y la eficacia en seguridad contra incendios.

Antonio J. Pajuelo, Jefe del Servicio de Protección Civil. Emergencia 112 de Sevilla, presentó los datos estadísticos de Andalucía sobre muertes por incendio (en 2014, 26 fallecidos; en 2015, 22 muertos, y en lo que va de 2016, 14 personas han muerto por incendio). En este sentido matizó que «es de extrema importancia la concienciación y formación ciudadana, e implementar y mantener los planes de autoprotección».

Pajuelo comentó que Sevilla es la primera provincia de Andalucía en disponer el 100% de los municipios de Plan Emergencia Municipal (105 localidades).

Antonio Tortosa, vicepresidente de Tecnifuego-Aespi, y Ramón F. Becerra, del Colegio de Aparejadores de Sevilla.

Por otro lado, añadió que «las llamadas al 112 en nuestra Comunidad Autónoma poseen la georeferencia de la emergencia, lo que sin duda permite acortar los tiempos de respuesta de los Servicios Operativos ante los avisos de urgencia o emergencia que son recibidos en esta plataforma, incluidas las relacionadas con incendios de vivienda, edificios, empresas o de infraestructuras».

A continuación, Juan de Dios Fuentes, coordinador del Comité de Detección de Tecnifuego-Aespi introdujo el debate, denunciando que «la Protección contra Incendios (PCI) es un sector olvidado y mucho más la detección, debido a que está en "reposo" hasta que se activa por una emergencia». En este sentido, Fuentes calificó la detección como el sistema troncal de la PCI, «la primera en actuar, la que hace que se activen los demás sistemas y da la alarma a las personas».

En el ámbito sectorial y de reglamentación, Fuentes comentó que «Hay que tener en cuenta que el sector de la detección incluye también todo lo relativo a alarma, y que este subsector está en pleno proceso de desarrollo. En este sentido, necesitamos con urgencia una buena reglamentación y normalización del sector».

Juan de Dios Fuentes habló también del reto que supone para el sector intentar dar soluciones a las necesidades


**Juan de Dios Fuentes, coordinador del Comité de Detección de Tecnifuego-Aespi.**

sociales cambiantes, dada la evolución tecnológica intrínseca a la detección. Finalmente quiso transmitir un mensaje a la sociedad en general: «Debemos concienciar a la población de que la detección de incendios debe ser un equipo más que entre dentro de las viviendas para garantizar la seguridad y tranquilidad de las familias frente a un posible incendio».

La siguiente intervención fue la de Manuel Martínez, coordinador del Comité de Instalación y Mantenimiento de Tecnifuego-Aespi, que hizo hincapié en la importancia de una correcta instalación y mantenimiento de las instalaciones para garantizar su puesta en marcha y eficacia.

El ponente matizó que para que el sector evolucione se deben adaptar y actualizar todas las reglamentaciones que están en estos momentos paralizadas (RIPCI, RSCIEI, CTE), incluyendo los últimos desarrollos normativos de la serie de Normas UNE 23.580.

Igualmente, insistió en la necesidad de formación continua por parte del personal de las empresas instaladoras y mantenedoras de PCI.

José A. Merat, de la Gerencia de Urbanismo del Ayuntamiento de Sevilla, por su parte, quiso señalar el reto que suponen las reformas en edificios anteriores al CTE. En este sentido defendió que «dadas las características de los edificios, cuando se emprende una reforma, no se puede cumplir con el CTE. Ello obliga a soluciones alternativas donde la detección es primordial». Así, comentó que dentro del diseño prestacional, «es muy importante la interacción del sistema de detección y alarma con otros sistemas».

Según, la experiencia del Ayuntamiento de Sevilla entre los principales grupos de riesgo para la notificación de alamas y gestión de su evacuación son los ocupantes con auxilio, cubiertos en gran medida por la normativa; los casos individuales personales, conocidos, que se deben tutelar; y las personas con problemas para evacuar «desconocidas», no tuteladas.

Ahondando en esta problemática de la evacuación por incendio, Juan Nogales, experto del Comité de Detección de Tecnifuego-Aespi, expuso que para la evacuación segura de un edificio se requiere un tiempo mínimo determinado que depende de las características y uso del mismo, «lo que se denomina tiempo de evacuación seguro, y por otro lado está el tiempo de evacuación necesario que corresponde a la suma del tiempo de premovimiento más el tiempo de recorrido».

Así, el objetivo de la detección y alarma es el de acortar lo más posible el tiempo de premovimiento, «esto se consigue con un buen sistema de detección y alarma. Las instrucciones verbales (a través de megafonía asociada) mejoran la efectividad del sistema de alarma».

Le tocó el turno a José Antonio Arenilla, Ingeniero del Hospital Virgen del Rocío SAS, que presentó la evolución de los sistemas de detección en el citado centro sanitario, partiendo de la base de que su objetivo principal es la evacuación segura teniendo en cuenta la realidad de un hospital. Para ello, dijo, «los sistemas modernos disponen de más prestaciones y menores barreras de comunicación. Pero los sistemas de detección han de ir acompañados de un plan de autoprotección».

Asimismo Arenilla se congratuló de que con los nuevos sistemas se han reducido las falsas alarmas, y los conatos de incendio detectados se han podido sofocar cuando solo eran eso, un conato.

«La gestión de la notificación de la alarma está muy dirigida –dijo-, y se incluyen entre otras vías, alarmas por SMS a diferentes responsables de la gestión de una emergencia. Además, debido a la renovación de los sistemas, se produce una reducción de la partida de correctivo en sistemas antiguos, con lo cual se pueden incrementar las partida de inversiones en nuevos equipos».

Luis Manuel López, jefe de Extinción de Incendios SPIS del Ayuntamiento de Sevilla, trató de la importancia de la formación y concienciación ciudadana para la PCI. Informó de las actividades que realizan desde su departamento en ese sentido, como por ejemplo la formación en edades escolares sobre la reacción ante un incendio.

Destacó especialmente que sería interesante que los usuarios conocieran las medidas de seguridad de que disponen. Esto facilitaría mucho la labor de los bomberos y las acciones que han

OPTEX
Sensing Innovation

## Mucho más que una pared a sus espaldas

Llevamos más de 35 años siendo el fabricante líder en Europa de sensores de detección de intrusión en exteriores. Además, fuimos los creadores del primer sensor externo que hubo en el mundo. Una historia y una experiencia de las que nos sentimos orgullosos, sostenidas por nuestro deseo constante de innovar, de desarrollar soluciones con las mejores prestaciones y fiabilidad de detección, de trabajar junto a los mejores socios del sector. Nuestras soluciones han sido probadas sobre el terreno.

**Cuando el rendimiento es lo que cuenta, cuenta con Optex.**

Puede encontrar más información sobre nosotros y nuestros sensores visitando nuestra página web **www.optexiberia.com** o escribiéndonos a **marketing@optex-europe.com**

de emprender en los distintos recintos donde se encuentren cuando se da una alerta por incendio.

El siguiente en intervenir fue Florencio Madrid, subdirector del Servicio de Mantenimiento de la Universidad de Sevilla, que trasladó las operaciones emprendidas en este centro universitario «compuesto por 56 edificios diferentes con una casuística propia: aulas, laboratorios, bibliotecas, salón de actos, recintos deportivos, cocinas, almacenes, salas de ordenadores…) y los usuarios, entre estudiantes y personal docente y laboral».

Florencio Madrid informó del trabajo para el desarrollo de planes de protección y en la concienciación y formación tanto de los estudiantes como del personal. «El concepto de alarma debe tener un ámbito muy global en el que se incorpora la PCI, y debido a estructura de multiedificio, un software de gestión ayuda a uniformizar la gestión. Además, estoy muy de acuerdo en algo que ya se ha dicho aquí: la alarma por voz mejora los tiempos de evacuación».

Manuel Campos, director de Seguridad del Cabildo de la Catedral de Sevilla, explicó las peculiaridades para la PCI en la catedral: «Dada la tipología de la catedral se han desarrollado planes de autoprotección específicos. Por ejemplo, la alarma se produce en dos fases, primero a los responsables, que incluye un proceso de verificación, y posteriormente la evacuación, en caso de ser necesario».

Campos destacó que están trabajando en los sistemas de comunicación y alarma integrando los dispositivos de audio-guías que utilizan los visitantes, y en este sentido el responsable de Seguridad cree que «hay un choque entre las nuevas tecnologías y la normativa, que se debería resolver cuanto antes por el bien de la seguridad de las personas y bienes».

El siguiente turno correspondió a Jon Michelena, director de Cepreven, que centró su intervención en la dificultad que tenemos en España para implantar las nuevas tecnologías «dado que la reglamentación es muy prescriptiva para la implantación de nuevas tecnologías».

En relación a los sistemas de detección, comentó que han de ir acompañados de un plan de autoprotección. «Esto hace necesario la concienciación y formación del personal y de los usuarios, y desde luego el mantenimiento y el control de las instalaciones de PCI para garantizar su utilidad y eficacia».

Tras la ronda de presentaciones el moderador, Ramón Fernández Becerra, comentó la importancia por un lado de la concienciación y formación del personal y usuarios; y por otro que los sistemas de alarma deben ser capaces de dar una solución para personas con discapacidad, tanto en avisadores acústicos como visuales, y desarrollar nuevos diseños adaptados de los mismos.

«Se dice que actualmente el CTE está trabajando en accesibilidad universal, tanto para facilitar la entrada de toda persona a los recintos como garantizar su evacuación en caso de emergencia, deseamos que esto sea cierto y lo veamos pronto reflejado en la normativa una vez hayan publicado la esperada actualización».

## Conclusiones

Al finalizar la mesa redonda y debate, Juan de Dios Fuentes hizo un listado de conclusiones que pasamos a resumir:

- Necesidad de concienciación y formación de usuarios y profesionales.
- Una correcta gestión de los sistemas de detección y alarma para garantizar un correcto funcionamiento.
- El sistema de detección y alarma es el primero en actuar y debe dar pie a sistemas automatizados y por otro a facilitar la evacuación de los edificios.
- Necesidad de adaptarse a las nuevas tecnologías. Aparece como clave de futuro el teléfono móvil, que es un vínculo personalizado para cada ocupante.
- Integración de los sistemas de detección y alarma con otros sistemas.
- Para los usuarios es clave hacer la instalación «suya».
- La incorporación de nuevas tecnologías choca frontalmente con la normativa.
- La renovación de los sistemas conlleva una reducción drástica de las falsas alarmas, y una reducción de los costes del correctivo.

**Vista general de la Mesa de Debate.** *Fotos: Tecnifuego-Aespi*

EL ENCUENTRO PROFESIONAL SE CELEBRÓ EL 20 DE OCTUBRE EN ALBACETE

# El uso de **drones (RPAS)** en la **seguridad privada**

## Éxito de asistencia en el II Taller UAS-Cuadernos de Seguridad, bajo la organización de AESAB y FEDA

Cerca de 50 profesionales acudieron el pasado 20 de octubre, en la sede de la FEDA (Federación de Empresarios de Albacete), a una jornada que, bajo la temática «El uso de los drones (RPAS) en la seguridad privada», y englobada en el II Taller UAS-CUADERNOS DE SEGURIDAD, organizó la Asociación de Empresas de Seguridad de Albacete (AESAB) –institución integrada en la Unión de Asociaciones de Seguridad (UAS)- en la ciudad de Albacete. El encuentro tuvo como objetivo analizar las últimas novedades sobre la normativa actual referente al uso de los drones en España, así como debatir los retos y oportunidades que puede ofrecer al sector de la Seguridad Privada.

El acto de presentación contó con la presencia del Comisario Jefe de la Comisaría del Cuerpo Nacional de Policía, José Francisco Roldán Pastor; el Teniente Coronel de la Comandancia de la Guardia Civil, Jesús Manuel Rodrigo; el presidente de la Asociación de Empresas de Seguridad de Albacete (AESAB), Jesús Castillo; y Paloma Velasco, miembro del Comité Ejecutivo de la Unión de Asociaciones de Seguridad (UAS).


Paloma Velasco, miembro del Comité Ejecutivo de UAS; y Jesús Castillo, presidente de AESAB.

### Normativa de drones

El turno de intervenciones comenzó con la ponencia «Normativa de drones en España» a cargo de Manuel López, piloto y experto de la Escuela de Formación Aeronaútica, quien centró gran parte de su exposición sobre el marco regulatorio actual en nuestro país: Ley 18/2014 de 15 de octubre. Así sobre la base de la normativa, el ponente realizó un recorrido por la legislación que afecta en determinados aspectos a esta nueva actividad, el uso y pilotaje de drones, como es la constitución española –el derecho al honor, la intimidad y a la propia imagen o que el domicilio es inviolable–, la Ley de Navegación Aérea 48/1960, la Ley de Seguridad Aérea 21/2003, así como la Ley 18/2014 que especifica los requisitos para pilotar, entornos autorizados para el uso de RPAS, en función de las características del equipo, lugar, peso, etc., o requisitos del operador que debe acreditar.

### Tipología de drones

Por su parte Alejandro G. Tendero, responsable del departamento Técnico de BUCKER, centró su intervención en

Manuel López, piloto y experto de la Escuela de Formación Aeronaútica, EFA.

«Durante la jornada se puso de manifiesto el interés del sector de la seguridad privada por los usos y aplicaciones que ofrecen los RPAs»

«Tipología de Drones». Tras llevar a cabo una descripción de estos dispositivos –vehículo aéreo no tripulado pilotado a distancia, con varios rotores y que pesa menos de 25 kg–, pasó a enumerar algunas de las ventajas y desventajas que implica el uso de este tipo de aeronaves. «Se trata de dispositivos –señaló– de fácil manejo, que suponen una reducción de costes, permiten llegar a zonas de difícil acceso, movilidad territorial,…». Mientras que apuntó entre sus inconvenientes: limitaciones técnicas, limitaciones morales –implica la protección de datos–, así como la falta de regulación.

Alejandro G. Tendero, responsable del departamento Técnico de Bucker.


Además de su aplicación para actividades de cartografía, medioambiente, servicio de transporte e incluso en el ámbito del patrimonio cultural, el ponente destacó su utilización para la supervisión y vigilancia de infraestructuras críticas o puertos, o para el control de vertidos o de perímetros, así como la identificación de intrusos o en temas de rescate. «El mundo de los drones –explico– avanza a grandes zancadas. Los drones han venido para facilitar las tareas que hacemos».

## Protección de datos

«La Protección de Datos personales derivada del uso de RPAS» fue el tema que abordó Luis de la Mora, abogado especialista en protección de datos y nuevas tecnologías, de Lant Abogados, quien nada más comenzar su ponencia puso sobre la mesa dos aspectos a tener en cuenta: el impacto del uso de drones en el ámbito de la privacidad – «el dron puede captar imágenes –explicó- que cada vez puede ser más invasivo para el ciudadano»– y la necesidad actual de regular su uso, en base al principio de calidad –limitación de su finalidad, proporcionalidad y minimización de los datos, para, entre otros aspectos, poder adoptar las medidas de seguridad adecuadas.

Luis de la Mora, abogado especialista en protección de datos y nuevas tecnologías de Lant Abogados.

Además el ponente señaló que en el uso de drones, en el ámbito de la seguridad, se deben tener en cuenta las distintas áreas en las que se pueden utilizar, el principio de proporcionalidad a la hora de utilizar sistemas de vigilancia mediante estos dispositivos, así como la necesidad de estar perfectamente delimitados los diferentes actores a participar en el tratamiento de datos personales. «No se pueden obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia», matizó.

Vista general de los asistentes.

## Drones & Seguridad Privada

«La utilización de drones para finalidades de seguridad privada», fue el título de la ponencia de Julio Camino, inspector de la Unidad Central de Seguridad Privada, quien lanzó a los asistentes una pregunta: ¿es legal el uso de drones en el ámbito de la seguridad privada?. La Ley de Seguridad Privada y su normativa, explicó, ni recoge «ni regula el uso de drones, que no es una medida de seguridad. Estos dispositivos pueden ser considerados como un medio material usado con fines de seguridad privada. El dron es un medio».


Julios Camino, inspector del CNP de la Unidad Central de Seguridad Privada.

En cuanto a los servicios de videovigilancia, el ponente añadió que el uso de este tipo de dispositivos, previa autorización administrativa, tendrá la finalidad de vigilar para prevenir infracciones, evitar daños a las personas o bienes objeto de protección. Sólo vigilantes de seguridad y guardas rurales podrán prestar estos servicios.

La jornada contó con el patrocinio de la empresa BUCKER.

La Unión de Asociaciones de Seguridad (UAS) y la revista CUADERNOS DE SEGURIDAD, firmaron un acuerdo de colaboración para la puesta en marcha de los Talleres UAS-CUADERNOS DE SEGURIDAD, encuentros dirigidos a profesionales de la seguridad cuyo objetivo principal será convertirse en una plataforma y foro de conocimiento y debate sobre los temas de actualidad más relevantes para el sector (normativa y legislación, Protección de Datos, RPA´S, Ciberseguridad y delitos informáticos, terrorismo islamista, etc.). ●

*Texto y Fotos: Gemma G. Juanes*

EL ENCUENTRO TUVO LUGAR EL PASADO 19 DE OCTUBRE

# III Jornada **Guardia Civil-Empresa**

## Durante la jornada se procedió a la entrega de los Premios «Duque de Ahumada»

Bajo la premisa «La confianza de un país depende de la confianza que generan sus empresas», Arsenio Fernández de Mesa, director general de la Guardia Civil en esos momentos, inauguró la III Jornada Guardia Civil-Empresa, encuentro anual, en el que personal de la Institución y de diversas empresas, así como profesionales del sector de la Seguridad Privada analizaron cuestiones como la obtención, gestión e intercambio de información relevante para la seguridad en el ámbito interno de las propias compañías, entre corporaciones diferentes, y entre ellas y las FF. y CC de Seguridad.

El director general comenzó su intervención diciendo que «tras las dos ediciones anteriores, nuestra intención sigue siendo convertir esta reunión en un referente de la colaboración pública y privada, para el intercambio de buenas prácticas, y la búsqueda conjunta de soluciones a los riesgos para la seguridad que nos amenazan.

Fernández de Mesa destacó que ya hay más de 400 empresas que están adheridas a los programas de colaboración «Coopera» y «Plus Ultra», con los que el Cuerpo trabaja en beneficio de la sociedad.

Las empresas, continuó, el director general, con su despliegue por el territorio nacional e internacional, se convierten en muchas ocasiones en un sensor de los riesgos y amenazas que existen para la seguridad. En este sentido, son un agente fundamental para su detección y su gestión, basado en el conocimiento directo y continuo que tiene el establecimiento en un municipio, ciudad, región o país.

Según explicó Fernández de Mesa, la Guardia Civil considera la comunicación y el intercambio de información como herramientas fundamentales para la mejora global de la seguridad.

El primer bloque de intervenciones, bajo el tema «Gestión de la Información de Seguridad I» contó con la intervención de Andrés Sanz Coronado, Coronel Jefe del Servicio de Protección y Seguridad (SEPROSE) de la Guardia Civil, quien destacó la necesidad de potenciar el intercambio de información entre Seguridad Pública y Seguridad Privada, a través de diferentes instrumentos como protocolos de actuación, programas de colaboración Seguridad Pública-Privada, planes de protección específicos o planes de apoyo operativo, y teniendo siempre en cuenta qué información puede ser relevante para las empresas, en función de la casuística de la misma. «Hay que crear una cultura de comunicación en materia de seguridad», apuntó.

Por su parte, Óscar Téllez Carbajo, secretario de la Sociedad Española del Derecho de Seguridad, analizó aspectos relacionados con la captación y tratamiento de datos de carácter personal desde el punto de vista del departamento de Seguridad de las empresas, así como la gestión de la información, donde estos departamentos deben estar alineados con otras áreas de la compañía –RRHH, áreas operativas y de explotación, directivos y empleados– para poder compartir esa información.

Ya en el segundo turno de intervenciones, bajo la misma temática, tuvo la palabra Francisco Muñoz Usano, presidente de la Sociedad Española del Derecho de Seguridad, quien comenzó su intervención haciendo hincapié en la necesidad por parte de las empresas de atender la previsión de riesgos, especialmente aquellos de origen antisocial. Tras incidir en la comunicación inmediata entre compañías ante diferentes riesgos, el ponente destacó como factores esenciales a la hora de garantizar la seguridad: razonabilidad, intervención mínima, idoneidad y proporcionalidad.

Acto seguido, y en el ámbito del intercambio de información con las Fuerzas y Cuerpos de Seguridad, el Comandante de la Unidad Técnica de Policía Judicial de la Guardia Civil, Miguel Fayos Maestre, abordo la gestión de la información –que la institución recibe a través de e-mail, llamadas telefónicas, comunicaciones del Plan Coopera,...–, tras su previa clasificación, así como la implementación del sistema de investigación de la misma.

Acto seguido Arsenio Fernández Mesa hizo entrega de los premios «Duque de Ahumada», durante el acto de clausura de la III Jornada Guardia Civil-Empresa.

Con objeto de estimular la acción de los departamentos de Seguridad Corporativa y concienciar a las empresas de su importancia, se crearon estos premios anuales, concedidos por la Guardia Civil en cuatro modalidades. Este año han sido galardonados:

• Renfe, con el premio a la excelencia en seguridad corporativa, que distingue a las empresas cuyo departamento de Seguridad haya conseguido el mayor grado de excelencia a nivel global.

• Instituto de Continuidad «Continuam», premio a la mejor acción exterior, galardón que distingue a las empresas españolas que implementen las mejores soluciones de seguridad en el exterior.

• Correos, premio a la mejor trayectoria de colaboración, que reconoce la proactividad de empresas y departamentos de Seguridad en la colaboración continuada con la Guardia Civil.

• Feex, premio a la mejor acción de difusión de la cultura de seguridad, que premia el esfuerzo en la difusión de la cultura de seguridad por parte de cualquier institución pública o privada.

*Texto y Fotos: Gemma G. Juanes/MIR*

EL ENCUENTRO SE CELEBRÓ LOS DÍAS 18 Y 19 DE OCTUBRE EN LEÓN

# El sector de la ciberseguridad a análisis en 10ENISE

**Más de 6.000 personas siguieron, de forma presencial o a través de internet, el evento organizado por el Instituto Nacional de Ciberseguridad (INCIBE)**

Expertos y profesionales de la ciberseguridad de toda España y de una decena de países como Estados Unidos, Alemania, Italia, Bélgica, Tailandia, Chile o México participaron en el décimo Encuentro Internacional de Seguridad de la Información (10ENISE) que se celebró los días 18 y 19 de octubre en León bajo el lema «Trabajando por el desarrollo de la industria y la ciberseguridad».

Analizar los avances más significativos en materia de ciberseguridad, dar a conocer las oportunidades que ofrece el sector como generador de empleo y fomentar el acercamiento entre la oferta y la demanda, fueron algunos de los objetivos de este evento, organizado por el Instituto Nacional de Ciberseguridad (INCIBE), entidad dependiente del Ministerio de Industria, Energía y Turismo, a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. En la inauguración, el secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, Víctor Calvo-Sotelo, aseguró que este evento permite analizar los principales avances y retos en materia de ciberseguridad y ser más eficaces a la hora de abordarlos. Tras recordar que el año pasado su CERT de Seguridad e Industria atendió más de 45.000 incidentes, destacó que INCIBE es además la columna vertebral para «generar un potente ecosistema nacional en materia de ciberseguridad».


Por su parte, el secretario de Estado de Seguridad, en esos momentos, Francisco Martínez Vázquez, resaltó la estrecha colaboración entre las Fuerzas y Cuerpos de Seguridad del Estado, el Centro Nacional de Protección de Infraestructuras Críticas e INCIBE. En este sentido, señaló que en 2015, se registraron más de 60.400 ciberdelitos (un 25% más que en 2014 y un 61% más que hace cuatro años). Asimismo, refirió que en lo que va de año, el CERT de Seguridad e Industria ha detectado 231 incidentes relacionados con infraestructuras críticas, «son más en número, sofisticación y agresividad, pero ponen de manifiesto que la colaboración con operadores privados se ha potenciado y que se está avanzando en la dirección correcta».

## Cooperación y colaboración

Del mismo modo, el secretario de Estado de Cooperación Internacional y para Iberoamérica, Jesús Gracia, aseguró que «el mundo digital es un mundo que no conoce fronteras y tenemos que potenciar la cooperación y la colaboración con otros países». Asimismo, indicó que España cuenta con una «buena posición a nivel internacional porque cuenta con capacidad

tecnológica, con personas formadas, un mundo universitario importante, un marco normativo muy adecuado y la voluntad política del gobierno de seguir adelante».

Esta décima edición ha despertado un gran interés en el sector de la ciberseguridad. Más de 6.000 personas siguieron, de forma presencial o a través de internet, el evento. Las más de 95 ponencias corrieron a cargo de relevantes figuras procedentes de Reino Unido, República Checa, Alemania, Perú, Rumanía, Italia, Canadá o Japón, y en ellas se analizaron las tendencias más significativas del sector e identificado los retos y desafíos más inminentes.


## Emprendimiento y transferencia tecnológica

Por su parte, más de 500 personas asistieron a la sesión paralela dedicada al emprendimiento y la transferencia tecnológica, en el que un total de 74 ponentes de referencia y emprendedores compartieron experiencias y consejos en diferentes paneles y mesas redondas. La cita también sirvió para que inversores y empresarios conocieran los 29 proyectos innovadores seleccionados dentro de la incubadora CiberEmprende, finalizando las jornadas con la presentación de la aceleradora internacional de proyectos de negocio en ciberseguridad, en la que participan la Junta de Castilla y León a través de ADE Inversiones y Servicios, el Ayuntamiento de León, CDTI e ICEX.

Entre los temas que se abordaron en 10ENISE se encontraban los desafíos en la lucha contra el cibercrimen y el ciberterrorismo, las oportunidades de internacionalización para la industria de Ciberseguridad en España, los retos de la Ciberseguridad en los sectores de energía y financiero o la industria 4.0. Todo con el objetivo de internacionalizar el mercado español, generar tejido empresarial y empleo a través del emprendimiento y apoyar la innovación como herramienta de transformación del mercado digital.

En la clausura del acto, Miguel Rego, director general del INCIBE en esos momentos, hizo un balance altamente satisfactorio de 10ENISE, tanto por la alta participación como por la calidad de las ponencias, y destacó que «la ciberseguridad requiere un esfuerzo colectivo, que se ha visto reflejado en este evento, que ha estado apoyado por tres Ministerios diferentes, por la Junta de Comunidades de Castilla y León y por el Ayuntamiento de León.

*Texto y Fotos: Redacción/INCIBE*

ORGANIZADO POR EL CENTRO DE ESTUDIOS EN CIBERSEGURIDAD DE ISMS FORUM

# V Foro de la **Ciberseguridad**

## Security Intelligence, clave para la Transformación Digital

El Centro de Estudios en Ciberseguridad de ISMS Forum celebró el pasado 28 de septiembre en Madrid la quinta edición del Foro de la Ciberseguridad, presentado y dirigido por Daniel Largacha como director de la iniciativa y Global Control Center Assitant Director de Mapfre. El Foro congregó a más de 250 profesionales de la seguridad y la protección de datos, con el objetivo de examinar la evolución de los sistemas tradicionales de seguridad de la información hacia nuevos entornos basados en el análisis y la compartición de información, para mejorar la resiliencia empresarial ante un panorama de ciberamenazas cada vez más sofisticado, unido a la transformación digital que experimenta la Industria.

En las palabras de bienvenida, César Arranz, presidente de la Asociación Española de Ejecutivos y Financieros (AEEF), destacó la creciente preocupación que la ciberseguridad supone para ejecutivos y financieros, debido al impacto que tienen las ciberamenazas en los activos de la empresa. Además, nuevos fenómenos como el Cloud o el Big Data, hacen ver que el uso masivo de la tecnología supone una mayor exposición a los riesgos asociados. «Hay una preocupación creciente» por este nuevo negocio, explicaba Arranz, exponiendo los recientes casos de Yahoo, MySpace, LinkedIn, Adobe, Dropbox, entre otros.

La ponencia inaugural corrió de la mano de Paul Cornish, director del Centro Global de Ciberseguridad de Oxford University y director del área de Estudios de Rand Europe. Durante su discurso trató de responder a una cuestión clave: cómo la ciberseguridad se convierte en un importante catalizador para la Transformación Digital. Y una de las claves que apuntó Cornish es la resiliencia como elemento principal para afrontar los nuevos retos tecnológicos. Empresas de todo el mundo acumulan pérdidas anuales por valor de quinientos mil millones de dólares debido a ciber-incidentes, lo que hace cobrar máxima importancia a las herramientas para hacer frente a las ciberamenazas.

A continuación, tenía lugar una interesante mesa redonda para abordar la protección de la información que se encuentra fuera de las empresas. Un nuevo escenario que afecta a la seguridad de la información y, por tanto, es imprescindible examinar las herramientas que necesitamos para hacer frente a las ciberamenazas. La mesa redonda fue moderada por Eduvigis Ortiz, Global Alliances & Innovation Director Cybersecurity de Prosegur, y formada por Javier Santiago, Responsable de Ciberseguridad y Networked Defense de Trend Micro; Alberto Cita, SE Manager, Southern Europe de Blue Coat (Symantec); Félix Martín, EMEA Security Consulting Lead de HPE; y Manuel Díaz, Chief Information Security Officer de Huawei España. Fabricantes y pro-

veedores de seguridad coincidieron en que la creciente demanda de seguridad en entornos Cloud hace necesario un reenfoque de la seguridad hacia soluciones basadas en el dato. Arquitecturas que puedan seguir a los servidores, visibilizar y controlar el uso y la compartición de los datos corporativos, y que permitan la gestión de identidades de las aplicaciones. «Herramientas que se integran en la Nube y están dirigidas a proteger la Nube», apuntaban los miembros de la mesa. Además, es necesario tener en cuenta los aspectos regulatorios, como el nuevo Reglamento Europeo de Protección de Datos, que introduce la extraterritorialidad, un principio que supone que los datos deben estar protegidos allá donde estén.

Un caso práctico sobre un gran ataque de denegación de servicio, presentado por Marco Pacchiardo de Akamai, ponía de manifiesto los posibles efectos devastadores para la actividad de las empresas, medidos en tiempo de inactividad e inoperatividad.

Continuaba una de las sesiones más esperadas, protagonizada por Troels Oerting, Chief Information Security Officer de Barclays para Europa, para hablarnos acerca del nuevo Centro de Operaciones de Ciberseguridad de próxima generación de Barclays. Una inversión en capacidades de inteligencia, señalaba Oerting, que permitirá utilizar grandes volúmenes de datos para mejorar la estrategia defensiva de la compañía y adaptarse a un futuro hiperconectado.

Para abordar el futuro del antimalware, se organizó una mesa con los principales fabricantes. Formaban la mesa redonda, Rosa Díaz, directora General para España de Panda Security; Mario García, Country Manager Iberia de Check Point; Carlos Muñoz, Iberia Presales Manager de Intel Security; y Luis Miguel Garrido, Sales Manager de Fortinet. Como principales conclusiones, los nuevos entornos de IoT y movilidad fueron el punto de atención. Los

nuevos escenarios no estarán limitados a una serie de dispositivos, por lo que será necesario implementar soluciones analíticas que nos lleven de una seguridad preventiva a una seguridad que implemente elementos correctivos, con una arquitectura integrada y escalable adaptada al nuevo panorama. En la seguridad corporativa, por el contrario, encontramos carencias todavía muy importantes. Xavier González, co-fundador y CTO de OpenCloud Factory, presentó la solución Opennnac, una herramienta para el control y la monitorización de las redes y los dispositivos corporativos, que garantiza la seguridad y el cumplimiento normativo. Una herramienta para mejorar la securización de una red corporativa identificando usuarios, dispositivos, casos de uso y comprobando el comportamiento, basándonos en la política de seguridad aplicada e independientemente de la tecnología utilizada.

Y no menos importante es la seguridad de los sistemas SAP. Peter Maier-Borst, director ejecutivo de Virtual Forge Iberia, analizó las principales características de SAP, concluyendo que existen particularidades que no pueden ser cubiertas por las normas generales de seguridad TI. Estas particularidades hacen que sean frecuentes algunas vulnerabilidades que permiten acceder a los datos, provocar tiempos de inactividad o tomar el control del sistema.

En la sesión vespertina, Bryn Norton, Director - Solutions Architecture EMEA de Level 3 Communications, abordó la necesaria adaptación de los sistemas de Inteligencia ante amenazas para mejorar la respuesta ante posibles incidentes. Mientras el número de dispositivos conectados aumenta rápidamente, también lo hace el número de vulnerabilidades.

Continuando con las amenazas en entornos IoT (Internet de las Cosas), Stephan Gerhager, Chief Information Security Officer de Allianz Deutschland AG e investigador en el área de movilidad e Internet de las Cosas, ofreció una magnífica visión de los vectores de ataque que utilizan los ciberdelincuentes en el sector de la automoción y las posibles consecuencias de la digitalización de un sector altamente sensible.

El foro llegó a su fin con la intervención de THIBER, The Cybersecurity Think Tank, con una demostración del proceso de perfilado de usuarios a través de la información que voluntaria o involuntariamente asociamos en las distintas plataformas y, por ende, la realización de ejercicios de atribución. ●

*Texto y Fotos: ISMS Forum*

SOLUCIONES INTELIGENTES PARA UN MUNDO INTERCONECTADO

# Experience Day. Connected Security

## Bosch Security Systems celebra su evento anual para profesionales de seguridad y comunicaciones

Bosch, el proveedor mundial en tecnología y servicios, celebró el Experience Day, foro anual de profesionales del sector de seguridad y comunicaciones, en el que presentó propuestas innovadoras en productos, sectores de aplicación e integración de sistemas.

CELEBRADO en el Mirador del Museo Thyssen-Bornemisza, el evento tuvo dos sesiones, de mañana, enfocada a productos y tecnologías para su canal de distribución e integradores de sistemas, y de tarde, de soluciones integradas para proyectos para consultores y departamentos especializados de usuarios finales.

Bajo el lema «Connected Security», la jornada fue inaugurada por Frank Seidel, presidente del Grupo Bosch en España, quien destacó que Bosch factura cerca de 70.600 millones de euros a través de sus cuatro áreas de negocio: Soluciones de Movilidad, Tecnología Industrial, Bienes de Consumo y Tecnología para la Energía y la Edificación. En los últimos cinco años, ha destinado más de 21.000 millones de euros a actividades de I+D (en 2015, el 9% de sus ventas).

Con su experiencia en los tres niveles del «Internet of Things» (IoT) –sensores, software y servicios–, Bosch es una de las compañías de referencia mundial en esta área. La compañía está buscando nuevas oportunidades de negocio derivadas del «Internet of Things» y de la conectividad, especialmente en el campo de la movilidad conectada, de las Smart Homes, así como de la industria conectada. Una de las dedicaciones más importantes de Bosch es el desarrollo de entornos seguros, como la Bosch IoT Suite, plataforma de almacenamiento en la nube, que gestiona ya decenas de aplicaciones de la compañía.

A continuación, Johan Jubbega, vicepresidente para Ventas EMEA de Bosch Security Systems, presentó la apuesta de la división Bosch Security Systems en un mundo conectado. Bosch identifica una serie de macrotendencias en el mundo actual, que son: el incremento demográfico, la creciente concentración de la población en áreas urbanas, la necesidad energética y la hiperconectividad. Esto plantea grandes posibilidades para el Internet of Things y grandes retos para la seguridad, de la que compañías como Bosch deben tomar la iniciativa.

Bosch trabaja desde hace años para ofrecer soluciones de seguridad y comunicaciones interconectadas entre sí y con otros dominios de la industria. Bosch cuenta con más de 3.000 profesionales que trabajan en el desarrollo de funcionalidades y aplicaciones seguras en el IoT.

**Frank Seidel inauguró la jornada «Connected Security».**

**Johan Jubbega, Bosch Security Systems en un mundo interconectado.**

Jeroen Dickhoff, director general de Bosch Security Systems en Iberia, fue el encargado de presentar el ecosistema que permite que Bosch proporcione a los usuarios soluciones integradas inteligentes de la mano de los agentes más importantes del sector: integradores, distribuidores, consultores y otros influenciadores y terceros desarrolladores que forman parte del Integration Partner Program de Bosch.

Jeroen Dickhoff, el ecosistema de Bosch Security Systems.

Gerardo Estalrich, en su intervención sobre oportunidades en seguridad.

Bosch propone una completa gama de soluciones de seguridad y comunicaciones, en la que incorpora las últimas tecnologías y funcionalidades exclusivas del fabricante, que las hacen únicas: innovaciones como starlight, la altísima sensibilidad exclusiva de sus cámaras, transcodificación dinámica, o calidad de imagen adaptable al ancho de banda para gestión remota, Data Security, un sistema de cuatro pasos para garantizar la seguridad de los dispositivos o la analítica inteligente de vídeo, de serie en todas sus cámaras; la más completa gama de equipos de sonorización EN54 y conferencias de todo tipo; detección de intrusión EN50 que muestra la mayor fiabilidad y óptima relación calidad-precio a través del concepto de coste de la propiedad en el ciclo de vida del producto; o lo último en detección precoz de incendios mediante vídeo detección con Aviotec; la recientemente incorporada plataforma de gestión de seguridad BIS y la gama de control de accesos; o el certificado «Trusted Platform Module» de alta seguridad para operaciones criptográficas.

Para finalizar las presentaciones de la compañía, Gerardo Estalrich, director de Desarrollo de Negocio para Iberia, planteó los retos futuros como el almacenamiento y transporte de la gran cantidad de datos generados y la seguridad a lo largo de todo el proceso de seguridad, desde la generación de un dato (captura de una imagen) y seguridad en los procesos, hasta su tratamiento y utilización definitiva (análisis forense).

Bosch Security Systems aplica certificados digitales y analítica de vídeo «en origen», embebida en las cámaras para garantizar la seguridad de los datos y la total confianza en el proyecto de seguridad realizado con las soluciones de la marca, desde la infraestructura de la red hasta los equipos instalados.

Por último, la jornada contó con la intervención de Miguel Ángel Molina, director de Seguridad del Museo Thyssen-Bornemisza, que presentó el reciente e innovador proyecto de digitalización de la central receptora y el sistema de videovigilancia del Museo.

El Museo, pionero en España por sus iniciativas en el ámbito museístico, ha realizado un estudio de sus necesidades de seguridad, y ha incorporado, de la mano de Bosch, su partner en este proyecto, innovaciones como el análisis inteligente de vídeo, la gestión remota de la videovigilancia desde tablet adaptada a través de la transcodificación dinámica, o las cámaras en red Panoramic 360º que ofrecen funcionalidades como la visión completa «esférica 360º» de una zona con una sola cámara o la utilización en «modo museo» para proteger las obras.

Tras las presentaciones, los asistentes realizaron un carrusel de demostraciones, un tour guiado por distintas estaciones demo que mostraban las innovaciones más destacadas de la compañía, con aplicaciones en los más diversos campos de la seguridad y comunicaciones, como el BIS-Building Integration System, en el que, bajo un escenario propuesto de una sala de control, se realizaban diversas simulaciones de alarma y evacuación en tiempo real desde el laboratorio central de la compañía en Holanda, gestionadas en remoto por BIS desde el museo, o como BVMS-Bosch Video Management System, sistema abierto de gestión de vídeo de elementos propios y de terceros fabricantes o VRM-Video Recording Management, sistema de grabación redundante que garantiza la fortaleza del sistema instalado; MAP 5000, panel modular de detección de intrusión EN50 para grandes instalaciones. ●

**Miguel Ángel Molina, director del Museo Thyssen-Bornemisza explicando el proyecto pionero de videovigilancia implantado en el museo.**

*Texto y Fotos: Bosch*

Contactos de empresas, p. 9.

COMPLIANCE OFFICER, CIBERSEGURIDAD,... FUERON ALGUNOS DE LOS TEMAS QUE SE TRATARON

# VI Congreso de **Directores de Seguridad**

## El encuentro se celebró bajo el lema «Futuro condicionado, evolución permanente»

Más de 350 profesionales acudieron el pasado 29 de septiembre en Madrid a la sexta edición del Congreso de Directores de Seguridad, para analizar la realidad actual de esta figura profesional. Bajo el lema «Futuro condicionado, evolución permanente», el encuentro que se celebra bienalmente fue organizado por la Asociación Española de Directores de Seguridad (AEDS), el Capítulo Español de ASIS International, la Asociación de Directivos de Seguridad Integral (ADSI), y Seguritecnia.

Durante la celebración del congreso se abordaron entre otros los siguientes temas: la resiliencia, la organización corporativa, la evangelización de la seguridad, el cumplimiento normativo, la formación, la protección de infraestructuras críticas o la figura del compliance officer, la responsabilidad del director de Seguridad ante una emergencia, la ciberseguridad, la importancia de la convergencia, el impacto del modelo PIC en los sectores del transporte, energía, agua y financiero, entre otros temas. El encuentro contó con la intervencción de un total de 25 ponentes, que fueron desgranando estos temas en tres paneles de ponencias y una mesa redonda.

El comisario principal Esteban Gándara, jefe de la Unidad Central de Seguridad Privada, afirmó en la inauguración del congreso que el Ministerio del Interior continúa trabajando «un documento que cada vez se acerca más a ser un borrador del Reglamento de Seguridad Privada y que ha partido de todas las propuestas que habéis hecho sobre la Ley de Seguridad Privada», añadió dirigiéndose a los presentes.

Por su parte, El coronel Andrés Sanz, jefe del Servicio de Protección y Seguridad de la Guardia Civil, destacó en la clausura el desarrollo del evento por la multitud de temas tratados y la variedad de perfiles profesionales asistentes, más allá de los directores de seguridad.

**ENCUENTRO ORGANIZADO POR EL INSTITUTO DE PROBÁTICA E INVESTIGACIÓN CRIMINAL (IPIC) Y LA ASOCIACIÓN PROFESIONAL DE DETECTIVES PRIVADOS DE ESPAÑA (APDPE)**

# Éxito del II Curso sobre «Investigación de Desaparecidos»

## En el curso se abordaron, entre otros temas, los perfiles de la víctima o la influencia mediática

Cerca de 50 personas –detectives privados, alumnos de criminología, guionistas de TV, etc.– acudieron al II Curso sobre Investigación de Desaparecidos, encuentro profesional organizado por el Instituto de Probática e Investigación Criminal (IPIC) y la Asociación Profesional de Detectives Privados de España (APDPE), y en el que se abordaron, entre otros temas, los perfiles de la víctima e hipótesis de lo ocurrido, la influencia mediática o la posible acción en la escena fantasma.

PROPORCIONAR al profesional de la investigación privada que toma parte en una averiguación y/o instrucción de desaparecidos, una formación acorde con la materia que debe tratar, para que conozca las dificultades a las que deberá hacer frente y la mejor forma de afrontarlas; la necesidad de averiguar cómo se desarrolló, la metodología de investigación, son, entre otros, algunos de los objetivos del curso.

### Destacados profesionales: investigadores, abogados,...

Todo ello de la mano de destacados profesionales, entre los que se encuentran investigadores, abogados, juristas, psicólogos y peritos en probática de reputado prestigio, que han participado de manera activa en la resolución de casos de desaparecidos de una gran repercusión social y mediática.

### La escena fantasma, la prueba indiciaria,...

Así algunos de los contenidos que se abordaron fueron «Organización básica de la información», «La escena fantasma» «La prueba indiciaria», a cargo de Ángel Galán, presidente del IPIC; «La relación con la víctima. Perfil de la víctima», por la psicóloga Ana I. Gutiérrez; «La acción en la escena fantasma y metodología de investigación de desaparecidos», a cargo del investigador del Cuerpo Nacional de Policía, Luis M. Muñoz; o «De la vieja del visillo a faro coche 2.0», a cargo de Elisenda Villena, detective privado.

Las mesas de debate celebradas al finalizar cada sesión de trabajo analizaron casos reales de desaparecidos: Aurora Mancebo, Niños Bretón, Madeleine MacCann, y Fernando Caldas. ●

# Access to Quality SLU adquiere la marca Leopard

ACCESS to Quality SLU ha adquirido la marca Leopard de equipos para seguridad de perímetros. La citada marca fue propiedad de Perimetral Sallen Technologies y Grupo Sallen Tech hasta el pasado mes de junio.

Access to Quality SLU. fabrica y distribuye en exclusiva todos los productos perimetrales Leopard y está incorporando nuevos desarrollos a los conocidos equipos perimetrales de fibra óptica.

Leopard es una marca española referente en fabricación de sensores perimetrales de fibra óptica, como muestra tienen los perímetros fronterizos de Ceuta y Melilla, los cuales fueron protegidos en su totalidad con equipos Leopard.

La gama de equipamiento Leopard la compone el equipamiento para protección de vallados, suelos en intemperie, paredes y muros frente a perforación y robo de cableados.

Access to Quality SLU tiene sus oficinas centrales en Monzón (Huesca) y tiene como actividad principal el diseño y fabricación de equipamiento electrónico de seguridad. Para más información se puede visitar su nueva página web: www.leopardperimeter.com.

# Diid nuevo mayorista de Axis

AXIS Communications ha firmado un acuerdo con la empresa Diid Logística y Distribución para comenzar a distribuir y comercializar sus soluciones de vídeo IP en España.

Axis Comunications, especialista del mercado en vídeo en red, es una compañía con un modelo de comercialización 100% indirecto. Por ello, todos sus socios son una prolongación de su propio equipo y desempeñan una función clave en la estrategia de mercado y en el éxito global de la empresa. Como novedad, las soluciones de vídeo IP de Axis Communications comenzarán a ser distribuidas y comercializadas por Diid Logística y Distribución. Gracias a un acuerdo entre ambas compañías con vigencia desde el 1 de

# Gran éxito de los cursos de formación en Dahua Iberia

El Programa de Formación de Dahua Technology para Instaladores ya ha dado comienzo y se están celebrando dos sesiones formativas cada semana en su nuevo showroom ubicado en la sede de Dahua Iberia en Madrid. Dahua Technology, proveedor mundial en videovigilancia, después de una completa y exhaustiva organización, ha introducido recientemente sus sesiones de formación en España.

El curso está estructurado de modo teórico y práctico. Durante el desarrollo de ambos contenidos, todos los integradores, instaladores y profesionales vinculados a la industria de la videovigilancia, no sólo adquieren nuevos conocimientos y prueban directamente el funcionamiento de los productos Dahua, sino que también comparten ideas y puntos de vista sobre la industria de la seguridad. No hay duda que el programa de formación está resultando muy exitoso y, además, para finalizar estos interesantes programas formativos, todos los asistentes disfrutan de una estupenda cena y valiosos regalos.

El programa de formación se lleva a cabo gracias al esfuerzo del equipo organizador de los diferentes apartados del curso. Al igual que está en permanente colaboración con los partners, también Dahua Iberia está comprometida a proporcionar cursos de formación técnica altamente cualificados para todos los clientes del sector de la seguridad. Su constante innovación, los numerosos casos de éxito y el experimentado equipo de expertos hacen que Dahua realice una excelente aportación al mercado español de la videovigilancia. Estamos concentrados en apoyar a nuestros socios para que ofrezcan los mejores productos y soluciones Dahua, y satisfagan la amplia variedad de retos de seguridad que plantean los clientes.

La simplicidad de su trabajo y el crecimiento de su negocio nunca ha sido tan fácil, ven y únete a nosotros, ¡vamos a avanzar hacia la nueva era de la industria de la seguridad juntos!

Escanee el código QR y ¡regístrese ya en el programa de formación!

VPS
PROTECT MANAGE MONITOR

# PROTEGE EL PATRIMONIO DE TUS CLIENTES Y SU ENTORNO

- **Coste directo por okupación:**
  **25.000€**. Por no alquilar o vender el inmueble, por reformas, por gastos legales.

- **Coste social por okupación:**
  Problemas de convivencia vecinal, vandalismo, efecto llamada para okupas, efecto expulsión para vecinos.

## SOLUCIÓN: PUERTAS ANTIOKUPA VPS

- **Reduzca el riesgo de intrusión.**
- **Reduzca el deterioro del inmueble.**
- **Evite problemas vecinales.**

**Protegemos lo que es tuyo**

Para más información:
spain@vpsitex.es

octubre de 2016, el mayorista utilizará la estructura de ventas en España para ofrecer los productos y soluciones del fabricante.

«Estamos encantados de incluir a Diid en nuestra estructura de mayoristas, y se convierte en una pieza estratégica de cara al futuro», afirmó Julio Castillo Sevilla, responsable del Canal de Distribución de Axis Communications para España y Portugal.

Diid Logística y Distribución es un proveedor dedicado a la comercialización y logística de materiales de seguridad y CCTV.

«Para nuestra estrategia de negocio es fundamental encontrar partners que no sólo aporten productos y soluciones de vanguardia, sino que además dispongan de una estructura de apoyo técnica y comercial que nos permita generar ventajas competitivas en el mercado y lograr armar una propuesta de valor adecuada para nuestros clientes», concluye Ignacio Barandiarán, CEO de DiiD.

Contactos de empresas, p. 9.

## Nuevas instalaciones de Detnov en Barcelona

EN el año 2012 Detnov se estableció en la población de Sant Boi de Llobregat, provincia de Barcelona. Gracias al crecimiento que la empresa ha tenido durante los dos últimos años se ha visto obligado a trasladar al equipo comercial y de administración a una nueva nave ubicada a 150 metros de la localización anterior. El almacén de producto terminado estará en las nuevas oficinas, con un espacio de más 700 m² de superficie, para poder atender con mayor comodidad a los clientes que vienen a recoger mercancía, y para preparar los pedidos de exportación.


En estos momentos se está terminando de preparar la sala de demostraciones, donde estará toda la gama de produtos de la empresa, en completo funcionamiento, para poder enseñar a clientes y usuarios las prestaciones de nuestros productos. En la nave antigua se mantendrán: la fabricación, el departamento de I+D, los bancos de pruebas y ensayos y el almacén de materia prima. Con estas nuevas instalaciones, Detnov mejora y amplía los servicios prestados, con la intención de seguir creciendo y proporcionar una excelente atención y mejor servicio, en beneficio de los clientes y colaboradores con las mejores condiciones de trabajo. Con las nuevas instalaciones Detnov quiere contribuir más, si cabe, a lograr los tres objetivos primordiales de la empresa: Seriedad, Calidad y Servicio.

La nueva oficina se situa en la siguiente dirección: calle de l'Alguer nº 18 en Sant Boi de Llobregat (Barcelona)

## Vanderbilt se hace con Access Control Technology

Vanderbilt, especialista mundial en sistemas de seguridad de vanguardia, ha anunciado la finalización de la

compra de Access Control Technology (ACT) Ltd. La incorporación de la línea de productos ACT a la oferta principal de Vanderbilt aporta más opciones para control de accesos y videovigilancia a nivel empresarial, al mismo tiempo que ofrece una nueva solución global basada en la nube. La marca ACT seguirá existiendo para los productos más conocidos incorporados a la oferta de Vanderbilt, como ACTpro, ACTenterprise y ACT365.

ACT365 de ACT es una solución integrada de software de control de accesos y de gestión de vídeo basada en la nube que ofrece aún más opciones a la línea de productos de Vanderbilt. ACT365 ofrece a los usuarios la posibilidad de administrar y gestionar el sistema desde cualquier lugar, en cualquier momento y en cualquier dispositivo.

«ACT ofrece una complementariedad estratégica a Vanderbilt, sacando el máximo rendimiento de su negocio sólido y rentable en R.U. e Irlanda», dijo Joe Grillo, director ejecutivo de Vanderbilt. «La incorporación de un control de acceso integrado y de una plataforma de vídeo es un paso lógico para hacer crecer nuestro negocio a nivel internacional en las áreas de control de accesos, videovigilancia e intrusión».

# CAJAS FUERTES

# PUERTAS Y CÁMARAS ACORAZADAS

# SISTEMAS DE ANCLAJE Y RAMPAS

# VALIJAS Y SUBMOSTRADORES


# SISTEMAS DE INGRESOS Y CONSIGNAS

FERRIMAX
WORLDWIDE SECURITY SERVICES
www.ferrimax.com

Armarios de Seguridad, Armeros, Blindajes de Vehículos, Bases ATM, Buzones Electrónicos, Cajón Anti-atraco, Cerraduras Electrónicas y Biométricas, Compartimentos de Alquiler, Instalaciones Bancarias, Placas de Anclaje, Porta Videos, Productos Ignífugos, Puertas Blindadas, Sistema Anti-gas, Submostradores, Vitrinas Blindadas.

Servicio Técnico y Mantenimiento.

# Bunker: los detectores SIP de Redwall en el catálogo de Prodextec

Dentro de la completa gama de productos para seguridad perimetral que presenta el catálogo de Prodextec, se encuentra la línea de detectores de exterior de largo alcance SIP de Redwall.

Se trata de sistemas de detección inteligentes que se instalan en altura y proporcionan detección volumétrica para aplicaciones de exterior, basada en el análisis de los cambios de temperatura entre un objeto en movimiento y la temperatura ambiental, con la finalidad de detectar intrusos. Existen diferentes modelos tanto en función de su cobertura, alcanzando hasta una anchura máxima de 50m x 30m o una longitud máxima de 100m x 3m como de sus características: cableados o vía radio, con/sin ángulo cero, con cámara, compatibles IP/PoE. Estos últimos, los SIP-IP están integrados en las principales plataformas VMS.

Estos detectores disponen de zonas de detección independientes que permiten activar las cámaras PTZ y proporcionar confirmación visual, estando preparados además para ajustes de sensibilidad independientes para cada zona, aspecto de gran relevancia en equipos que se instalan en exteriores para protección perimetral. Para más información, consulte la web www.prodextec.es o contacte con (info@prodextec.es).

# Vivotek amplía sus soluciones H.265

Vivotek, proveedor mundial de vigilancia IP, ha anunciado que agregará cinco nuevos productos de vigilancia H.265/HEVC a su línea actual: una cámara de red con zoom tipo bala, IZ9361-EH, las cámaras de red tipo domo de alta velocidad full-HD modelos SD9161-H y SD9363-EHL, y dos cámaras de red tipo ojo de pez de 5 megapíxeles FE9182-H y FE9382-EHV. Con estos nuevos productos Vivotek completa su línea de soluciones H.265/HEVC que abarca 24 diferentes modelos de cámaras de red, 4 grabadores de vídeo de red y el avanzado software profesional de gestión de vídeo VAST.


# Hanwha Techwin: nueva serie Wisenet P 4k con compresión exclusiva WiseStream

Hanwha Techwin ha presentado tres nuevas cámaras de la serie Wisenet P de Samsung equipadas con compresión H.265 y WiseStream, una tecnología complementaria de compresión, que controla de forma dinámica la codificación, buscando el equilibrio entre calidad y compresión de acuerdo al movimiento en la imagen. Como resultado de ello, los requisitos de ancho de banda y almacenamiento de las imágenes con resolución de 12MP, capturadas por las cámaras Wisenet P, se han visto drásticamente reducidos y son similares a los de cámaras Full HD con H.264 de menor resolución.

«La nitidez y claridad de las cámaras 4K son increibles, pero a costa de un ancho de banda muy elevado», afirma José Luis Romero, General Manager Spain & Portugal de Hanwha Techwin. «Las imágenes multipíxel de alta definición pueden ocupar con demasiada rapidez el espacio de almacenamiento disponible en un NVR o servidor cuando se graban a una resolución y frecuencia de cuadro completas. Por suerte, los ingenieros de diseño de Hanwha Techwin han resuelto este problema de manera inteligente desarrollando nuestra exclusiva tecnología WiseStream».

Contactos de empresas, p. 9.


EL AYER ES HISTORIA,
EL MAÑANA ES UN MISTERIO;
SIN EMBARGO,
EL HOY ES UN REGALO.
POR ESO SE LE LLAMA
"PRESENTE".

Feliz Navidad
y próspero
2017

CUADERNOS DE SEGURIDAD

Peldaño

# ÍNDICE

## MATERIALES, EQUIPOS Y SISTEMAS DE SEGURIDAD



## SERVICIOS DE SEGURIDAD



## ALARMA Y CONTROL

**Techco Security**
C/ Barbadillo 7
28042 Madrid
+34 91 312 77 77
www.techcosecurity.com
tcs@techcosecurity.com

**GAROTECNIA**
Valdelaguna, 4 local 3
28909 Getafe (Madrid)
Tel.: 916 847 767 - Fax: 916 847 769
**garotecnia@garotecnia.com**
**www.garotecnia.com**
**Autorizada por la D.G.P. con el nº 2.276**

**Tyco Integrated Fire & Security**

Edificio Ecu-I
Ctra. de La Coruña, km 23,500
28290 Las Rozas (Madrid)
Tel.: 902 444 440 - Fax: 91 631 39 78
**www.tyco.es**

San Fructuoso, 50-56 - 08004 **Barcelona**
Tel.: 934 254 960* - Fax: 934 261 904
**Madrid:** Matamorosa, 1 - 28017 Madrid
Tel.: 917 544 804* - Fax: 917 544 853
**Sevilla:** Tel.: 954 689 190* - Fax: 954 692 625
**Canarias:** Tel.: 928 426 323* - Fax: 928 417 077
**Portugal**
Rua Ilha da Madeira, 13 A
Olival Basto 2620-045 Odivelas (Lisboa)
Tel.: 219 388 186* - Fax: 219 388 188
**www.bydemes.com**

FUNDADA EN 1966
INSTALACIONES A SU MEDIDA
ISO 9001
Antoñita Jiménez, 25
28019 Madrid
Tel.: 91 565 54 20 - Fax: 91 565 53 23
**seguridad@grupoaguero.com**
www.grupoaguero.com

**Central Receptora de Alarmas/Videovigilancia**
Autorizada por la D.G.P. con el nº. 729
Avda de Olivares 17 – Plg. Industrial PIBO
41110 Bollullos de la Mitación (Sevilla)
Tlfno. 902194814 – 954108887
Fax. 954002319
gerencia@gruporomade.com
SERVICIOS EN TODA ESPAÑA

Accesos | CCTV | Incendio | Intrusión
*Oficina Central:*
*Maresme, 71-79 · 08019 Barcelona*
*Fax 933 518 554*
***902 202 206*** *www.casmar.es*



Calle López de Neira, nº3, oficina nº 301
36202 Vigo España
Tel.: +34 986 220 857 / 693 422 688
FAX: +34 986 447 337
**www.aforsec.com**
**aforsec@aforsec.com**

## CONTROL DE ACCESOS ACTIVO

**TALLERES DE ESCORIAZA, S. A. U.**
Barrio de Ventas, 35
E-20305 Irún • SPAIN
Tel.: +34 943 669 100
Fax: +34 943 633 221
**tesalocks@tesa.es • www.tesa.es**

**Líderes en Gestión de Horarios y Accesos desde 1978**
**SKL** Smart Key & Lock
Ferrerías 2,
20500 MONDRAGÓN -SPAIN-
**+34 943 71 19 52**
**spec@grupospec.com**
**www.skl.es**

**CONTROL DE ACCESO, HORARIO, TIEMPO Y PRESENCIA**
C/Samonta 21
08970 Sant Joan Despi
Tel.: +34 934774770
info@primion-digitek.es
www.digitek.es

**GRUPO SPEC**
Líderes en Gestión de Horarios y Accesos desde 1978
C/ Caballero, 81
08014 Barcelona
Tel. 93 247 88 00 • Fax 93 247 88 11
spec@grupospec.com
**www.grupospec.com**

# MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

**BIOSYS**
**(Sistemas de Tecnología Aplicada)**

C/ Cinca, 102-104
08030 BARCELONA
Tel. 93 476 45 70
Fax. 93 476 45 71
**comercial@biosys.es - www.biosys.es**



**bydemes**
avanzando juntos hacia el futuro

San Fructuoso, 50-56 - 08004 **Barcelona**
Tel.: 934 254 960* - Fax: 934 261 904
**Madrid:** Matamorosa, 1 - 28017 Madrid
Tel.: 917 544 804* - Fax: 917 544 853
**Sevilla:** Tel.: 954 689 190* - Fax: 954 692 625
**Canarias:** Tel.: 928 426 323* - Fax: 928 417 077
**Portugal**
Rua Ilha da Madeira, 13 A
Olival Basto 2620-045 Odivelas (Lisboa)
Tel.: 219 388 186* - Fax: 219 388 188
**www.bydemes.com**

RISTER
PRESENTCO®

Avda. Roma, 97
08029 BARCELONA
Tel.: 93 439 92 44 • Fax: 93 419 76 73

**Delegación Zona Centro:**
Sebastián Elcano, 32
28012 Madrid
Tel.: 902 92 93 84

accesor

**Soluciones integrales en control de Accesos y seguridad**

DDS
Building Security Together

Carrer Esperança, 5
08500 Vic (Barcelona)
Tel.: 902 447 442
Fax.: 938 864 500

info@accesor.com
**www.accesor.com**

DORLET

**DORLET S. A. U.**

Parque Tecnológico de Álava
C/Albert Einstein, 34
01510 Miñano Mayor - ALAVA - Spain
Tel. 945 29 87 90 • Fax. 945 29 81 33

**e-mail: comercial@dorlet.com**
**web: http://www.dorlet.com**

setelsa link
Sistemas Electrónicos y Telecomunicación S.A.

**SETELSA**
Polígono Industrial de Guarnizo - Parcela 48-C Naves "La Canaluca" 2 y 4
39611 GUARNIZO-CANTABRIA. ESPAÑA
**Tel.: 942 54 43 54**
**www.setelsa.net**

## DETECCIÓN DE EXPLOSIVOS

COTELSA

**COTELSA**
Basauri, 10-12, Urb. La Florida
Ctra. de La Coruña, Aravaca
28023 Madrid
Tel.: 915 662 200 - Fax: 915 662 205
**cotelsa@cotelsa.es**
**www.cotelsa.es**

TECOSA

TELECOMUNICACIÓN, ELECTRÓNICA Y CONMUTACIÓN

**Grupo Siemens**
**Infraestructure & Cities Sector**
División Building Technologies
Ronda de Europa, 5
28760 Tres Cantos - Madrid
Tel.: +34 91 514 75 00
Asistencia Técnica: 902 199 029
www.tecosa.es

TARGET TECNOLOGIA

**TARGET TECNOLOGIA, S.A.**
Ctra. Fuencarral, 24
Edif. Europa I - Portal 1 Planta 3ª
28108 Alcobendas (Madrid)
Tel.: 91 554 14 36 • Fax: 91 554 45 89
**info@target-tecnologia.es**
**www.target-tecnologia.es**

## SISTEMAS DE EVACUACIÓN

OPTIMUS
SOUND & COMMUNICATION

**OPTIMUS S.A.**

C/ Barcelona 101
17003 Girona
T (+34) 972 203 300

**info@optimus.es**
**www.optimusaudio.com**

## PROTECCIÓN CONTRA INCENDIOS. ACTIVA

detnov

C/ Alguer nº8 08830 Sant Boi de Llobregat (Barcelona)

Tel: +34 93 371 60 25
Fax:+34 93 640 10 84

**www.detnov.com**
**info@detnov.com**


bydemes
avanzando juntos hacia el futuro

San Fructuoso, 50-56 - 08004 **Barcelona**
Tel.: 934 254 960* - Fax: 934 261 904
**Madrid:** Matamorosa, 1 - 28017 Madrid
Tel.: 917 544 804* - Fax: 917 544 853
**Sevilla:** Tel.: 954 689 190* - Fax: 954 692 625
**Canarias:** Tel.: 928 426 323* - Fax: 928 417 077
**Portugal**
Rua Ilha da Madeira, 13 A
Olival Basto 2620-045 Odivelas (Lisboa)
Tel.: 219 388 186* - Fax: 219 388 188
**www.bydemes.com**


aguilera

**GRUPO AGUILERA**

**FABRICANTES DE SOLUCIONES PCI DETECCIÓN Y EXTINCIÓN DE INCENDIOS**

**SEDE CENTRAL**
C/ Julián Camarillo, 26 28037 MADRID
Tel. 91 754 55 11 • Fax: 91 754 50 98
www.aguilera.es

**Delegaciones en:**
Galicia: Tel. 98 114 02 42 • Fax: 98 114 24 62
Cataluña: Tel. 93 381 08 04 • Fax: 93 381 07 58
Levante: Tel. 96 119 96 06 • Fax: 96 119 96 01
Andalucía:Tel. 95 465 65 88 • Fax: 95 465 71 71
Canarias: Tel. 928 24 45 80 • Fax: 928 24 65 72
Portugal: Tel.+351 213 563 295 • Fax:+351 213 563 295

**Factoría de tratamiento de gases**
Av. Alfonso Peña Boeuf, 6. P. I. Fin de Semana
28022 MADRID
Tel. 91 312 16 56 • Fax: 91 329 58 20

**Soluciones y sistemas:**
** DETECCIÓN **
Algorítmica • Analógica • Aspiración • Convencional • Monóxido • Oxyreduct® • Autónomos • Detección Lineal
** EXTINCIÓN **
Agua nebulizada • Fe-13™ • Hfc-227ea • $Co_2$

pefipresa
FIRE, SAFETY & SECURITY

**PEFIPRESA, S. A. U**

**INSTALACIÓN Y MANTENIMIENTO DE SISTEMAS DE SEGURIDAD Y CONTRA INCENDIOS**

**www.pefipresa.com**

**Oficinas en:** A Coruña, Algeciras, Barcelona, Bilbao, Madrid, Murcia, Santa Cruz de Tenerife, Sevilla, Valencia y Lisboa.

**Atención al cliente: 902 362 921**
info.madrid@pefipresa.com


**¿No cree...**
**... que debería estar aquí?**

**El directorio es la zona más consultada de nuestra revista.**

**Módulo: 660€/año***

**Más información:**
**Tel.: 91 476 80 00**
**e-mail: publi-seguridad@epeldano.com**
* Tarifa vigente 2016

# MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

## PROTECCIÓN CONTRA INCENDIOS. PASIVA

### solexin

Calle Alberto Alcocer, 28, 1º A
28036 Madrid
Tel. 913 685 120

**info@solexin.es**
**www.solexin.es**

### DICTATOR Española

**DICTATOR ESPAÑOLA**
Mogoda, 20-24 • P. I. Can Salvatella
08210 Barberá del Vallés (Barcelona)
Tel.: 937 191 314 • Fax: 937 182 509
**www.dictator.es**
**dictator@dictator.es**

## PROTECCIÓN CONTRA INTRUSIÓN. ACTIVA

### bydemes

avanzando juntos hacia el futuro

San Fructuoso, 50-56 - 08004 **Barcelona**
Tel.: 934 254 960* - Fax: 934 261 904
**Madrid:** Matamorosa, 1 - 28017 Madrid
Tel.: 917 544 804* - Fax: 917 544 853
**Sevilla:** Tel.: 954 689 190* - Fax: 954 692 625
**Canarias:** Tel.: 928 426 323* - Fax: 928 417 077
**Portugal**
Rua Ilha da Madeira, 13 A
Olival Basto 2620-045 Odivelas (Lisboa)
Tel.: 219 388 186* - Fax: 219 388 188
**www.bydemes.com**

### DAITEM

**ATRAL SISTEMAS**
C/ Miguel Yuste, 16 5ª Planta.
28037- Madrid
www.daitem.es

### RISCO GROUP

Creating Security Solutions

**RISCO Group Iberia**
San Rafael, 1
28108 Alcobendas (Madrid)
Tel.: +34 914 902 133
Fax: +34 914 902 134
**sales-es@riscogroup.com**
**www.riscogroup.es**

### Honeywell

**Honeywell Security España S. A.**
**Soluciones integradas de intrusión, vídeo y control de accesos**
Avenida de Italia, 7
C. T. Coslada
28821 Coslada
Madrid
Tel.: 902 667 800 - Fax: 902 932 503
**seguridad@honeywell.com**
**www.honeywell.com/security/es**

### Tecnoalarm

Hi-Tech Security Systems

**TECNOALARM ESPAÑA**

C/ Vapor, 18 • 08850 Gavà (Barcelona)
Tel.: +34 936 62 24 17
Fax: +34 936 62 24 38
www.tecnoalarm.com
tecnoalarm@tecnoalarm.es

### VANDERBILT

**VANDERBILT ESPAÑA Y PORTUGAL**

Avenida de Monteclaro s/n
Edificio Panatec
CP 28223, Pozuelo de Alarcón, Madrid
Teléfono +34 91 179 97 70
Fax +34 91 179 07 75
**info.es@vanderbiltindustries.com**
**www.vanderbiltindustries.com**

## PROTECCIÓN CONTRA ROBO Y ATRACO. PASIVA

### AGA

LA INDUSTRIA DE LA CERRAJERÍA

Talleres AGA, S.A.
C/ Notario Etxagibel, 6
20500 Arrasate-Mondragón (Gipuzkoa)
Tel.: +34 943 79 09 22
talleresaga@aga.es www.aga.es

### diid

**Diid Seguridad Gestión y Logística**
Pol. Ind. Mies de Molladar D3
39311 CARTES – CANTABRIA
Tlfno.: 902565733 – FAX: 902565884
**administracion@diid.es**
**www.diid.es**

## TELECOMUNICACIONES

### Alai Secure

**La solución de seguridad M2M definitiva para las comunicaciones de su CRA**

Condesa de Venadito 1, planta 11
28027 Madrid
T. 902.095.196 • F. 902.095.196
**comercial@alai.es • www.alaisecure.com**

## VIGILANCIA POR TELEVISIÓN

### HIKVISION

**HIKVISION SPAIN**
C/ Almazara 9
28760- Tres Cantos (Madrid)
Tel. 917 371 655
**info.es@hikvision.com**
**www.hikvision.com**

### SAMSUNG Wisenet

**Hanwha Techwin Europe Ltd**
Avda. De Barajas, 24, Planta Baja, Oficina 1
28108 Alcobendas (Madrid)España(Spain)
Tel.: +34 916 517 507

**www.hanwha-security.eu**
**hte.spain@hanwha.com**

### GRUPO iPTECNO

Tel. 902 502 035 - Fax 902 502 036
iptecno@iptecno.com - www.iptecno.com

SEDE BARCELONA
**IPTECNO Videovigilancia S.L.**
C. Pla del Ramassar, 52, Nave 19
08402 Granollers

SEDE MADRID
**IPTECNO Seguridad S.L.**
Avda. Tenerife, 2 - Blq. 2, Pta. 3
28703 S. S. de los Reyes

### alhua TECHNOLOGY

**DAHUA IBERIA**
C/ Juan Esplandiú 15 1-B. 28007
Madrid

Tel: +34 917649862
**sales.iberia@global.dahuatech.com**
**www.dahuasecurity.com**

# MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

**Visiotech**
Avenida del Sol, 22
28850, Torrejón de Ardoz (Madrid)
Tel.: 911 836 285 • Fax: 917 273 341
info@visiotech.es
www.visiotech.es

**Ballerup, Dinamarca.**
**Tlf. +34 902 65 67 98**
**ventas@ernitec.com**
**www.ernitec.com**

**AXIS COMMUNICATIONS**
C/ Yunque, 9 - 1ºA
28760 Tres Cantos (Madrid)
Tel.: +34 918 034 643
Fax: +34 918 035 452
**www.axis.com**

## EVENTOS DE SEGURIDAD

**Expertos en VIDEOVIGILANCIA**

LSB, S.L.
C./ Enero, 11 28022 Madrid
Tf: +34 913294835
info@lsb.es

**DALLMEIER ELECTRONIC ESPAÑA**
C/ Princesa 25 – 6.1 (Edificio Hexágono)
Tel.: 91 590 22 87
Fax: 91 590 23 25
28008 • Madrid
**dallmeierspain@dallmeier.com**
**www.dallmeier.com**

**GEUTEBRÜCK ESPAÑA**
Edificio Ceudas
Camino de las Ceudas, 2 Bis
28230 Las Rozas (Madrid)
Tel.: 902 998 440
Fax: 917 104 920
**ffvideo@ffvideosistemas.com**
**www.geutebruckspain.com**

**SECURITY FORUM**
Tel.: +34 91 476 80 00
Fax: +34 91 476 60 57
www.securityforum.es
info@securityforum.es

C/ Aragoneses, 15
28100 Alcobendas, Madrid
Tlf. 902 902 337

**seguridad@eeteuroparts.es**
**www.eeteuroparts.es**

A Western Digital® Company

**WD ESPAÑA**
4 boulevard des Iles
92130 Issy les Moulineaux · Francia
florence.perrin@wdc.com
Tel.: 615 235 013
www.wdc.com

**Grupo Alava Ingenieros**
**Área Seguridad**

C/Albasanz, 16 – Edificio Antalia
28037 Madrid
Telf. 91 567 97 00 • Fax: 91 567 97 11
**Email: alava@alava-ing.es**
**Web: www.alavaseguridad.com**



Avda. Roma, 97
08029 BARCELONA
Tel.: 93 439 92 44 • Fax: 93 419 76 73

**Delegación Zona Centro:**
Sebastián Elcano, 32
28012 Madrid
Tel.: 902 92 93 84

**Canon España, S.A**
Avenida de Europa 6
28108 Alcobendas
Madrid

Tel: +34915384500
www.canon.es
**camarasip@canon.es**

Josep Estivill, 67-69
08027 Barcelona, Spain.
**www.ata98.com**
**info@ata98.com**
**Tel. +34 931 721 763**

## ASOCIACIONES

San Fructuoso, 50-56 - 08004 **Barcelona**
Tel.: 934 254 960* - Fax: 934 261 904
**Madrid:** Matamorosa, 1 - 28017 Madrid
Tel.: 917 544 804* - Fax: 917 544 853
**Sevilla:** Tel.: 954 689 190* - Fax: 954 692 625
**Canarias:** Tel.: 928 426 323* - Fax: 928 417 077
**Portugal:**
Rua Ilha da Madeira, 13 A
Olival Basto 2620-045 Odivelas (Lisboa)
Tel.: 219 388 186* - Fax: 219 388 188
**www.bydemes.com**

**BOSCH SECURITY SYSTEMS SAU**
C/ Hermanos García Noblejas, 19
Edificio Robert Bosch
28037 Madrid • Tel.: 902 121 497
**Delegación Este:**
Plaça Francesc Macià, 14-19
08902 L'Hospitalet de Llobregat (Barcelona)
Tel.: 93 508 26 52 • Fax: 93 508 26 21
**Delegación Norte:** Tel.: 676 600 612
**es.securitysystems@bosch.com**
**www.boschsecurity.es**

Viladecans Business Park
Edificio Australia. C/ Antonio Machado 78-80, 1ª y 2ª planta
08840 Viladecans (Barcelona)
**Web: www.ingrammicro.es**
**Teléfono: 902 50 62 10**
**Fax: 93 474 90 00**
Marcas destacadas: Axis y D-Link.

C/ Alcalá 99
28009 Madrid
Tel. 915765255
Fax. 915766094

**info@uaseguridad.es**
**www.uaseguridad.es**

# MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD



AECRA
Asociación Europea de Profesionales para el conocimiento y regulación de actividades de Seguridad Ciudadana

C/ Emiliano Barral, 43
28043 Madrid
Tel 91 564 7884 • Fax 91 564 7829
**www.aecra.org**

AEINSE
Asociación Española de Ingenieros de Seguridad

**ASOCIACIÓN ESPAÑOLA DE INGENIEROS DE SEGURIDAD**

C/ San Delfín 4 (local 4 calle)
28019 MADRID
**aeinse@aeinse.org**
**www.aeinse.org**

ACAES
Associació Catalana d'Empreses de Seguretat

C/ Viladomat 174
08015 Barcelona
Tel.: 93 454 48 11
Fax: 93 453 62 10
**acaes@acaes.net**
**www.acaes.net**



tecnifuego AESPI

**ASOCIACION ESPAÑOLA DE SOCIEDADES DE PROTECCION CONTRA INCENDIOS**
C/ Doctor Esquerdo, 55. 1º F.
28007 Madrid
Tel.: 914 361 419 - Fax: 915 759 635
**www.tecnifuego-aespi.org**

**ASOCIACION ESPAÑOLA DE DIRECTORES DE SEGURIDAD (AEDS)**
Rey Francisco, 4 - 28008 Madrid
Tel.: 916 611 477 - Fax: 916 624 285
**aeds@directorseguridad.org**
**www.directorseguridad.org**

anpasp

**ANPASP**
**Asociación Nacional de Profesores Acreditados de Seguridad Privada**
C/ Anabel Segura, 11 - Edificio A - Planta 1ª
28108 Alcobendas (MADRID)
**info@anpasp.com • www.anpasp.com**

ADSI

**ADSI - Asociación de Directivos de Seguridad Integral**
Gran Via de Les Corts Catalanes, 373 - 385
4ª planta (local B2)
Centro Comercial **Arenas de Barcelona**
08015 Barcelona
**info@adsi.pro • www.adsi.pro**

AES

**ASOCIACION ESPAÑOLA DE EMPRESAS DE SEGURIDAD**
Alcalá, 99
28009 Madrid
Tel.: 915 765 225
Fax: 915 766 094

aproser

**ASOCIACIÓN PROFESIONAL DE COMPAÑÍAS PRIVADAS DE SERVICIOS DE SEGURIDAD**
Marqués de Urquijo, 5 - 2ºA
28008 Madrid
Tel.: 914 540 000 - Fax: 915 411 090
**www.aproser.org**

ASELF
Asociación Española de Lucha Contra el Fuego

**ASOCIACION ESPAÑOLA DE LUCHA CONTRA EL FUEGO**
Calle Escalona nº 61 - Planta 1
Puerta 13-14 28024 Madrid
Tel.: 915 216 964
Fax: 911 791 859

**¿No cree... ... que debería estar aquí?**

**El directorio es la zona más consultada de nuestra revista.**

**Módulo: 660€/año***

**Más información:**
**Tel.: 91 476 80 00**
**e-mail: publi-seguridad@epeldano.com**
*** Tarifa vigente 2016**

apdpe

**APDPE**
Asociación Profesional de Detectives de España
Marqués de Urquijo, 6, 1ºB
28008 - Madrid
Tel.: +34 917 581 399
Fax: +34 917 581 426
**info@apdpe.es • www.apdpe.es**

ASEPAL

**ASOCIACIÓN DE EMPRESAS DE EQUIPOS DE PROTECCION PERSONAL**
Alcalá, 119 - 4º izda.
28009 Madrid
Tel.: 914 316 298 - Fax: 914 351 640
**www.asepal.es**

ASIS INTERNATIONAL
Advancing Security Worldwide™
CAPITULO 143 – ESPAÑA
143 CHAPTER - SPAIN

**ASIS-ESPAÑA**
C/ Velázquez 53, 2º Izquierda
28001 Madrid
Tel.: 911 310 619
Fax: 915 777 190

cepreven

**ASOCIACIÓN DE INVESTIGACIÓN PARA LA SEGURIDAD DE VIDAS Y BIENES CENTRO NACIONAL DE PREVENCIÓN DE DAÑOS Y PÉRDIDAS**
Av. del General Perón, 27
28020 Madrid
Tel.: 914 457 566 - Fax: 914 457 136

FES

**FEDERACIÓN ESPAÑOLA DE SEGURIDAD**
Embajadores, 81
28012 Madrid
Tel.: 915 542 115 - Fax: 915 538 929
**fes@fes.es**
**C/C: comunicacion@fes.es**

AJSE
Asociación de Jefes de Seguridad de España

**ASOCIACIÓN DE JEFES DE SEGURIDAD DE ESPAÑA**

Avd. Meridiana 358. 4ºA.
08027 Barcelona
Tel. 93-3459682 Fax. 93-3453395
**www.ajse.es presidente@ajse.es**

sae

**ASOCIACIÓN VASCA DE PROFESIONALES DE SEGURIDAD**
Parque tecnológico de Bizkaia
Ibaizabal Kalea, 101
**sae@sae-avps.com**
**www.sae-avps.com**

# MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

**ASOCIACIÓN NACIONAL DE TASADORES Y PERITOS JUDICIALES INFORMÁTICOS (ANTPJI)**

C/ Juan de Mariana, 5
28045 Madrid
Tlf 91 / 469.76.44
**www.antpji.com**
**contacto@antpji.com**



## APLICACIONES INFORMÁTICAS

**FUNDADA EN 1966**

**INSTALACIONES A SU MEDIDA**

Antoñita Jiménez, 25
28019 Madrid
**ISO 9001**
Tel.: 91 565 54 20 - Fax: 91 565 53 23
**seguridad@grupoaguero.com**
www.grupoaguero.com

## FORMACIÓN DE SEGURIDAD

**Homologado por el Ministerio del Interior y la Junta de Andalucía.**

Avda de Olivares 17 • Plg. Industrial PIBO.
41110 Bollullos de la Mitación (Sevilla).
Tlfno. 902194814 – 954108887
Fax. 954002319
gerencia@gruporomade.com

## INTEGRACIÓN DE SISTEMAS

**ARQUERO SISTEMA CORPORATIVO**

**Avda. de la Feria 1**
**Edificio Incube - sala 8**
35012 Las Palmas de Gran Canaria
Tel.: **928 09 21 81**
www.sci-spain.com

## INNOVATIVE

Software de gestión de alarmas

**SOFTWARE DE GESTIÓN DE ALARMAS**

Gestión de Incidentes – Plataforma de Vídeo
Mapas Interactivos – Dispositivos Móviles
Innovative Business Software
**Tel.: 691 540 499**
info@innovative.es
**www.innovative.es**

**SEGURIDAD**
Control accesos / Intrusión / CCTV / Detección incendios / Megafonía / Interfonía / Consultoría

**ENERGÍA**
Eficiencia energética / Gestión inteligente de infraestructuras / Electricidad / Climatización / Consultoría energética

**www.ambarsye.es**
**ambarsye@ambar.es**
**902 55 08 01**

## CENTRALES DE RECEPCIÓN Y CONTROL

**ALARMAS SPITZ S. A.**
Gran Vía, 493 - 08015 Barcelona
Tel.: 934 517 500 - Fax: 934 511 443
**Central Receptora de alarmas**
Tel.: 902 117 100 - Fax: 934 536 946
**www.alarmasspitz.com**

## INSTALACIÓN Y MANTENIMIENTO

**Techco Security**
C/ Barbadillo 7
28042 Madrid
+34 91 312 77 77
www.techcosecurity.com
tcs@techcosecurity.com

**INSTALACIÓN Y MANTENIMIENTO**
INTRUSIÓN – CCTV – INCENDIO – ACCESOS
SUBCONTRATACIÓN
ALICANTE, VALENCIA, MURCIA, ALBACETE
www.seguridadlevante.com
**902 400 022**
info@seguridadlevante.com

## PUBLICACIONES WEB

**PUNTOSEGURIDAD.COM**
TF: 91 476 80 00

**info@puntoseguridad.com**
**www.puntoseguridad.com**

Avda. Manzanares, 196
28026 Madrid
Tel.: 914 768 000 - Fax: 914 766 057
**publi-seguridad@epeldano.com**
**www.instalsec.com**

# MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

## MATERIAL POLICIAL

**SABORIT INTERNATIONAL**
Avda. Somosierra, 22 Nave 4D
28709 S. Sebastián de los Reyes (Madrid)
Tel.: 913 831 920
Fax: 916 638 205
**www.saborit.com**

## VIGILANCIA Y CONTROL

**SECURITAS SEGURIDAD ESPAÑA**
C/ Entrepeñas, 27
28051 Madrid
Tel.: 912 776 000
email: info@securitas.es
**www.securitas.es**

**Grupo RMD**
Autorizada por la D.G.P. con el nº. 729
Avda de Olivares 17 – Plg. Industrial PIBO
41110 Bollullos de la Mitación (Sevilla)
Tlfno. 902194814 – 954108887
Fax. 954002319
gerencia@gruporomade.com
SERVICIOS EN TODA ESPAÑA



## TRANSPORTE Y GESTIÓN DE EFECTIVO

**LOOMIS SPAIN S. A.**
C/ Ahumaos, 35-37
Poligono Industrial La Dehesa de Vicálvaro
28052 Madrid
Tlf: 917438900
Fax: 914 685 241
**www.loomis.com**

# Detector Volumétrico de Exteriores de Triple Tecnología y Anti-masking

Pyronix
HIKVISION


# XDH10TT-AM

## Características

- Alcance 10m
- Tres frecuencias de microondas para anti-colisión
- Triple lógica de detección
- Triple tecnología de anti-masking
- Incluye lentes adicionales
- Fácil ajuste
- Tamper de tapa y de pared
- RFL para salidas de alarma, tamper y anti-masking
- Compensación digital de temperatura
- Regulación de alcance de microondas y anti-masking

Para recibir más información, regístrese aquí

HIKVISION

## UN PARTNER SÓLIDO, COMPROMETIDO, INNOVADOR, FIABLE, PRESENTE.

El valor de un partner tecnológico se mide por su capacidad de generar ventaja competitiva, así como por su actitud y el poder de transmitir determinación, entusiasmo, y motivaciones siempre nuevas. Hikvision garantiza profesionalidad, solidez empresarial, compromiso, fiabilidad tecnológica, innovación continua y un alcance global con presencia local.

**Hikvision Spain**
C/ Almazara, 9
28760 Tres Cantos (Madrid)
T +34 91 7371655
F +34 91 8058717
info.es@hikvision.com

www.hikvision.com