# CUADERNOS DE SEGURIDAD

Núm. 309 • MARZO 2016 • 10 euros

PUNTOSEGURIDAD.com

## Seguridad en casinos

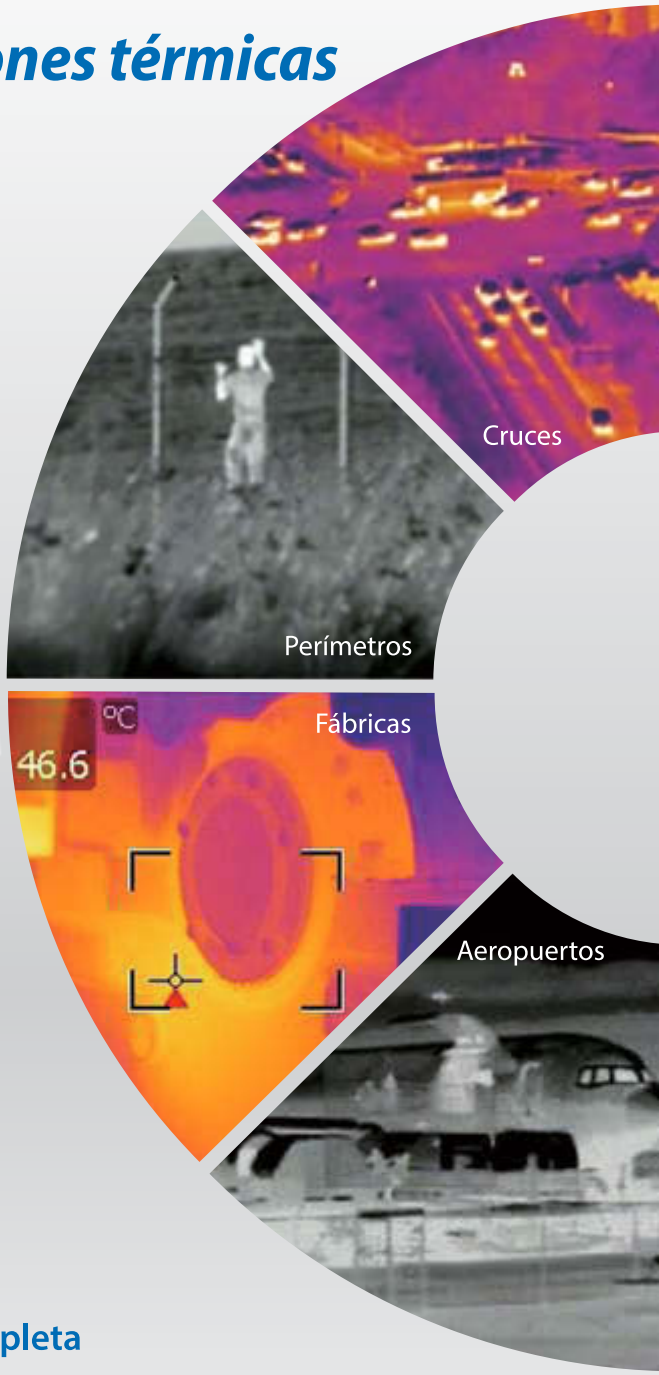
## Control de accesos

I Jornada Técnica
**RPAS y Seguridad Privada**

**Crónica del encuentro profesional**

# Detección en Oscuridad Total

## — *Soluciones térmicas*




- Análisis inteligente de vídeo
- Medición de temperatura
- Salida Tri-híbrida: IP/ HDCVI/ Analógico
- Solución & Monitorización Térmica Completa

España

Portugal

ISO 9001:2000


**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

## I JORNADA DE RPAS Y SEGURIDAD PRIVADA

# Retos y oportunidades a debate

Ante un aforo completo se celebró el pasado 4 de febrero en Madrid la I Jornada de RPAS y Seguridad Privada. El encuentro, organizado por Peldaño y la Federación Empresarial Española de Seguridad (FES), congregó a más de 170 profesionales, que han confirmado la consolidación de esta jornada de debate y análisis del presente y futuro de la utilización de los RPAS en el ámbito de la seguridad privada, así como de nuevo modelo de negocio en la industria de este sector.

La jornada sirvió de tribuna para poner de manifiesto el interés del sector de la Seguridad Privada por los usos y aplicaciones que ofrecen los RPAS a las soluciones y medidas de protección y seguridad. Isabel Maestre, directora de la Agencia Estatal de Seguridad Aérea (AESA), destacó el gran potencial de aplicaciones y económico del sector de los drones en España, en el que la «administración debe trabajar para favorecer su desarrollo con la seguridad como principal prioridad y adaptándose a las necesidades de las evoluciones tecnológicas». Tres fueron los actores principales de este encuentro profesional de debate: por un lado la administración, que debe establecer las garantías legales y normativa necesaria para el desarrollo y aplicación de esta tecnología en seguridad; la industria del sector de RPAS para que adapten sus especificaciones a su aplicación en seguridad, así como las propias empresas de servicios de seguridad para que puedan disponer de herramientas eficaces y eficientes para el cumplimiento de su cometido; y, finalmente, los usuarios, que deberán exigir todas las garantías necesarias para poder afrontar la contratación de estos nuevos sistemas.

El encuentro aglutinó un enriquecedor programa de ponencias y mesas de debate donde los profesionales pudieron intercambiar y compartir conocimientos y experiencias sobre el presente y futuro de la normativa de drones en España, así como la utilización de RPAS con fines de seguridad en entornos autorizados. Además se abordaron aspectos relacionados con las tipologías de RPAS y su adaptación a servicios de seguridad privada, la normativa de seguridad privada aplicada a la utilización de RPAS; o la responsabilidad civil y penal ante un incidente de seguridad.

Y, además, el equipo de Peldaño, continuando con su objetivo de servicio al sector, sigue trabajando en la organización de los contenidos y desarrollo de la cuarta edición de Security Forum, que se celebrará los días 25 y 26 de mayo en Barcelona, y que volverá a posicionarse como excepcional plataforma de networking donde atender las necesidades e intereses de un colectivo que demanda encuentros de estas características para revitalizar el tejido empresarial. El salón contará de nuevo con una zona de exposición –al cierre de esta edición ya estaba reservada más de la mitad del espacio– con áreas sobre CCTV, integración de sistemas, seguridad física, seguridad lógica, Ip/redes, y además, con dos sesiones diferenciadas en el congreso Security Forum: Global Day, dedicada a la seguridad global, donde los asistentes podrán descubrir desde una visión multidisciplinar aspectos de gran interés como son los *insiders*, el nuevo perfil del delincuente del siglo XXI o las últimas tendencias en coaching para departamentos de seguridad; y Ciber Day, centrada en la ciberseguridad con temas sobre la protección de la información, los delitos informáticos y amenazas en la protección de infraestructuras.


© Sebastian Duda / Dollar Photo Club


CUADERNOS DE SEGURIDAD

www.puntoseguridad.es

Nº 309 • MARZO 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 y 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, Anuario Mab Oro, www.puntoseguridad.com

# ABRIL 2016- Nº 310

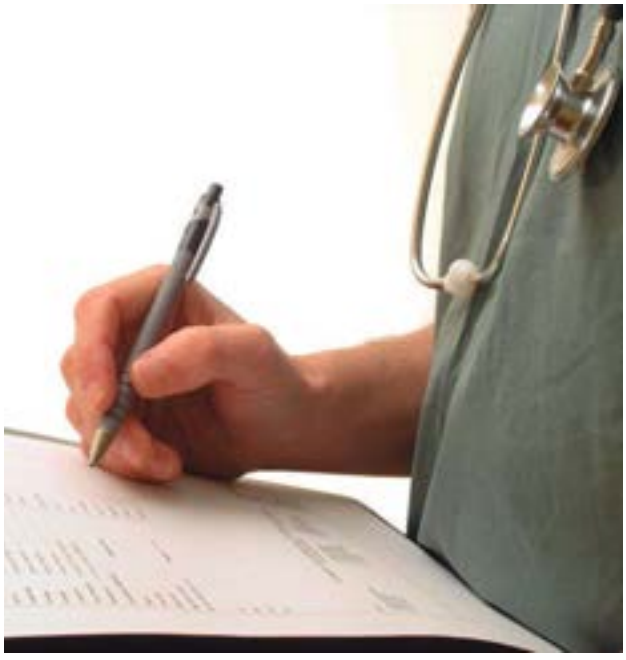
# EN PORTADA

## AVANCE SECURITY FORUM 2016

La organización de Security Forum 2016 sigue avanzando. El encuentro, que se celebrará los días 25 y 26 de mayo en el CCIB de Barcelona, contará con una zona expositora donde las empresas mostrarán las novedades, tendencias y avances tecnológicos en el campo de los equipos y soluciones de seguridad. Además se celebrarán dos días de ponencias y mesas de debate: Ciber Day y Global Day, donde reconocidos expertos compartirán con los asistentes su visión sobre el nuevo perfil del delincuente del siglo XXI, las últimas tendencias de coaching para departamentos de Seguridad o la protección ante las ciberamenazas y los nuevos retos ante la ciberseguridad.

## CRÓNICA SICUR 2016

IFEMA fue escenario del 23 al 26 de febrero de la celebración del Salón Internacional de la Seguridad SICUR 2016, donde se mostró un panorama global de las últimas novedades tecnológicas, productos, servicios y soluciones que ofrece el mercado internacional. Además, el contenido de SICUR se complementó con el desarrollo de un extenso programa de actividades, conferencias, presentaciones de productos, demostraciones, etc. En este contexto, se celebró Foro Sicur, un espacio de análisis y debate de los temas de máxima actualidad. En el próximo número, el lector encontrará un completo resumen de todo lo acontecido allí.



## SEGURIDAD EN HOSPITALES

Una coordinada labor de gestión, en la que la seguridad juega un papel imprescindible, es un factor decisivo en el adecuado funcionamiento de un centro hospitalario. Y es que, este tipo de instalaciones, además de contar con los medios necesarios para desempeñar su específica función, deben disponer también de medios y medidas de seguridad concretos que se dirijan a conseguir un nivel óptimo de seguridad... Una seguridad que se apoyará, como hemos reiterado desde estas mismas páginas, en un elemento fundamental: la tecnología. Las necesidades de estas instalaciones hospitalarias han variado y han sido, de manera concreta, las innovaciones tecnológicas las que han hecho posible contar con equipos y sistemas que ayudan a conseguir una adecuada seguridad en los centros hospitalarios.

Además de medios técnicos, es necesario contar con la labor de una figura que ha adquirido un papel imprescindible en la gestión de la seguridad: el director de Seguridad.

**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 |
|---|---|---|---|
| Aforsec | 87 | 986220857 | www.aforsec.com |
| Alai Secure | 37 | 902095196 | www.alaisecure.com |
| Arquero | 78 | 902544504 | www.arquero.es |
| ATA 98 | 105 | 931721763 | www.ata98.com |
| Binary | 3ª Cub | 911847606 | www.binary.com |
| Casmar | 70 | 933406408 | www.casmar.es |
| Cyrasa Seguridad | 23 | 902194749 | www.cyrasa.com |
| Dahua | 2ª Cubierta, 101 | 865718768883 | WWW.dahuasecurity.com |
| Dallmeier | 103 | 915902287 | www.dallmeier-electronic.com |
| Delta Informatica | 104 | 932151036 | www.deltainformatica.es |
| Digitek | 57 | 934774770 | www.digitek.es |
| Dorlet | 47 | 945298790 | www.dorlet.com |
| Eset | 106 | 902334833 | www.ontinet.com |
| Eulen Seguridad | 102 | 902355366 | www.eulen.com/es/seguridad |
| Eurocloud | 73 | 910113303 | www.eurocloudspain.org |
| Evva | 74 | 431811651227 | www.evva.com |
| FF Videosistemas | 59,64 | 902998440 | www.geutebruckspain.com |
| Flir Systems | 97 | 31765794190 | www.flir.es |
| Hikvision | 11,41,62,4ª Cubierta | 917371655 | www.hikvision.com |
| Ingram Micro | 101 | 902506210 | www.ingrammicro.com |
| Iseo | 89 | 918843200 | www.ise-iberica.eu |
| Kaba | 15,99 | 917362474 | www.kaba.es |
| LSB | 68 | 913294835 | www.lsb.es |
| Mecanizados Argusa | 25 | 934247545 | www.argusa.com |
| Mobotix | 35,98 | 911115824 | www.mobotix.com |
| Morse Watchmans | 13,66 | 1159671567 | www.morsewatchmans.com |
| Persax | 103 | 902010564 | www.persax.com |
| Rister | 100 | 934399244 | www.rister.com |
| Saborit | 103 | 913831920 | www.saborit.com |
| Samsung Techwin | 105 | 916517507 | www.samsungsecurity.co.uk |
| Security Forum | 9 | 914768000 | www.securityforum.es |
| Setelsa | 31 | 942544354 | www.setelsa.net |
| Siemens | 91 | 915148000 | www.siemens.es |
| STI Card | 80 | 913274474 | www.sticard.com |
| Talleres Aga | 104 | 943790922 | www.aga.es |
| Tesa | 51,76, 102 | 943669100 | www.tesa.es |
| Vanderbilt | 19,99 | 911799770 | www.vanderbiltindustries.com |
| Videofied | 106 | 33390206640 | www.videofied.com |
| Vigilant | 71 | 965856457 | www.vigilant.es |
| Visiotech | 17 | 911883611 | www.visiotech.es |
| Vivotek | 100 | 886282455282 | www.vivotek.com |

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


## ÍNDICE DE ANUNCIANTES

EL ENCUENTRO SE CELEBRARÁ EL 25 Y 26 DE MAYO EN BARCELONA

# Las empresas vuelven a apostar por Security Forum

**El área de exposición contará con un apartado denominado «Panel de Expertos», donde profesionales debatirán las últimas tendencias en soluciones de seguridad**

Las empresas del sector siguen reservando su espacio en el área de exposición de Security Forum 2016. A poco más de dos meses para la celebración del salón, los empresarios del sector vuelven a confiar en un formato novedoso donde dar a conocer sus soluciones e iniciativas innovadoras. Y además, consolidado como un foro de intercambio de conocimiento y debate, la organización da las últimas pinceladas al programa de expertos que formarán parte de las intervenciones y ponencias con las que se articulará Global Day y Ciber Day.

CONSOLIDADO ya como un espacio de networking, esta nueva edición sigue apostando por la innovación y los nuevos valores empresariales en el sector de la Seguridad. Y es que 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 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; etc.


## Global Day y Ciber Day

Y respecto al Congreso, cabe destacar que se desglosará por primera vez en dos sesiones diferenciadas:

– **Global Day**: la primera jornada estará dedicada a la seguridad global. Los asistentes podrán descubrir desde una visión multidisciplinar aspectos y perfiles de gran interés como son los insiders, el nuevo perfil del delincuente del siglo XXI, a cargo del doctor José Cabrera, experto psiquiatra forense, que analizará los rasgos psicológicos de una persona que comete un delito, la influencia del entorno y las circunstancias que le rodean, y los indicios que pueden ayudar a un responsable de Seguridad a detectar este tipo de comportamientos; o las últimas tendencias en coaching para departamentos de Seguridad, así como una Mesa de Debate sobre «El empleado infiel» y otra sobre legislación en Seguridad.

– **Ciber Day**: la segunda jornada se

Security FORUM

International Security Conference & Exhibition

**CCIB**
Centro de Convenciones Internacional de Barcelona

25 y 26 de mayo
BCN2016

# VER PARA CREAR

#SecurityForumBCN2016

www.securityforum.es
info@securityforum.es
+34 914 768 000
@SecurityForumES

IBERIA renfe

Peldaño


centrará en la ciberseguridad. Temas como la protección de la información, los delitos informáticos y los nuevos retos y amenazas en la protección de infraestructuras centrarán el debate de esta edición.

Además, sigue abierta la fecha de recepción de los **premios Security Forum**, que pretenden promover y potenciar la investigación, el desarrollo y la innovación de la industria de la seguridad en España, a través del reconocimiento a los responsables de proyectos actuales de investigación en materia de seguridad, y a aquellos proyectos de carácter significativo ejecutados, que puedan ser modelo y escaparate internacional del amplio potencial de nuestra industria.

En la categoría Premio Security Forum I+D+i puede participar cualquier miembro o equipo de investigación de departamentos de universidades o escuelas de negocio españolas y aquellos investigadores o estudiantes, cuyos trabajos de fin de carrera o actividad investigadora no esté ligada a ninguna actividad empresarial.

En el Premio Security Forum al Mejor Proyecto de Seguridad realizado en España tendrán derecho a participar empresas que formen parte del propio proyecto y directores de seguridad.

Los premiados tendrán la oportunidad de realizar una presentación de su proyecto durante la celebración de Security Forum 2016, y el acto de entrega de premios se realizará el 25 de mayo durante una cena-cóctel.

La dotación de los premios será:

- Premio Security Forum I+D+i:
  - –Primer Premio: cheque valorado en 3.000 euros + trofeo conmemorativo
  - –Finalista: Trofeo conmemorativo.
- Premio Security Forum al Mejor Proyecto de Seguridad:
  - –Primer Premio: Trofeo conmemorativo.
  - –Finalista: Trofeo conmemorativo.

Las memorias deben ser recibidas antes del día 31 de marzo de 2016. El fallo del jurado se producirá antes del 30 de abril. ●

*Fotos: **Xavi Gómez***

## Ficha técnica

**Fechas:** 25 y 26 de mayo de 2016.

**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

## 2 MEGAPÍXELES FULL HD
## CÁMARAS PARA LUMINOSIDAD ULTRABAJA
## UNA MIRADA PROFUNDA EN LA OSCURIDAD

Las características avanzadas Smart hacen posible que las nuevas cámaras Darkfighter Smart IP de Hikvision proporcionen imágenes excepcionalmente nítidas incluso en condiciones de baja luminosidad, tanto de día como por la noche. Al combinar un rendimiento extraordinario con una gran comodidad y facilidad de uso, estas cámaras sofisticadas están llevando la vigilancia de vídeo a un nivel completamente nuevo, siendo la opción de seguridad ideal para almacenes, grandes comercios, aeropuertos y otros lugares delicados.

smart 2.0

**Hikvision Europe**
Parellaan 24, 2132 WS Hoofddorp
The Netherlands
T +31 23 5542770
F +31 23 5631112
info.eu@hikvision.com

www.hikvision.com

ENCUENTRO ORGANIZADO POR LA FEDERACIÓN EMPRESARIAL ESPAÑOLA DE SEGURIDAD (FES) Y PELDAÑO

# RPAS y Seguridad Privada, **un mundo de oportunidades**

## Más de 170 profesionales acudieron el 4 de febrero en Madrid a la I Jornada Técnica «RPAS y Seguridad Privada», foro de análisis y debate sobre el uso y aplicaciones de estos dispositivos en el ámbito de la Seguridad Privada

Ante un aforo completo se desarrolló el pasado 4 de febrero en Madrid la «I Jornada de RPAS y Seguridad Privada», organizada por Peldaño y la Federación Empresarial Española de Seguridad (FES). Un encuentro profesional que puso de manifiesto el interés del sector de la Seguridad Privada por los usos y aplicaciones que ofrecen los RPAS (popularmente llamados drones) a las soluciones y medidas de protección y seguridad. Un espacio de debate y análisis que congregó tanto a representantes del ámbito público y privado de la seguridad, como a profesionales de la industria de RPAS, que analizaron el presente y futuro de la utilización de estos dispositivos con fines de seguridad privada, así como su implantación como nuevo modelo de negocio en la industria del sector de la Seguridad.

**Luis González Hidalgo, secretario general de FES; Iván Rubio, director del Área de Seguridad de Peldaño; Isabel Maestre, directora general de la Agencia Estatal de Seguridad Aérea (AESA); Ignacio Rojas, presidente de Peldaño; y José Manuel López, presidente de (FES).**

LA jornada –celebrada en el Auditorio de Cecabank–, que contó con la conferencia inaugural de Isabel Maestre, directora general de la Agencia Estatal de Seguridad Aérea (AESA), comenzó con las palabras de Iván Rubio, director del Área de Seguridad de Peldaño, quien destacó la importancia de propiciar espacios de encuentro sectorial donde se analicen las nuevas e innovadoras soluciones y medidas de protección y seguridad adaptadas a sistemas, servicios y metodologías del sector de la Seguridad Privada, industria y mercado, donde la tecnología es pilar fundamental. Tres fueron, según Rubio, los actores principales de este foro de debate: la Administración, estableciendo las garantías legales y normativa necesaria para el desarrollo de la industria y la aplicación de la tecnología en seguridad; la propia industria del sector, desde el I+D+i y los fabricantes de los equipos para que «adapten sus especificaciones a su aplicación en seguridad, y las empresas de servicios de seguridad para que puedan disponer de herramientas eficaces para el cumplimiento de su cometido»; y los usuarios, que «exigirán todas las garantías necesarias para poder afrontar la contratación de estos nuevos sistemas».

Acto seguido tomó la palabra José Manuel López, presidente de la Federación Empresarial Española de Segu-

# INTEGRADO

## Líderes en la evolución del control de llaves.

Desde un solo gabinete hasta una solución en red completamente integrada con el Internet de las Cosas, tenemos lo que necesita para proteger, controlar y rastrear cada llave de su empresa. Nosotros inventamos la administración de llaves, y seguimos mejorándola para usted.

Puerta del producto no aparece en la imagen.
Lector de huellas opcional.

**Visite morsewatchmans.com para saber más**

MORSE WATCHMANS

piense en la caja.

ridad (FES), que agradeció su presencia a los asistentes, profesionales que desmuestran un innato interés por el avance y nuevas tecnologías aplicadas al mundo de la seguridad. «Desde la Federación Empresarial Española de Seguridad (FES), siempre hemos apostado por las nuevas tecnologías», matizó

A lo largo de la jornada –en páginas siguientes el lector encontrará una detallada crónica sobre lo acontecido, así como una amplia galería de imágenes– se abordaron entre otros los siguientes temas: presente y futuro de la normativa sobre drones en España; tipología de RPAS y su adaptación a servicios de seguridad privada; centros de formación, licencias de operador y piloto: requisitos y capacitación; utilización de RPAS con fines de seguridad privada en entornos autorizados; normativa de seguridad privada aplicada a la utilización de RPAS; la responsabilidad civil y penal ante un incidente de seguridad; y la captación y transmisión de imágenes en RPAS y su utilización en seguridad privada. Además, el debate estuvo presente con dos interesantes mesas redondas sobre «La utilización de RPAS como nuevo modelo de negocio para el sector de la seguridad privada» y «Oportunidades y amenazas del uso RPAS para la seguridad». ●

*Fotos: Pedro Galán*

**Vista general de los profesionales asistentes a la I Jornada RPAS y Seguridad Privada.**

**Isabel Maestre, directora general de la Agencia Estatal de Seguridad Aérea (AESA), durante su intervención.**


**José Manuel López, presidente de la Federación Empresarial Española de Seguridad (FES), en su intervención a los asistentes.**


**Iván Rubio, director del Área de Seguridad de Peldaño, en su discurso de bienvenida.**


BEYOND SECURITY

KABA®

# Un único lenguaje: El de su seguridad

Todos sabemos que para hablar un idioma se necesita el vocabulario adecuado. Al igual que para un sistema de control de acceso se necesitan las herramientas y componentes adecuados.
En Kaba sabemos que no todas las puertas se abren y se cierran de la misma manera. Por esta razón, se desarrolló una solución capaz de integrar cualquier tipo de puerta, no importa si se trata de una puerta sencilla con una cerradura mecánica, una puerta con un control de acceso autónomo o una puerta conectada que requiere todo el potencial de un control de acceso a tiempo real.

**Iberkaba S.A.**
**María Tubau 4**
**28050 Madrid**
**Teléfono +34 902 224 111**
**Fax +34 902 244 111**
**info.es@kaba.com**
**www.kaba.es**

**ISABEL MAESTRE.** DIRECTORA DE LA AGENCIA ESTATAL DE SEGURIDAD AÉREA (AESA)

# «La normativa debe favorecer **el desarrollo del sector**»

**Isabel Maestre, directora general de AESA, inauguró la I Jornada profesional RPAS y Seguridad Privada con una ponencia titulada «Presente y futuro de la normativa de drones en España».**

DURANTE su intervención, Isabel Maestre remarcó la actual situación de apogeo que vive el sector de los RPAS, ofreciendo a las empresas una multitud de posibilidades y utilidades, siempre y cuando se utilicen de forma apropiada y guardando las debidas medidas de seguridad.

Directamente relacionado con esto, la directora de la Agencia Estatal de Seguridad Aérea (AESA) defendió que es imprescindible la profesionalización del sector de los drones para asegurar que el crecimiento que está experimentando se mantiene en el tiempo y crece de forma robusta.

La falta de conciencia social sobre los riesgos que entraña un mal uso de los drones es, para Maestre, uno de los grandes riesgos que puede poner freno al aparentemente imparable desarrollo del sector: no en vano la CE prevé que en un plazo de diez años el 10% del mercado de la aviación europea estará constituido por drones.


## La normativa que espera todo el sector

AESA desempeña un papel esencial, trabajando por el desarrollo de una normativa regulatoria completa, y apostando por profesionalizar el sector. La administración debe trabajar para favorecer el desarrollo del sector pero con la seguridad como principal prioridad y adaptándose a las necesidades de las evoluciones tecnológicas.

En ese sentido, Maestre indicó que el objetivo de AESA es impulsar y promover el desarrollo de la industria de drones en España, pero ésta siempre tiene que ir acompañada de la mejora de la seguridad, tanto de la seguridad aérea como la de la ciudadanía cuando se realizan operaciones con drones.

La legislación de las aeronaves pilotadas por control remoto debe ser coherente con el ámbito internacional. Se prevé que Europa tenga un reglamento al respecto en un plazo de 3 años. Actualmente, Isabel Maestre recordó que España cuenta con la Ley 18/2014, de 15 de octubre, que es un régimen transitorio, pero que está en línea con el resto de los países europeos que cuentan con legislación y está sirviendo de base para la futura norma europea. Está tramitándose un nuevo Real Decreto que dote al sector de un marco regulatorio y que cumpla los dos objetivos ya mencionados: la profesionalización del sector y asegurar un crecimiento robusto del mismo.

HomeControl+

Pyronix Cloud

# Pyronix®

www.pyronix.com

Pyronix ofrece una amplia gama de equipamientos cableados e inalámbricos EN50131 aprobados en Grado 2 y 3.

## SERIE XD

Inalámbrico/Cableado

GPRS o LAN

ENFORCER

tecnología inalámbrica bidireccional

## Serie KX

Inalámbrico/Cableado

## Serie Deltabell

Inalámbrico/Cableado

## Serie PCX

Technologia Cableada

VISIOTECH

Avenida del Sol 22,
28850, Torrejón de Ardoz (España)
Telf.: 911 836 285
comercial@visiotech.es

www.visiotech.es

**LORENZO DÍAZ DE APODACA.** CEO DE AIRESTUDIO GEOINFORMATION TECHNOLOGIES

# «El **uso, la superficie de trabajo** y la autonomía son aspectos a tener en cuenta a la hora de **elegir un dron**»

## Tipología de RPAS y su adaptación a servicios de Seguridad Privada

BAJO el título «Tipología de RPAS y su adaptación a servicios de Seguridad Privada», Lorenzo Díaz de Apodaca, CEO de Airestudio Geoinformación Technologies, intervinó en la I Jornada RPAS y Seguridad Privada, celebrada en Madrid el pasado 4 de febrero, donde llevó a cabo una académica exposición sobre las tipos de drones y sus elementos básicos, los factores a tener en cuenta para su utilización, así como su implantación en los servicios de seguridad privada.

### Tipos de drones

Tras analizar, a modo de introducción, el concepto de dron como «vehículo aéreo capaz de navegar de forma autónoma sin intervención humana», Díaz de Apodaca detalló los diferentes tipos de drones por uso (militar, civil: recreacional/ocio y profesional), por formato (tipo copter y ala fija) y por peso (menos de 2 kg, entre 2 y 2,5 kg, y entre 25 y 150 kg), y explicó de manera detallada aquellos elementos básicos de este tipo de dispositivos para, acto seguido, aclarar que es «indispensable conocer la aplicación en la que vamos a utilizar el dron, ya que no todos los equipos valen para todo», factor también relacionado con la superficie sobre la que se va a trabajar, la autonomía o tiempo de que se dispone en cada operación para la captura de datos, y la carga de peso.

Y es que tal y como apuntó «el dron es una herramienta que nos va a permitir conseguir un fin».


### De forma integrable

Desglosó los elementos a tener en cuenta para poder llevar a cabo un trabajo «todo de forma personalizable, integrable y escalada», entre los que destacó sensores adecuados a los objetivos, sistemas de comunicación y/o almacenamiento, software de tratamiento y análisis, sistemas de navegación para georeferenciación de datos, etcétera.

Lorenzo Díaz de Apodaca hizo hincapié en que no se debe confundir datos con información. «La información son datos procesados y analizados, es el punto de partida indispensable para no equivocarnos en la toma de decisiones». Además apuntó que desde su compañía se da una gran importancia a facilitar la utilización de esos datos por el cliente, es decir, hacerlos no solo útiles sino usables. ●

*Fotos: Pedro Galán*

# Acuda al mejor equipo de seguridad

VANDERBILT

## Un nuevo nivel de protección

Cuente con el mayor fabricante independiente de seguridad del mundo para ofrecerle protección total allí donde la necesite. Estará en las mejores manos gracias a nuestros 30 años de experiencia, productos innovadores y fiables y una completa asistencia técnica y comercial.

Aproveche los beneficios de trabajar con una empresa independiente, con un equipo que le proporciona una respuesta rápida y una flexibilidad en cualquier situación.

INTRUSIÓN | CONTROL DE ACCESOS | CCTV

**www.vanderbiltindustries.com**

**TONI CABALLERO.** COMMERCIAL MANAGEMENT & CO-FOUNDER. TSA CENTER

# «Una **correcta formación** es el elemento clave para el **piloto de RPAS**»

## Centros de formación, licencias de operador y piloto. Requisitos y capacitación

LOS requisitos que han de cumplir los pilotos y los operadores, así como las capacitaciones extraordinarias y/o específicas y el papel que desarrollan las ATOS (Approved Training Organization) fueron los aspectos sobre los que se centró la intervención de Toni Caballero, Commercial Management & Co-founder de TSA Center, en el marco de la I Jornada de RPAS y Seguridad Privada celebrada en Madrid.

### Marco regulatorio

«El sector ha crecido y se ha desarrollado con la legislación», fueron sus primeras palabras al hacer referencia al marco regulatorio actual en nuestro país –Ley 18/2014 de 15 de octubre– haciendo especial hincapié en el Apéndice I, revisión 2 donde se recogen los «Medios aceptables para acreditar el cumplimiento de los requisitos para la formación y certificación de los pilotos que operan aeronaves pilotadas por control remoto». El ponente detalló los requisitos teóricos:

– Licencias y certificados genéricos no específicos para RPAS (licencias de piloto, vigentes o haberlo estado hasta un máximo de 5 años antes de su presentación), acreditaciones de conocimientos teóricos, y licencias militares de pilotos al servicio de las Fuerzas Armadas Españolas y la Guardia Civil.

– Certificados específicos para RPAS (curso de formación básica y curso de formación avanzada).


Y ante la pregunta ¿quién puede expedir un certificado de aptitud para el pilotaje de RPAS?, Caballero fue contundente al explicar que solo podrán ser emitidos por un ATO. «Únicamente las organizaciones de formación –ATOs– aprobadas por la Agencia Estatal de Seguridad Aérea (AESA) pueden impartir los cursos para la obtención de los certificados para pilotar RPAS. La adecuada formación es elemento clave para el piloto de RPAS. Y es que la seguridad tiene que ser prioritaria en este sector».

Acto seguido el ponente pasó a detallar las materias y conocimientos que engloba la formación práctica de un futuro piloto de RPAS. Un curso que tiene como objetivo el conocimiento de la aeronave que vaya a operar el alumno y su equipo de control, y en el que además de la instrucción en vuelo incluirá un mínimo de 20 despegues y aterrizajes, así como una prueba de vuelo presencial, entre otros aspectos.

Para finalizar, Caballero enumeró los requisitos que han de cumplir los pilotos, así como los operadores.

*Fotos: Pedro Galán*

**ANDRES SANZ.** CORONEL. JEFE INTERINO DEL SERVICIO DE PROTECCIÓN Y SEGURIDAD (SEPROSE). GUARDIA CIVIL

# «Las Infraestructuras Críticas deberían poder disponer de RPAS»

## Utilización de RPAS con fines de seguridad privada en entornos autorizados

LA experiencia en el uso de RPAS por parte de la Guardia Civil, sirvió como elemento de referencia a la intervención de Andrés Sanz, Coronel. Jefe Interino del Servicio de Protección y Seguridad de la Guardia Civil (SEPROSE), sobre «Utilización de RPA´s con fines de Seguridad Privada en entornos autorizados», dentro de la I Jornada Técnica de RPAS y Seguridad Privada. «Lo que puede ser utilizado para la seguridad pública –señaló–, lo puede ser para la privada», si bien matizó que las actuales limitaciones técnicas y legales, son los principales condicionantes para el uso de esta tecnología en el ámbito de la Seguridad Privada.

Tras enumerar los entornos autorizados para el uso de RPAS en función de las características del equipo, del lugar, así como del peso, entre otros aspectos, el ponente explicó algunas de las posibilidades futuras de utilización de estos dispositivos, si bien mostrando la cautela precisa hasta la aprobación del futuro marco normativo ahora en proyecto.

### Entornos operativos en la Guardia Civil

Catástrofes, control de masas, vigilancia de zonas sensibles, control de fronteras, seguimiento de eventos, o control de fronteras, son algunos de los entornos operativos en los que la Guardia Civil ha utilizado este tipo de tecnología a través de sus diferentes servicios y agrupaciones. El capitán Carlos Nuñez del Grupo de Acción Rápida, acompañado del Cabo 1° Najera, piloto de drones, narraron su experiencia con el uso de estos dispositivos en operaciones concretas, y destacaron, entre otras conclusiones la no existencia de un único sistema capaz de adecuarse a todos los requerimientos de las diferentes unidades de la Guardia Civil, diferentes escenarios requieren diferentes capacidades de los sistemas o que los RPAS, equipados con adecuados sensores, pueden aumentar las capacidades de detección, seguimiento e identificación.

Andrés Sanz destacó aquellas actividades de Seguridad Privada, actividades compatibles, así como aquellos servicios coordinados por las FF y CC. de Seguridad en los que cabría la posibilidad de utilización de RPAS, para concluir matizando que en el caso de Infraestructuras Críticas «debería poder contar con estos medios».

*Fotos: Pedro Galán*

**ANSELMO MURILLO.** INSPECTOR JEFE. JEFE DE LA SECCIÓN DE INSPECCIÓN DE LA BRIGADA CENTRAL DE INSPECCIÓN E INVESTIGACIÓN. UNIDAD CENTRAL DE SEGURIDAD PRIVADA. CUERPO NACIONAL DE POLICÍA

# «Las aplicaciones en **seguridad privada** son infinitas, pero siempre bajo el **marco legal**»

## «Normativa de Seguridad Privada aplicada a la utilización de RPAS»

LA normativa de Seguridad Privada: aplicación a la utilización de RPAS, fue el tema central de la intervención de Anselmo Murillo, inspector jefe. Jefe de la Sección de Inspección de la Brigadad Central de Inspección e Investigación de la Unidad Central de Seguridad Privada del Cuerpo Nacional de Policía, en el marco de la I Jornada Técnica RPAS y Seguridad Privada.

Tras exponer a grandes rasgos el concepto de dron –«Aeronave no tripulada», sus aplicaciones –múltiples y dependientes de los dispositivos que se acoplen a este tipo de vehículos: cámaras fostográficas, vídeo, GPS...–, así como su ámbito de regulación, el ponente hizo hincapié en las aplicaciones en el ámbito de la Seguridad Privada, abordando las actividades específicas recogidas en el art. 5.1 de la Ley de Seguridad Privada; actividades compatibles, en el art. 6 de la LSP; y las actividades a nivel de usuarios –actividades excluidas y autoprotección–, recogidas en los artículos 7 y 51.8 de la LSP: «Las aplicaciones en el ámbito de la seguridad privada son infinitas, pero siempre en el marco legal», matizó Murillo.

Acto seguido, Anselmo Murillo abordó los servicios de videovigilancia conformados por aquellos medios, cámaras, videocámaras o cualquier otro elemento técnico, capaces de captar y grabar imágenes y sonidos, y cuya finalidad, según explicó, es vigilar para «prevenir infracciones, evitar daños a las personas o bienes objeto de protección e impedir accesos no autorizados».

«Los sistemas de vídeo –añadió–son la máxima aplicación de los drones». Y ¿quiénes pueden prestar estos servicios?, los vigilantes de seguridad y guardas rurales en el ejercicio de sus funciones legalmente reconocidas.

Murillo insistió en que el uso de cámaras con drones debe desarrollarse bajo los principios de proporcionalidad, idoneidad e intervención mínima, así como que las grabaciones no deben destinarse a otro uso, la obligación de conservarlas y custodiarlas, así como de entrega inmediata a las Fuerzas y Cuerpos de Seguridad o autoridades judiciales.

Por otro lado, analizó los aspectos relevantes en cuanto a su utilización por parte de las empresas de seguridad, donde insistió en que el controlador de las aeronaves en servicio, vigilante de seguridad o guarda rural, debe tener licencia o título propio, así como las funciones a desarrollar por las diferentes unidades de seguridad privada, entre las que expuso, el control preventivo del intrusismo, control del ámbito territorial autorizado a la empresa, y la constatación documental de homologaciones y autorizaciones de las aeronaves por organismos competentes, y comunicación, en su caso, de aquellas irregularidades detectadas.


*Fotos: Pedro Galán*

# CYRASA

## ALQUILER DE EQUIPAMIENTOS PARA EVENTOS

**Alquiler de equipos por días-mes-año**

Ofrecemos servicio de consultoría, instalación y puesta a punto de sistemas de grabación digital de alta calidad, domos, cámaras, cámaras inalámbricas, cámaras simuladas, monitores, soportes y cableados. Supervisado por nuestros técnicos en el lugar si así lo requieren, servicio de desarme y retiro del equipamiento.

**✓ Cobertura nacional**

### ESPECIALISTAS

- Exposiciones
- Controles continuos
- Controles discontinuos
- Cadenas de montaje
- Cadenas de producción

### ABSOLUTO COMPROMISO

- Calidad y medio ambiente
- Última tecnología
- Servicio profesional
- Asistencia técnica y trato personalizado

### OTROS SERVICIOS:

- Control de masas
- Vigilantes de Seguridad
- Control de accesos y CCTV
- Drones patrulla NOVEDAD*

**¡¡Contacte con nosotros!!**

**cyrasa@cyrasa.com**

Polígono Industrial Sepes Carretera de Motilla- Calle Arcas nº 3 Cuenca 16004

CYRASA

Polígono Industrial SEPES
C/ Arcas, nº 3
16004 CUENCA
www.cyrasa.com

Tel. Oficinas 902 194 749
C.R.A. 902 033 222
Fax 969 230 623
cyrasa@cyrasa.com

**MERITXELL CODINA.** CONSEJERA DELEGADA DE EURANIA, PERITO Y CONSULTORA AERONÁUTICA

# «El sector debe **profesionalizarse**»

## La consejera delegada de Eurania resalta la importancia de garantizar la seguridad y el cumplimiento de la ley en los servicios con aeronaves no tripuladas

MERITXELL Codina abrió su conferencia sobre "La responsabilidad civil y penal ante un incidente de Seguridad" asegurando que la llegada de los RPAS es una revolución, una revolución que avanza rápidamente y que se convierte en evolución de un sector que ha emergido con mucha fuerza y con ganas de romper.

Pero dentro de esta rápida sucesión de acontecimientos, surge la cuestión de la responsabilidad por parte de las empresas de Seguridad privada que empiezan a operar en un ámbito hasta el momento reservado al sector aeronáutico.

La consejera delegada de Eurania, alertó sobre la responsabilidad que debe tener el sector de la seguridad privada que quiera ofrecer servicios con drones y la seguridad que deben cumplir en los servicios con aeronaves no tripuladas con fines civiles y comerciales.

Codina alertó que a las operaciones y servicios que pretendan realizarse desde el sector de la Seguridad Privada con drones se les aplicará la Ley 18/2014 que regula las operaciones con aeronaves no tripuladas con fines civiles y comerciales. Pero también deberán cumplir, además de todo lo relacionado con su propio ámbito de actuación, "aquellos requisitos establecidos por la Agencia Estatal de Seguridad Aérea (EASA)" que, recordó, son "de obligado cumplimiento y exigidos a las empresas operadoras de drones para obtener la habilitación correspondiente".

¿Qué responsabilidades debe tener el sector de la seguridad privada en el manejo de drones? Codina apuntó a la responsabilidad derivada directamente de una utilización indebida de aeronaves en la que se pueda incurrir en infracciones contra la seguridad de la aviación. Pero también responsabilidades civiles y penales (por ejemplo ante la revelación de secretos o los daños físicos o materiales causados a terceros), además de los derechos fundamentales y libertades públicas recogidas en la Constitución (derecho al honor, a la intimidad personal y familiar, y a la propia imagen y a la inviolabilidad del domicilio).


"Garantizar la seguridad de las operaciones en todos los aspectos es la clave para que el sector pueda desarrollar todo su potencial", aseguró.

La consejera delegada de Eurania resaltó el "potencial incalculable por desarrollar" que tiene el sector de los RPAs (drones) y las "múltiples aplicaciones" que puede tener en el ámbito de la Seguridad Privada". Asimismo, Codina defendió que se tiene que "dar un paso más allá para profesionalizarse".

Codina apuntó que el "gran reto" y "la clave" para emplear los drones es conseguir que vuelen de forma segura y, ello se consigue "con la tecnología y con el personal cualificado". La directora de Eurania remarcó que en la actualidad hay muchos pilotos de drones "pero pocos de ellos están realmente cualificados". "Formación escasa, o muy justa, con pocas horas de vuelo y por ende, con poca destreza, ya que esta aumenta con la experiencia", remarcó Codina, que considera que los pilotos se acabarán especializando y tendrán ventaja los que tengan más experiencia.

26-28
ABRIL
2016
STAND 1239

EXPO SEGURIDAD

CONTROL DE ACCESOS

ARGUSA
CONTROL DE ACCESOS

# MÁS DE 30 AÑOS

## FABRICANDO LAS MEJORES SOLUCIONES

WWW.ARGUSA.COM

**Fábrica y oficinas** Avda. de los Trabajadores, s/n - Pol.Ind. Los pradillos, Parcela 2 Ctra. de toledo A-42 , Salida 35 Illescas(Toledo 45200) – España **Tlf.:+34 925 501 719**
**Delegación Barcelona** Avda. Roma, 142 Local 1 Barcelona 08011 – España **Tlf: +34 93 424 75 45**
**Mexico** C/ Dante, 36 Oficina 702 Col. Anzures ( Del. Miguel Hidalgo ) 06030 – México DF - México **Tlf.:+52 (55) 5546 7815**

**Manuel Oñate.**
Presidente de la asociación española de rpas (AERPAS)

**Raúl Beltrán.**
Presidente de la asociación profesional de guardas jurados de caza.

**Jorge Rodríguez.**
Vocal de la junta directiva de fes.

# Las empresas piden una ley más flexible para incorporar el uso de **RPAS**

## Mesa de Debate: La utilización de RPAS como nuevo modelo de negocio para el sector de la Seguridad Privada

LAS actuales limitaciones legales son, a juicio de las empresas, el principal escollo para obtener pleno rendimiento de la aplicación de la tecnología de RPAS al negocio de la seguridad privada. En esta idea central coincidieron los representantes del sector que participaron en la mesa-debate «La utilización de RPAS como nuevo modelo de negocio para el sector de la Seguridad Privada», dentro de la I Jornada Técnica RPAS y Seguridad Privada.

En palabras de Jorge Rodríguez, vocal de la Junta Directiva de FES, «hay campo para hacer cosas, pero la normativa está en fase embrionaria y eso lastra el potencial comercial que se puede obtener». «Al cliente final no le interesa contratar los servicios de RPAS por las limitaciones que impone la ley», apuntó Rodríguez, para quien esta situación «continuará así mientras la normativa actual sea transitoria y no haya desarrollo reglamentario».

Para el representante de FES es clave que «técnica y legislación vayan de la mano» para avanzar en el aprovechamiento comercial de los RPAS en servicios de seguridad privada y responder así a la «curiosidad» que existe entre los usuarios.

Vista general de la Mesa de Debate.

### Una oportunidad..., un problema

Las mismas reservas mostró Raúl Beltrán, presidente de la Asociación Nacional de Guardas Jurados de Caza, para quien la utilización de RPAS «puede ser una oportunidad pero también será un problema». Beltrán reconoció que desde su entidad «estamos expectantes viendo cómo influye» esta tecnología, ya que, en su opinión, «aún es pronto hablar de RPAS en Seguridad Privada».

El punto discordante lo puso Manuel Oñate, presidente de la Asociación Española de RPAS (AERPAS), para quien aludir a la legislación como una limitación «es una excusa para el 'Que inventen ellos', ya que el problema es la falta de visión de negocio». En este sentido, animó a las empresas a «trabajar en el desarrollo de aplicaciones, porque los RPAS constituyen una oportunidad sin explorar», a lo que unió que «en verano ya habrá un escenario normativo más claro». «Hay que ponerse a trabajar, ver qué cosas se pueden hacer, si merece

Manuel Oñate, presidente de la Asociación Española de RPAS (AERPAS).

Jorge Rodríguez, vocal de la Junta Directiva de la Federación Empresarial Española de Seguridad. (FES).

la pena tener un RPAS y si eso aporta valor», recalcó Oñate, quien no dudó en afirmar que esta tecnología va a ser «una revolución» para el sector, «como lo fue en su día la aparición de las cámaras de CCTV».

## Campos de aplicación de los RPAS

Entre los campos de aplicación de los RPAS en el sector la seguridad privada, el vocal de FES Jorge Rodríguez destacó «las infraestructuras críticas, las fincas, las canteras, las minas y las superficies comerciales, siempre que estén cerradas, para optimizar el uso de vigilantes».

Respecto a su empleo en zonas abiertas, Raúl Beltrán afirmó que los RPAS «darán opción a modificar el binomio espacio-tiempo en la forma de reaccionar ante un incidente», mientras que Manuel Oñate subrayó como una de las utilidades claras de estos aparatos el poder actuar «siempre que el desplazamiento de un vigilante entrañe peligro, como ya ocurre en el ámbito militar».

Para hacer frente a las posibles amenazas que pueda suponer el uso de RPAS en seguridad privada, Rodríguez incidió en la necesidad de «elaborar un catálogo de riesgos» y de que los profesionales del sector «cuenten con una formación específica» en el manejo de estos dispositivos. A este respecto, Beltrán recordó que un RPAS «puede violar la ley de protección de aves, lo que ocasiona a los guardas problemas a la hora de defenderse de RPAS mal utilizados».

Durante la mesa debate también se puso de manifiesto la conveniencia de que las empresas de seguridad privada denuncien a quien contrate operadores de drones para hacer servicios ilegales, aunque la actual legislación ya permite a las Fuerzas y Cuerpos de Seguridad del Estado actuar de oficio ante cualquier posible infracción. ●

*Texto: Emilio. S. Cófreces*

*Fotos: Pedro Galán*

Raúl Beltrán. Presidente de la Asociación Profesional de Guardas Jurados de Caza.

**ANDRÉS CALVO MEDINA.** JEFE DE ÁREA. RESPONSABLE DE SEGURIDAD DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AGPD)

# La UE reforzará la **protección de datos** en el uso de RPAS

## La captación y transmisión de imágenes en RPAS y su utilización en Seguridad Privada

EL nuevo reglamento europeo de protección de datos contribuirá a reforzar el control legal del uso de RPAS en tareas de videovigilancia. La norma, aplicable en países de la UE, obligará a que el diseño de estos dispositivos se efectúe teniendo en cuenta el impacto de su uso en la privacidad y en los derechos de los ciudadanos, y a que se realice un análisis previo de los riesgos que supone su utilización para la correcta captación y tratamiento de los datos personales que recoja.

Por datos personales se entiende, según reza la Ley Orgánica de Protección de Datos (LOPD), «cualquier información concerniente a personas físicas identificadas o identificables». Así lo expuso Andrés Calvo, jefe de Área Responsable de Seguridad de la Agencia Española de Protección de Datos (AGPD) durante la ponencia «La captación y transmisión de imágenes en RPAS y su utilización en seguridad privada» que ofreció durante la I Jornada Técnica RPAS y Seguridad Privada.

El nuevo texto legal recoge las sugerencias del Grupo de Trabajo del Art. 29 (compuesto por representantes de todas las autoridades de protección de datos de la UE, el SEPD y la Comisión Europea). Entre ellas, incorpora la creación de un responsable de protección de datos (DPO). El grupo del artículo 29 también considera clave ofrecer información y transparencia a los ciudadanos sobre las operaciones, garantizar la seguridad de los datos y la proporcionalidad en su conservación, reforzar la cooperación entre las autoridades aéreas y las de protección de datos así como elaborar un código de conducta o de buenas prácticas.

Para lograr estos objetivos, Calvo señaló que el organismo europeo apuesta por la «concienciación de operadores, fabricantes y pilotos y de todo el personal implicado en las operaciones». En este sentido, el Grupo de Trabajo aconseja que el fabricante informe al comprador del dispositivo en relación al impacto sobre la privacidad derivado de su uso. Además, apunta como deseable que la protección de datos y la privacidad se integren en la formación de pilotos, así como en las normativas de regulación del sector y en programas de certificación.

Calvo recordó que «no existe un marco legitimador distinto para las operaciones con RPAS que implican un tratamiento de datos personales». Ese marco, según indicó, lo determina la propia LOPD, así como la Ley Orgánica de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. No obstante, recalcó que los RPAS presentan «un mayor riesgo de impacto sobre la privacidad y el tratamiento de datos que las aeronaves tradicionales».

Por ello, el experto de la AGPD consideró que el respeto a las normas de protección de datos busca fomentar la confianza de los ciudadanos en estos dispositivos, lo cual «es una garantía fundamental para el desarrollo de la industria y las operaciones con RPAS». ●

*Emilio S. Cófreces*

**Francisco Poley.** Presidente de la asociación de directivos de seguridad integral (ADSI)

**Francisco Lázaro.** Director del centro de estudios en movilidad. (CEM). ISMS FORUM.

**Ildefonso Polo.** Secretario general de la asociación española de directores de seguridad (AEDS)

**Alfonso Castaño.** Vicepresidente de ASIS España

# RPAS, una **realidad en el sector de la seguridad**

## Oportunidades y amenazas del uso de RPAS para la Seguridad

LOS drones son una realidad. Han llegado al sector de la seguridad para quedarse, y será necesario hacer un uso responsable de esta tecnología». Esta fue una de las conclusiones que puso el broche final a la mesa de debate que sobre «Oportunidades y amenzas del uso de RPAS para la seguridad» se desarrolló en el marco de la I Jornada de RPAS y Seguridad Privada celebrada el pasado 4 de febrero en Madrid.

A lo largo de más de una hora diversos expertos analizaron en un interesante y ameno coloquio las posibilidades de uso de esta tecnología, así como los diferentes riesgos y amenazas a los que está expuesta, en el ámbito de la seguridad. Entre los participantes a la mesa, que fue moderada por Luis González Hidalgo, secretario general de la Federación Empresarial Española de Seguridad (FES), se encontraban Francisco Poley, presidente de la Asociación de Directivos de Seguridad Integral (ADSI); Francisco Lázaro, director del Centro de Estudios en Movilidad (CEM) del ISMS Forum; Ildefonso Polo, secretario general de la Asociación Española de Directores de Seguridad (AEDS), así como Alfonso Castaño, vicepresidente de ASIS España.

**Vista general de la Mesa de Debate «Oportunidades y amenazas del uso de RPAS para la seguridad».**


Los ponentes destacaron las posibilidades que ofrece hoy en día esta tecnología en el ámbito de la seguridad, si bien matizaron, que la legislación actual restringe mucho su utilización.

En este sentido Alfonso Castaño, vicepresidente de ASIS España, insistió en las «posibilidades reales de aplicación de los drones, como es el caso de grandes superficies comerciales, estadios de fútbol,... Podrían realizar incluso las rondas de patrulla que realiza un vigilante de seguridad».

De la misma opinión se manifestó Ildefonso Polo, secretario general de la Asociación Española de Directores de Seguridad (AEDS) para quien, reiteró, si la legislación lo permitiese, esta tecnología «sería ideal para superficies grandes, infraestructuras ferroviarias,... Además, hoy la tecnología nos permite manejar desde un centro de control un dron para que haga rondas de patrulla».

Para Francisco Poley, presidente de la Asociación de Directivos de Seguridad Integra (ADSI), la utilización de este tipo de dispositivos incrementaría el sistema de seguridad de una instalación, como sería el caso de un centro comercial, pero fuera del horario

de apertura al público, «ya que si no supondría un riesgo para las personas».

Francisco Lázaro, director del Centro de Estudios en Movilidad (CEM) del ISMS Forum mostró su convicción de que esta tecnología dispondrá de múltiples aplicaciones, pero insistió que «el adecuado desarrollo de RPAS pasa por la seguridad».

Las vulnerabilidades y amenazas fue otro de los aspectos tratados a lo largo del foro de debate, donde los ponentes pusieron sobre la mesa aspectos como la utilización fraudulenta, el secuestro de drones, e incluso la dinámica actual de consumo masivo de este tipo de dispositivos... En este sentido, Francisco Lázaro matizó que estamos ante vulnerabilidades similares a las presentes en otras tecnologías. «Los sistemas embutidos dentro de los drones son igual de vulnerables que otros sistemas», explicó, al tiempo que insistió en que «es más fácil atacar que defender». Por ello hizo hincapié en la importancia de la concienciación y sensibilización en la seguridad de la información. Opinión compartida por Alfonso Castaño, para quien es preciso hacer un uso responsable de esta tecnología.

Para Francisco Poley otro de los aspectos que más dificultades plantea a la hora de utilizar estos dispositivos es la ausencia de una normativa acorde a las necesidades de un sector, el de la seguridad, en el que la tecnología juega un papel fundamental. «La tecnología va siempre por delante de la legislación. Es necesario dar una respuesta rápida al sector de la seguridad privada en estas nuevas aplicaciones».

Para finalizar Ildefonso Polo apuntó que «los drones son ya realidad en el sector de la seguridad» ●

**Alfonso Castaño, vicepresidente de ASIS España.**

**Ildefonso Polo, secretario general de la Asociación Española de Directores de Seguridad (AEDS).**

**Francisco Poley, presidente de la Asociación de Directivos de Seguridad Integral (ADSI).**

**Francisco Lázaro, director del Centro de Estudios en Movilidad. ISMS Forum.**

*Fotos: Pedro Galán*

Luis González Hidalgo, secretario general de la FES; Iván Rubio, director del Área de Seguridad de Peldaño; Isabel Maestre, directora general de la Agencia Estatal de Seguridad Aérea (AESA); Ignacio Rojas, presidente de Peldaño; y José Manuel López, presidente de (FES).

Carmen Moraleda, representante de la Guardia Civil; Juan Muñoz, presidente de ASIS-España; Ana Aisa, gerente de ACAES; Paloma Velasco, directora ejecutiva de AES; y Gemma G. Juanes, redactora-jefe de Cuadernos de Seguridad.

Lorenzo Díaz de Apodaca, CEO de Airestudio Geoinformation Technologies (primero por la dcha), junto a algunos de los asistentes a la jornada.

Toni Caballero, comercial management & Co-founder. TSA Center, que participó en la jornada con una ponencia (segundo por la izq), junto a Luis González Hidalgo, y otros asistentes al encuentro profesional.

Andrés Calvo Medina. Jefe de Área. Responsable de Seguridad de la Agencia Española de Protección de Datos (AGPD).

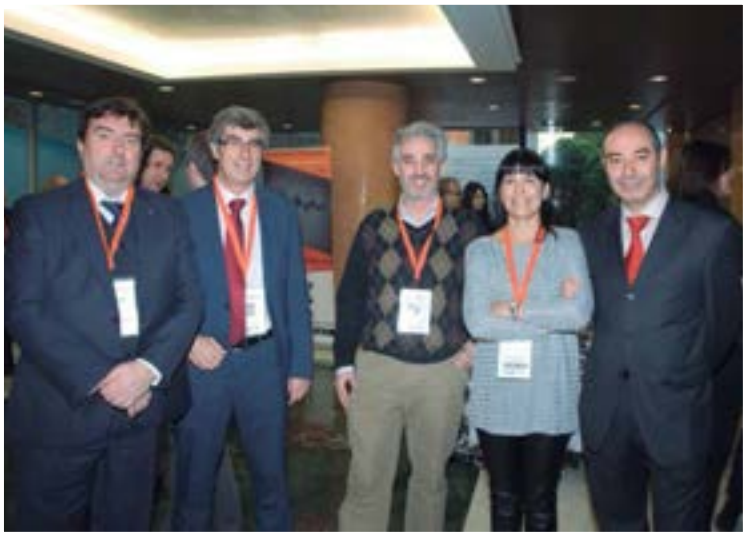
Meritxell Codina, consultora aeronáutica y CEO de Eurania (en el centro de la imagen), junto a Gemma G. Juanes, redactora jefe de Cuadernos de Seguridad, y Arantxa García, consultora del Área de Seguridad.

Un momento de la Mesa de Debate «Oportunidades y amenazas del uso de RPAS para la Seguridad».

Integrantes de la Mesa de Debate «La utilización de RPAS como nuevo modelo de negocio para el sector de la Seguridad Privada», tras sus intervenciones.

José Manuel López, presidente de FES, en animada charla con Andrés Sanz. Coronel. Jefe interino del SEPROSE, de la Guardia Civil.

Segundo Pareja, jefe de Seguridad del CC Tres Aguas (Madrid), Francisco Javier Domingo, gerente comercial de Seguriber; Miguel Ángel Gallego, director de Seguridad de Estación Sur de Autobuses (Madrid); Gemma G. Juanes, redactora jefe de Cuadernos de Seguidad; y Juan Carlos Carracedo, director de Seguridad de Campofrío.



Emilio Sánchez, consultor del Área de Seguridad de Peldaño, junto a Luciano Valladares, director de Eulen Seguridad; Víctor Manuel Hernández Segovia, director de Operaciones de Eulen Seguridad.

Anselmo Murillo, Inspector Jefe. Jefe de la Sección de Inspección de la Brigada Central de Inspección e Investigación de la Unidad Central de Seguridad Privada. CNP.

Equipo de Peldaño que estuvo al frente de la I Jornada RPAS y Seguridad Privada.

Sergio Picallo, secretario sectorial de Seguridad y Servicios Auxiliares de UGT-Fes; Benjamín Sánchez de la Dirección Sectorial de Seguridad y Servicios Auxiliares. UGT-Fes, junto a Gemma G. Juanes.

Representantes del Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) que asistieron a la I Jornada RPAS y Seguridad Privada.

*Fotos: Pedro Galán*

**MOBOTIX** Building Solutions

# Vigilancia profesional.

Control de edificios, vídeo, alarma y acceso.


Laden im App Store

Google Play

**MOBOTIX**

MOBOTIX AG • Kaiserstrasse • D-67722 Langmeil • Tel: +49 6302 9816-103 • Fax: +49 6302 9816-190 • sales@mobotix.com • www.mobotix.com

TECNOLOGÍA, FORMACIÓN, NORMATIVA...

# Seguridad en **casinos**

## Directores y responsables de Seguridad analizan el momento actual de la seguridad en los casinos

¿CON qué medios y medidas de seguridad cuentan los casinos de nuestro país? ¿Qué papel juega hoy en día la figura del director de Seguridad en este tipo de instalaciones? A día de hoy los directores de Seguridad de los casinos españoles aspiran a que el futuro Reglamento de Seguridad Privada regule aspectos clave de su actividad sin condicionarla en exceso. Para muchos de ellos esta cobertura jurídica dotará a estos profesionales de mayores garantías ante los retos que abordan en su labor.

### Continuos cambios

Y es que el avance de la sociedad ha propiciado también que los casinos hayan tenido que ir adaptándose a los continuos cambios de la misma, y en el caso que nos ocupa, en el ámbito de la seguridad. Un avance y adaptación que vendrá de la mano, igualmente, del tan esperado Reglamento de Seguridad Privada. Por eso, son ellos, en esta ocasión, los directores de Seguridad de los casinos, quienes toman la palabra para explicarnos, entre otros aspectos, su visión profesional ante los cambios que se avecinan con esta nueva normativa. Pero también de la implantación de nuevos medios y medidas de seguridad, concretamente de prevención y protección. Medidas que también tienen su punto de apoyo en las tecnologías que avanzan rápidamente.


Por eso toca ahora preguntarnos: ¿Cómo ha cambiado la seguridad de los casinos en estos últimos años? ¿Cómo gestionan en estos momentos los directores de Seguridad de estas instalaciones la seguridad integral? ¿Cuáles son los riesgos a los que se enfrentan habitualmente? ¿Qué aspectos del futuro Reglamento de Seguridad Privada afectarán al sector de la Seguridad en Casinos? ●

Fotos: Freepik

# Alai Secure, operador M2M en Seguridad

**"Nuestra apuesta en firme por el I+D**, nos permite disponer de un portfolio de **servicios M2M** de vanguardia, exclusivo **para empresas de seguridad".**


VPN itinerante para instaladores

Nuevo servicio Secure IP: Redireccione las IP de sus dispositivos al instante desde la Plataforma de Alai.

Salida de Red redundada (activo - activo)

**Alai Secure**

**M2M Security Operator**

**www.alaisecure.com**

## VISÍTENOS EN:

**Security Forum 2016**
**Stand 072**
**Barcelona**
**25 y 26 de Mayo**

**ÁNGEL PÉREZ ALCARRIA.** DIRECTOR DE SEGURIDAD. CASINO GRAN MADRID

# *«Nuestros **casinos** son elegantes y confortables, pero ante todo son establecimientos **muy seguros**»*

LOS casinos son centros de ocio en los que nuestros clientes vienen a pasar una velada "distinta", por lo que nuestra obligación es garantizarles su seguridad en todos sus ámbitos, con una serie de medidas que para ellos pasen totalmente desapercibidas, para nuestros negocios sean preventivas y para los que vienen con otras intenciones sean disuasorias», explica Ángel Pérez Alcarria, director de Seguridad de Casino Gran Madrid, quien a lo largo de la entrevista aborda los aspectos que debería contemplar un sistema de gestión de seguridad implantado en un casino, entre otros temas.

**—En primer lugar, ¿cuál es el día a día de un responsable de Seguridad de un casino, como son las instalaciones de Casino Gran Madrid?**

—El día a día en la seguridad de un casino es, ante todo, distinto al anterior. La rutina y la monotonía no existen en un casino. Se evalúa todo lo acontecido en la jornada anterior. Se comprueba que los procedimientos establecidos se han cumplido en cada una de las áreas de trabajo, corrigiendo cualquier anomalía para que esto no vuelva a producirse. También se planifica el trabajo para ese día según los eventos que vayan a producirse, ya que independientemente de la actividad propia de un casino como puede ser el juego, no hay que olvidar que estos establecimientos son zonas de ocio, por lo que tenemos convenciones, jornadas gastronómicas, actuaciones musicales, etc., donde el departamento de Seguridad juega un papel esencial para que todo se desarrolle con la más absoluta normalidad. Nuestros casinos son establecimientos donde la seguridad es fundamental, contando con la tecnología más avanzada. Son lugares elegantes, atractivos, confortables…, pero ante todo, muy seguros.

**—¿Qué aspectos debería contemplar un sistema de gestión de seguridad implantado en un gran casino?**

—El sistema de gestión de seguridad implantado en un casino debe ser integral para implantar las distintas actividades que allí se producen. Debe integrar en primer lugar la seguridad lógica con la seguridad física. En los casinos, durante muchos años, ha prevalecido siempre la seguridad física, ya que los riesgos que se evaluaban así lo requerían. De unos años a esta parte, la Seguridad de la Información es un tema vital para nuestra actividad. La aparición del juego on line ha conllevado un cambio en las políticas de seguridad. Los casinos son centros de ocio en los que nuestros clientes vienen a pasar una velada «distinta», por lo que nuestra obligación es garantizarles su seguridad en todos sus ámbitos, con una serie de medidas que para ellos pasen totalmente desapercibidas, para nuestros negocios sean preventivas y para los que vienen con otras intenciones sean disuasorias.

**—¿Han variado los riesgos y amenazas a los que debe hacer frente el área de Seguridad del Casino?**

—Aunque podríamos decir que no, ya que el riesgo de los casinos sigue siendo el mismo que hace casi 40 años, cuando se legalizó el juego en España, que en definitiva es salvaguardar la integridad de nuestros clientes, evitar cualquier tipo de alteración del desarrollo del juego, velar por los bienes de la empresa y garantizar el cumplimiento de los procedimientos establecidos, la realidad es que el tipo de amenazas para nuestras empresas ha cambiado considerablemente.

Han aumentado las bandas organizadas que se desplazan por todos los casinos de Europa con la intención de delinquir. Han aparecido nuevas formas para intentar manipular el juego electrónico. La seguridad informática ha pasado a un primer plano en esta actividad, siendo actualmente uno de nuestros mayores retos. Hace 20 años, para intentar hacer trampas en el casino, había que estar físicamente en él. Ahora, desde miles de kilómetros, se puede estar manipulando el azar. Por eso, al igual que el resto de la sociedad en que vivimos, los casinos han ido evolucionando también en cuanto a riesgos y amenazas, realizando grandes inversiones en nuevas tecnologías para anular si es posible o en el peor de los casos intentar minimizar al máximo dichos riesgos.

**—Hoy en día, el sector apuesta por la convergencia de la seguridad como un concepto integral, ¿cree que los casinos españoles están preparados para asumir este concepto?**

—Los responsables de Seguridad de los casinos españoles llevamos años trabajando para garantizar una seguridad integral en nuestras empresas. No se puede trabajar con todos los servicios y sistemas de seguridad existentes de manera independiente. Los servicios de seguridad exterior, la seguridad interior y la seguridad informática deben estar consideradas como una sola herramienta de trabajo, la cual debe complementar una a otra y producir sinergias que conlleven al acercamiento de una seguridad, sino total, si cercana a la excelencia.

**—¿Se han llevado a cabo en los últimos años mejoras en cuanto a infraestructuras de seguridad en el Casino?**

—Se han realizado constantes mejoras en nuestros casinos. Se ha implementado la radiofrecuencia en las fichas de juego, para garantizar su control interno y evitar la falsificación de las mismas. La identificación facial para garantizar la identidad de quienes nos visitan. La identificación de matrículas en el acceso a nuestras instalaciones. Las cámaras IP. La grabación digital de alta resolución, etc.

Los casinos españoles realizan constantes inversiones en tecnología punta para garantizar la seguridad de nuestros visitantes y de nuestras instalaciones.

**—¿Cómo ha variado la seguridad, en cuanto a estrategia y logística, en los grandes casinos españoles?**

—Los departamentos de Seguridad de los casinos han ido variando su estrategia conforme ha ido evolucionando la sociedad. Allá por los años 80, se esperaba que hubiese un problema para solucionarlo de la mejor manera posible. Poniendo mucho empeño y muchas ganas, pero con pocos medios y escasos procedimientos. Hoy en día se

evalúan los riesgos de forma constante, con una prevención activa y con una búsqueda de tecnología que nos ayude a que la atmósfera de seguridad que se respira en nuestras instalaciones, invite a quienes nos visitan, a sentirse seguros y protegidos.

**—¿Cuáles considera que son hoy en día los pilares sobre los que debe asentarse una adecuada seguridad en los casinos?**

—Principalmente son tres: recursos humanos. Recursos Tecnológicos. Procedimientos.

Los Recursos Humanos están integrados por una seguridad exterior compuesta por Vigilantes de Seguridad especialistas en este tipo de instalaciones. Son la primera imagen que reciben nuestros clientes cuando llegan al casino. Su responsabilidad es el control de accesos, los sistemas contra incendios, la custodia de los bienes, el CCTV de las zonas exteriores y la reacción activa ante cualquier incidente que pudiera producirse. La Seguridad Interior compuesta por Fisonomistas y Recepcionistas especializados en el control del juego, control de procedimientos, revisiones de jugadas, etc. Son los que garantizan la total transparencia de nuestra actividad. Son los responsables de garantizar que las personas que nos visitan perciban esa sensación de seguridad tan difícil de conseguir, y que obtengan esa sensación de que todo lo que ocurre en el casino está bajo control.

El segundo pilar es la tecnología. Contamos con los sistemas más avanzados de CCTV. En los casinos, todo lo que ocurre queda grabado. Se visualiza el juego en tiempo real y se revisan posteriormente las grabaciones. Todo se analiza.

Y por último, y no menos importante, los procedimientos. En un casino todo esta procedimentalizado. Nada se deja al azar excepto el juego. Cada actividad del casino tiene sus procedimientos, los cuales se deben cumplir con total exactitud, siendo labor del departamento de Seguridad reconducir al momento cualquier anomalía que pudiera producirse

**—Hace ahora poco más de un año se puso en marcha la Asociación Española de Seguridad en Casinos (AESCA), ¿qué actividades y proyectos se han llevado a cabo en estos meses?**

—Efectivamente. Hace ya un año se creó la Asociación Española de Seguridad en Casinos de Juego (AESCA) de la que actualmente soy el presidente. La finalidad de la misma es mantener una comunicación entre todos los responsables de seguridad de los casinos españoles en la que intercambiemos información, experiencias y conocimientos para estar preparados ante cualquier fraude que pudiera intentarse en nuestras empresas. Unificamos criterios a la hora de impartir formación tanto interna como externa, realizando jornadas con todos los responsables. De hecho, y con motivo de SICUR, nos volveremos a reunir con el Cuerpo Nacional de Policía y con la Asociación de Casinos Españoles para continuar con esa colaboración. Estamos ya en disposición de prestar colaboración allá donde nos lo pidan, bien con la FFCC de Seguridad, con la Administración, con Universidades o con cualquier tipo de organización o asociación que nos lo pidan.

**—Para finalizar y entrando en temas normativos, ¿qué aspectos le gustaría que recogiese el Reglamento de Seguridad Privada?**

—Lo primero es que el esperado Reglamento vea la luz lo antes posible. Llevamos más de un año esperándolo y por diversos motivos todavía no sabemos cuándo saldrá. Es importante que se recoja de una forma clara todo lo relacionado con la formación de nuestros profesionales. Las buenas intenciones deben dejar paso a una realidad acorde con los tiempos que corren. La Seguridad Privada tiene excelentes profesionales en todos sus ámbitos, pero necesitan un mayor reconocimiento de la sociedad en general y de la Administración en particular, y para que esto ocurra, deberíamos estar mejor preparados. ●

*Texto: Gemma G. Juanes.*
*Fotos: Casino Gran Madrid*

HIKVISION


FISHEYE
CÁMARAS IP MEGAPÍXEL

COMERCIOS

# VISIÓN 360°

# APLICACIONES 360°

Una vista global de toda la situación desde un punto de grabación, en vez de desde varios ángulos confusos: esto fue lo que inspiró a Hikvision a diseñar una única cámara que pudiera supervisar una superficie compleja entera, con un nivel de detalle totalmente claro y sin puntos ciegos. La cámara Fisheye de Hikvision es la opción perfecta para las instalaciones profesionales en los centros comerciales, los hipermercados y los grandes comercios, en los que el gran tamaño de sus superficies tanto interiores como exteriores requieren una supervisión panorámica y muy detallada.

- Sensor de hasta 12 megapíxeles
- 1 Fisheye a 25 fps
- 4 PTZ a 25 fps
- Visión panorámica 360º
- Iluminación de infrarrojos integrada hasta 15 m
- Tecnología inteligente Smart 2.0

Vsmart 2.0

**Hikvision Europe**
Parellaan 24, 2132 WS Hoofddorp
The Netherlands
T +31 23 5542770
F +31 23 5631112
info.eu@hikvision.com

www.hikvision.com

**DAVID VASSELIN.** DIRECTOR DE SEGURIDAD. GRUPO ORENES

# «Hoy en día es **fundamental** contar con un **sistema integral de seguridad**»


LOS factores principales que favorecen las convergencias de nuestros negocios son: las tecnológicas, la formación, las amenazas, los proveedores y la colectividad de la seguridad», señala David Vasselin, director de Seguridad de Grupo Orenes, quien además explica, entre otros aspectos, los elementos que debería contemplar un sistema de gestión de seguridad implantado en un casino: conocimiento del negocio, formación, sistemas de seguridad y gestión del departamento de Seguridad.

**—En primer lugar, ¿qué objetivos se ha planteado tras su incorporación como director de Seguridad de Grupo Orenes?**

—Mi objetivo principal es seguir con el legado de mi predecesor. El Grupo Orenes está en un momento de expansión, tanto nacional como internacional, y nos vemos obligados a buscar soluciones de seguridad según nos van entrando proyectos nuevos. Por ponerle un ejemplo, desde mi incorporación a mediados de noviembre, se ha proyectado el estudio e iniciado las obras de ampliación de medidas de seguridad en treinta y dos salones de juego.

Otro de mis principales objetivos es crear una Central Receptora de Alarmas de uso propio, con el fin de poder controlar todos nuestros salones.

También nos hemos marcado potenciar el área de Investigación y de Auditorías, del mismo modo que hemos ampliado recientemente nuestro departamento de Seguridad, creando un área Técnica, para potenciar entre otras cosas el I+D en materia de seguridad.

El departamento de Seguridad está concienciado y está trabajando duramente en buscar las mejores soluciones, para que nuestros negocios no sean objetivos apetecibles para los que se dedican hacer el mal. En otras palabras, como los malos siempre van a existir, vamos hacer que se busquen objetivos más sencillos.

**—¿Cuál es el día a día de un responsable de Seguridad de un casino?**

—Teniendo en cuenta que trabaja normalmente por las noches, el día a día de un director de Seguridad de un casino es tener todas las áreas del negocio controladas. Conocer a sus clientes, a los proveedores, a todos los empleados del casino.

Debe supervisar que se cumplan los procedimientos de seguridad por parte de los Vigilantes de Seguridad, así como comprobar las novedades que pudiera haber en las auditorías y controles de procedimientos que se realizan por sus operadores especialistas en materia de juego.

Es fundamental que el director de Seguridad de un casino deba mantenerse al día de todo lo que sucede en el mundo de los casinos. Es muy importante que mantenga una relación constante con otros colegas, y una obligación que lo hagan con los que están más próximos a su casino.

Debe controlar los problemas técnicos que pudieran ocasionar el sistema de seguridad, con el fin de buscar soluciones con la empresa mantenedora de sus sistemas de seguridad.

Y mantendrá sus relaciones con las Fuerzas y Cuerpos de Seguridad del Estado.

**—¿Qué aspectos debería contemplar un sistema de gestión de seguridad implantado en un gran casino?**

—Grosso modo y de forma resumida, estos son los puntos que debería

contemplar un sistema de gestión de seguridad:

1. Conocimiento del negocio. Es fundamental conocer el mundo en el que te mueves y crear los procedimientos necesarios de control.

2. Formación. Por norma general los departamentos de Seguridad de los casinos controlan dos áreas diferentes: Por un lado tienen a los expertos de CCTV en materia de juego, que se encargan de velar por el buen funcionamiento del juego y solucionar las reclamaciones en materia de juego. Y por otro lado a la Seguridad Externa, ejercida por los Vigilantes de Seguridad Privada, y que tienen como función principal las marcadas en el Art. 32 de la Ley 5/2014 de Seguridad Privada, y de conocer el Plan de Autoprotección del Casino.

3. Sistemas de Seguridad. Ya me he pronunciado en otras ocasiones y sigo teniendo claro que hoy en día es fundamental tener un sistema integral de seguridad. Tener una herramienta ágil, fácil en su utilización y a la vez que su configuración sea manejable. Por la tipología de negocio, nos vemos a menudo en la obligación de dar respuestas a incidencias delicadas, donde el tiempo de respuesta por parte de nuestro departamento es de vital importancia. Por eso, es fundamental tener un software de gestión de imágenes rápido y operativo.

4. Gestión del departamento de Seguridad: un buen gestor de seguridad deberá como mínimo saber supervisar el trabajo de tu equipo, controlar tu presupuesto, mantener en condiciones los sistemas de seguridad, comunicación constante con las Fuerzas y Cuerpos de Seguridad del Estado y con los directores de Seguridad de los otros casinos, etc.

**—¿Han variado los riesgos y amenazas a los que debe hacer frente el área de Seguridad del Casino?**

—Nuestras amenazas siguen siendo prácticamente las mismas, no han variado mucho; por un lado seguimos teniendo tramposos profesionales, así como oportunistas que van buscando hacer daño en nuestras mesas. Estos primeros son más complicados de detectarlos dado que son muy hábiles y, muchos de ellos, acceden con documentaciones falsas. Para nuestras empresas es muy importante descubrirlos con prontitud para minimizar nuestras pérdidas.

Como directores de Seguridad uno de nuestros objetivos es velar por los intereses del casino, y eso conlleva también velar por nuestros clientes. Desde hace mucho tiempo, los casinos tienen la obligación de controlar toda persona que acceda a sus instalaciones con el objetivo de marcar a clientes destacados para luego en la calle poderlos robar.

No podemos olvidar la utilización de las nuevas tecnologías para la realización de fraude, por ello, como comentaba anteriormente, auditorías y conocer a nuestros clientes, de manera que podamos controlar todo cliente no conocido.

**—Hoy en día, el sector apuesta por la convergencia de la seguridad como un concepto integral,**

**¿cree que los casinos españoles están preparados para asumir este concepto?**

—Por supuesto, de hecho creo que en mayor o menor medida lo llevan asumiendo desde hace tiempo. Ya hemos avanzado mucho en las distintas convergencias para llegar a una unificación total. La unificación de las convergencias nos garantizará un control total de las necesidades de nuestros negocios. Creo que sin lugar a duda los factores principales que favorecen las convergencias de nuestros negocios son: las tecnologías, la formación, las amenazas, los proveedores y la colectividad de la seguridad.

**—¿Se han llevado a cabo en los últimos años mejoras en cuanto a infraestructuras de seguridad en los casinos del Grupo Orenes?**

—La verdad es que los casinos nacionales e internacionales con los que cuenta el Grupo Orenes son relativamente nuevos, y cuentan con la mejor tecnología en materia de seguridad. El casino Rincón de Pepe ubicado en Murcia ha sido el último en cambiar las grabaciones analógicas a digital.

**—¿Cómo ha variado la seguridad, en cuanto a estrategia y logística, en los grandes casinos españoles?**

—Creo que tanto los grandes casinos como los pequeños han tenido que variar sus estrategias de seguridad debido en gran parte a la crisis. Se han reducido en gran medida los medios humanos y, en el mejor de los casos, se han podido suplir con medios técnicos. Para seguir cosechando buenos resultados hemos tenido que hacer encajes de bolillos, por ejemplo hemos tenido que establecer políticas de seguridades con todos los departamentos operativos del casino, haciéndolos partícipes en la prevención de los riesgos. Para eso, hemos tenido que dar formación a estos departamentos ajenos al de seguridad, con el fin de concienciarlos en la importancia de su implicación para estos temas. Y la verdad es que se han obtenido grandes resultados.

**—Para finalizar y entrando en temas normativos, ¿qué aspectos le gustaría que recogiese el Reglamento de Seguridad Privada?**

—Al igual que me pronuncié en su día alegrándome de la introducción de la figura del director de Seguridad en la nueva Ley de Seguridad Privada, espero y deseo que en el Reglamento de Seguridad Privada, se haga mención a los departamentos de Seguridad. Me gustaría creer que tener legalmente constituido un departamento de Seguridad no fuera solamente por el mero hecho de cumplir con la normativa, sino que se le debe pedir mucho más. Mucha más colaboración por parte de los dos actores. Es cierto que en los últimos años se ha avanzado mucho con la RED AZUL y el PLAN COOPERA, pero al margen de los cuerpos policiales que están directamente vinculados con la Seguridad Privada, todavía estamos lejos de estar totalmente aceptados y conocidos con todas las FFCCSS. ●

*Texto: Gemma G. Juanes.*
*Fotos: Grupo Orenes*

**CARLOS ESTEBAN CUELLO DE ORO ROZAS.** DIRECTOR DE SEGURIDAD. GRAN CASINO COSTA BRAVA

# «El departamento de **Seguridad** no descansa, siempre **tiene que estar alerta**»

La convergencia de la seguridad como un concepto integral es el presente de la seguridad en los casinos; si se quiere tener un sistema integral en la seguridad, los departamentos que se encargan de la IT deben de ir de la mano con la imagen del departamento de Seguridad. Sabemos que cada vez hay más ataques y delitos informáticos, robo de información, sabotaje y espionaje informático, no dejando de ser riegos que debemos asumir y analizar constantemente los profesionales que nos dedicamos a este sector», así lo asegura Carlos Esteban Cuello de Oro, director de Seguridad del Gran Casino Costa Brava, quien explica además los pilares sobre los que debe asentarse una adecuada seguridad en los casinos.

**—En primer lugar, tras su incorporación como director de Seguridad del Gran Casino Costa Brava ¿cuál es el día a día de un responsable de Seguridad de un casino?**

—Primero de todo aprovecho para dar las gracias por el interés y el apoyo mostrado por parte de mi entorno profesional, por la oportunidad y la confianza que me han mostrado en esta nueva etapa profesional como responsable de Seguridad en el Gran Casino Costa Brava.

El departamento de Seguridad del Casino no descansa y siempre ha de estar en alerta. Como tarea obligada del responsable de Seguridad es velar y supervisar su correcto funcionamiento, integral y normativo. Decir que el día a día está marcado por una serie de tareas continuas y marcadas, siguiendo un patrón definido a la hora de inspeccionar, auditar y analizar los riesgos de las diferentes áreas del Casino, para que así se puedan cumplir los procedimientos establecidos, y otro patrón más dinámico y operativo cuando la operación del Casino está abierta al público.

**—¿Cuáles son los riesgos o amenazas a los que tiene que hacer frente de una forma más habitual?**

—Las amenazas que cubrimos con más habitualidad desde el área de juego son los descuideros, hurtos, carteristas, conflictos, trampas y disputas entre clientes en los diferentes juegos, etc. Y desde el área de vigilancia patrimonial los riesgos y amenazas más habituales son actos vandálicos, prevención en control de accesos para restringir la entrada de personas que no están en condiciones de acceder al interior, el consumo de estupefacientes en las instalaciones…

Desde nuestro departamento damos una gran importancia en caso de evacuación o confinamiento por los riesgos derivados en estos casos, teniendo en constante formación al personal del Casino y creando manuales operativos en caso de incendios o primeros auxilios.

**—¿Qué aspectos debería contemplar un sistema de gestión de seguridad implantado en un gran casino?**

—En primer lugar considero que ha de haber una correcta organización departamental para poder cumplir los procedimientos de las políticas de seguridad aplicables, y así poder derivar las funciones y las responsabilidades a cada empleado. De esa manera la implantación de los procedimientos en caso de cualquier incidencia puede dar un resultado y una respuesta positiva.

En segundo lugar la identificación, el análisis y la evaluación de riesgos, como área obligada de los directores de Seguridad, es una tarea que en caso de los casinos, particularmente, es una constante, ya que las nuevas tecnologías y

las tendencias de los clientes más jóvenes abren las puertas a nuevos riesgos. Y por último el departamento de Seguridad, como figura auditora, es otro componente indispensable para que en un negocio de este tipo esté bajo supervisión y control, alejando a aquellos individuos u organizaciones que tienden a las malas artes.

**—Hoy en día, el sector apuesta por la convergencia de la seguridad como un concepto integral, ¿cree que los casinos españoles están preparados para asumir este concepto?**

—Sin lugar a duda, de hecho es el presente de la seguridad en los casinos, si se quiere tener un sistema integral en la seguridad, los departamentos que se encargan de la IT deben de ir de la mano con la imagen del departamento de Seguridad. Sabemos que cada vez hay más ataques y delitos informáticos, robo de información, sabotaje y espionaje informático, no dejando de ser riegos que debemos asumir y analizar constantemente los profesionales que nos dedicamos a este sector.

**—¿Se han llevado a cabo en los últimos años mejoras en cuanto a infraestructuras de seguridad en el Casino?**

—Piense que el gran Casino Costa Brava hace seis años que abrió sus puertas y se hizo una gran inversión en toda la estructura de seguridad. Las medidas que actualmente tenemos en el Casino están muy por encima de otros negocios, y teniendo en cuenta el freno económico que llevamos desde hace unos años, producto de la famosa crisis, las inversiones que se han realizado en casi todas las empresas han sido las de optimización económica. Aún así la empresa sigue apostando, ya que actualmente hay proyectos de implantación de medidas electrónicas para mejorar el control de accesos, conteo de aforos, alarmas integradas en los sistemas informáticos de seguridad, etc.

Por supuesto, desde que se modificaron por ley el número de personal de control por parte de las administraciones.

**—¿Cuáles considera que son hoy en día los pilares sobre los que debe asentarse una adecuada seguridad en los casinos?**

—Es esencial que haya un equipo de seguridad independiente con la formación cualificada para este tipo de negocio, en este caso me he encontrado con un equipo con una alta formación gracias al esfuerzo de mi predecesor en el cargo. Esto ha de ir acompañado por un buen sistema de

CCTV que abarque todas las áreas del Casino llevado por agentes de sala especializados; añadir un buen sistema de control de accesos y de llaves, y un equipo de vigilancia privada preparada para atender las diferentes incidencias que están a su cargo.

De esta manera podemos dar una imagen transparente y colaboradora si los órganos de control y seguridad de las Administraciones lo precisaran.

**—Para finalizar y entrando en temas normativos, ¿qué aspectos le gustaría que recogiese el Reglamento de Seguridad Privada?**

—La Ley 5/2014 creo que ha dado un salto cualitativo a la hora de entender la situación legal en la cual se encuentra la imagen del director de Seguridad, ya que le da un nuevo rango legal, ahora falta que el reglamento recoja los aspectos específicos para esta nueva imagen que anteriormente se recogía como una especialidad del jefe de Seguridad.

El terrorismo yihadista o el terrorismo informático, como paradigma de la situación en la seguridad social actual, hace que desde la perspectiva del profesional de la seguridad de los casinos no generen dudas como figura obligatoria dentro de este ámbito empresarial, no solo por la especialización que se tiene que tener a la hora de poseer unos conocimientos adquiridos para entender según que riesgos en una sala

> «Es necesario una correcta organización departamental para poder cumplir los procedimientos de las políticas de seguridad aplicables»

de juego, sino como evaluadores de riesgos constantes, en nuestro caso el de un negocio donde el movimiento de efectivo y el continuo y ascendente paso de personas en un sector de ocio que va en auge, haga que los casinos tengan una cierta sensibilidad, necesitando la figura de un profesional que constantemente esté velando por un entorno que puede conformarse como objetivo para el fraude o el atraco, por ejemplo. ●

*Texto: Gemma G. Juanes.*
*fotos: Gran Casino Costa Brava*

**VICENTE ALTEMIR GISTAU.** JEFE DE INSPECCIÓN DE RIESGOS Y SEGURIDAD. CASINO MARBELLA

# «Los casinos españoles tienen a **grandes profesionales de la seguridad** al frente»

EL funcionamiento diario de un casino requiere de la coordinación de las diferentes áreas, así pues, es necesaria la interactuación de todos para la consecución de un mismo fin: cerrar el día sin incidentes pero con los rendimientos económicos pretendidos», así lo asegura Vicente Altemir Gistau, jefe de Inspección de Riesgos y Seguridad de Casino Marbella, quien además analiza, entre otros aspectos, cómo han variado los riesgos y amenazas a los que hoy en día deben hacer frente este tipo de instalaciones.

**—En primer lugar, ¿cuál es el día a día de un responsable de Seguridad de un Casino?**

—El responsable de Seguridad de un casino, no es alguien ajeno a la organización empresarial. Existen reuniones diarias con la Gerencia y los diferentes responsables departamentales: Juego, Recursos Humanos, Alimentos y Bebidas, Contabilidad, etc. El funcionamiento diario requiere la coordinación de las diferentes áreas del casino, así pues, es necesaria la interactuación de todos para la consecución de un mismo fin, cerrar el día sin incidentes, pero con los rendimientos económicos pretendidos. Un casino es un negocio que está en funcionamiento 24 horas al día, unas horas con clientes y abierto al público, y otras horas preparándose para poder atender en condiciones a este público. Proveedores, reparaciones en las instalaciones, mejoras, etc., forman parte del día a día. A esto hay que añadir la responsabilidad que el departamento de Seguridad tiene en la protección de personas, inmuebles, imagen de la marca, etc.

El responsable del departamento de Seguridad ha de estar al corriente de las situaciones presentadas en la instalación y en el entorno. La comunicación con los Cuerpos y Fuerzas de Seguridad, se debe enmarcar dentro de las comunicaciones diarias. Situaciones de orden público y delincuencia son analizadas para, en su caso, poner a la instalación fuera del alcance de las mismas.

**—¿Qué aspectos debería contemplar un sistema de gestión de seguridad implantado en un gran casino?**

—Cuando hablamos de sistema de gestión de seguridad, siempre pensamos en los sistemas anti-atraco, robo, intrusión, detección de incendio, el control de accesos o el Circuito Cerrado de Televisión. Todos son aspectos que la instalación de seguridad en un casino debe tener, pero es necesario avanzar y, para ello, estos medios técnicos deben estar comunicados entre sí y la interacción con el usuario final debe ser fácil e intuitiva. Las alarmas producidas en las instalaciones deben poder ser verificadas por el usuario, visualmente y de forma automática, sin que sea necesaria la intervención del mismo. Contar con controles de accesos que interactúan con sistemas de reconocimiento facial y que hacen más ágil la gestión que se realiza con proveedores y contratistas, la automatización de acciones rutinarias como la conexión o desconexión de zonas de alarma, el análisis de vídeo enfocado no solo a los aspectos de seguridad, como es la invasión de zonas o cambios en la iluminación, proporcionan un sistema de seguridad potente, pero es necesario considerar dónde está el corazón del negocio que es en el juego. Aplicar a través de análisis de vídeo inteligente la interpretación de las normas de los juegos y por supuesto los intentos de fraude, sin duda otorgan ventajas incalculables en la autoprotección. Es obvio añadir que el sistema de integración debe tener contemplada la posibilidad de comentar por parte del usuario cada uno de los eventos registrados por el sistema, en una estructura que a posteriori permita unos reportes adecuados y clarificadores, con posibilidades de seguimiento histórico de cada uno de los eventos registrados y los movimientos relacionados.

**—¿Han variado los riesgos y amenazas a los que debe hacer frente el área de Seguridad del Casino?**

—Los riesgos y las amenazas han sumado. Los avances de la sociedad se ven reflejados en los avances de las amenazas a las que hacer frente y hay que sumar. Hace veinte años había determinadas amenazas contra el negocio. Hoy en día, los avances tecnológicos, la globalización, la eliminación de fronteras, traen consigo un incremento de las amenazas que suman a las ya existentes. Vimos hace pocos años cómo se producían varios atracos con armas de guerra en casinos europeos, utilizando para ello una violencia nunca vista. Todo esto no lo podemos ignorar y, por supuesto, estar preparados frente a las nuevas amenazas tecnológicas y no solo físicas. La interconexión de dispositivos que forman un sistema de seguridad integral se realiza por red, e incluso


en algunos casos, esta red puede estar saliendo a la web. La amenaza de un ataque externo vía web, o de un ataque desde el interior, pondrá en riesgo evidente a toda la instalación, todos los sistemas pasarían a estar controlados por desconocidos, que incluso podrían acceder a la información empresarial, tanto estratégica como confidencial.

**—Hoy en día, el sector apuesta por la convergencia de la seguridad como un concepto integral, ¿cree que los casinos españoles están preparados para asumir este concepto?**

—Entiendo que si no están preparados, deberán hacer todo lo posible para estarlo y estoy convencido de que todos están en esa línea, pues así lo trasmiten sus responsables en las diferentes reuniones que mantiene la Asociación de Directores de Seguridad de Casinos (AESCA). Los casinos en España tienen a unos grandes profesionales al frente. Estos profesionales de la seguridad, entienden que la organización de las empresas en la actualidad lleva al concepto de convergencia. El departamento de Seguridad, sus medios técnicos y sus medios humanos se encuentran dentro de la organización. Todos los departamentos se encuentran implicados en el funcionamiento y mejora de los procesos de producción, en determinadas circunstancias, los propios procedimientos de seguridad o las mejoras propuestas, pueden causar roces entre departamentos, converger antes de la implantación de los mismos y encontrar direcciones afines para todos, lleva al éxito con mayor facilidad.

Por otro lado, los avances tecnológicos que los departamentos de Seguridad han implementado a través de la integración, facilitan que una gran cantidad de acciones en las que la seguridad se excluía por filosofía, hoy en día sean fácilmente asumibles y realizables.

**—¿Se han llevado a cabo en los últimos años mejoras en cuanto a infraestructuras de seguridad en el Casino?**

—La crisis por la que ha pasado y está pasando el sector en España hace muy difícil la inversión por parte de las empresas en los «intangibles». No obstante, Casino Marbella es consciente de que las mejoras y la adaptación de los medios a la situación actual es necesaria y los responsables de Seguridad debemos entender hasta dónde llegan y pueden llegar los esfuerzos económicos de las empresas para alcanzar dicho fin. Históricamente las empresas han funcionado de una manera que en la actualidad, por la situación existente, es muy difícil de asumir. Aquel histórico hacer de, «necesito este sistema de CCTV y lo compraré completo», en la actualidad es inviable, y es necesario ser creativos y proactivos a la hora de planificar las inversiones en infraestructuras. Los productos que en la actualidad existen en el mercado, permiten alcanzar las mismas mejoras pero ser realizadas por partidas y repartidas en el tiempo.

El departamento de Seguridad de Casino Marbella está satisfecho con las inversiones realizadas. Nos encontramos desde hace tres años inmersos en la migración a sistema de CCTV por IP, cámaras IP megapíxel, implementación

de un sistema de Gestión de Eventos, donde se integran todos los medios técnicos de seguridad y sistemas de reconocimiento facial. Integrando todo lo mencionado en lo existente y en un plazo de dos años, hablaremos de la Instalación de seguridad integral completa más exigente.
Todo esto se habrá conseguido sin que la empresa haya tenido que hacer una elevada y única inversión. Puedo decir que en la actualidad, Casino Marbella tiene unas infraestructuras de seguridad, mejores que en la década anterior y esto a pesar de la crisis. Las mejoras en los sistemas de seguridad han de ser continuas y es función del responsable de Seguridad que los sistemas no queden en la obsolescencia. Con inversiones continuas pero razonables, Casino Marbella consigue que su sistema de seguridad pueda hacer frente a las nuevas amenazas.

**—¿Cómo ha variado la seguridad, en cuanto a estrategia y logística, en los grandes casinos españoles?**
—Se podría definir con una palabra, resiliencia. La crisis ha obligado a las empresas a revisar sus costes desde todas las perspectivas, incluida por supuesto la Seguridad. Los recortes aplicados, tanto en medios humanos como en medios técnicos, han obligado a los responsables de Seguridad en los casinos a buscar la creatividad, a ser proactivos ante contextos adversos y dejar a un lado la rigidez de los conceptos para llegar a ser moldeables y adaptables a nuevas circunstancias. Los conceptos de Seguridad Integral y Convergencia de la Seguridad, bajo mi punto de vista, llevan a la resiliencia y todo esto nos hace cambiar nuestras perspectivas y análisis de riesgos, imaginando amenazas presentes y futuras para elaborar los mapas de gestión del riesgo, minimizar los daños y asegurar la continuidad del negocio en base a estas predicciones.

**—¿Cuáles considera que son hoy en día los pilares sobre los que debe asentarse una adecuada seguridad en los casinos?**
—El riesgo tiene tres componentes acumulativos:
–La Amenaza. Por fraude, el ataque a las personas, el ataque a las instalaciones tanto físicas como lógicas.
–La Posibilidad. Que ocurra la amenaza y que ésta sea inminente, largo plazo, permanente y, finalmente,
–Las Consecuencias. Personas, materiales, imagen de marca.
Para hacer frente al riesgo, los pilares sobre los que fundamentar la seguridad adecuada son:
–Procedimientos. En primer lugar, se deben elaborar procedimientos perfectamente definidos para todos los procesos internos y externos que suceden en un casino.

–Aceptación. Debe haber una aceptación de estos procedimientos por parte de todos. Clientes internos y externos. Solo si están aceptados estos procedimientos, se conseguirá el cumplimiento por parte los implicados.

–Normativa de Seguridad. Además de estos procedimientos, debe haber una normativa de Seguridad adaptada y propia del casino. Cada casino se encuentra en un emplazamiento diferente, fuera o dentro del núcleo urbano, ciudad grande o pequeña, ubicación del casino más o menos conflictiva, la oferta de más o menos servicios como aparcamiento, sala de fiestas, etc. Toda esta variedad exige una normativa específica para cada casino.

–Información. La información debe seguir siendo fundamental para la Seguridad. Más tarde, esta información habrá de ser tratada de forma transversal dentro de la empresa para que cada uno de los implicados conozca las amenazas que existen dentro de su área y de ésta forma, aceptar las recomendaciones de Seguridad.

**—Para finalizar y entrando en temas normativos, ¿qué aspectos le gustaría que recogiese el Reglamento de Seguridad Privada?**

—A mi entender, la Ley 5/2014 está acertada en cuanto a las necesidades del sector y específicamente de los casinos. No obstante, será en el Reglamento que la desarrolle donde de verdad se podrá ver si efectivamente supone un avance en cuanto a los temas que nos afectan. Creo que es necesario que la reglamentación de un sector que contiene un abanico tan grande en cuanto a la diversidad de las actividades que contempla, necesita ser flexible y sobre todo, sería deseable que supiera interpretar la norma y considerar el todo dentro de una actividad extraordinariamente regulada por las administraciones. ●

*Texto: Gemma G. Juanes.*
*Fotos: Casino Marbella*

**JUAN BUADES.** JEFE DE SEGURIDAD. CASINO MEDITERRÁNEO

# «La **inversión en seguridad** bien diseñada y planificada siempre será **rentable**»

LAS nuevas tecnologías que han ido apareciendo, optimizan los sistemas de vigilancia y hacen mucho más liviano el trabajo del personal de seguridad. Sin embargo, la tecnología por sí sola no es un factor relevante, sino que debe ser utilizada de manera eficaz aprovechando su potencial al máximo», así lo asegura Juan Buades, jefe de Seguridad de Casino Mediterráneo, quien aborda en esta entrevista los pilares sobre los que debe asentarse una adecuada seguridad en estos establecimientos, entre otros aspectos

**–En primer lugar, ¿cuál es el día a día de un responsable de Seguridad de un Casino?**

—El día a día no difiere sustancialmente del de otro director de Seguridad de cualquier empresa, con las lógicas diferencias por la actividad de su sector. Las funciones de un responsable de Seguridad abarcan las 24 horas del día. Debemos estar informados y ser conocedores de cualquier anomalía en el devenir del funcionamiento de nuestros casinos, y para ello contamos con un departamento de Seguridad altamente profesionalizado.

En cuanto al trabajo habitual dentro de nuestras instalaciones en Casino Mediterráneo tenemos una premisa y es el continuo aprendizaje. Debemos ser pioneros e innovadores creando nuevas formas de trabajo que nos hagan ser si cabe más eficaces.

Y además de todo esto tenemos el trabajo diario de cualquier responsable, tal como asistir a reuniones, supervisar el trabajo in situ, comunicación con las Fuerzas y Cuerpos de Seguridad... es un puesto que requiere muchas horas y dedicación.

El responsable obligatoriamente tiene que preocuparse por los resultados del trabajo y, según los conceptos de calidad vigentes, debe esmerarse para que esos resultados sean cada vez mejores. Debe conocer perfectamente su actividad, buscando el perfeccionamiento constante y la actualización técnica.

El responsable de Seguridad debe supervisar si las directivas han sido bien comprendidas y ejecutadas. Asimismo es el responsable de transmitir a la Dirección General, los resultados de las auditorías que realiza el departamento de Seguridad.

**—¿Qué aspectos debería contemplar un sistema de gestión de seguridad implantado en un gran casino?**

—Las personas que buscan premios y diversión no necesitan preocuparse por su integridad dentro del establecimiento, por lo que los empresarios del sector deben estar atentos a las nuevas tendencias en seguridad.

Un sistema de gestión de seguridad en un casino, ya sea grande o pequeño, a día de hoy debe abarcar innumerables ámbitos que lo hace sin duda un gran reto para los responsables de Seguridad. Por una parte se debería de partir de un sistema informatizado de gestión integral, que abarque todas las vertientes de la seguridad, como anti-incendios, anti-intrusión, control de accesos… Un sistema centralizado que unifique los medios de control y respuesta; y por otra, para nuestra actividad son primordiales los sistemas de control CCTV de última generación, así


como un software específico que pueda sacar todo el rendimiento que estos sistemas son capaces de aportar.

No nos olvidemos del elemento humano, indispensable contar con personal cualificado para poder gestionarlo con éxito.

La seguridad y vigilancia en casinos requiere de una vasta experiencia y una profesionalización constante de los actores en las respectivas gestiones, como por ejemplo el conocimiento de toda la estructura operativa de la empresa, el dominio de los juegos y los factores que interfieren en el rendimiento de los mismos.

**—¿Han variado los riesgos y amenazas a los que debe hacer frente el área de Seguridad del Casino?**

—En la sociedad actual, donde la inseguridad es tema relevante todos los días, los casinos y salas de juego no escapan a esta realidad. La vigilancia en casinos y salas de juegos deben llevarse a cabo por personal que comprenda y esté familiarizado con el universo de personas que a diario ingresan en estos establecimientos.

El personal de vigilancia en un casino se debe ocupar de verificar el cumplimiento de las normas en todos los sectores.

Los sistemas de vigilancia que velan por la seguridad externa e interna de los casinos, tienen como principales actores a clientes y empleados. Ambos universos son los puntos de partida para comprender la problemática de la seguridad en los casinos.

Además en el ámbito externo, debemos de tener una comunicación directa con el resto de casinos, así como con las Fuerzas y Cuerpos de Seguridad, ya que el tema de la delincuencia en el mundo del Juego está en continua evolución y debemos adelantarnos a los acontecimientos.

Punto importante, es la constante actualización en el estudio y dominio de la utilización de nuevas tecnologías aplicadas al fraude. La informática avanza tanto para los buenos como para los malos, y las formas de delinquir cada día son más sofisticadas.

**—Hoy en día, el sector apuesta por la convergencia de la seguridad como un concepto integral, ¿cree que los casinos españoles están preparados para asumir este concepto?**

—Están preparados y en nuestro caso es un elemento que se viene desarrollando con éxito. En Casinos del Mediterráneo contamos con un Plan de Autoprotección que nos hace estar preparados para cualquier contingencia, teniendo una respuesta inmediata y eficaz por parte de nuestro personal. Los miembros de nuestro departamento han de estar preparados para solventar cualquier dificultad, bien en el área de auditoría de juego, de prevención de riesgos laborales o de cualquier otra de las funciones que realizamos. Lo que nos hace estar en un continuo aprendizaje para adaptarnos a los continuos cambios ya sea de normativa o de medios de erradicar cualquier incidencia sea del tipo que sea.

**—¿Se han llevado a cabo en los últimos años mejoras en cuanto a infraestructuras de seguridad en el Casino?**

—Las mejoras han sido tantas y tan notables que hemos pasado sin darnos cuenta entre otras cosas, del sistema de grabación analógico a la grabación digital. Contamos con tecnología

puntera que hasta hace muy poco no podíamos ni imaginar, tales como el reconocimiento dactilar, gestión informatizada de llaves, alarmas y demás dispositivos.... Intentamos aplicar la última tecnología a nuestra forma de trabajar para que ésta sea más eficaz y conseguir con ello intentar ser instalaciones lo más seguras posible.

Las nuevas tecnologías que han ido apareciendo, optimizan los sistemas de vigilancia y hacen mucho más liviano el trabajo del personal de seguridad. Sin embargo, la tecnología por sí sola no es un factor relevante, sino que debe ser utilizada de manera eficaz aprovechando su potencial al máximo.

**—¿Cómo ha variado la seguridad, en cuanto a estrategia y logística, en los grandes casinos españoles?**

—El cambio ha sido notable. Primero en cuanto al tipo de clientes, hemos pasado de tener un público muy concreto y de una franja de edad, a abrirnos a un abanico mucho más amplio.

Un público joven que antes no venía a participar en los juegos tradicionales, dícese Ruletas, Poker... acude ahora a nuestras instalaciones sobre todo ávidos de jugar en nuestros torneos Póker Series Juegging y a participar en las apuestas deportivas Juegging. Nuevos tiempos, nuevas estrategias.

Hemos pasado de los grandes casinos alejados de la urbe a otros más céntricos. Un claro ejemplo es nuestro caso, hablando de la sede de Casinos del Mediterráneo, nos hemos trasladado de las afueras de Villajoyosa al centro de la ciudad de Alicante, a los que se suman el Casino de Orihuela Costa y Benidorm, situados en zonas céntricas y transitadas. Todo ello nos ha hecho adaptarnos a los nuevos tiempos que corren.

Si hablamos de lo que es el edificio del Casino en sí, hoy en día son centros dotados de la última tecnología que nos


permiten reducir los riesgos al máximo. Todo ello unido a otros cambios han hecho que la logística y la estrategia haya cambiado.

**—¿Cuáles considera que son hoy en día los pilares sobre los que debe asentarse una adecuada seguridad en los casinos?**

—Desde mi punto de vista, los pilares pueden ser diversos, pero me gustaría destacar dos ante todo.

En primer lugar: el factor humano. Sin él no seríamos capaces de llegar a las cotas tan altas de eficacia con las que goza nuestro sector, sin la gran profesionalidad de éste todas las mejoras tecnológicas dejarían de tener sentido. Asimismo, una adecuada seguridad en un casino, debe mantener a sus empleados bien informados, dentro de lo que permite el principio de compartimentación de la información. Inspirar el profesionalismo y el espíritu de equipo en su gente. Instruir y motivar a los profesionales bajo su mando para desempeñar la actividad de seguridad. Desarrollar una política de concienciación de la necesidad de cooperar con todo lo que tiene que ver con la seguridad, mostrando los beneficios que a todos les trae esa actitud.

Y en segundo lugar: las nuevas tecnologías. Que nos dotan de unos elementos de trabajo que nos permite estar a la vanguardia de la seguridad. Hoy en día no se puede imaginar un casino sin tecnología de vídeo seguridad.

La inversión en seguridad bien diseñada y planificada, siempre será rentable.

**—Para finalizar y entrando en temas normativos, ¿qué aspectos le gustaría que recogiese el Reglamento de Seguridad Privada?**

—Tengo que reconocer que se ha dado un gran paso con la elaboración de la actual Ley de Seguridad Privada, donde se destaca el grado de colaboración y complementariedad entre la seguridad privada y pública.

La nueva normativa plantea las bases del desarrollo futuro de esta actividad, dándole un enfoque de acuerdo con los tiempos en que vivimos, creando un clima de mayor confianza y apoyo que nos va a permitir alcanzar cotas mayores de seguridad en nuestros establecimientos.

La Ley de Protección de Datos nos impide en muchos casos, que cierta información relevante no pueda ser tratada como realmente nos gustaría tanto para el sector como para la fluidez de la comunicación con las FFCC de seguridad del Estado. ●

*Texto: Gemma G. Juanes.*
*Fotos: Casino Mediterráneo*

**ELIES FRADE.** DIRECTOR DE SEGURIDAD. CASINOS GRUP PERALADA

# «En los **casinos** debemos estar muy **atentos** a las **nuevas amenazas**»

CADA vez es más importante estar al día en nuevas tecnologías de seguridad, en nuestro caso I+D, es imprescindible para ir dos pasos por delante de las nuevas amenazas que nos rodean», asegura Elies Frade, director de Seguridad de Grup Peralada, quien en esta entrevista explica que los procedimientos que se utilizan en los casinos han de estar alerta sobre todas las amenazas que puedan surgir, y «el director de Seguridad, jefes de Seguridad y el personal que pertenece al departamento de Seguridad ha de reciclarse día a día».

**—En primer lugar, ¿cuál es el día a día de un responsable de Seguridad de un casino?**

—A mi entender es una mezcla de procedimientos de trabajo y proactividad, en ellos, el director de Seguridad ha de velar constantemente porque se cumplan los procesos de trabajo establecidos por la Dirección del Casino a nivel procedimientos, combinar con las directrices de la Direccion General y marcar las políticas de seguridad a seguir en el departamento y sus prioridades. Recibir la información sobre todo lo concerniente en seguridad al momento para poder actuar sobre los riesgos, y reportar casi en tiempo real, si fuera necesario, en circunstancias que salgan fuera de la normalidad. Las anomalías dan indicativos de posibles amenazas que nos puedan poner en riesgo y tomar medidas sobre ello. No es fácil el día a día y más en instalaciones que están abiertas 24 horas y en el centro de una ciudad de Barcelona, o ciudades turísticas; creo que su proactividad es básica y pilar principal en la gestión de los centros.

**—¿Qué aspectos debería contemplar un sistema de gestión de seguridad implantado en un gran casino?**

—Cada vez es más importante estar al día en nuevas tecnologías de seguridad, en nuestro caso I+D es imprescindible para ir dos pasos por delante de las nuevas amenazas que nos rodean. Los reconocimientos biométricos, las tecnologías de cámaras IP y las constantes novedades en los controles de accesos, nos hacen ser mucho más precisos en la seguridad de investigación y asimismo en tiempo real. Tener en nuestro equipo personas formadas para que puedan aprovechar todos los nuevos recursos tecnológicos, que se implementan cada año, y analizar nuevas propuestas de tenología, así como la formación constante del equipo de

seguridad en general, contando con la formación de la seguridad presencial en nuevas alertas que se están produciendo en nuestra sociedad, cada vez más importantes y más peligrosas.

**—¿Han variado los riesgos y amenazas a los que debe hacer frente el área de Seguridad del Casino?**

—Desde hace ya unos años la tipología ha variado de forma exponencial. En el área de juego cada vez hay más producto híbrido, que fusiona juego tradicional con soporte informático; llevamos años preparándonos para hacer frente a incursiones exteriores informáticas, así como velar por el buen funcionamiento de las Slots. Desde ya hace algún tiempo los sistemas de análisis trabajan en conjunto con el departamento de Seguridad, es la única manera de poder dar una rápida respuesta a amenazas que puedan producir una merma del negocio silenciosa. Es nuestra obligación estar muy atentos a estas nuevas amenazas.

En cuanto a la parte física, la crisis económica varió el perfil del carterista, oportunista, etc., esto supuso revisar todos los protocolos de seguridad de las instalaciones, y también variar el seguimiento de otros grupos de riesgo, ya que al ser un centro de ocio,

estamos expuestos de una manera bastante importante, y nuestro deber es dar garantía a nuestro visitante de que su estancia será agradable y sin ningún tipo de incidencia ni durante ni después de su estancia.

**—Hoy en día, el sector apuesta por la convergencia de la seguridad como un concepto integral, ¿cree que los casinos españoles están preparados para asumir este concepto?**

—Creo que en nuestro caso fue una de las misiones principales de la preparación de ese nuevo reto. La seguridad integral de los centros funciona. Nuestro grupo está totalmente en esta línea, creo que el sector está preparado y en unos años será algo normal, siempre teniendo en cuenta que necesitamos y tenemos la colaboración de la Direccion General de nuestro grupo, que ha sido la primera interesada en que el funcionamiento de la seguridad del grupo fuera un concepto integral de todo él, y en ello hemos invertido y avanzado, y seguimos poniendo nuestro día a día en el empeño de mejorarlo.

**—En los últimos años de crisis, ¿se han llevado a cabo mejoras en cuanto a infraestructuras de seguridad en el Casino?**

—En estos últimos años la inversión de mejoras no ha variado en nuestro

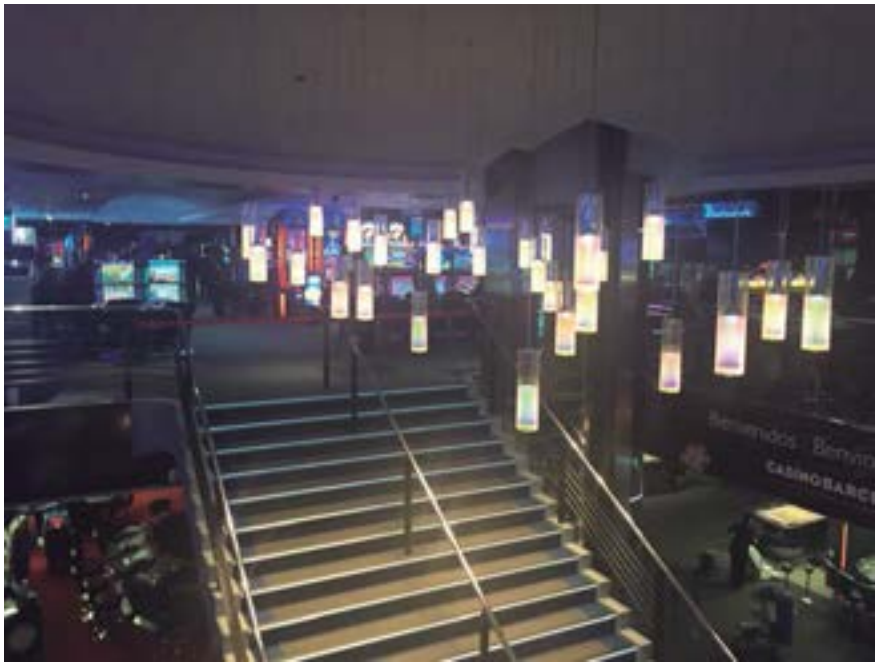
caso, tal como explicaba, la Dirección de nuestro grupo ha apostado por la modernización de los sistemas y entre ellos, en lo referente a la seguridad, queríamos estar preparados para el cambio de ciclo, y han sido sensibles con estos temas y entendieron que más que nunca nos teníamos que proteger en todos nuestros centros y modernizar los sistemas, y en ello hemos trabajado con diferentes empresas del sector, siempre atentos a nuevas oportunidades y nuevos sistemas, que las diferentes empresas del sector nos han ido presentando, y hemos mejorado en ello sustantivamente.

**—¿Cómo ha variado la seguridad, en cuanto a estrategia y logística, en los grandes casinos españoles?**

—Como ya decía en la pregunta anterior, las nuevas tecnologías nos han abierto un frente muy importante del cual estamos muy atentos. Los nuevos escenarios, como trabajar 24 horas abiertos, nos ha obligado a reinventar todos los procedimientos de trabajo y adaptarlos a nuevas situaciones y nuevos retos: Los Vigilantes de Seguridad desempeñan un papel básico en este nuevo reto, y la formación que se les da y las directrices, las cuales han de ser claras y concisas, son parte importante en esta nueva situación. Los cambios en sistemas de recaudación de nuestros centros han tenido que ser modificados de manera sustancial, con un trabajo por parte de CCTV que lo coordina en todo momento. Asimismo los nuevos sistemas implementados han ayudado y mucho en la excelencia y consiguiente resultado de los objetivos del departamento de Seguridad.

**—¿Cuales considera que son hoy en día los pilares sobre los que debe asentarse una adecuada seguridad en los casinos?**

—El pilar mas importante son sus CCTV. Todos y cada uno de los procesos de trabajo en seguridad están pensados para que sean visualizados correctamente desde estos sistemas. Los sistemas mejorados y coordinados con los Vigilantes de Seguridad para el control en su máxima diligencia y seguridad. La formación y la constante renovación de sistemas y procedimientos en el departamento de Seguridad han de ser elementos vivos, que se adapten al día a día y a las nueva exigencias de nuestros visitantes. Nuestros procedimientos han de estar alerta sobre todas las amenazas que puedan surgir, asimismo el director de Seguridad y los jefes de Seguridad y el personal que pertenece al departamento ha de reciclarse día día también, debido a la rapidez en los cambios que se están produciendo en nuestra sociedad y, al mismo tiempo, como no podía ser de otra forma, en nuestros centros con los nuevos sistemas tecnológicos y las nuevas alertas, y lógicamente con todo lo que conllevan esos cambios.



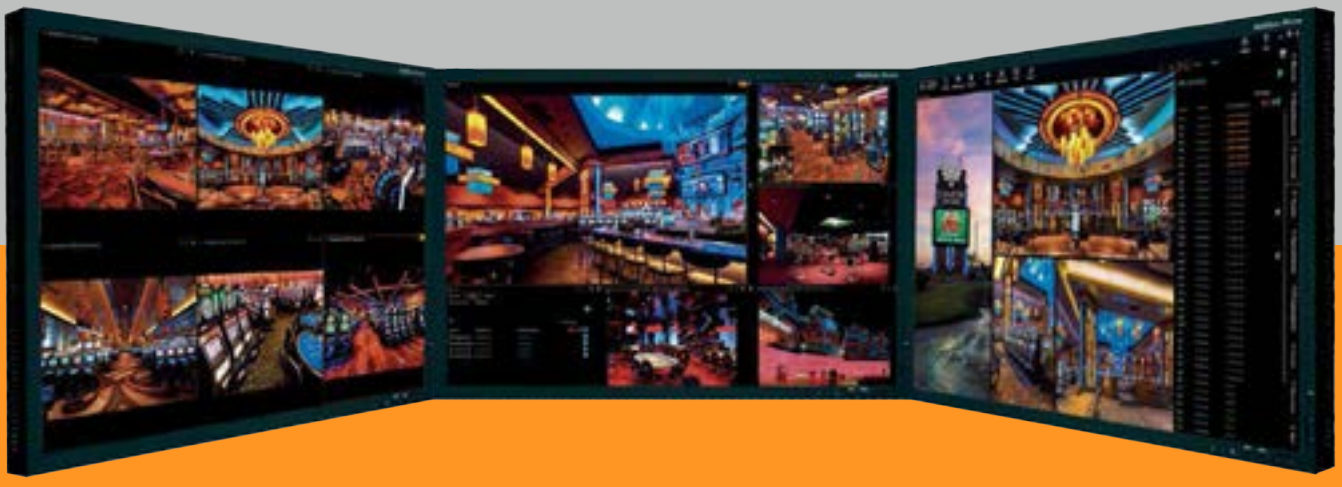
**—Para finalizar, y entrando en temas normativos, ¿qué aspectos le gustaría que recogiese el Reglamento de Seguridad Privada?**

—Me gustaría que se clarificara la proteccion jurídica que está un poco coja, y que no queda clara en la ley, sobre la protección del vigilante como agente de la autoridad, y que este reglamento sea de interpretación más amplia y no restrictivo en el tema de seguridad privada, y vea a la seguridad privada como lo que es, un apoyo y fiel colaborador de la seguridad pública, y que está colaboración sea uno de los principios del reglamento. ●

*Texto: Gemma G. Juanes.*
*Fotos: Grup Peralada*

GEUTEBRÜCK
Excellence in Video Security

# No ponga limitaciones a su Casino
# G-SIM de GEUTEBRÜCK



## AUDITORÍA - OPTIMIZACIÓN PERMANENTE DE LOS PROCESOS

Todo lo que hacen sus usuarios queda registrado: todos los mensajes, todas las cámaras mostradas, todas las medidas adoptadas. De este modo puede saber sin excepción qué, cuándo, cómo y dónde algo ha sucedido

## ORGANIZACIÓN - COLABORACIÓN ENTRE TODOS LOS USUARIOS

La configuración, presentaciones, plantillas, que tenga un usuario puede enviarse a otro usuario o conjunto de usuarios. También es posible enviar tareas, alarmas y mantener conversaciones entre usuarios vía chat

## INFORMES - DOCUMENTACIÓN DETALLADA

Algunas veces es necesario un informe. Con ayuda de un filtro ajustable es fácil realizarlo.¿Desea imprimir el informe? ¿Enviarlo por correo electrónico? ¿O guardarlo en formatos de exportación como CSV, Excel y PDF? Realice auditorias de la forma más completa

G-SIM, gestor de información exclusivo para sistemas **GEUTEBRÜCK** ofrece Multitud de funciones:

· Manejo: simple, cómodo, individual;
· Procesamiento de alarmas: seguro, sin estrés, prioritario;
· Gestión del sistema: eficiente, flexible, segura;
· Gestión de tolerancia ante fallos: Failover;
y mucho más...

**F.F Videosistemas S.L.**
www.geutebruckspain.com
Tel. 902 99 81 10
ffvideo@ffvideosistemas.com

F.F Videosistemas

distribuidor exclusivo
GEUTEBRÜCK

**HELIODORO GINER.** SECRETARIO GENERAL. ASOCIACIÓN ESPAÑOLA DE CASINOS DE JUEGO. (AECJ)

# *«La globalización de la delincuencia hace que la **seguridad en los casinos** se plantee de manera **integral**»*

**EN primer lugar, ¿podría explicarnos a quién engloba la Asociación Española de Casinos de Juego, que actividades promueve, número de socios...?**

—La Asociación Española de Casinos (AECJ) data del año 78, siendo de las primeras asociaciones empresariales del país. Desde entonces ha estado sirviendo al sector en todos los ámbitos, desde abogando por una normativa adecuada y garantista para los derechos de los consumidores, pero sin por ello suponer una mera lista de obstáculos, como en ocasiones ocurre, para el desempeño de una actividad legal con un alto, altísimo, e irracional, si se me permite, nivel impositivo.

Otra de las grandes tareas de la AECJ es la formación de los profesionales que trabajan en las empresas que la integran.

La AECJ es la única asociación de ámbito nacional que representa los citados intereses. Tiene un alto nivel de representación, al incorporar a empresas que facturan, aproximadamente, el 60 % de los ingresos del total del sector. En cualquier caso, como todas las asociaciones, trabajamos por incorporar al mayor número de empresas posible.

Tenemos una dilatada presencia en la Asociación Europea (ECA), siendo uno de los cinco miembros fundadores, y en cuyo seno, a día de hoy la AECJ desempeña, a través de mi persona, la vicepresidencia de Asuntos Legales de la misma.

**—¿Cuáles considera que son los pilares sobre los que tiene que asentarse la seguridad de un gran casino?**

—La seguridad es un área en la que el componente humano tiene un peso muy grande. En el sector de casinos, además, este componente humano tiene que tener una formación muy específica y una experiencia importante, dada la tipología del servicio que prestan nuestros establecimientos. La velocidad y cantidad de partidas que se producen, la gran afluencia de público en determinados momentos y el uso de efectivo y asimilado (fichas), hacen que la actividad presente una serie de características muy específicas y que precisen de un control y examen «caso por caso».

La tecnología, sin lugar a dudas, es una herramienta, como en tantos otros sectores, que presta una asistencia muy importante. La capacidad de almacenaje y calidad de las grabaciones digitales, la calidad de las cámaras y la posibilidad de análisis, gracias a las prestaciones que los nuevos equipos incorporan, facilitan el trabajo de los departamentos.

**—¿Han variado los riesgos y amenazas a los que deben hacer frente los responsables de Seguridad de los casinos?**

—La respuesta es claramente afirmativa. Como en cualquier otro área de la vida, las amenazas en materia de seguridad en casinos han evolucionado. Han evolucionado, básicamente, por dos razones. Una tiene que ver, también, con el uso de la tecnología por parte del público en general y, en el fondo, es la plasmación de la evolución natural de las cosas. Hace años, para atracar un establecimiento, no había más posibilidad que personarse en el mismo, con los evidentes riesgos que ello conlleva, desde la perspectiva del criminal. Hoy día, una estafa cometida a través del uso de nuevas tecnologías, puede situar a nuestro potencial delincuente a miles de kilómetros del establecimiento, sin riesgo personal para él. Existen además, y esto no es una novedad, territorios, países o jurisdiccio-

nes donde el control policial es bajo, lo que permite que allí residan los ciberdelincuentes a salvo de las policías de los países donde delinquen. Evidentemente, como en la mayoría de los sectores, además, muchos de los casinos tienen su operación on line, donde el fraude, las trampas y demás amenazas, cambian por completo su aspecto.

El segundo factor que ha hecho evolucionar el tipo de riesgos que encontramos en los casinos, es la propia capacidad de los departamentos de Seguridad para neutralizar las amenazas tradicionales. En ese aprendizaje, nuestros minuciosos servicios de seguridad han hecho evolucionar a los potenciales delincuentes hacia nuevas modalidades de picaresca, fraude, estafa, etc.


**—Hoy en día, el sector apuesta por la convergencia de la seguridad como un concepto integral, ¿cree que los casinos españoles están preparados para asumir este concepto?**

—Los profesionales de la seguridad de casinos, si se me permite la valoración, están a un nivel muy elevado. Ello es consecuencia directa al grado de atractivo que presentan estos establecimientos a determinado tipo de delincuencia o picaresca.

Conscientes de ellos, los departamentos de Seguridad de los casinos españoles están constantemente formándose. La globalización de la delincuencia hace que la seguridad en los casinos se plantee de manera integral, sin descuidar ningún tipo de riesgos.

**—Desde un punto de vista profesional, ¿cuál cree que es actualmente el nivel de seguridad de los casinos en nuestro país? ¿Y en relación con Europa?**

—La Asociación Española de Casinos, a la que represento, tiene una fuerte presencia institucional a nivel europeo, lo que nos hace conocedores de las prácticas en otros paíes. Además, se organizan eventos de seguridad, en muchos casos con presencia de Policía (Interpol, Servicio Secreto, etc), donde se comparten mejores prácticas y experiencia. Dicho eso, creo que puede decirse que somos punteros en seguridad. El nivel de seguridad en nuestros casinos nada tiene que envidiar a los casinos de nuestro entorno, muy al contrario.

Una de las razones, es que, España, al tener un ordenamiento jurídico muy garantista, importa delincuencia y fraude, lo que conlleva a que nuestros casinos tengan que estar muy preparados para minimizar cualquier riesgo que se pueda producir en nuestras instalaciones


**—¿Cómo ha variado la seguridad, en cuanto a estrategia y logística, en los grandes casinos españoles?**

—Al evolucionar el tipo de delincuencia, hemos tenido que variar en nuestras instalaciones nuestros procedimientos. Con los años, hemos pasado de una seguridad reactiva, a una seguridad preventiva, todo ello gracias a la evolución humana y tecnológica que se ha dado dentro de los departamentos de Seguridad. ●

*Texto: Gemma G. Juanes.*
*Fotos: Flickr/Archivo*

**PABLO CAMPOS CORTÉS.** TECHNICAL SUPPORT ENGINEER. HIKVISION SPAIN


# Tecnología y soluciones completas al servicio de la seguridad

LOS casinos son uno de los escenarios más complejos a la hora de llevar a cabo una vigilancia efectiva. En ellos encontramos escenas en constante movimiento con múltiples contrastes y fuertes contraluces. Debido a sus altas exigencias de seguridad, y las diversas situaciones a las que prestar atención, como las mesas de juego, las máquinas, las cajas fuertes o las grandes aglomeraciones de personas, la máxima calidad de imagen y última tecnología son requeridas.

## Requerimientos en casinos

Todas estas condiciones hacen complicada la visualización de imágenes con claridad. Por ello se requiere de cámaras que tengan la capacidad de mostrar desde los colores más vivos a los más oscuros. Ciertos fabricantes de CCTV han desarrollado cámaras con un WDR de 140dB, que permiten obtener una imagen nítida por muy grande que sean los contraluces y en cualquier condición de luminosidad.

Así como cámaras que utilizan tecnologías específicas para situaciones de baja luminosidad, permitiendo visualizar imágenes que con las cámaras tradicionales serían imposibles de ver sin la ayuda de iluminación adicional.

## Alta calidad de imagen

En estos entornos que cuentan con múltiple información en escena y numerosos objetos a los que prestar atención, el poder apreciar pequeños detalles como el color de una ficha, o el valor de un billete es lo que marca la diferencia.

El uso de cámaras con resoluciones 4K proporciona una enorme mejora con respecto a las resoluciones megapíxel tradicionales, permitiendo aumentar el zoom digital sobre la imagen sin perder detalle, obteniendo así una imagen de gran calidad. Estas ventajas también tienen el inconveniente de un mayor consumo de ancho de banda y almacenamiento, por ello las soluciones de compresión como H.264+ o el H.265 se hacen imprescindibles cuando usamos estas resoluciones.

## Gran capacidad de gestión y almacenamiento

Debido a los altos requisitos en cuanto a almacenamiento y ancho de banda, se requiere de sistemas de grabación capaces de gestionar numerosos flujos de vídeo simultáneos de la manera más eficiente, y disponer de gran capacidad de grabación, permitiendo albergar un gran número de discos duros. Para resolver estos problemas, se utilizan los llamados «Super NVR», grabadores capaces de recibir 128 o 256 flujos de vídeo en una sola máquina, con grandes posibilidades de almacenamiento.

Además, en estas instalaciones se requiere visualizar las imágenes a una

alta velocidad en tiempo real, para permitir ver todos los detalles de las acciones a ritmo vertiginoso que tienen lugar en un casino. En estas ocasiones se necesitan dispositivos capaces de representar altas tasas de imágenes por segundo, llegando a alcanzar en algunos casos hasta las 60 ips, de manera que no se pierda ningún detalle por muy rápido que sea.

Otra de las principales características identificativas de este tipo de instalaciones es que es imprescindible tener el mayor nivel de detalle posible en la visualización en directo y en la reproducción. Es importante tanto una visualización en directo ágil, donde podamos dar un tiempo de respuesta rápido, como obtener un gran nivel de detalle en las grabaciones para poder, por ejemplo, hacer búsquedas forenses a posteriori de todos los elementos de la escena. Por esta razón es muy importante el uso de tecnologías que permiten hacer búsquedas inteligentes, de manera que podamos ahorrar tiempo a la hora de reproducir las grabaciones, identificando los eventos importantes que hayan tenido lugar.

## Visión general y en detalle

Las cámaras de 360º permiten obtener imágenes panorámicas de un gran escenario, mientras con los PTZ virtuales se pueden observar detalles dentro de esa misma escena con una única cámara, lo que permite disminuir el número de cámaras totales, ahorrando en el coste total de la infraestructura sin sacrificar en ningún momento la capacidad de visualización del sistema.

Algunos fabricantes disponen también de domos PTZ capaces de hacer un seguimiento automático de objetos, e incluso de enlazar la imagen de 360º con los domos PTZ, para que en caso de que suceda un evento o que se identifique un objeto interesante en la escena panorámica, el domo PTZ enfoque a ese objeto y le haga un seguimiento automático.

Puesto que los casinos y las salas de juego requieren de visualización de imágenes en altas resoluciones, es importante también invertir en el apartado de la visualización. Todas estas imágenes requieren de mucho procesamiento, por ello es necesario la utilización de dispositivos específicos, pensados exclusivamente en ofrecer la mejor imagen posible, como son los sistemas de decodificación.

Son estos sistemas los que nos permiten hacer video walls y grandes multipantallas, aportando gran facilidad a la hora de visualizar múltiples imágenes simultáneamente, y en un tamaño que aporte una mejor visibilidad a la hora de vigilar la instalación.

## Dar un valor añadido a la solución

Hoy en día es imprescindible que las cámaras de vigilancia aporten un valor añadido a nuestro sistema, además de la propia seguridad. Por ello se precisa que puedan aportar información valiosa a otros departamentos, como el de marketing o el de finanzas, desde donde se pueda tener acceso a datos como cuánta gente ha entrado durante el día y a qué horas lo han hecho, qué pasillos o zonas tienen más tránsito, y por tanto saber qué máquinas o mesas tienen más movimiento, reconocer qué personas han accedido al recinto o identificar matrículas importantes.

Para ello los fabricantes del sector han desarrollado soluciones específicas que permiten aunar esfuerzos entre estos departamentos, con cámaras para conteo de personas, que permiten conocer cuánta gente entra a nuestro recinto y a qué horas hay más afluencia. También existen soluciones que elaboran mapas de calor y permiten identificar qué zonas tienen más tránsito. O cámaras de detección facial, que nos proporcionan particularidades de los clientes para poder darles una mejor atención.

Además también existen soluciones para el reconocimiento de matrículas, en las que por ejemplo podemos tener un aviso cuando hay un acceso de un VIP, o de la llegada de un vehículo por el que se necesita avisar al departamento de Seguridad.

Por todos estos motivos, cada día es más importante la utilización de tecnologías y soluciones completas, que nos permitan hacer uso de todas estas nuevas herramientas para poder dar la mejor solución a nuestro sistema de seguridad. ●

**Fotos: Hikvision.**

Contactos de empresas, p. 7.

**ANA MAZO.** PROJECT MANAGER. TELECOMMUNICATION ENGINEER. FF. VIDEOSISTEMAS. GEUTEBRÜCK

# Tecnología, indispensable para salvaguardar la seguridad

SOLEMOS tratar la figura del casino como una instalación crítica desde un punto de vista de manejo de efectivo. Uno de los mayores retos a los que se enfrentan los casinos es la seguridad y la creación de una atmósfera de estabilidad forma parte de su objetivo diario, no sólo para salvaguardar la seguridad de los clientes y de los trabajadores ante un posible ataque externo de cualquier índole, sino que es indispensable para evitar que un casino tenga pérdidas.

Dentro de un casino existen dos tipos de entornos claramente diferenciados, de acuerdo a las necesidades que se desea cubrir en cuanto a seguridad. En primer lugar, existe una seguridad global, de seguimiento y control. Esto nos permite observar, de forma general, el paso de clientes y personal; sus movimientos y acciones, para saber en cada momento hacia dónde se dirige cada persona o grupo de personas, cómo se han dividido y cómo actúan. Por otro lado, existe la seguridad en cuanto al fraude del juego: la distinción de las cartas, la denominación de las fichas, además de ver el juego y el manejo del dinero.


Bien es sabido la cantidad de personal que tienen dedicado los casinos exclusivamente a la vigilancia: director, jefe y subjefes de seguridad, fisonomistas, recepcionistas y operadores TV, vigilantes de seguridad, etc., pero la tecnología es indispensable para salvaguardar esta seguridad, y han de apoyarse en ella y en sus avances para aprovechar las ventajas que brindan.

Todos los fabricantes ofrecen soluciones que se adaptan a las instalaciones críticas como los casinos y las salas de juego, y trabajan de una forma similar: acceso a las imágenes en tiempo real, a las grabaciones, registrar eventos, grandes capacidades de almacenamiento, centros de control con videowall, permisos de usuario, etc., y que a primera vista puede ser suficiente, pero siempre se puede mejorar.

Las cámaras vigilan su instalación y las imágenes se almacenan en su hardware, los vigilantes supervisan las escenas pero, ¿quién controla que todos los procesos se están llevando a cabo correctamente? ¿Estamos sufriendo algún sabotaje interno? ¿Los operadores cumplen las normas? Este es el talón de Aquiles de los gestores de vídeo.

Realizar una investigación para supervisar que se ha seguido el protoco-

lo correcto ante una incidencia supone una recopilación tediosa de datos manuales que la mayoría de las veces no aclaran la situación.

¿Sería necesario que el software le permitiera acceder a todos los movimientos que el vigilante ha tratado con un sólo clic? ¿Podríamos acceder al entorno de trabajo del vigilante en cualquier momento de su jornada laboral para supervisar su trabajo? ¿Seríamos capaces de ver en tiempo real los movimientos de los operadores? ¿Quién ha realizado una copia de seguridad y qué contenía esta copia? Con el nuevo gestor de la seguridad G-SIM esto y más es posible.

G-SIM es el potente sistema de gestión integral de la información de la seguridad para las soluciones de videovigilancia de Geutebrück que, con un manejo muy intuitivo, facilita la labor al vigilante del casino, optimizando el tiempo de respuesta y su toma de decisiones, reduciendo fallos humanos y carga de trabajo y ahorrando tiempo a la hora de tratar una incidencia, lo que supone un gran beneficio para el casino a la hora de mantener la discreción de la sala y la tranquilidad de los clientes.

Con la planimetría integrada en G-SIM accedemos simultáneamente a diferentes planos de la instalación y nos aporta la comodidad de arrastrar y soltar cámaras del plano al visor o viceversa para ubicar al operador en cada plano.

Como la organización y la colaboración entre usuarios en un casino es fundamental, este software permite enviar tareas, alarmas o mantener chats entre usuarios, así como compartir sus configuraciones, plantillas y demás funciones con las que cuenta. Además, tenemos la posibilidad de bloquear los permisos de los operadores locales en tiempo real, evitando así el acceso a información delicada.

> «¿Seríamos capaces de ver en tiempo real los movimientos de los operadores? ¿Quién ha realizado una copia de seguridad y qué contenía? Con el nuevo gestor de la seguridad G-SIM esto y más es posible

G-SIM permite asignar operadores con privilegios para el tratamiento de alarmas para poder asumir, revisar, confirmar éstas e incluso transferirlas a otro usuario para su análisis, evitando, así, la duplicidad de la gestión.

Además, con este sistema de gestión de la información, todo lo que hacen los vigilantes queda registrado: mensajes, cámaras que visualizan, sus medidas adoptadas, etc. De este modo podemos saber, sin excepción, qué, cómo, cuándo y dónde ha sucedido algo en todas y cada una de las instalaciones conectadas al servidor central de G-SIM. Así, ante cualquier duda, G-SIM ofrece la posibilidad de realizar informes detallados para documentar cualquier situación, imprimirlo en cualquier formato y enviarlo por correo electrónico. Realizando auditorías de la forma más completa.

No debemos olvidar la disponibilidad del sistema. Aportar una redundancia transparente al operador donde GSIM gestione la recuperación automática del equipo o equipos de respaldo, clonando las configuraciones de los equipos principales, manteniendo la operatividad de los usuarios de la instalación es imprescindible en este tipo de instalación.

En un casino, el dinero no sólo se lo juegan los clientes. Debemos tener muy presente que el negocio del casino requiere una inversión que sólo será rentable si se eligen los productos adecuados. Productos que estén en consonancia con las nuevas tecnologías, que se adapten a futuros cambios y que reúnan las características que G-SIM aporta para no realizar inversiones adicionales posteriores tanto de hardware como de software. ●

Fotos: FF Videosistemas

Contactos de empresas, p. 7.

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

# Sistemas automatizados de control de llaves en Casinos

## La solución ofrece acceso regulado y estructura de informes combinado con comodidad

EN regiones donde los juegos de azar autorizados tienen presencia, la seguridad para casinos se rige por normas y regulaciones estrictas que son establecidas por diversos organismos. Una de las áreas más críticas de la seguridad de casinos, la cual es objeto de estos convenios, es el control de llaves. Las llaves físicas se utilizan para acceder a todas las áreas más delicadas y de alta seguridad del casino, incluyendo salas de conteo y cajas de depósito, por lo que las normas y reglamentos que se relacionan con el control de llaves son muy importantes para mantener un control estricto y minimizar las pérdidas y el fraude.

Los reglamentos relativos al control de llaves se extienden desde los procedimientos necesarios para acceder a las cajas de depósito fuera del horario programado, hasta el número de firmas necesarias para acceder a las llaves que requieren que un usuario obtenga varios permisos para la llave específica solicitada. Cada actividad debe ser registrada y/o reportada para fines de auditoría.

Los casinos que anteriormente utilizaban registros manuales para el control de llaves estaban en riesgo constante debido a las imprecisiones inherentes al sistema, tales como las relativas a firmas faltantes o ilegibles. El proceso manual de registro de salida para las llaves era lento y propenso a errores. El análisis, la notificación e investigación eran muy laboriosos, ya que requerían revisar pilas y cajas de hojas de registro, por lo que también dificultaba mantener un control exacto del uso de la llave. Estos inconvenientes, junto con el impacto del cada vez mayor número de normas de cumplimiento, han llevado a que la administración de los casinos pase de los sistemas manuales a soluciones de sistemas electrónicos de control de llaves más confiables y convenientes.


Los sistemas electrónicos de control de llaves son una solución predefinida que ofrece múltiples capas de seguridad para el acceso, así como funciones de presentación de informes automatizados. Pueden acceder a las llaves protegidas en los armarios a prueba de manipulación las personas autorizadas, que presenten su identificación y hayan sido aprobados por el sistema para acceder a la llave solicitada. En algunos casos en los que es necesario acceder a ciertas llaves o juegos de llaves que

son altamente delicados, las regulaciones de cumplimiento requieren las firmas de tres individuos, cada uno de un departamento distinto. A menudo, los tres individuos incluirían un miembro del equipo de depósito, un cajero y un oficial de seguridad. La puerta del armario se abrirá y liberará las llaves solamente después de que los tres accesos requeridos estén completos y las credenciales verificadas.

La devolución de llaves altamente delicadas puede estar aún más regulada, y requiere múltiples niveles de seguridad. Por ejemplo, las regulaciones que obligan a «Full Secure» requerirían que los mismos usuarios que sacan la llave también la devuelvan, mientras que el «Departament Secure» sólo requeriría que las credenciales del primer usuario coincidan exactamente, mientras que los otros dos usuarios tendrían que coincidir por departamento.

Reglas adicionales especifican con más detalle quién puede tener acceso a las llaves y quién no. El acceso a las llaves de liberación de la caja de depósito de la mesa de juego está limitado a los empleados específicos que están autorizados para retirarlas. A estos mismos individuos se les impediría tener acceso a las llaves para el contenido de la caja de depósito de la mesa de juego, al mismo tiempo que hayan sacado las llaves de liberación de las mismas.

Las regulaciones de los juegos de azar exigen que se realice regularmente una cantidad de auditorías de diferente tipo para garantizar que el casino está en pleno cumplimiento de la normativa. Por ejemplo, en relación con los empleados, firmando para sacar o guardar las llaves de la caja de depósito de la mesa de juegos, los reglamentos de los juegos de azar de Nevada indican que se deben mantener informes independientes indicando la fecha, hora, número de mesa de juego, motivo para el acceso y/o firma electrónica. Los informes que detallan el acceso no programado, incluyendo la razón por la cual se produjo el acceso (por ejemplo, máquina atascada, disputa al cliente, reubicación o mantenimiento de la máquina) también son requeridos por muchas agencias de juegos de azar estatales y tribales. En el entorno móvil de hoy en día, los correos electrónicos y/o mensajes de texto SMS pueden generarse automáticamente y ser enviados a la gerencia en cualquier momento que se acceda a dichos juegos de llaves para depósitos no programados.

«Los sistemas electrónicos de control de llaves son una solución predefinida que ofrece múltiples capas de seguridad»

Además de simplificar el cumplimiento de estas reglas y regulaciones distintas, los sistemas electrónicos de control de llaves mejoran la comodidad de acceso a las llaves. Cuando se utiliza la función de liberación instantánea de llave, los usuarios sólo tienen que ingresar sus credenciales y el sistema sabe si ya han retirado sus llaves específicas. Si no lo han hecho, el sistema se desbloquea y sus llaves quedan inmediatamente disponibles para ellos. Devolver las llaves es igual de rápido y fácil.

El proceso ahorra tiempo, reduce la necesidad de capacitación y ayuda a superar cualquier barrera del idioma. El personal como las amas de llave y asistentes de piso de tragamonedas pueden ser organizados en «grupos». Por cada grupo, el hotel y casino tendrían disponibles múltiples copias de los mismos juegos de llaves respectivos; el sistema libera el siguiente juego disponible a cada usuario autorizado de un grupo y hace ciclos a través de los juegos, de manera que cada uno las use por igual.

En comparación con los sistemas manuales, los sistemas electrónicos de control de llaves son siempre una buena opción. ●

Fotos: Designed by Freepik

Contactos de empresas, p. 7.

**DEPARTAMENTO DE MARKETING.** LSB

# Aproximación al concepto de **control de accesos**

Los sistemas de control de accesos se utilizan en aplicaciones en las que es necesario restringir o delimitar el acceso de personas y/o vehículos a determinadas áreas (despachos, garajes, recintos deportivos, etc.), y en función a criterios diversos. El control debe aplicarse sobre elementos tales como puertas, tornos, barreras, ascensores, etc.

LA necesidad no es nueva pero sí los elementos y la forma de resolverla. En los últimos tiempos se detecta una enorme evolución en las soluciones que aporta el mercado. Dicha evolución se basa fundamentalmente en dos aspectos:

**–Desarrollo de numerosas aplicaciones de software para la gestión de los accesos**.

Se consigue básicamente almacenar en una base de datos toda la realidad que se produce en el día a día en los accesos controlados. Información valiosa si pensamos en cuestiones tanto de mero control como de seguridad.

Tradicionalmente han sido los fabricantes del hardware para control de acceso los que se han ocupado de añadir un software básico de gestión para sus sistemas; últimamente son los propios desarrolladores de software de monitorización de vídeo (VMS), los que implementan en sus aplicaciones una capa dedicada al control de accesos con gran funcionalidad, y se encargan de integrar en ellas diferentes variantes de hardware.

**–Introducción de la biometría en el hardware de control.**

Los antiguos elementos de identificación de la persona (tarjetas, claves, etc.) son ahora insuficientes (permiten olvido, robo, intercambio, etc.), y se imponen los sistemas biométricos (huella dactilar, iris, rostro, etc.) por tratarse de elementos de identificación inequívoca de la persona.

En el mercado existen básicamente dos arquitecturas diferentes para resolver las instalaciones:

1–lectores + placa controladora + software de gestión **(Imagen 1**)

Lectores esclavos cableados mediante diferentes protocolos de comunicación (Wiegand, RS-485, etc.), a una placa controladora central, la cual posee la inteligencia y gestiona toda la electrónica.

Recomendada en instalaciones más sofisticadas. Mayores posibilidades de hardware (entradas, salidas, relés, etc.)

Se abarata en el coste unitario de los lectores pero aparece el coste de la placa controladora, el cual se va incrementando según aumenta el número de salidas a controlar.

2-lectores-controladores + software de gestión **(Imagen 2)**

Lectores autónomos que a la vez son controladores y que se conectan directamente con la aplicación de software mediante diferentes protocolos de comunicación (TCPIP, RS485, etc.).

Recomendada para instalaciones con menos accesos a controlar y con menos necesidades de hardware (entradas, salidas, relés, etc.).

Desaparece el coste de la placa controladora aunque se incrementa el coste unitario de los lectores.

**Imagen 1**

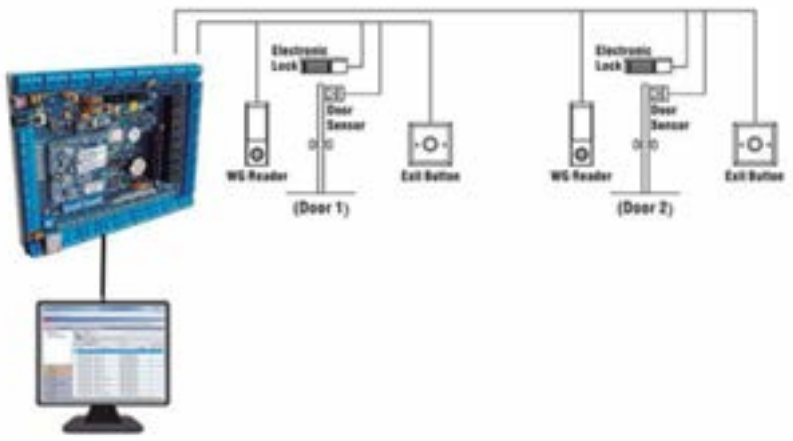


Imagen 4

Imagen 2


Imagen 3

**Componentes más importantes presentes en la instalación:**

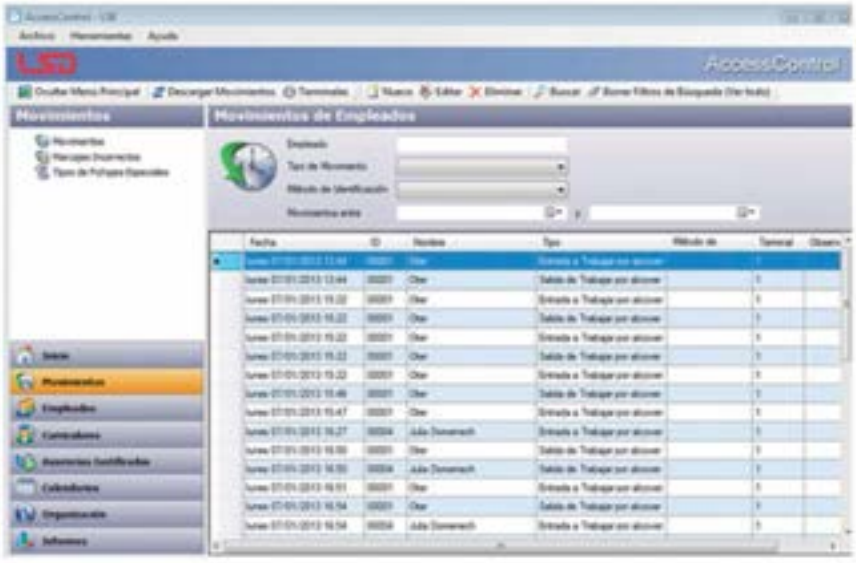
–Lectores **(Imagen 3)**

Existen múltiples tipos de lectores en función del método de reconocimiento que utilizan: Tarjetas de proximidad, huella dactilar, iris, etc. Atendiendo a aspectos de fiabilidad/precio, la huella dactilar es hoy por hoy el patrón biométrico más extendido. Se imponen los lectores que permiten el reconocimiento combinado (huella+tarjeta, huella+PIN, etc.) y aportan mayor seguridad. Como hemos comentado antes, existen lectores autónomos que recogen y almacenan la información y que posteriormente la pueden volcar a la base de datos de una aplicación de software, y lectores «aliviados» de electrónica, ya que funcionan como esclavos de una placa principal que les controla y que es la que almacena la información que recoge de ellos.

–Controladoras **(Imagen 4)**

Existen diferentes formatos de placas controladoras y sus variaciones se basan fundamentalmente en el número de accesos que permiten controlar (2,4,8); también de la cantidad de entradas y periféricos adicionales a los que den cabida (cerraduras eléctricas, pulsadores eléctricos, sensores magnéticos de apertura, alarmas, etc.)

Imagen 5



–Software **(Imagen 5)**

Como ya hemos comentado antes, el software aloja una base de datos que almacena los diferentes movimientos que se van produciendo en los diferentes accesos. Previamente existe un capítulo de configuración donde fundamentalmente se han de establecer una serie de filtros tales como los grupos, fechas y franjas horarias asignados a los usuarios y que delimitarán sus permisos de acceso.

El software permitirá generar valiosos informes y gestionar diferentes alarmas dependiendo de las necesidades de la instalación.

*Fotos: LSB*

Contactos de empresas, p. 7.

**AGUSTÍN LLOBET.** JEFE DE PRODUCTO DE CASMAR

# Tendencias en **control de accesos**

## Convergencia de Seguridad Mecánica y Electrónica

Desde los orígenes, la innovación ha sido una constante para la evolución de los sistemas de cierre mecánicos hasta nuestros días. En los últimos 10 años, y especialmente en los últimos 3, la incorporación de inteligencia a las cerraduras mecánicas está siendo una auténtica «revolución» tecnológica, que está cambiando de manera vertiginosa la forma de afrontar cualquier proyecto de gestión y control de accesos.

HAY algunas tendencias que nos pueden ayudar a entender este cambio de paradigma en el mundo de control de accesos:

1. Comunicaciones. La evolución de las redes de comunicaciones, la tecnología IP, los anchos de banda móviles 3G y 4G, permiten ahora gestionar cualquier sistema de Control de Accesos con facilidad y desde cualquier lugar, y nos permite además contar con sistemas de control de accesos 100% wireless online.

2. Movilidad. En paralelo a lo anterior, la proliferación de dispositivos móviles tipo smartphones y/o tablets, así como la facilidad de uso a través de Apps, ha propiciado inmediatez en la recepción de información de los accesos y en la gestión de los mismos, permitiendo incluso la apertura y/o bloqueo de puertas en movilidad y de una forma segura. «España es uno de los principales países de la Unión Europea con mayor penetración de teléfonos móviles inteligentes. El éxito de estos dispositivos en nuestras fronteras sigue en alza. Además, el consumo de redes sociales se extiende incluso a la empresa en un uso más profesional. En concreto, los smartphones ya están presentes en el 53,7% de la población española a partir de los 15 años, mientras que las tabletas llegan al 28,5% de los hogares españoles.» Fuente: ONTSI, Estudio «Sociedad en Red 2014»

3. Tecnología Inalámbrica. Al igual que ocurrió con los sistemas de intrusión a finales del siglo XX, cuando comenzaron a proliferar los sistemas de intrusión basados en comunicaciones wireless 433 MHz y 868 MHz, esta tecnología de comunicación inalámbrica bidireccional, encriptada y segura, permite ahora crear un ecosistema de accesos, que permite la conexión con las cerraduras inteligentes sin necesidad de desplegar un solo cable. Según el análisis de mercado realizado por IHS Research (Edición 2015), durante este año 2016 la demanda de controles de accesos inalámbricos crecerá un 1,2% por encima de los sistemas cableados en España, los cuales crecerán un 4,1% respecto a 2015. Las tecnologías de transmisión de datos de

# Con el TELÉFONO MÓVIL

## Qué puede hacer VIGILANT®

# NFC por tí

**Magnífica herramienta para la gestión de múltiples tareas en tiempo real.**

- INSPECCIONES
- SUPERVISIONES
- CONTROL DE TAREAS
- RONDAS
- CHECK LIST
- MANTENIMIENTOS
- RUTAS


VIGILANT®

SISTEMAS DE CONTROL

www.vigilant.es - info@vigilant.es - +34 965 856 457

corto alcance RFID y NFC, y de medio alcance como el BLE 4.0, son ya una realidad y se utilizan de manera habitual en muchos de los sistemas de acceso basados en cerraduras inteligentes autónomas.

4. Ahorro. Hemos podido comprobar durante los últimos 4 o 5 años, la importancia de poder economizar a la hora de afrontar cualquier proyecto de inversión, ya sea de nueva construcción o de reforma. Los sistemas de Control de Accesos basados en cerraduras inteligentes pueden resultar hasta un 60% más económicos que los sistemas cableados tradicionales, aportando como mínimo las mismas funcionalidades para el usuario final y con un mayor nivel de seguridad, puesto que no se necesita debilitar el conjunto de la puerta instalando cerraderos eléctricos. Se mantiene la seguridad en el conjunto puerta/marco.

5. Eficiencia energética. La alimentación autónoma mediante baterías, genera igualmente ahorros de hasta el 40% en el consumo de electricidad, frente a los viejos sistemas cableados que continúan necesitando de alimentación a 12 V y/o a 220 V.

La velocidad a la que están evolucionando los sistemas basados en cerraduras inteligentes, está siendo mucho mayor comparativamente hablando que la evolución de los sistemas cableados tradicionales de control de accesos. Desde el punto de vista de innovación, la incorporación de todas las ventajas tecnológicas que son tendencia, a las cerraduras, está siendo disruptivo en el mundo del control de accesos. Esta situación ha generado una oportunidad de negocio enorme, para aquellas empresas y profesionales que han dado el paso y han comenzado a trabajar con estas soluciones para cubrir las necesidades de sus clientes de una forma más segura y eficiente.

El norte de Europa y EEUU son en estos momentos las regiones más avanzadas en este campo, existiendo ya una nueva categoría profesional y compañías denominados «Híbridos», formadas por profesionales de la cerrajería en su mayoría, que han incorporado a su día a día las habilidades tecnológicas necesarias para poder vender, instalar y mantener soluciones basadas en cerraduras electrónicas. De la misma manera, los profesionales de la seguridad electrónica han dado el paso para incorporar conocimiento y habilidades mecánicas de seguridad, con el fin de desarrollar este nuevo negocio.

> «En breve las cerraduras inteligentes serán de aplicación también en nuestras casas, estamos solo en el principio...»

España, y más concretamente el País Vasco, es desde hace décadas cuna de la innovación tecnológica aplicada a los sistemas de cierre, liderando a nivel mundial la creación de esta nueva categoría basada en «cerraduras inteligentes», donde convergen seguridad mecánica y electrónica.

Ha nacido una nueva categoría de productos y soluciones mecánico/electrónicas, que requieren que las empresas instaladoras tradicionales de cerrajería y de electrónica de control de accesos salgan de su zona de confort. Desde el punto de vista de desarrollo de nuevos negocios, hay un inmenso «Océano azul lleno de peces, esperando a los nuevos e intrépidos pescadores». No podemos dejar escapar la oportunidad. Los nórdicos y los americanos ya lo están haciendo.

En breve las cerraduras inteligentes serán de aplicación también en nuestras casas, estamos sólo en el principio... ●

***Para la redacción de este artículo se ha contado con la colaboración de Tesa.**

*Fotos: Casmar*

Contactos de empresas, p. 7.

#EuroCloudExpo

EuroCloud ESPAÑA

EXPO 2016

LA NUBE ES PARA TODOS

# HAGAMOS SENCILLO LO COMPLEJO

## EUROCLOUD EXPO 2016

### TU CITA CON EL CLOUD

31 Marzo y 1 Abril - Madrid Rolling Chamartín

¡TE ESPERAMOS!

Regístrate en:
www.eurocloudspain.org

Organizan EuroCloud ESPAÑA TPI Grupo

EVVA

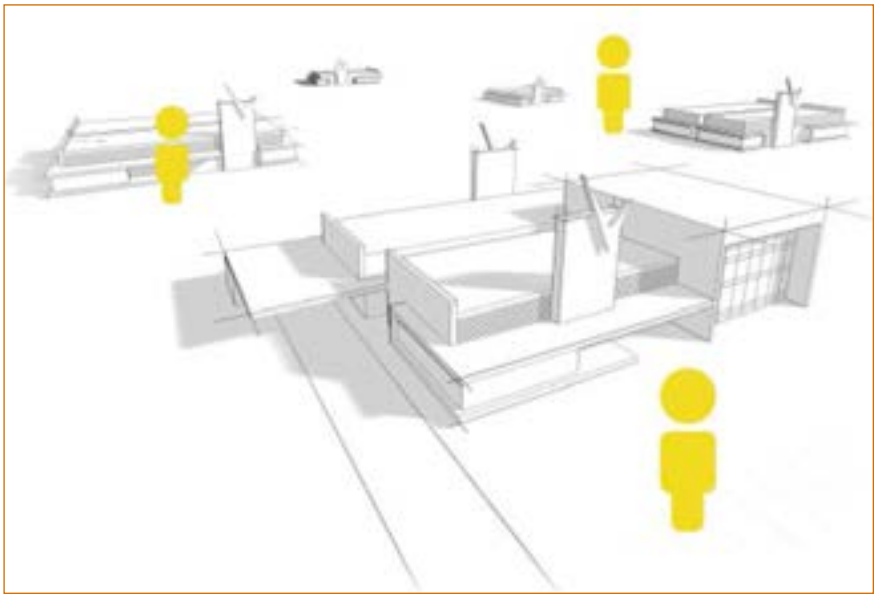
# Soluciones mecánicas perfectas + soluciones electrónicas innovadoras

EVVA es uno de los principales fabricantes europeos de soluciones de control de acceso, con una larga tradición en el diseño y fabricación de productos de alta seguridad. En 2014, EVVA presentó dos innovadores sistemas electrónicos de cierre: Xesar y AirKey, ambos resultado de muchos años de experiencia en soluciones electrónicas.

EVVA es una empresa familiar con sede en Viena (Austria), fundada en 1919 y dedicada en exclusiva a la alta seguridad. Las soluciones de EVVA, ampliamente testadas y probadas, ofrecen una protección óptima y de gran calidad, avalada por empresas, instituciones públicas y hogares de todo el mundo que depositan su confianza día tras día en los productos de EVVA.

Nuestros socios y partners en todo el mundo ofrecen soluciones personalizadas adaptadas a las necesidades de cada mercado. La continua labor del departamento de I+D, así como de los más de 730 empleados de la empresa –en la sede de Viena y en las nueve filiales en Europa–, deja huella en el sector europeo de la seguridad gracias a sus notables innovaciones. El objetivo a día de hoy es seguir ampliando la cartera de productos en el futuro y consolidar la presencia del Grupo EVVA en Europa de forma permanente.

EVVA está modernizando constantemente su proceso de fabricación sin aceite ni agua. La conocida como «fabricación limpia» ofrece grandes ventajas, especialmente para el medio ambiente. EVVA ha recibido numerosos premios gracias a la innovación permanente en el ámbito de la sostenibilidad.



## AIRKEY: el smartphone es la llave

Este sistema de control de acceso electrónico ofrece soluciones flexibles para el día a día, negocios con horarios flexibles y en particular empresas con varias sedes. Con AirKey, la llave se envía a través de Internet, a cualquier lugar del mundo y en cuestión de segundos. Todo lo que se necesita es un teléfono móvil compatible con NFC, conexión a Internet y un cilindro o un lector mural AirKey. La administración online permite especificar quién tiene los derechos de acceso, a qué instalaciones, durante qué periodo de tiempo y durante qué periodo de validez.

### Ventajas

AirKey es el primer sistema que ofrece a los propietarios o a las empresas, sin necesidad de infraestructura de TI propia, la opción de gestionar directamente el sistema de control de acceso desde la nube. Esto resulta especialmente útil a las organizaciones con la necesidad de gestionar varios establecimientos con una continua entrada y

salida de personas. Este sistema aporta numerosos beneficios para todos: A los usuarios les aporta una gran flexibilidad, y los propietarios tienen un control absoluto de todos los componentes de cierre. Asimismo la protección de datos está garantizada, ya que el sistema permite ajustar individualmente cada equipo según las pautas legales de protección de datos de cada país. AirKey aporta a las empresas con varias sedes o con estructuras complejas de personal una gestión sencilla de la solución de control de acceso. El sistema multi-administrador de AirKey permite la asignación de varios administradores que no sólo pueden gestionar cada uno de sus propios establecimientos por separado, sino que pueden controlar el sistema de control de acceso del conjunto de los establecimientos de la compañía.

### Fácil administración online

Nunca ha sido tan sencillo gestionar un sistema de control de acceso. Por ejemplo, se pueden conceder autorizaciones simplemente mediante «arrastrar y soltar» con el ratón. El nivel de anonimato y la gestión de los datos de acceso personales se pueden ajustar según las pautas legales de privacidad. Los datos permanecen siempre almacenados de forma segura en los servidores de alta seguridad de EVVA.

## XESAR: La solución de seguridad integral

El sistema de control de acceso electrónico Xesar ofrece a las empresas una amplia variedad de productos, áreas de aplicación junto con un diseño estilizado y atemporal. Xesar puntúa alto entre los usuarios gracias a su fácil instalación, el software gratuito y el sistema de KeyCredits exclusivo de EVVA.

### Flexible y seguro

Xesar no sólo asegura los edificios desde el interior y el exterior, sino que también facilita la administración del sistema, permite un ahorro de costes y si la empresa crece, Xesar crece con ella. Las áreas exteriores de los edificios son cada vez más transparentes, especialmente debido a la tendencia a construir con paneles frontales de cristal. La seguridad interior, obviamente, también es de suma importancia: salas de servidores, archivos de documentos, oficinas de los directivos y administradores… Todas estas áreas se deben asegurar de forma individual.

### La seguridad de un vistazo

Cada componente Xesar tiene su función y potencial. El producto ideal para cada situación se adapta a la ubicación de la instalación, las demandas de seguridad y el nivel de comodidad requerida. El escudo Xesar es el componente todoterreno, con una gran facilidad de manejo y perfectamente adecuado para aplicaciones en exteriores o interiores. Los cilindros Xesar son ideales si lo que se busca es seguridad y fácil adaptación, ya que cierra de forma segura y es fácil de instalar. La manilla Xesar es la solución ideal para cualquier puerta interior incluidas las puertas de vidrio. El lector mural Xesar está equipado con una unidad de control para accionar los componentes de cierre electrónico (por ejemplo, puertas correderas). El lector mural también puede ser utilizado como actualizador y representa así un elemento central dentro de la Red Virtual Xesar. El software gratuito es fácil de instalar y los KeyCredits de EVVA garantizan que el cliente pague lo que realmente necesita. Y lo mejor de todo: No se requiere cableado para la instalación (salvo para el lector mural).

### Combinación de seguridad mecánica y electrónica

Un sistema mecánico que se combina con un sistema electrónico reúne lo mejor de ambos mundos. Los sistemas mecánicos de control de acceso han sido tradicionalmente un elemento clave en la construcción de la seguridad. Son robustos, duraderos y extremadamente estables. Cuando se combinan con la tecnología de control de acceso electrónico, se obtienen soluciones de seguridad versátiles. El sistema de control de acceso electrónico permite a su vez la autorización de acceso restringido y el control del tiempo, las listas de eventos y el seguimiento posterior. La combinación de ambos tipos de sistema es particularmente importante para el acceso a zonas altamente sensibles. ●

*Fotos: EVVA*

Contactos de empresas, p. 7.

**CARLOS VALENCIANO.** SALES MANAGER SMARTAIR™. TESA ASSA ABLOY

# M-Commerce

## Nuevo modelo de negocio disruptivo aplicado al control y gestión de accesos

¿Qué es el M-Commerce? «M-Commerce o comercio móvil (del anglicismo Mobile Commerce) toma sus bases del e-commerce, solo que llevando todas las transacciones a nivel de poder ser ejecutadas desde un teléfono móvil o SMARTphone u otros dispositivos inalámbricos móviles.» Wikipedia.
Esta es la evolución natural de los modelos de negocio actuales de e-commerce, llevados al siguiente nivel, o dicho de otra manera, es la capacidad de interactuar con nuestros smartphones con el mundo físico y realizar transacciones de datos.


ALGUNOS ejemplos de aplicación diaria del M-Commerce: Tarjetas de crédito virtualizadas, billetes y/o tarjetas de transporte (Bus, Tren, etc), tarjetas de fidelización y controles de accesos.

Vamos a centrarnos en este nuevo aspecto de los controles de accesos, y más concretamente en la virtualización de las credenciales habituales como tarjetas, tags, pulseras, etc, convirtiendo el smartphone en la «llave» para acceder a nuestros sistemas de control de accesos.

Convergen en estos momentos en el mercado varias tendencias tecnológicas que han madurado durante los últimos 10 años, y que han hecho posible esta nueva realidad de poder interactuar con nuestro smartphone a modo de credencial con nuestras puertas y accesos:

1.**Comunicaciones**. La evolución de las redes de comunicaciones, la tecnología IP, los anchos de banda móviles, 3G, 4G, la proliferación de sistemas de accesos basados en inteligencia distribuida en cerraduras inteligentes y autónomas, permiten ahora gestionar cualquier sistema de control de accesos con facilidad y desde cualquier lugar, y nos permite además contar con sistemas de control de accesos 100% wireless online.

2.**Movilidad**. En paralelo a lo anterior, la proliferación de dispositivos móviles tipo smartphone y/o tablets, así como la facilidad de uso a través de apps ha propiciado inmediatez en la recepción de información de los accesos y en la gestión de los mismos, permitiendo incluso la apertura y/o bloqueo de puertas en movilidad y de una forma segura. «España es uno de los principales países de la Unión Europea con mayor penetración de smartphones. El éxito de estos dispositivos en nuestras fronteras sigue al alza. En concreto, los smartphones ya están presentes en el 59,3% de la población española a partir de 15 años, mientras que el 95,3% de los hogares españoles disponen de telefonía móvil.» Fuente: ONTSI, Estudio «Sociedad en Red 2015».

3.**Tecnología inalámbrica.** Al igual que ocurrió con los sistemas de intrusión a finales del siglo XX, cuando comenzaron a proliferar los sistemas de intrusión basados en comunicaciones wireless 433 mHz y 868 mHz, esta tecnología de comunicación inalámbrica bidireccional, encriptada y segura, permite ahora crear un ecosistema de accesos, conectando con los dispositivos inteligentes sin necesidad de desplegar un solo cable. Según el análisis de mercado realizado por IHS Research (Edición 2015), durante este año 2016, la demanda de controles de acceso inalámbricos crece un 1,3% por encima de los sistemas cableados en España que crecerán un 4,1%. Las tecnologías de transmisión de datos de corto alcance RFID y NFC y de medio alcance como el BLE 4.0 son ya una realidad, y se utilizan de manera habitual en muchos de los

sistemas de control de accesos basados en cerraduras inteligentes autónomas.

España y la ingeniería española, una vez más se colocan a la vanguardia en el diseño de soluciones innovadoras y disruptivas, que cambiarán la forma de interactuar con nuestras puertas en el siglo XXI.

El pasado mes de noviembre de 2015, se ha producido un hito para la innovación dentro del marco del M-Commerce, el desarrollo y el trabajo conjunto de dos compañías, una de telecomunicaciones (Vodafone España) y otra fabricante de sistemas de controles de accesos basados en cerraduras inteligentes SMARTair™ (TESA Assa Abloy), ha propiciado el lanzamiento de la primera solución de accesos corporativos del mundo donde el elemento físico para la apertura de las puertas es un smartphone, y donde la información sensible de identificación de accesos se guarda en la tarjeta SIM (el lugar más seguro de un SMARTphone). Un gesto tan sencillo como es el de acercar nuestro móvil a una cerradura y que ésta se abra, se convertirá en algo cotidiano gracias a esta importante innovación.

¿Cuál es la arquitectura y las tecnologías que hay detrás de este gesto tan sencillo?

Los elementos necesarios para que el smartphone interactúe con los dispositivos de control de accesos inteligentes son:

1. La red de Vodafone: es la base de todas las comunicaciones OTA (over the air), necesarias para ofrecer el servicio de gestión de accesos en la SIM de Vodafone.

2. La SIM NFC con tecnología MIFARE de Vodafone: Donde se guardan las claves de acceso del empleado de forma totalmente segura, de acuerdo a los estándares técnicos definidos por Global Platform.

3. La integración técnica entre Vodafone y TESA Assa Abloy a través de sus respectivos partners, para permitir que la tarjeta de acceso de TESA Assa Abloy se envíe y se guarde en la SIM de Vodafone en el dominio de seguridad correspondiente.

4. Dispositivos de cierre SMARTair™ de TESA Assa Abloy (manillas y cilindros electrónicos y lectores murales), los HUB RF que envían y recogen información de esos dispositivos y que lo comunican con el servidor de gestión central a través de la licencia de software TS1000 de SMARTair™.

5. La aplicación gratuita Vodafone Wallet disponible en Google Play: actúa como cartera virtual para las tarjetas de clientes (pagos, transporte, cupones, tarjetas de puntos…) entre las que se encuentran las tarjetas de acceso corporativas.

6. Un móvil con tecnología NFC: Más del 75% de los móviles que distribuye Vodafone ya cuentan con esta tecnología. ●

*Fotos: Fotos: TESA Assa Abloy*

Contactos de empresas, p. 7.

**JUAN SANDOVAL GONZÁLEZ.** DIRECTOR DE I+D. ARQUERO SISTEMA CORPORATIVO

# Implantación de la **gestión de visitas**

## Arquero ha implantado la solución de seguridad física de DHL Freight en su centro de Coslada

Los sistemas de gestión de visitas, control de accesos, intrusión, vídeo vigilancia e incendios se monitorizan y operan de una forma integral. El centro logístico de Coslada de DHL ha recibido la certificación TAPA donde Arquero ha aportado la solución tecnológica para la gestión de visitas integrada con el control de accesos y vídeo vigilancia.

EL centro se ha estructurado en tres grandes áreas de acceso para visitantes, el exterior, almacén y oficinas, con sendos puntos de control e identificación de visitantes.

El acceso al centro logístico se controla en la garita de acceso desde la vía pública. En este punto se identifica al visitante y se le entrega una etiqueta adhesiva, con sus datos personales y datos de la visita, que debe llevar visible durante su estancia.

La introducción de los datos personales se puede realizar mediante un escáner OCR o manualmente. Para evitar la duplicación de la ficha de visitante cuando éste presenta un nuevo documento identificativo (DNI, carné de identidad de otro país, carné de conducir, tarjeta residente, pasaporte…) , se realiza una búsqueda previa con su nombre, apellidos y fecha de nacimiento. La ficha de un visitante soporta hasta cuatro documentos identificativos, almacenando las imágenes del anverso y reverso de cada uno de ellos.


En esta fase se determina el empleado al que visita y se le asigna como derecho de acceso sólo el itinerario (conjunto de puertas) que da paso a la entrada de las oficinas y del almacén.

El visitante debe personarse en el punto de control del almacén o de las oficinas, según su destino. Es en este punto donde, de una forma muy simple (seleccionando la visita en el listado de visitas activas), se le amplía la visita asignándole una tarjeta y ampliando el conjunto de itinerarios por los que puede transitar.

## Parametrización avanzada

Además de los datos básicos de los visitantes (nombre, apellidos, fecha nacimiento, teléfono, dirección, empresa…) Arquero permite configurar hasta treinta campos de libre disposición. Las visitas, además de identificar al visitante, trabajador visitado, fecha y hora de

entrada y salida y derechos de acceso, permite la configuración de diez campos de libre disposición.

Estos campos, además de una etiqueta personalizada permiten definir el tipo de dato que almacenan, permitiendo datos numéricos, cadenas de caracteres, booleanos y enumerados (un conjunto de valores). El tipado de los campos simplifica el trabajo del operador (en un booleano sólo tiene que clicar sobre un check, en un enumerado sólo tiene que seleccionar el valor en un desplegable), además de reducir los errores y el tiempo de operación.

Entre los campos que se suelen usar para los visitantes podemos destacar «tipo», enumerado con «subcontrata», «comercial», «pariente trabajador»,...; y «habitual», booleano. En la visita la actividad, enumerado «carga», «descarga», «servicio», «visita», «otro»; el tipo de vehículo, «coche particular», «furgoneta», «camión», «moto», otro; la matrícula de la cabeza tractora, la matrícula del remolque y color del vehículo.

Los derechos de los operadores de los puntos de control están configurados para que sólo puedan realizar visitas a un subconjunto de los itinerarios (rutas de tránsito de personas y vehículos) existentes. El operador de la garita sólo puede crear visitas para el exterior de los edificios, el de almacén para este itinerario, mientras que el operador de oficinas dispone de la facilidad de asociar cualquiera de los múltiples itinerarios configurados en su ámbito.

## Aplicación punto de control

El objetivo de la aplicación del punto de control es la sencillez y rapidez de uso. Por ello toda la visita se gestiona con un proceso guiado («wizard»), permitiendo sólo los procesos simples, visita de un invitado para el día actual o como máximo para su salida al día siguiente. El uso del escáner OCR permite la recuperación de todos los datos del visitante y, si ya existe en la base de datos, pasar directamente al resto de los datos de la visita. Si no existe la pantalla de alta permite la edición y ampliación de los datos.

## Aplicación administrador

A diferencia del punto de control esta aplicación es más versátil, permitiendo la creación de visitas para múltiples visitantes y con cualquier rango temporal.

## Seguridad Avanzada

Al ser la base de datos única para toda la corporación (con una copia replicada en cada centro) se comparten los datos de los visitantes, reduciendo los tiempos del proceso de registro y permitiendo también declarar a una persona «non-grata» y que este estado se aplique automáticamente en todas las instalaciones.

Una persona non-grata podría tratar de burlar la seguridad enseñando un documento identificativo distinto (la primera vez el DNI y la siguiente el pasaporte o carné de conducir). Para evitarlo el sistema busca en la base de datos de forma automática registros de visitantes que tengan el mismo nombre, apellidos y fecha de nacimiento y muestra al operador las coincidencias para que tome una decisión.

Cualquier actividad desarrollada por los visitantes, normalmente en su paso por los controles de acceso, queda registrada. A partir de estos registros y con independencia del proveedor de los sistemas de vídeo, se puede obtener la grabación de las cámaras que monitorizaron el evento.

*Fotos: Arquero*

Contactos de empresas, p. 7.

**PEDRO NIETO.** DIRECTOR DE MARKETING Y DESARROLLO DE PRODUCTO. STI CARD

# Una apuesta por la **biometría**

En nuestra sociedad, en la que la tecnología sufre avances a pasos agigantados en ámbitos muy diversos de lo cotidiano, es habitual encontrarse aún con sistemas tradicionales de seguridad en un control de accesos, basados en barreras físicas controladas por personal de vigilancia. Tampoco es extraño que los trabajadores sigan utilizando sistemas de fichaje basados en un soporte físico como la tarjeta plástica de banda magnética o, en el mejor de los casos, de proximidad RFID.

La seguridad en nuestro país sigue estancada en el uso de algo que tenemos, la tarjeta, o algo que sabemos, una contraseña o clave, que son todo, menos seguras. Sistemas vulnerables con presunción de «personal e intransferible». Nada más lejos de la realidad.

Frente a los sistemas tradicionales, se impone cada vez más una solución de control de accesos y control horario basada en el uso de un rasgo único y distintivo del individuo, algo que somos, es decir, la biometría.

El uso de terminales biométricos reporta beneficios importantes para las empresas, aumentando la seguridad, reduciendo las posibilidades de intrusión y fichajes fraudulentos, así como disminuye los costes de mantenimiento de los sistemas de seguridad y autenticación que existen previamente.

Lo que también parece evidente es que aquí, donde la tecnología biométrica aún está en su fase embrionaria en cuanto a implantación y aceptación, no resulta aconsejable ni rentable implementar sistemas biométricos complejos, siendo la biometría de huella dactilar o el reconocimiento facial los más recomendables por su sencillo manejo.


Las huellas digitales son patrones definidos de elevación de los poros de la piel. Los puntos formados por las líneas que describen dichos patrones, reciben el nombre de minucia y pueden ser replicados usando diferentes técnicas fraudulentas, desde las más sencillas como una fotocopia de la superficie del dedo, hasta complejos moldes en látex o silicona. Fabricar una huella falsa artificial, hecha de silicona, goma, película, papel o gelatina, es relativamente sencillo, con tutoriales al alcance de cualquiera en Youtube.

## Lectores biométricos

La mayoría de los lectores biométricos de huella dactilar existentes en el mercado, pueden ser superados usando una variedad de métodos comúnmente conocidos. Esto conduce a una tecnología biométrica inútil, ya que el nivel de seguridad no protege a las empresas de las pérdidas derivadas de fichajes fraudulentos y además no brindan el nivel de seguridad requerido por la administración pública, aeropuertos, cuerpos de seguridad, ejército y organizaciones comerciales.

Sin embargo, existen terminales biométricos que incorporan una patente del fabricante para la detección de huellas dactilares falsas (Fake Fingerprint Detection), que permite diferenciar un dedo real (vivo), de una huella

falsa. La mayoría de los terminales de control de acceso y presencia VIRDI se basan en la tecnología biométrica de reconocimiento de huellas dactilares, con dicha patente, combinadas con otras tecnologías como el reconocimiento facial o el uso de tarjetas de proximidad.

Los sensores de huella dactilar patentados de los terminales VIRDI, incorporan un sistema de detección basado en la capacitancia o detección y medición de esta característica electromagnética de un dedo humano, presentado sobre la superficie de un sensor óptico. Además, emiten una luz infrarroja sobre el dedo colocado en el escáner, midiendo la frecuencia de reflexión de éste para identificar su composición química.

El sensor sólo emite luz LED de color blanco al detectar la presencia de un dedo vivo, ahorrando energía y aumentando la durabilidad del propio dispositivo.

Por último, un algoritmo patentado del fabricante analiza la deformación y puntos característicos de la imagen (crestas y valles de la huella dactilar), consiguiendo diferenciar falsificaciones fabricadas en otros materiales.

## Reconocimiento facial

En cuanto a la biometría de reconocimiento facial, a pesar de ser una tecnología más sencilla para el usuario, resulta a veces tediosa en el registro y la autenticación, puesto que depende de condiciones de luz diversas, de la altura y apariencia del individuo, e incluso obliga a cómicas muecas y genuflexiones delante del propio dispositivo de reconocimiento.

Sin embargo, VIRDI resuelve este problema con un dispositivo de reconocimiento facial como el AC-7000, en el que se integran dos cámaras auto basculantes de color e infrarrojos. Estas dos cámaras y su funcionamiento simultáneo permiten detectar la presencia de una cara a dos metros y medio de distancia, facilitando la autenticación del usuario rápidamente, pivotando sobre el eje vertical, a tan solo 80 centímetros. Y por si fuera poco, el lector biométrico permite combinar esta tecnología avanzada de reconocimiento facial con un lector de huellas capaz de detectar falsificaciones y certificación PIV del FBI, así como emplear una tarjeta de proximidad RFID dual e incluso una clave numérica, introducida a través de una pantalla táctil de gran tamaño.

## Entorno móvil

Vivimos en un entorno móvil, donde el uso de teléfonos inteligentes es una realidad. El sector de la Seguridad no puede permanecer ajeno a todo esto y ya es posible que el usuario emplee su propio teléfono para abrir una puerta. VIRDI incorpora en sus nuevos dispositivos la funcionalidad de «llave en el móvil» que permite, a través de una app, emplear una llave virtual, almacenada en un Smartphone para abrir puertas mediante conectividad bluetooth, simplemente acercando su teléfono al terminal biométrico de control de accesos. Sin duda, se trata de un valor añadido sobre los sistemas existentes, permitiendo que los usuarios accedan a una oficina, hotel, vivienda, etc., con sus propios dispositivos móviles sin necesidad de tener que llevar consigo llaves o tarjetas de acceso.

*Fotos: STI Card*

Contactos de empresas, p. 7.

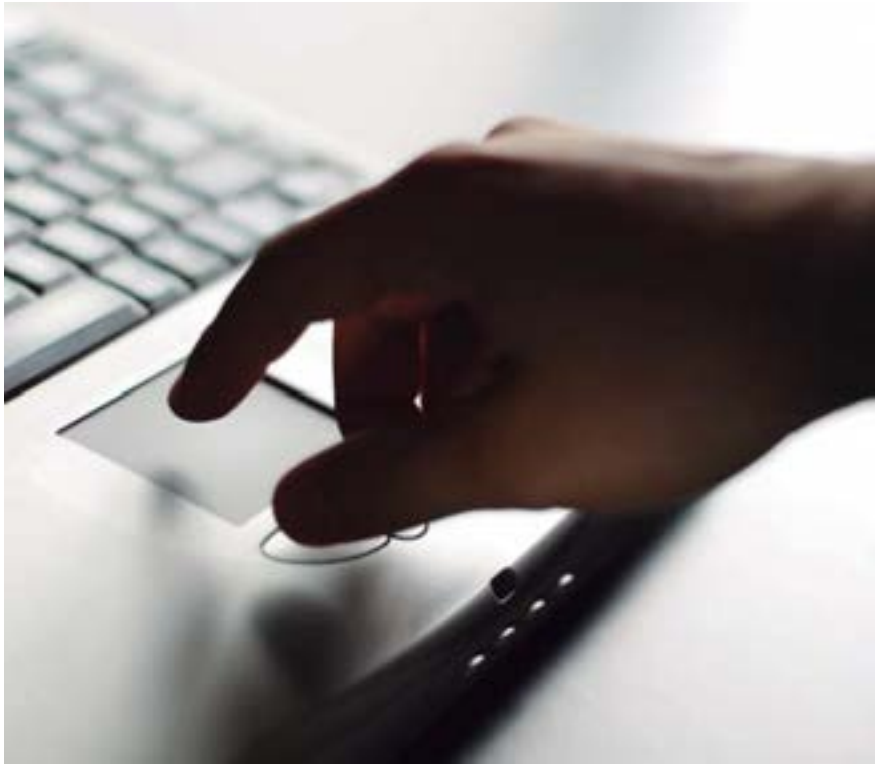
**MARÍA JOSÉ DE LA CALLE.** COFUNDADORA, DIRECTORA DE COMUNICACIÓN & ANALISTA SENIOR DE ITTI. mjdelacalle@ittrendinstitute.org

# El «Ábrete sésamo» digital

**«The age of the password is over. We just haven´t realized it yet»[1] Mat Honan -Wired 11/2012**

Diciendo las palabras entrecomilladas que forman parte del título de este artículo, se abría la puerta de la cueva donde los ladrones del cuento «Alí Babá y los 40 ladrones» guardaban su botín. Creían que esta contraseña era segura dado que sólo la conocían ellos, craso error, no pensaron que alguien los estuviera espiando y la escuchara, con lo cual, como no la cambiaban después de su uso, esa persona -Alí Babá- podía franquear la entrada cuando quisiera y apoderarse de parte del botín.

LAS contraseñas son tan viejas como la civilización y al mismo tiempo siempre ha habido personas dispuestas a hacerse con ellas o, en el caso digital, a «crakearlas». Por una parte, éstas se colocan con el fin de proteger un bien de la vista o acceso público, y así prevenir un daño que la revelación o el robo pudiera causar al bien en sí, a una organización o a las personas; y por otra, los atacantes quieren obtener algún beneficio que el acceso a ese bien les proporcione, normalmente en contra de los intereses de los atacados.



Cuando se llegó al mundo de los ordenadores y se quiso controlar el acceso a estos, se crearon unas pequeñas aplicaciones de acceso para capturar una identificación de usuario (UserID) que quería entrar y una contraseña asociada, la cual validaba al usuario, a diferencia del caso del cuento, en el que la contraseña era la llave de la puerta, independientemente de quién la tuviera.

Uno de los primeros ordenadores con control de acceso fue, allá por 1961, el «Compatible Time-Sharing System» del MIT, usando un login –usuario y contraseña, que conformaban un proceso de autenticación– con el fin de repartir y controlar el tiempo de uso del mismo. Sin embargo, en 1962 un estudiante de doctorado llamado Allan Scherr quiso conseguir más tiempo del autorizado, para lo cual engañó al login con un simple ataque –hack–: localizó el fichero que contenía las contraseñas y las imprimió, con lo que consiguió tanto tiempo como deseara.

## ... Y llegó internet

En el caso de la ciberseguridad, lo que se quiere proteger es la información, entendida ésta tanto como el código que define lo que la máquina puede hacer co-

*Las notas, debido a su extensión, aparecen al final del artículo.

mo los datos que residen en ellas o que están en tránsito por redes y otros elementos que intervienen en las comunicaciones, así como la identidad de todo ello: tipo de máquina, sistema operativo y su versión, protocolo, etc. Para ello se instrumentan controles de acceso a las máquinas y redes, inspecciones de lo que circula por ellas, y, como los sistemas son vulnerables en mayor o menor grado, se cifra toda la información –o sería conveniente hacerlo–.

En su inicio las redes de ordenadores de las empresas eran privadas y sin acceso desde el exterior. Para buscar los usuarios y contraseñas de acceso, había que hacerlo desde dentro.

En los primeros años de desarrollo de la web, eran pocas las aplicaciones que estaban en la nube, una de las cuales fue el correo electrónico. Para el acceso se tenía un usuario –la propia dirección de correo– y una contraseña, usuario que serviría más adelante a otras aplicaciones, y práctica que se conserva en muchos casos, haciendo crecer la vulnerabilidad de la información: con un único usuario –y quizás la misma contraseña del correo– se accede a más sitios.

Un ejemplo sería el uso en las redes sociales del correo corporativo, susceptible al envío de phising a los empleados a través de las mismas, indetectable por los antivirus de correo, y creando un vector de ataque para desplegar malware, tal y como contaba Yelena Osin el pasado julio de 2015[2] sobre el ataque sufrido por W.W.Grainger, proveedor industrial de EEUU.

Con la generalización del uso de Internet, no sólo se tenía acceso al correo, también al banco, a la Administración del Estado, a diversas tiendas para realizar compras, a las redes sociales, y así un largo etcétera, y los tipos de dispositivos desde los cuales se podía acceder también se multiplicaron y se hicieron móviles, siendo utilizados profusamente para la vida cotidiana.

En cuanto a las empresas, en lugar de conectar sus ordenadores vía redes privadas, se conectaron vía Internet, facilitando la entrada desde el exterior de la organización. A esto hay que añadir que, al igual que en el ámbito privado, el terminal desde el cual se accedía a las aplicaciones y datos de la empresa también se hizo móvil y ya no estaba encuadrado dentro de unas paredes, pudiendo estar siempre conectados desde cualquier sitio y en cualquier momento. Los límites de la empresa dejaron de ser físicos, como eran las puertas, pudiendo ahora servir de «puerta» cualquier dispositivo que tuviera una conexión a la empresa, no necesariamente por cable.


«El sistema de contraseña, que se ha visto ineficaz, se basa en el factor de autenticación de lo que el usuario sabe»

Con todo esto, el número de ataques a los sistemas aumentó, tanto por la facilidad de acceso como porque lo que se podía encontrar buceando por dispositivos y redes también devolvía más réditos.

Las intenciones de aquellos que entraban sin permiso cambiaron. Lo que al principio eran meros ataques con la intención de curiosear, de hacerse para uso propio con algún material para, como en el caso de Allan Scherr, obtener un beneficio personal, se transformó en delitos organizados de robos de información para terceros, robo de dinero, daños a instalaciones, y todo un glosario de delitos cuya novedad principal era –y es– la forma de llevarlos a cabo, desde cualquier sitio del planeta, sentado tranquilamente en una habitación, realizado de forma anónima en la medida de lo posible –en internet todo deja rastro–, y desde países distintos del objetivo del ataque, dificultando con ello su persecución -Internet es global pero las leyes son locales.

Según un informe[3] de Symantec publicado en abril del 2014, en el año 2012 se produjeron 156 violaciones de seguridad con 93 millones de identidades divulgadas, en el año 2013 el número aumentó hasta 253 –62% más– con 552 millones de identidades divulgadas –493 % más–.

Las violaciones de seguridad en las


empresas en 2014 aumentaron un 46% con respecto a 2013, según Gemalto en su «Breach Level Index 2014»[4]. Éstas ocasionan pérdidas monetarias, robo o destrucción de datos y daños a la imagen de la empresa, por citar algunas consecuencias no deseadas. Según un informe[5] de «Kaspersky Lab» de septiembre de 2015, la media del presupuesto requerido para recobrarse de uno de estos incidentes de seguridad es de 551.000 $ para empresas grandes, y para pequeñas y medianas empresas es de 38.000 $.

## Las contraseñas se fortifican: ¿y sirve de algo?

A pesar de que el sistema de contraseñas parecía ser un poco débil, no se ha abandonado esta forma de control de acceso nacido en una época antes de Internet, más bien se ha querido reforzar con las llamadas «contraseñas fuertes», contraseñas de al menos 8 caracteres sin significado, combinando letras, números y símbolos tipográficos, mayúsculas y minúsculas.

Pero tanto débiles como fuertes, las maneras de obtener ilícitamente dichas contraseñas se han revelado bastantes efectivas. Entre ellas podemos citar: la fuerza bruta –ir probando contraseñas extraídas de los llamados diccionarios o listas de las mismas recopiladas a través de los años–; los programas keylogger –recogen códigos de las teclas pulsadas–; el uso de los procesos habilitados para, en caso de olvido, poder dar de alta una contraseña sin conocer la anterior, utilizados por los atacantes que, suplantando al propietario del «UserID», consiguen unas nuevas credenciales asociadas al usuario; o los ataques de phising.

Es cierto que las empresas han adoptado la medida de seguridad de cifrar las contraseñas, sin embargo millones de hashes –contraseñas cifradas– más o menos crakeables, se descargan en los ataques a empresas como Linkedin, Yahoo, eHarmony o Ashley Madison y, los «buenos» las publican, los «malos» las venden, con lo que la práctica de reutilizar usuarios y contraseñas para distintos sitios de la web no es nada recomendable.

¡Ay! Somos humanos y lo de recordar largas contraseñas que no respondan a patrones, que no signifiquen nada, que mezclen distintos tipos de caracteres en mayúsculas y minúsculas y, además distintas para cada sitio al cual se acceda, y además tener que cambiarlas periódicamente, es una tarea poco menos que imposible.

Para poder cargar con esta pesada carga se han creado programas de gestión de contraseñas, los cuales se supone que con una sola que conozcamos que nos permita ejecutar dicho programa para editar las demás, éstas permanecerán, cifradas, a buen recaudo. Claro, que esto tiene el peligro de que al «poner todos los huevos en la misma cesta», si se rompe la cesta nos quedamos sin nada. Esto es lo que le pasó al gestor de contraseñas «LastPass»[6] en el que el pasado 15 de junio de 2015 la empresa que lo administra detectó una intrusión en sus servidores. Aunque parece que se consiguió mantener en secreto las contraseñas de los usuarios, se filtraron detalles importantes como direcciones de correos de usuarios y correos recordando contraseñas olvidadas.

El sistema de contraseña, que se ha visto ineficaz, se basa en el factor de autenticación de lo que el usuario sabe. Pero hay otros factores de autenticación como «lo que se posee», un token, por ejemplo, que no hay que recordar nada pero se puede perder o se puede robar; o «lo que se es», es decir, la autenticación biométrica, aunque ésta, más que constituir una contrase-

ña es más bien el UserID; o incluso «lo que se hace», llamado factor de comportamiento.

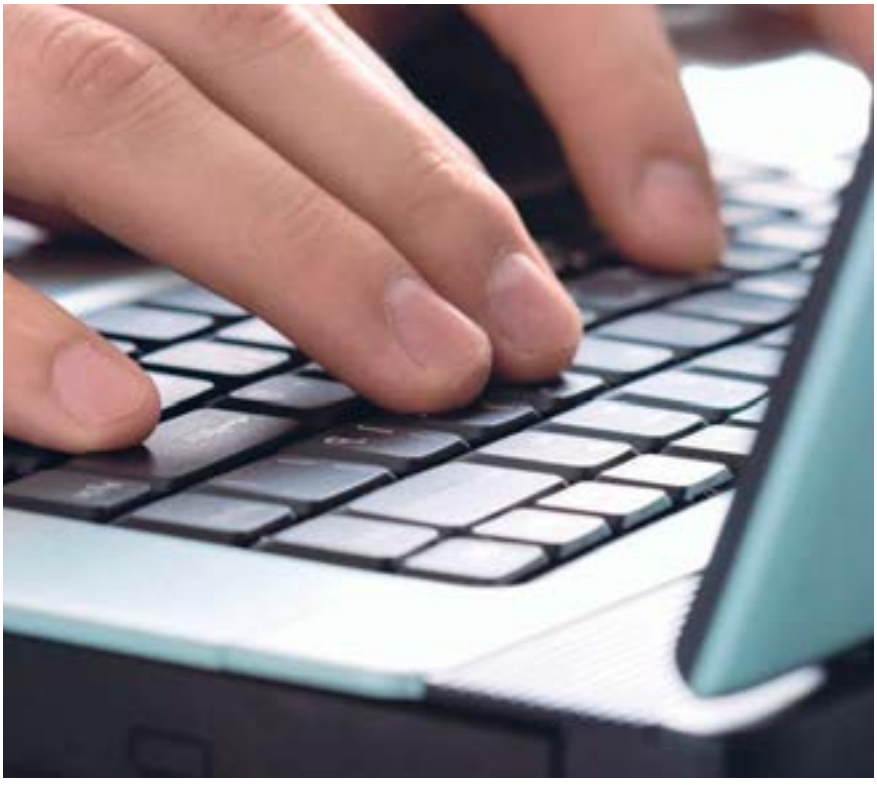
## La autenticación biométrica: ¿tendremos que «reseteárnos»?

Aparentemente el factor de autenticación por «lo que se es» tiene muchas ventajas ya que no hay que llevar nada adicional encima con lo que no se puede perder ni nos lo pueden robar –ya veremos–, no hay que recordar nada con lo que no se puede olvidar, y no se puede repudiar una acción que se haya realizado ya que es algo que nos define físicamente de forma única, y es muy difícil de falsificar.

Sin embargo, los sistemas biométricos no son perfectos y se caracterizan por unas tasas de falsos positivos o FAR (False Accept Rate), que indican la frecuencia de reconocimiento de un usuario cuando no debería serlo, y de falsos negativos o FRR (False Reject Rate), que indican la frecuencia de no reconocimiento del usuario, cuando debería haberlo sido. Según la Agencia de Seguridad Nacional[7] de EEUU, la NSA, la mayoría de los sistemas biométricos declaran un FAR que está en un rango de 1 entre 10.000 a 1 entre 1.000.000. Esto no pasa con las contraseñas habituales.

Por otro lado, todo tiene dos caras, y las características que en principio pueden suponer una ventaja, por su propia definición también pueden suponer una desventaja.

Pongamos como ejemplo el atributo de que nos definen «de forma única», el cual, por definición, se puede considerar como una invasión de la privacidad y crear resistencia a la cesión de dicha información, ya que las características biométricas que se vayan a utilizar de cara a una autenticación hay que digitalizarlas y almacenarlas en un servidor, lo que conduce a otra desventaja, que paso a explicar.



Apunté anteriormente que las características biométricas no se podían robar, a lo que habría que añadir no se puede robar el objeto físico, como un dedo, en el caso de la huella dactilar o el iris del ojo; pero después de que dichas características estén digitalizadas, ya tienen la misma vulnerabilidad que cualquier otro dato virtual en una máquina, como tal susceptible de ser hackeada. No nos roban el iris del ojo pero sí sus características en forma de ceros y unos, que, para el caso, es lo mismo ya que es precisamente esto lo que interesa a la máquina que verifica la identidad del usuario.

Llegados a este punto y volviendo al hecho de que son una característica física, suponen una clara desventaja frente a las contraseñas o los token ya que estos se pueden resetear si se roban o revelan, pero con aquellas no es posible hacer esto sin pasar por la mutilación.

En el «Black Hat»[8] de Amsterdam del año 2008, Matthew Lewis, un investigador de seguridad británico, realizó una demostración de un sistema –un biologger– para interceptar datos de autenticación biométricos que el scanner enviaba al servidor de procesamiento. Matthew puso de relieve la importancia de que los datos enviados deberían estar cifrados, cosa que, según él en ese momento –año 2008– la mayoría de los sistemas biométricos no cumplían.

Sin llegar a sofisticaciones ni herramientas especiales, un elemento biométrico fácil de copiar son las huellas dactilares ya que continuamente estamos tocando cosas donde se quedan las huellas como una mancha y se pueden obtener de ahí, sin enterarse el propietario de las mismas. Al fin y al cabo eso es lo que la policía científica viene haciendo en la escena del delito, desde tiempos de Sherlock Holmes[9]

Por consiguiente, se puede concluir, que la teórica seguridad de este tipo de autenticación no lo es tanto.

## El último factor: Lo que se hace, el comportamiento

Realmente lo que hacemos responde a unos patrones, patrones que aprovechan muy bien los departamentos de Marketing para inundarnos con información de cosas que nos pueden gustar o amigos que podríamos hacer, o dependiendo de nuestros gustos y de dónde nos encontremos, lo que podemos hacer y visitar.

Estos patrones se podrían aprovechar para verificar nuestra identidad, para en caso de encontrar inconsistencias, solicitar algún dato más. Para ello se necesitaría un sistema que hiciera uso de lo que la nube ya tiene acerca de nosotros, qué sistema estamos utilizando, desde qué servidor, quiénes somos, con quién hablamos, dónde vamos y qué hacemos ahí, de qué somos propietarios y qué nos gusta, lo que decimos, cómo lo decimos y nuestro tono de voz, y hasta cómo pensamos[10].

¡Uff! ¿Hasta qué punto queremos ceder nuestra privacidad –si es que no lo hemos hecho ya– para conseguir en teoría, más seguridad?

## El sistema de múltiple autenticación

Como todas por separado tienen más o menos debilidades, se están implantando nuevas formas de autenticación basadas en la combinación de al menos dos claves de distintos factores, llamado el sistema de doble autenticación. Un ejemplo de esto sería cuando después de autenticarnos con un usuario y contraseña al uso (lo que sabemos), nos envían al móvil (lo que tenemos) un código para confirmar una operación; otro ejemplo sería la propia tarjeta de crédito, que sería lo que tenemos, y el PIN, lo que sabemos.

Especulando un poco y viendo los avances en Inteligencia Artificial, es posible que en un futuro cercano las máquinas nos reconozcan de manera análoga a como nosotros reconocemos a otras personas, simplemente con presentarnos y tendiendo una mano, con lo que somos y con lo que hacemos, confiando en que también habrán aprendido a tomar medidas de seguridad para no dejar «hackear».

## La ciberseguridad en la cumbre

De lo que hay que ser conscientes es de que la seguridad nunca está garantizada al 100%. En cada organización, alineados con la política de riesgos y la política de seguridad definidas, tendrán que existir unos umbrales de aceptación de falta de seguridad, de lo que pueda suponer de freno al negocio por lo que pueda constreñir, o de cambio de costumbres, según el activo, y establecer cuánto dinero se está dispuesto a gastar en su protección.

Estos límites y normas relacionados con los riesgos en el uso de las TI son responsabilidad, en última instancia del órgano de gobierno de cada organización y debería formar parte de la agenda de dicho órgano de gobierno. Según la Organización Internacional de Normalización (ISO, International Organization for Standardization), el Gobierno Corporativo de las TI es «el sistema mediante el cual se dirige y controla el uso actual y futuro de las TI. [...] ... y es un subconjunto del gobierno de la organización o del gobierno corporativo.»[11]

Del 20 al 23 de enero se ha celebrado la reunión del Foro de Davos y que, de acuerdo con Fortune[12] y la propia página del «Word Economic Forum»[13], este año han dominado los temas tecnológicos frente a los bancarios de otras convocatorias, concretamente el de la Industria 4.0 y el de la ciberseguridad. Con esto parece que la tecnología va a estar muy presente a partir de ahora en los consejos de administración. ¡Por fin! ●

*Fotos: Archivo/Freepik*

---

[1] «La era de la contraseña ha terminado. Solo que aún no nos hemos dado cuenta de ello». Honan, Mat (11-15-2012) «Kill the Password: A String of Characters Won't Protect You», Ed. Wired. url [a 02-02-2016] http://www.wired.com/2012/11/ff-mathonan-password-hacker/.

[2] Osin, Yelena (07-15-2015) «The Problem With Corporate Email Addresses on Social Networks». blog SecuryScorecard. url [a 02-02-2016] http://blog.securityscorecard.com/2015/07/17/grainger-breach-social-engineering/?utm_content=17987083&utm_medium=social&utm_source=twitter.

[3] url [a 02-02-2016] http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

[4] url [a 02-02-2016] http://breachlevelindex.com/pdf/Breach-Level-Index-Annual-Report-2014.pdf.

[5] url [a 02-02-2016] http://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf?_ga=1.154714040.1257202996.1454180547.

[6] url [a 02-02-2016] http://cso.computerworld.es/seguridad-en-cifras/las-mayores-brechas-de-seguridad-de-datos-en-2015.

7 url [a 02-02-2016] https://www.nsa.gov/ia/_files/factsheets/i73-009r-007.pdf.

[8] url [a 02-02-2016] https://www.blackhat.com/presentations/bh-europe-08/Lewis/Presentation/bh-eu-08-lewis.pdf.

[9] url [a 02-02-2016] http://www.britannica.com/topic/Sherlock-Holmes-Pioneer-in-Forensic-Science-1976713.

[10] Honan, Mat (11-15-2012) «Kill the Password: A String of Characters Won't Protect You», Ed. Wired. url [a 02-02-2016] http://www.wired.com/2012/11/ff-mathonan-password-hacker/.

[11] «ISO/IEC 38500:2015 applies to the governance of the organization's current and future use of IT including management processes and decisions related to the current and future use of IT. [...] ... defines the governance of IT as a subset or domain of organizational governance, or in the case of a corporation, corporate governance.» url [a 02-02-2016]: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=62816.

[12] url [a 02-02-2016] http://fortune.com/2016/01/26/davos-cybersecurity-challenge-business/.

[13] url [a 02-02-2016] http://www.weforum.org/agenda/archive/fourth-industrial-revolution.

**FRANCISCO TRIGUEROS.** DIRECTOR COMERCIAL AFORSEC

# Aforsec, tecnología puntera al servicio de los clientes

Desde AFORSEC, queremos en primer lugar agradecer a todas las personas y empresas que nos visitaron en nuestro stand de SICUR 2016. AFORSEC es una empresa de carácter técnico comercial dedicada a la distribución para profesionales en todo el territorio nacional, en las líneas de equipamiento para la seguridad anti intrusos, protección contra incendio (PCI), circuito cerrado de televisión (CCTV), control de acceso y presencia, y automatización / domótica.

SOMOS la filial española del grupo empresarial IVV SGPS, de origen portugués y con presencia en varios países.

Nuestro grupo dispone de una alta capacidad técnica y desarrollamos ingeniería de hardware y software, con una amplia y consolidada experiencia.

Somos fabricantes en sistemas profesionales de CCTV con nuestra empresa alemana MAZI SECURITY, marca con la que estamos siendo referencia en Europa. También fabricamos sistemas de gestión de colas, y marketing digital con nuestra empresa Q-BETTER ubicada en Portugal, somos proveedores de las principales cadenas de telefonía, ropa deportiva de renombre mundial, entre otros clientes. En sistemas de automatización y domótica disponemos de la marca MORDOMUS, de altas prestaciones, escalable y muy accesible para el usuario final, también fabricando en Portugal.

Somos distribuidores de primeras marcas del mercado internacional, como es JABLOTRON, con quien llevamos casi 15 años siendo el principal distribuidor de la marca, suministrando todas sus soluciones de intrusión, seguimiento GPS y automatizaciones. Representamos en sistemas de detección de incendios las marcas UNIPOS y ZETA, donde disponemos de un amplio catálogo de soluciones de PCI, en el que cubrimos todo el espectro de instalaciones que se nos plantean, desde una sencilla y económica instalación convencional, hasta los más complejos proyectos en redes de centrales analógico direccionales.

Con la marca ROGER en sistemas de control de acceso disponemos de una solución que permite de forma sencilla, eficaz y robusta realizar todo tipo de instalaciones, contando con sencillos sistemas autónomos hasta de gran capacidad y versatilidad a un óptimo coste.

Y como director comercial de AFORSEC, Francisco Trigueros, con ya casi 30 años de experiencia en la fabricación/distribución en todas las líneas de producto que distribuimos, y complementados con la sólida estructura y saber hacer de nuestro grupo y personal, podemos ofrecer al cliente una ágil y profesional respuesta para acompañarles sin duda en el éxito de sus proyectos y en su día a día.

Este es el espíritu con el que nació AFORSEC, con el que seguimos trabajando, innovando y aportando las últimas tecnologías («state of art»), consiguiendo la confianza y fidelidad de nuestros clientes. ●

*Foto: Aforsec*

Contactos de empresas, p. 7.

**MARIANO J. BENITO GÓMEZ.** COORDINADOR, CLOUD SECURITY ALLIANCE, CAPÍTULO ESPAÑOL. CISO GMV SECURE E-SOLUTIONS.

**MANUEL CALDAS.** COORDINADOR, CLOUD SECURITY ALLIANCE, CAPÍTULO PERUANO. IT ARCHITECT CLOUD COMPUTING, IT/IS SECURITY MANAGER.

# Luces y sombras del **Estado del Arte** en **Seguridad Cloud**

Si ha habido en los últimos años un concepto de moda en el mercado de las Tecnologías de la Información, ese es sin duda la Nube. También llamado Cloud Computing. Sin entrar en demasiado detalle técnico, la Nube permite disponer de recursos de procesado de datos (servicios, programas, plataformas tecnológicas, espacio de almacenamiento, entre otras), de forma que puedan ser usados y facturados bajo demanda del cliente. Esta posibilidad puede estar disponible dentro de una organización, como una Nube Privada, pero más habitualmente está disponible «desde Internet» mediante servicios proporcionados desde una Nube Pública por otras organizaciones.

YA desde la irrupción en el mercado del concepto, existió por parte de los profesionales de la seguridad de la Información interés por la Nube. Tanto como potencial tecnología para mejorar la seguridad y protección de las organizaciones y sus activos, como potencial fuente de riesgos, problemas e incidentes de seguridad. Por ello, en el año 2009 un grupo de profesionales funda la Cloud Security Alliance (o CSA, www.cloudsecurityalliance.org) para coordinar los diversos esfuerzos e iniciativas emanadas por los profesionales. Desde entonces, CSA es la organización de referencia a nivel mundial en la seguridad del Cloud Computing, y a través de sus 84 capítulos regionales y sus iniciativas, proporciona al mercado guías de trabajo, metodologías, documentación y marcos de referencia para mejorar las condiciones de seguridad del Cloud.

La Computación en la Nube empieza a ser ya toda una veterana en el mundo de las Tecnologías de la Información, estando presente y disponible desde hace casi ya 10 años. Tiempo que fue en su día más que suficiente para la adopción generalizada por el mercado de casi todas las tecnologías de éxito. Pero que, aparentemente, no lo está siendo para el Cloud Computing. Los fabricantes de soluciones y los proveedores de servicios se lanzaron decididamente a ofrecer sus servicios desde la Nube, o a migrar sus productos a la Nube para poder estar disponibles para sus clientes desde allí, y no solo desde sus Centros de Datos.

En ocasiones, este recorrido ha sido una estrategia de rebranding de productos y servicios más que una genuina migración a la Nube. Pero como resultado, el mercado ya conoce términos como Saas, PaaS, IaaS, SecaaS. Y sin embargo, la respuesta desde los usuarios de estos servicios no ha sido tan decidida.

Cloud Security Alliance viene observando este fenómeno desde hace tiempo. Y, en particular, el capítulo español (CSA-ES, www.cloudsecurityalliance.es) ha tratado de averiguar la relación que existía entre este grado de adopción de los servicios cloud y la seguridad con que dichos servicios se proporcionan.

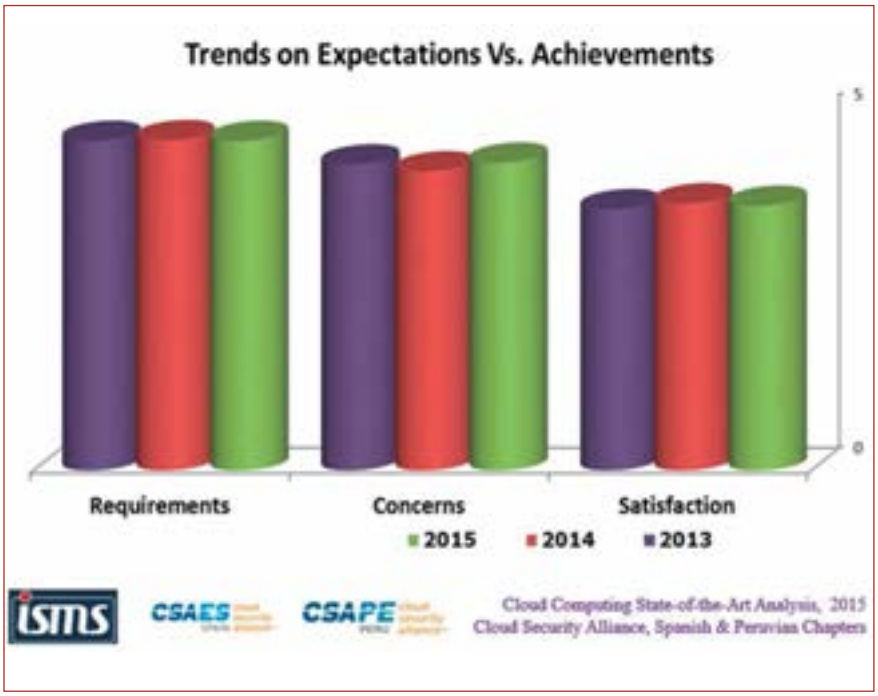
Por ello, inició en el año 2013 y 2014 sendos Estudios sobre el Estado del Arte en Seguridad Cloud, con los que ha tratado de desvelar esta relación y determinar si los clientes de cloud ven en la seguridad de los servicios un acicate o una barrera para su adopción, y si su satisfacción con estos servicios estaba

en línea con sus exigencias y expectativas. En el año 2015, esta línea de trabajo progresó gracias al ofrecimiento y colaboración del Capítulo Peruano de CSA (CSA-PE).

De esta forma, el esfuerzo conjunto de los profesionales y expertos de CSA de ambos lados del Atlántico cristalizó en el 3er estudio del Estado del Arte en Seguridad Cloud, que fue presentado en noviembre de 2015, y que contó con las aportaciones de 200 organizaciones de España, Perú, Estados Unidos y otros países latinoamericanos y europeos, realizado por un conjunto de 9 analistas españoles y peruanos.

El estudio obtiene una visión profunda y detallada de la situación de la seguridad en el Cloud Computing, incluyendo una perspectiva de evolución temporal de sus conclusiones.

De acuerdo a la información analizada, la tendencia de adopción de servicios en Cloud está en progresión, pasando de un 60% de organizaciones que se declaran usuarias de la Nube en 2013, a casi un 80% en el año 2015. Este porcentaje de usuarios podría ser aún mayor, puesto que en 2015 aparecen por primera vez organizaciones que declaran que fueron usuarias de la Nube en el pasado, pero ya no lo son.




«Los usuarios de servicios de almacenamiento utilizan en un 70% de los casos Nubes Privadas, frente al 30% de usuarios de Nubes Públicas»

Es en todo caso un porcentaje testimonial de organizaciones, pero que existe. A juicio de los analistas, es un síntoma de que el mercado Cloud está madurando: los servicios en Nube ya han podido utilizarse en tiempo y variedad suficiente, son evaluados en base a datos más que en expectativas y en algunos casos no son satisfactorios.

El estudio también apunta a que los proveedores de servicios Cloud, en su

entusiasmo por ofrecer servicios, están contribuyendo a crear expectativas de seguridad en sus clientes que luego no se ven suficientemente satisfechas. En un escenario que permanece en esta situación de forma sostenida en las diversas ediciones del Estudio.

Así, todos los clientes declaran expectativas muy altas en la seguridad de los servicios en Cloud (por encima de 4.5 puntos sobre 5), destacándose en particular las garantías esperadas sobre privacidad, confidencialidad y disponibilidad de los servicios.

A pesar de estas altas expectativas, los clientes de servicios cloud relajan sus exigencias a los proveedores (4.2 puntos sobre 5, como promedio) cuando las expectativas se traducen en requisitos del servicio, tales como ubicación geográfica del mismo, medidas de seguridad implantadas, capacidad de cambio de proveedores, certificaciones, posibilidad de realizar auditorías, etc. Por último, los clientes se declaran satisfechos con los servicios que reciben, aunque lo estén en menor proporción a sus expectativas y sus exigencias (4 puntos sobre 5).

El estudio también analiza las condiciones de seguridad en Cloud desde el punto de vista de los servicios que los clientes reciben. En este capítulo, el correo electrónico y los servicios de almacenamiento de datos son los servicios más demandados (al menos la mitad de los usuarios), seguidos ya a cierta distancia de los servicios basados en Web.

Este dato resulta muy revelador cuando se analiza más en profundidad para descubrir que los usuarios de servicios de almacenamiento utilizan en un 70% de los casos Nubes Privadas frente al 30% de usuarios de Nubes Públicas, mientras que en el resto de los servicios el uso de una u otro tipo de Nube es más equilibrado.

Ello apunta a que los usuarios no confían plenamente en los servidores de Nube Pública cuando quieren almacenar grandes cantidades de información y que, ante los posibles riesgos de accesos no deseados a esa información, no permiten la salida de esta información de sus organizaciones y se decantan por ello por el uso de Nubes Privadas sobre las Nubes Públicas para este servicio.

Resulta también interesante analizar los aspectos que los usuarios declaran como más necesarios en la prestación de los servicios Cloud. Entre todos ellos, las garantías de Continuidad de Negocio por parte del proveedor sigue siendo el criterio más valorado por sus clientes. A continuación, los clientes valoran las medidas de seguridad implantadas por el proveedor; su capacidad para el cumplimiento de las regulaciones legales vigentes; la existencia de acuerdos de nivel de servicio en Cloud y la capacidad de cumplimiento de los mismos. Y la preocupación de los clientes por no tener posibilidad de cambiar de proveedor cloud (también llamado «efecto locked-in»).

Destacaba entre todos los aspectos, que la ubicación geográfica del servicio en la Nube se muestre en el estudio como el criterio menos valorado. Desde una perspectiva histórica, la ubicación geográfica en la que estaba el proveedor de Cloud era considerada como un factor determinante de cara a su selección. En particular, en países europeos y debido a la existencia de regulaciones en materia de privacidad que requería, la ubicación del proveedor Cloud resultaba determinante en su selección.

Aparentemente, este factor ya no es tan determinante como lo fue en el pasado. A criterio del equipo de analistas, la respuesta está en la madurez del mercado Cloud, que ha permitido plantear respuestas eficaces a esta dificultad, disminuyendo la importancia pasada de este criterio.

El estudio aborda también el valor que aportan las certificaciones de seguridad a la hora de incrementar las garantías que los proveedores de servicios en Cloud proporcionan a sus clientes. Entre ellas, destacan las certificaciones de proveedores CSA-STAR, y las certificaciones de profesionales CCSK y CCSP, certificaciones que, en todos los casos, gozan de amplio reconocimiento y prestigio entre los participantes en el estudio, siendo valoradas por más del 50% como de valiosas o muy valiosas.

El estudio analizaba también el impacto del escenario conocido como Shadow IT. Es decir, la Nube puede facilitar la adquisición de recursos TIC por áreas de las Organizaciones sin control o conocimiento de los departamentos de Sistemas de la Información. El estudio apunta de forma mayoritaria hacia la no existencia o incluso la imposibilidad de que ocurra Shadow IT.

Por último, los proveedores de servicios en Cloud afirman recurrentemente que disponen de capacidades avanzadas de detección y respuesta a posibles incidentes de seguridad en la Nube, mejores de las que disponibles por sus clientes. En este sentido, los clientes de servicios Cloud declaran que, efectivamente, el uso de servicios Cloud mejora la situación sobre los incidentes de seguridad, tanto en volumen (se tienen menos incidentes o los mismos), como en criticidad (los incidentes que ocurren son de menor importancia). ●

*Fotos: **ISMS Forum***

1.– https://www.ismsforum.es/ficheros/descargas/estudio-del-estado-de-la-seguridad-en-cloud.pdf

2.– https://www.ismsforum.es/ficheros/descargas/csa-es-2014-cloudsecuritystateoftheart20141119.pdf

3.– http://www.ismsforum.es/ficheros/descargas/csa-es-pe-2015-estudio-estadodelarte-nube-es.pdf

**ENZO PEDUZZI.** DIRECTOR DE INDUSTRY AFFAIRS. SIEMENS BUILDING TECHNOLOGIES. PRESIDENTE DE EURALARM

# Ciudades Inteligentes

## Una revolución en cada aspecto de la vida

Según Naciones Unidas, la población mundial alcanzará casi los 8.500 millones de personas en 2030. A medida que aumenta la población, lo hacen también las ciudades. Actualmente más de la mitad de los habitantes de la tierra vive en áreas urbanas y cada semana más de un millón se muda del campo a la ciudad. Esta tendencia plantea exigentes demandas sobre las personas y las infraestructuras. Porque sólo cuando las comunicaciones, la energía, la seguridad de las personas y los bienes y la movilidad de éstos funcionan ininterrumpidamente sin problemas, es cuando las ciudades pueden ofrecer a sus ciudadanos una calidad de vida y una economía prósperas.

PARA los planificadores urbanos, la respuesta a todos estos desafíos es la «ciudad inteligente». Los pilares de la misma son unos estándares uniformes para soluciones de infraestructuras inteligentes, seguras y resilientes.

El proceso de urbanización actual se refleja no solamente en la escasez de viviendas y en los elevados alquileres. Las ciudades europeas, en particular, se construyeron en base a los principios del siglo XIX, y los sistemas de suministro individuales a menudo se miran de forma aislada. El gran crecimiento de la población está llevando rápidamente a las ciudades a sus límites en lo que al suministro de energía, la seguridad, las comunicaciones digitales, el transporte y el tráfico se refiere. El concepto de «ciudad inteligente» ofrece una respuesta: su misión fundamental es distribuir de forma eficiente los recursos existentes. Establecer una interconexión entre los sistemas de suministro individuales mediante soluciones técnicas debe permitir a las ciudades responder de forma dinámica a demandas puntuales, preservando así su funcionalidad.

### Las megaciudades como cuellos de botella para la seguridad

Los espacios urbanos son especialmente vulnerables. Los accidentes, los desastres naturales o los ataques terroristas y los problemas de abastecimiento que acarrean son aún más severos en el caso de grandes poblaciones, y de una infraestructura de transporte a menudo sobrecargada. Además, existe una correlación clara entre el tamaño de una ciudad y su tasa de delincuencia. El 80 por ciento de los crímenes registrados ocurre en ciudades que aglutinan el 50 por ciento de la población mundial. Aunque eso puede resultar normal en áreas urbanas con mucha densidad de población, siguen siendo necesarias unas contramedidas para proteger la vida y la propiedad como libertades y valores fundamentales.

El Banco Mundial ha estimado, dependiendo del país, que el coste total de la delincuencia puede llegar al 25 por ciento del Producto Interior Bruto (PIB). Según la Comisión Europea, incluso la Unión Europea comparativamente segura, gasta por lo menos un

cinco por ciento de su Producto Interior Bruto en paliar los costes derivados de la delincuencia y de los desastres naturales. Dichos eventos acarrean consecuencias considerables, no sólo para las personas directamente afectadas sino también para la comunidad en su totalidad. Las cadenas globales de creación de valor y la lucha por el talento enfrentan no sólo una economía contra otra sino también una ciudad contra otra. Si los planificadores urbanos fracasan en su intento de garantizar la seguridad de las personas y los bienes, así como el suministro, los inversores se marcharán y los trabajadores altamente cualificados se mudarán a aquellos lugares en los que esperan tener una mayor calidad de vida. Para mantener la competitividad global, las ciudades han de tener un interés vital en superar estos desafíos.

**La ciudad inteligente, la entidad desconocida**

El concepto de ciudad inteligente promete mejorar la calidad de los servicios públicos y privados a través de tecnologías digitales. Al mismo tiempo, los costes de la ciudad y su consumo de recursos disminuyen, lo cual aumenta el bienestar de todos. Visto desde esa perspectiva, cada ciudad, no importa su tamaño pequeño o grande, quiere ser «inteligente». ¿Pero qué significa eso realmente? ¿Cuáles son los criterios que hay que cumplir? Entre las cuestiones más apremiantes a las que se enfrentan las ciudades son el aumento constante del tráfico, el uso energético y las emisiones, la seguridad material y personal de la población, una red fiable de alta velocidad y por último, cómo financiarlo todo.

Sin embargo, a pesar de todo, no existe una definición consistente de lo que es realmente una ciudad inteligente. Distintas compañías y determinados medios han ofrecido índices iniciales, que varían entre sí y en consecuencia son inadecuados para otorgar con cierta transparencia la calificación de «ciudad inteligente» a algunos lugares por sí mismos. Para eso se necesitarían unos Indicadores Clave de Rendimiento o «KPIs».

Lo que sí comparten varios índices, sin embargo, es la ausencia de un KPI para indicar el grado de protección, seguridad y resiliencia de una ciudad. Pero una ciudad que no es segura no puede ser inteligente. Así que el enfoque de ciudad inteligente se tiene que mirar por entero y de forma global. Resulta necesario crear unos parámetros comparables y transparentes, teniendo en cuenta, al mismo tiempo, unos estándares elementales de seguridad personal y material.

**Necesidad de unos estándares uniformes**

Los inversores y expertos necesitan indicadores clave de rendimiento que sean transparentes para evaluar a las ciudades inteligentes, aunque las propias ciudades y sus diversos partícipes, como por ejemplo la administración, su policía, el departamento de Bomberos y Protección Civil también se apoyen en estándares. Sólo entonces será posible progresar de forma sistemática. Ya están patentes los resultados iniciales. El Grupo de Debate sobre las Ciudades Inteligentes y Sostenibles de la Unión Internacional de Telecomunicaciones (UIT), una organización especial de las Naciones Unidas, ofrece informes técnicos y especificaciones en los ámbitos de la seguridad cibernética y la protección de datos. Además, se han definido varios KPIs distintos para ayudar a clasificar las ciudades inteligentes respecto a aspectos como las telecomunicaciones. La UIT define la ciudad inteligente de esta forma: «Una ciudad sostenible e inteligente es una ciudad innovadora que usa las tecnologías de la información y de la comunicación (TICs) y otros medios para mejorar la calidad de vida, la eficiencia de los servicios urbanos y su operativa y la competitividad, asegurando a la vez que cumple con las necesidades de las generaciones presentes y de las futuras respecto a aspectos económicos, sociales y medioambientales.»

Igualmente a nivel internacional, la Organización Internacional de Normalización (ISO) ha definido en la normativa ISO 37120 un total de 100 indicadores para medir los servicios de una ciudad y la calidad de vida. Once de ellos giran alrededor de la seguridad personal y material. Se incluyen indicadores enfocados en la seguridad, la protección contra incendios y la gestión de crisis, además de otros sobre el agua, la energía y el transporte. Esto hace que la norma ISO 37120 sea la única norma con unos KPIs apropiados para la medición del grado de seguridad personal y material en ciudades a efectos comparativos. Aproximadamente 250 ciudades de 80 países participan en la in-

troducción de esta norma, incluyendo ciudades como Londres, Shanghai, Toronto y Rotterdam. Con este fin, reportan métricas tales como el número de muertes debidas a incendios por cada 100.000 habitantes, y el tiempo de respuesta de los departamentos de Policía y de Bomberos después de la llamada inicial. Esto hace que sea posible indicar de forma transparente y verificable cómo es de segura realmente una ciudad.

El hecho de que la norma ISO 37120 incluya diversos indicadores sobre la seguridad personal y material no es casual. Los especialistas en sistemas de seguridad de Siemens contribuyeron activamente al desarrollo de la norma dentro de los grupos de trabajo pertinentes. Esto dio paso al desarrollo de normas medibles y significativas de seguridad.

**La seguridad personal y material como cimiento de la ciudad inteligente**

La ciudad del futuro requiere soluciones inteligentes, seguras y resilientes para las infraestructuras. Las iniciativas para una ciudad inteligente que se concentran exclusivamente en la utilización inteligente de la energía no son suficientes. Hasta ahora, la seguridad personal, la seguridad material y la resiliencia se han visto a menudo como efectos colaterales que no necesitan una planificación individual. Sin embargo esta visión no es correcta. Una comunidad urbana sólo puede funcionar debidamente si se puede volver a la normalidad lo antes posible después de un incidente tal como un gran incendio o un ataque terrorista. Lo ideal, no obstante, sería que dichos incidentes se evitasen antes de producirse.

Esto requiere que se vinculen de forma inteligente los subsistemas individuales y que se saque provecho de las ventajas derivadas. Los sistemas interoperables ofrecen seguridad personal, seguridad material y estabilidad para las infraestructuras de vital importancia tales como aeropuertos y centros de datos. Un componente esencial es la seguridad física de las infraestructuras y las redes de TI. Incluso los cortafuegos más sofisticados son de poca utilidad si en la puerta hacia la sala de servidores falta un sistema de control de acceso fiable.

**Protección de la «red troncal virtual» de una ciudad**

Las ciudades no solamente albergan recursos económicos e intelectuales importantes tales como universidades, edificios públicos, oficinas y fábricas sino también redes de transporte e infraestructuras de vital importancia. En vista del papel cada vez más importante de las TI en la prestación de servicios urbanos, la protección de esta «red troncal virtual» se hace más y más esencial.

En la mayoría de los casos, salvaguardar las infraestructuras de vital importancia no requiere volver a inventar la rueda. Desde soluciones de seguridad en centros de datos y videovigilancia hasta la evacuación masiva e inteligente de personas, la industria de la seguridad ya ofrece un sinfín de soluciones operativas. La tarea es introducir estas soluciones de forma lógica dentro de un contexto de «ciudad inteligente». Esto requiere integrar varios sistemas –sistemas de comunicaciones, de alarma automática, de información y de videovigilancia– en una plataforma central de mando y control para asegurar una respuesta integral y coherente a los incidentes. Ahí está la esencia de una ciudad inteligente y segura.

La implementación de estas normas de seguridad requiere hacer partícipes a todos los involucrados – desde las administraciones públicas hasta las ONGs y los comités de normalización – para crear políticas que no sólo motiven su implantación sino también que establezcan normativas internacionales transparentes. La norma ISO 37120 y los informes y especificaciones técnicas de la UIT son un buen punto de partida. Hace falta definir los puntos débiles y las posibles contramedidas y hay que calcular los costes. Al mismo tiempo, no debemos perder de vista el hecho de que la resiliencia de las ciudades se tiende a sobreestimar considerablemente y que al final, la tecnología no es la solución para todo. Unos ciudadanos comprometidos y unas fuerzas de intervención eficientes son – y seguirán siendo – de vital importancia para la seguridad personal y material de una ciudad.

**La seguridad personal y material, clave para una competitividad global**

Las ciudades tienen su propio y fundamental interés en contar con estructuras inteligente transparentes y comparables, porque los entornos urbanos seguros son especialmente atractivos para la competitividad mundial. A menudo incluso las ciudades que se consideran inteligentes no abordan adecuadamente el tema de la seguridad personal y material. En consecuencia, una de las principales responsabilidades de la política es identificar los partícipes apropiados y participar en el desarrollo de soluciones. Este proceso requiere la definición de normas claras de seguridad personal y material para ciudades inteligentes, además de la prestación y creación de los medios e incentivos para su implantación.

El concepto de ciudad inteligente revolucionará la vida en las urbes de manera parecida al impacto que tuvo la revolución industrial. Para modelar con éxito esta revolución para el bien de todos, es absolutamente esencial crear los cimientos apropiados desde el principio. La seguridad personal y material no se deben dejar para el final del proceso. ●

*Fotos: Siemens*

Contactos de empresas, p. 7.

LA JORNADA SE CELEBRÓ EL 19 DE ENERO EN VALLADOLID

# XXVI edición de las **Jornadas Foro Efitec**

La ciudad de Valladolid acogió, con el patrocinio de Techco Security, la XXVI edición de las Jornadas Foro Efitec, que contaron con la presencia de mandos de los distintos cuerpos de seguridad con competencias en materia de Seguridad Privada: Cuerpo Nacional de Policía, Guardia Civil, Mossos d´Esquadra, Ertzaintza, y de directores y gestores de Seguridad de las entidades financieras que operan en nuestro país, así como asociados y profesionales de seguridad.

JUAN Manuel Zarco, presidente de la asociación Foro Efitec, fue el encargado de inaugurar la jornada, en la que agradeció al patrocinador y a los presentes su apoyo e interés en esta iniciativa, pionera en el sector de la seguridad.

A continuación, Alfonso Bilbao, director de Cuevavaliente Ingenieros, destacó en su presentación sobre «Lecciones aprendidas en la integración de la Seguridad Física y la Ciberseguridad» cómo esta integración nace como respuesta a actos delictivos en entidades financieras y su resistencia a las medidas de seguridad tradicionales. A su vez, genera nuevos riesgos y obliga a los responsables de la seguridad a salir fuera de su «zona de confort».

Durante su intervención explicó el mapa de nuevas amenazas basado en análisis de riesgos y su necesidad de permanente actualización. Así mismo, destacó la visión que la dirección general de la corporación debe tener ante esta realidad y la importancia de la Ciberseguridad frente a las nuevas amenazas.

Por tanto la seguridad como función transversal debe sustentar la figura de un nuevo director de Seguridad capaz de analizar riesgos físicos y lógicos, utilizando una métrica común y modelos de gestión basados en la mejora continua.

Posteriormente, José Pablo Álvarez, iSOC & Business Continuity Director de Caixabank, centró su intervención en el modelo de integración transversal de las actividades de seguridad bancaria a través de su centro de operaciones iSOC.

Este nuevo modelo de integración se motiva porque el paradigma de la seguridad ha cambiado. Es capital centralizar la información de seguridad, así como prevenir o minimizar la exposición de los incidentes de seguridad del grupo.

Para ello y a través de su centro, establecen medidas y procedimientos para cumplir tres objetivos fundamentales:

- Detectar y escalar los incidentes de seguridad.
- Analizar y automatizar los procesos en todo lo posible.
- Realizar reportings y cuadros de mando de seguridad mediante mediciones para mejorar los procedimientos de forma continua.

Carlos Vázquez, director de Seguridad de Barclays, expuso mediante su presentación el modelo organizativo de su entidad con presencia global a través del establecimiento de su estratégia CRES (Servicios Corporativos de Real State), en la que la actividad de seguridad se divide en Inmuebles, Health & Safety, Seguridad Corporativa, Compras y BCM.

Dentro de este modelo se establece un seguimiento a través de la unidad de fraude y servicios corporativos de investigación y, a través del modelo de seguridad corporativa, se establece la seguridad física de los ejecutivos, expatriados y medidas de inteligencia y concienciación de seguridad.

Entre otros factores también se tiene en cuenta para la protección de even-

**Foto de familia de los asistentes al XXVI edición de las Jornadas Foro Efitec.**


**Francisco Abad, director general de Techco Security.**

**Un momento del encuentro profesional celebrado en Valladolid.**

tos propios, situaciones de gestión de crisis y análisis de riesgos contra estándares, teniendo en cuenta las normativas locales de cada país.

De igual forma la vigilancia digital cobra un papel importante como modelo de gestión de la información para la prevención de amenazas.

Por su parte, José Antonio Galiñanes, director de Coordinación, Políticas y Estrategias del área de Seguridad Corporativa del Grupo Santander, centró su intervención sobre la historia de la configuración del departamento de Seguridad Corporativa del banco, y de cómo adquirió importancia en la entidad la necesidad de contar con profesionales vinculados al mundo empresarial y no solo al mundo de la seguridad pública. De igual forma superar el bajo conocimiento del personal de seguridad de otras geografías y de sus normativas locales supuso un reto importante para la entidad.

Se estableció un sistema participativo en el que todos los responsables locales de seguridad intercambiaban información para conocimiento de la entidad, así como recibían la formación adecuada a sus necesidades. Este procedimiento supuso un cambio en la visión del banco desde el punto de vista de la alta dirección para que pudiera percibir a las áreas de seguridad como generadoras de valor.

Durante la clausura de la jornada, Knuth Schmidt, director de Operaciones de Europa en Cobe Capital, intervino para explicar la historia familiar detrás del fondo de inversión y los logros obtenidos, así como los motivos de la adquisición por parte del fondo de inversión del negocio de Stanley Security y su confianza para convertir a Techco Security en el referente como socio tecnológico de seguridad en España.

Francisco Abad, director general de Techco Security, agradeció la presencia a todos los profesionales y explicó el modelo de negocio de la compañía, con un claro objetivo de empresa tecnológica orientada a ofrecer servicio a sus clientes. A su vez Techco Security ha establecido cuatro áreas de negocio lideradas por profesionales con amplia experiencia:

- Banca.
- Retail & Gas.
- Regional.
- Industria y grandes cuentas.

De igual forma avanzó las líneas estratégicas para establecer una fuerte inversión en soluciones a través de plataforma de software y soluciones remotas gestionadas desde el SOC.

Durante la celebración de la jornada, la asociación Foro Efitec ofreció un reconocimiento al inspector jefe del Cuerpo Nacional de Policía Rafael Navarro y al coronel de la Guardia Civil César Álvarez por su contribución al sector de la seguridad privada y su profesionalidad. ●

*Texto y Fotos: Redacción*

**Juan Manuel Zarco, presidente del Foro Efitec.**

JORNADA ORGANIZADA POR EL OBSERVATORIO SECTORIAL DE SEGURIDAD PRIVADA

# Formación y certificación de empresas, elementos clave de mejora para el sector

El Observatorio Sectorial de la Seguridad Privada, órgano de actuación formado por las organizaciones empresariales y sindicales más representativas del sector de la Seguridad Privada, celebró el pasado 27 de enero en Madrid una jornada sobre «Nuevos horizontes formativos y especialización en el sector de la Seguridad Privada», donde se puso de manifiesto que una mayor exigencia en el acceso a la profesión pasa por aumentar y mejorar la formación. En este sentido, el desarrollo de la nueva ley puede ser una gran oportunidad para dignificar un sector estratégico para la seguridad en nuestro país.

EL acto celebrado en la Escuela Julián Besteiro, el centro de formación confederal de UGT, fue inaugurado por José Miguel Villa, secretario general de Fes-UGT, que tras dar la bienvenida a los asistentes resaltó el importante papel del Observatorio.

Tanto Alicia Gómez, responsable de Gestión de Talento de Securitas, como Cruz Gutiez, responsable técnica de Formación Fes-UGT, que analizaron «Nuevos itinerarios para la habilitación del personal de Seguridad. Las especialidades y necesidades formativas provocadas por las nuevas tecnologías», coincidieron en que sin cualificación no hay avance posible y, aunque en los últimos tiempos se han dado importantes pasos hacia adelante, es necesario seguir trabajando en el refuerzo de la formación.

Acto de inauguración de la jornada del Observatorio Sectorial de Seguridad Privada.

Asimismo, Gutiez destacó el esfuerzo realizado en los últimos tiempos por las empresas en cuanto a programas formativos. Algo que se puede ver también complementado por la nueva Ley de Seguridad Privada ya que, además de proponer la creación de una Comisión Técnica para conseguir coherencia en el cumplimiento de los objetivos sectoriales, pretende coordinar las administraciones competentes en formación, cohesionar el sector y la unidad de acción, anticiparse a necesidades, buscar recursos, y defender los intereses sectoriales.

Otro de los grandes temas abordados en la jornada fue el relativo a los requisitos de certificación exigibles a las empresas.

En este sentido, Andrés Sanz, Coronel Jefe Servicio SEPROSE de la Guardia Civil, señaló que una mayor exigencia a las empresas en cuestiones de certificación supone «garantizar la calidad, el servicio al usuario y evitar que se resienta la seguridad de ciertas infraestructuras».

Durante la jornada se ha debatido sobre la repercusión de estos nuevos re-

quisitos de certificación a las empresas y sobre la cualificación del personal. Para José Luis Moya, responsable del Área de Gobierno del departamento Security Gas Natural Fenosa, la formación y la especialización son dos de los criterios más relevantes a la hora de contratar un servicio de seguridad privada.

Para Eduardo Cobas, secretario general de Aproser, «la certificación sólo tiene sentido si contribuye al estricto respeto de las reglas por parte de todos, porque sólo así se permitirá una mayor cualificación y sostenibilidad del sector». También se ha referido a la importancia de garantizar la máxima fiabilidad de las empresas que certifican a las compañías del sector de la Seguridad Privada, que cuenten con auditores especializados y establezcan plazos coherentes para este proceso.

Los representantes de los sindicatos, Sergio Picallo, secretario sectorial de Seguridad Privada de FeS UGT, Daniel Barragán, secretario de Negociación Colectiva de Construcción y Servicios de CCOO, y Basilio A. Flebes, Secretario de Formación de TFSPUSO, pusieron en valor la figura del vigilante. Asimismo, condenaron que las Administraciones Públicas contraten empresas que no cumplen con la normativa vigente.

Por su parte, Esteban Gándara, comisario Jefe de la Unidad Central de Seguridad Privada de la Policía Nacional, señaló que «la Seguridad Privada es un sector estratégico» y puso en valor las nuevas funciones de los vigilantes de seguridad privada que reconoce la Ley de Seguridad Privada de 2014.

En la clausura de la jornada el presidente de Aproser, Ángel Córdoba, explicó que «en menos de 18 meses, el sector ha sufrido dos decretos ley que han incrementado sus costes laborales en más de un 4%, algo que en una actividad con márgenes comerciales prácticamente inexistentes en el territorio nacional dificulta sensiblemente la mejora de los convenios colectivos, la creación de empleo de calidad y la inversión en el sector».

Por no hablar de la reforma laboral que, según Ángel Córdoba, para empresas intensivas en mano de obra, como es el caso de las empresas de seguridad privada, «ha facilitado, sin ser muy conscientes de ello, dudosos procesos de descuelgue de condiciones laborales o convenios de empresa, que ya impactan en más de 10.000 trabajadores con una disminución media de sus salarios superior al 10%, y algunos de ellos con porcentajes que incluso llegan al 30% con respecto a lo establecido en el convenio colectivo». «Esta situación –añade Angel Córdoba– ha generado una cada vez más extendida competencia desleal en los procesos de licitación pública basada, casi exclusivamente, en el precio ofertado para la adjudicación del servicio». ●

*Texto y Fotos: Aproser/Redacción*

# Mobotix España crece

MOBOTIX, el mayor fabricante mundial de sistemas en red de videovigilancia de cámaras megapíxel, está renovando su plantilla en España en los últimos meses.

Lucas San José.

Por un lado, se ha nombrado a Alfredo Gutiérrez Navarro, nuevo Business Development Manager para España y Portugal. Alfredo es ingeniero técnico superior en Telecomunicaciones por la E.T.S.I.T. de la Universidad Politécnica de Madrid. En 2012 se incorporó al equipo de Mobotix AG como responsable técnico de Proyectos para España y Portugal, cuyas funciones fueron la validación, homologación y certificación de productos Mobotix en grandes cuentas y en cliente final, así como labores de pre-venta, soporte de proyectos y formación técnica.

Alfredo Gutiérrez.

Tan sólo 3 años después, desde julio de 2015, Gutiérrez ha sido nombrado Business Development Manager para el mercado ibérico. Entre las nuevas responsabilidades de Gutiérrez se encuentran las gestiones de preventa en la región, la relación con los distribuidores y partners, el desarrollo del

# Tecnifuego-Aespi: sello de instalador y mantenedor de puertas cortafuego

Ante la necesidad de contar con profesionales cualificados y reconocidos por tercera parte, en el sector de puertas automáticas, las federaciones de empresarios del metal FEMEVAL, FEMPA y FREMM han decidido crear una «acreditación del profesional cualificado» y un «sello distintivo» a nivel nacional para profesionales y empresas, como garantía profesional y empresarial, así como de un ejercicio responsable de sus servicios y funciones. A esta iniciativa se ha unido TECNIFUEGO-AESPI a través del coordinador del Comité de Puertas Cortafuego y Señalización, José Vicente Andreu.

La primera fase del proyecto es coordinar la elaboración del programa y contenidos teórico-práctico para la formación del «Instalador y mantenedor de puertas automáticas: residenciales, comerciales, industriales y cortafuego», vinculándolo con la «acreditación del profesional cualificado» y el «sello distintivo», que ponga en relieve e identifique a profesionales y empresas con el máximo nivel para la instalación y mantenimiento de puertas automáticas.

Al encuentro, auspiciado por Puertas Automáticas Ediciones, asistieron representantes de TECNIFUEGO-AESPI (Comité de Puertas Cortafuego), AFIPA Murcia (Asociación de Fabricantes e Instaladores de Puertas Automáticas de la Región de Murcia, integrada en FREMM) y APA (Asociación Española de Fabricantes de Puertas Automáticas).

JORNADA EN FERIA DE VALENCIA

Además, el Comité de Puertas Cortafuego participó en las jornadas técnicas de la Feria Valencia, que se celebró el 4 de febrero. La jornada, organizada por PA ediciones, contó también con la participación de E.D.S.F. (Federación Europea de Fabricantes de Puertas).
www.tecnifuego-aespi.org//
www.puertasautomaticasediciones.com

canal, la gestión de cuentas clave, la coordinación de eventos y seminarios, y la implementación de la estrategia diseñada en la central de Mobotix junto con Rainer Artelt, sales director Europe, quien es ahora también responsable de Iberia, y con la ayuda de Tatiana Boquin (Inside Sales Manager Iberia) y Lucas San José.

San José, ingeniero en Informática por la Universidad Politécnica de Madrid, ha entrado a formar parte del equipo de Mobotix en diciembre de 2015 como Technical Project Engineer para España y Portugal. Las funciones que desempeña son las labores de preventa, soporte de proyectos y formador técnico en los seminarios que Mobotix ofrece a sus partners.

## Dorma y Kaba se han fusionado

DORMA y KABA se han fusionado para formar Dorma+Kaba. Esta unión se formalizó a partir del 1 de septiembre de 2015, después de cumplirse todas las condiciones necesarias, especialmente la aprobación de las autoridades de competencia en todos los países de relevancia.

La fusión acerca más a Kaba al objetivo de ofrecer a sus clientes soluciones integrales de alta calidad, así como la construcción y garantía de accesos y servicios de seguridad en todo el mundo. Este acuerdo entre Dorma y Kaba tiene como resultado una enorme mejora en eficacia, puesto que los productos y servicios ofrecidos por ambas entidades se complementan entre sí, creando sinergias de éxito. Se trata de una oportunidad única para las dos compañías, que unen sus fuerzas para el beneficio de socios y clientes.

## Vanderbilt: nuevo sitio web

Vanderbilt ha lanzado un nuevo sitio web. Con el fin de ahorrar tiempo y esfuerzo a sus clientes, parte fudamental de la oferta de Vanderbilt, la compañía ha desarrollado su nuevo sitio web para proporcionar un portal eficiente y sencillo de utilizar.

De esta manera la compañía proporciona a sus clientes toda la información y herramientas que precisa para sus proyectos de seguridad, por supuesto en adición al soporte directo que puedan prestarles.

¿Cuáles son las ventajas de la nueva web?

–Fácil acceso a la información

Dispondra de una plataforma de información con secciones claras y una navegación rápida y sencilla. Todo al alcance del usuario con unos pocos clicks. La subscripción online al newsletter asegurará no perderse nada de las novedades.

En definitiva nuestro nuevo portal proporcionará:

- Mejores rutas de documentación, sin reducir el soporte directo a través de los contactos técnicos y comerciales habituales.

– Área interna con valor añadido, toda la documentación e información de interés ubicada en un solo sitio.

– Los horarios de trabajo no afectan al negocio, la web está siempre disponible y a través de ella la compañía espera mejorar los canales de comunicación.

¿Qué puede encontrar en el nuevo sitio web?

En la nueva web se encontrará toda la oferta de productos al tratarse de un catálogo on-line permanentemente actualizado, mostrado producto por producto e incluyendo la mayor parte de la documentación técnica y comercial. Adicionalmente esta plataforma proporciona información acerca de la compañía, cómo trabaja, y consta con funciones útiles como newsletters y las novedades de productos, etc...

Desde su origen se han ido incorporando nuevas capacidades e información con el Download Center, que permite descargar software y firmware y la documentación técnica. Además incorpora seminarios, cursos en formato electrónico, notas técnicas de producto y de aplicación...

En definitiva una plataforma viva donde se irán encontrando todas las novedades del negocio de Vanderbilt.

La unión de las dos empresas resulta compatible, incluso desde el punto de vista histórico y cultural. Ambas entidades fueron fundadas hace más de cien años, cuentan con una fuerte tradición y empleados de gran experiencia. Asimismo, comparten una misma pasión por la innovación y el esfuerzo de ofrecer al cliente un valor añadido.

Tras la fusión, ambas empresas se encuentran actualmente en un periodo de adaptación en el que se están detallando las nuevas estructuras y responsabilidades. De cualqueir forma, por el momento, nada va a cambiar para los clientes, socios y proveedores de Kaba.

## Rister nuevo distribuidor de cámaras IP Vivotek y monitores de NEC

RISTER, con más de 35 años de experiencia en la distribución de productos de Circuito Cerrado de Televisión, ha sido nombrado nuevo distribuidor de la familia de productos IP del fabricante Vivotek y de toda la gama de monitores de NEC, tanto para uso comercial como profesional.

Vivotek, empresa taiwanesa fundada en el año 2000, diseña y fabrica soluciones de videovigilancia en alta definición que ofrecen la mejor calidad.


Las cámaras IP, su software y el sistema NVR conforman una solución completa de videovigilancia para ofrecer la mejor calidad de imagen del momento. Los sistemas Vivotek protegen y supervisan organizaciones en todo el mundo, incluyendo grandes corporaciones, instituciones gubernamentales, estadios deportivos, entornos comerciales, casinos o estaciones de transporte, entre otras, ofreciendo en todas ellas la calidad de imagen más avanzada.

Además, Rister incorpora en su portfolio de productos la distribución de monitores de la serie comercial y profesional de la marca NEC. Actualmente, NEC Display Solutions es el único fabricante que puede ofrecer una gama de soluciones tan amplia, con productos apropiados para todas las necesidades de sus clientes. NEC Display Solutions cuenta con una gran experiencia en el


## La Asociación Catalana de Empresas de Seguridad y Repsol fomentan el uso de autogas

El presidente de la Asociación Catalana de Empresas de Seguridad (ACAES), Gonzalo Castro Mata, y el director Territorial de Repsol Butano en Cataluña y Baleares, Joaquín Garrote Villar, han firmado un convenio para impulsar el uso del carburante AutoGas (o GLP de Automoción) entre las empresas adscritas a esta asociación.

El carburante AutoGas es un carburante alternativo ecológico de gran implantación en el mundo y Europa, donde respectivamente 25 y 11 millones de vehículos se benefician de las ventajas de este carburante.

Tal es la disminución de la contaminación con el uso del carburante AutoGas que las diferentes Administraciones estimulan la compra de este tipo de vehículos con diferentes medidas destinadas a fomentar su uso. A continuación se citan algunas de aplicación en Cataluña:

–Aportación del Plan MOVEA del Gobierno Central de hasta 3.500 € por la compra de un vehículo a GLP.

–Descuentos de hasta el 75% en el impuesto de circulación en numerosos ayuntamientos como por ejemplo Barcelona, Girona, Mataró, Badalona, L'Hospitalet de Llobregat, Manresa, Reus, Terrassa o Sabadell entre muchos otros o a nivel nacional Madrid, Málaga, Bilbao, Sevilla o La Coruña, etc.

–Bonificación del 30% en días laborables en los peajes de titularidad catalana de acceso a Barcelona, bonificación que además se suma a la bonificación por frecuencia de uso.

–Etc.

mercado para facilitar las soluciones visuales más completas en diversos mercados verticales. Su extensa gama de monitores incluye formatos que van desde la versión de escritorio de 17" a 32" hasta la versión Large Format Display de 32" a 98" con una resolución FullHD y 4K.

## Ingram Micro, acuerdo de distribución con Manhattan e Intellinet

EL pasado 15 de enero, en Halver, Alemania, Manhattan e Intellinet Network Solutions anunciaron el acuerdo de distribución con Ingram Micro España. Con este acuerdo las dos marcas accederán a toda la Península Ibérica, incluyendo España, Portugal, Andorra y Gibraltar. Gracias a este acuerdo Ingram Micro distribuirá una amplia gama de accesorios electrónicos de Manhattan y dispositivos de networking de Intellinet.

Ingram Micro España aumentará la presencia de los productos de Manhattan e Intellinet en el canal gracias a su amplia red de distribución, incluyendo integradores de sistemas, minoristas locales y canales de comercio electrónico. «Contando ya con relaciones duraderas y de confianza con Ingram Micro Estados Unidos y su filial en el Reino Unido, estamos orgullosos de añadir Ingram Micro


## Solución de Seguridad Dahua para la Seguridad Pública en Boa Vista (Brasil)

Dahua Technology, fabricante mundial de sistemas de Videovigilancia con sede en Hangzhou, China, provee una solución de ciudad segura para Boa Vista en Brasil.

Boa Vista (que significa Buena Vista) es la capital del estado brasileño de Roraima. Situada en el lado occidental del rio Branco, la ciudad dista 200 km de la frontera de Brasil con Venezuela. Siendo la única capital brasileña al norte del ecuador, Boa Vista experimenta un clima tropical con calor, con estaciones húmedas y de calor seco.

La sobrepoblación en las ciudades del interior da lugar a la delincuencia, vandalismo y un importante objetivo para el terrorismo. Esto afecta directamente al bienestar económico, político y personal de la comunidad de Boa Vista. Para prevenir el crimen y la violencia, y para crear un mejor ambiente para todas las personas que viven y trabajan allí, Dahua ofrece una solución de seguridad ciudad segura para Boa Vista.

La solución de seguridad ciudad segura Dahua se basa en una combinación de vídeo y datos multimedia. La instalación de cámaras de vigilancia de red Dahua se encuentra dentro de la CBD y opera 7 días a la semana, 24 horas al día. La instalación supervisa más de 100 cámaras en toda la región de Boa Vista. Las cámaras de red pueden observar y detectar incidencias en tiempo real. En cuanto al almacenamiento, Dahua ofrece su grabador de vídeo en red 4832, que soporta decodificación de flujo de vídeo de alta definición de 5 MP. Es compatible con el máximo de 32 canales de entrada de la cámara IP.

Para el formato de codificación de vídeo, que integra los algoritmos de compresión de vídeo H.264 / MJPEG, es compatible con el ancho de banda máximo entrante 200 Mbps y hasta resolución de 5MP vista previa y reproducción. El stream de video multicast consigue reducir aún más el ancho de banda necesario para la transmisión de vídeo de alta calidad. El grabador de vídeo de red 4832 de Dahua puede funcionar con varios tipos de cámaras en ambientes activos, en el lugar y de forma remota.

«La solución de seguridad ciudad segura Dahua habilita a Boa Vista para implementar el monitoreo en tiempo real y la grabación», dijo William Zhou, director de Ventas de América Latina y África en Dahua Technology. «Se jugó un papel importante en la atención de emergencias y para garantizar la seguridad de toda la ciudad.»

España a nuestros socios de distribución», dijo Mani Ramachandran, director de Desarrollo de Negocio de Manhattan e Intellinet. «El acceso directo de nuestro representante español de la marca tanto al canal como a la fuerza de ventas de Ingram Micro nos coloca en una excelente posición en el mercado ibérico.»

# Ágora UCA-Eulen: I Diálogo con expertos en Seguridad y Criminología

EULEN Seguridad, empresa decana en el sector de seguridad perteneciente al Grupo Eulen, empresa destacada en nuestro país en la prestación de servicios generales a empresas, ha participado en el Campus de Jerez de la Universidad de Cádiz en el I Diálogo con Expertos en Criminología y Seguridad, en el marco del Ágora UCA-Eulen.

Esta jornada, enmarcada en el Máster Oficial en Sistema Penal y Criminalidad, ha contado con el testimonio de la ex responsable de la lucha contra el crimen organizado de Chile, quien ha compartido su experiencia con el alumnado y egresados de este posgrado.

**Desarrollo de Negocio del área de Seguridad**

Asimismo, Eulen Seguridad, empresa colaboradora del Foro Ágora UCA– Eulen, participó con una ponencia impartida por Juan Manuel Armario, gerente de Desarrollo de Negocio del Área de Seguridad de la compañía en Andalucía y Ceuta, quien habló de la aplicación de la inteligencia y su lucha contra los delitos organizados. El ponente hizo especial hincapié en la globalización como factor de máxima influencia en el cambio de modus operandi de los delitos informáticos organizados que abarcan desde terrorismo a trata de blancas, entre otros.

El Ágora de Seguridad de la Universidad de Cádiz nace en 2011 y en 2014 pasa a denominarse Ágora UCA-Eulen en 2014, gracias a la colaboración y apoyo financiero de Eulen Seguridad a un proyecto dirigido a reflexionar y debatir las diferentes dimensiones del ámbito de la seguridad. Así, se articula a través de la presencia de destacados expertos en esta materia, procedentes de la administración, la política y el sector privado.

# TESA Assa Abloy: solución que permite a las empresas gestionar sus accesos con el móvil

A partir de ahora un smartphone, con tecnología NFC, puede sustituir a las llaves o tarjetas de empleado tanto en grandes corporaciones como en pymes. Se trata de una innovadora solución desarrollada por TESA ASSA ABLOY para clientes de empresa Vodafone. Con sólo descargar la app Vodafone Wallet se podrá gestionar el acceso del personal fijo u ocasional a aquellos recintos corporativos (oficinas, salas de reuniones, despachos...) que dispongan de un sistema de control de accesos electrónico.

Las principales ventajas para las empresas con esta nueva funcionalidad son el ahorro, la comodidad y la seguridad. En caso de pérdida del móvil -menos habitual que el extravío de una tarjeta- el administrador podrá de manera muy sencilla y con el uso de un intuitivo software eliminar la credencial almacenada de forma segura en la SIM. Además evita costes innecesarios en tiempo y dinero como el remplazo de llaves o la tramitación de nuevas tarjetas.

Con esta innovación TESA Assa Abloy se mantiene en la vanguardia tecnológica dentro de los sectores empresarial e institucional. Su sistema de control de accesos SMARTair™ –que permite el control y la seguridad de todas las puertas de un edificio de oficinas con una credencial electrónica inteligente sin contacto– se amplía y convierte la experiencia de apertura en una operación cómoda (cualquier modificación puede hacerse de modo remoto y no es necesario reprogramar la cerradura), adaptable (conviven las dos opciones: tarjeta y smarphone NFC) y segura.

Para disfrutar de este servicio TESA Assa Abloy se encarga de instalar su sistema de control de accesos a través de su red de instaladores homologados SMARTair™ y Vodafone dotará a los empleados con smartphones NCF adecuados para descargarse la aplicación Vodafone Wallet de Google Play.

Contactos de empresas, p. 7.

# Dallmeier: PService3, potente herramienta de configuración y gestión

Con PService3, Dallmeier presenta una nueva versión de su herramienta de configuración y gestión que ahora es aún más potente, más estructurada y más flexible.

PService3 es una aplicación de alto rendimiento para la configuración y gestión cómodas de sistemas amplios de VideoIP de Dallmeier. PService3 escanea la red de vídeo en busca de dispositivos Dallmeier, los reconoce de forma automática y los lista en una vista general. Si se necesita, PService3 proporciona la lista con una previsualización de las cámaras y filtrada según distintos criterios. De este modo se pueden gestionar cómodamente tanto cámaras como sistemas de grabación. Sus amplias funciones abarcan desde la modificación de direcciones IP, pasando por actualizaciones del software integrado, hasta la apertura directa de los diálogos de configuración.

PService3 es, en comparación con su versión anterior, aún más flexible y adaptable a las necesidades particulares de cada usuario. La interfaz de usuario ha sido revisada en su totalidad y se caracteriza por un diseño completamente modernizado y perfectamente estructurado que proporciona más claridad. Representación avanzada de sistemas de sensores multifocales Panomera®

La representación de sistemas de sensores multifocales Panomera® ha sido ampliada extensamente en la versión actual de PService3. Ahora se puede consultar información detallada de cada uno de los módulos de una cámara Panomera®. PService3 es compatible con todas las cámaras de red de Dallmeier, incluidos los sistemas de sensores multifocales Panomera®, así como con todos los dispositivos de grabación de Dallmeier a partir de la 4ª generación.

# Saborit: ropa táctica

La marca TRU-SPEC® presentó su nueva línea de ropa táctica «24-7» en el stand de Saborit International durante Sicur 2016.

La nueva línea «24-7» se caracteriza por ser muy versátil y ponible: como su nombre indica, el agente podrá llevar TRU-SPEC® las 24 horas del día, los 7 días de la semana, desarrollando la actividad que desee, estando de servicio o disfrutando de su tiempo libre, sin tener que renunciar a la calidad y a una buena imagen. La marca TRU-SPEC® es sinónimo de alta calidad, resistencia y comodidad en los EE.UU., su país de origen, donde es uno de los principales proveedores de uniformes y equipamiento a cuerpos militares y policiales y otros profesionales de la seguridad.

# PERSAX: sistema Extreme, seguridad en estancias

Persax Grupo, especialista en el sector de las persianas y fabricante de elementos de cerramiento desde 1976, lanza el sistema Extreme para aportar un extra de seguridad ante los robos con fuerza en domicilios, locales comerciales o cada vez más numerosos robos en trasteros, garajes...

Una de las formas más comunes de los delincuentes para acceder a los establecimientos es a través de puertas y ventanas. Según explica Lorenzo Herrero, director adjunto de Persax Grupo «la seguridad en las puertas comerciales o puertas de garaje y ventanas se hace fundamental, ya que son puntos vulnerables, quizá incluso más que la puerta principal de una vivienda, y por tanto requieren de una especial protección. El nuevo sistema de seguridad EXTREME 60 de Persax Grupo está especialmente indicado para aquellas zonas donde se requiere un extra de seguridad por el alto índice de robos, o para los puntos geográficos de climas extremos, ya que aporta un extra de seguridad con una resistencia al viento superior a un sistema normal. Compatible con las lamas Blockalum 60 y Segur 60, de las más seguras del mercado, el sistema Extreme consta de una guía y tapones especiales en los extremos de cada lama, que en conjunto impiden que ésta se salga, aportando un extra de resistencia y seguridad al conjunto de la ventana o puerta.

# AGA presenta la más innovadora línea de cerraduras electrónicas de alta seguridad

AGA lleva muchos años construyendo junto con sus clientes y colaboradores una imagen de marca fuerte y creíble. Reforzar la imagen y mejorar esa relación con aquellas personas que hasta ahora han confiado en AGA, ya sería un éxito. En Sicur, AGA presentó una nueva línea de cerraduras electrónicas que se suma a la amplia gama de productos de su catálogo y que tiene como objetivo principal, dar salida a la demanda del mercado nacional e internacional en soluciones integrales de alta seguridad.

«El conocimiento de un sector donde llevamos trabajando más de 50 años y la colaboración con la empresa alemana INSYS, nos ha permitido mejorar en los procesos de diseño y la fabricación de productos facilitando el lanzamiento de nuevas soluciones de alto valor tecnológico, que garantizan una mayor calidad y seguridad en nuestros sistemas de apertura y cierre.»

Esta nueva gama de cerraduras electrónicas que AGA presentó en Sicur, con un contrastado grado de seguridad ya que son sistemas certificados por VdS y ECBS, está destinada a ser una nueva forma de entender la protección y tranquilidad. Una nueva gama de cerraduras que además de por su calidad, sorprenderá por la fiabilidad, cuidado diseño y facilidad de montaje de sus componentes.

Si sus características técnicas son una cualidad destacable a todos los niveles, no lo son menos los beneficios y prestaciones para el usuario. Estos son algunos de ellos:

- Máxima facilidad de montaje. Adecuada para la reposición.
- Programación de calendarios y rutinas.
- Sencilla conexión al ordenador PC.
- Registro de accesos / eventos.
- Posibilidad de conexión a sistemas de detección de intrusos.
- Etc.

# Delta Informática: nuevo escáner de pasaportes y DNI con detección de documentos falsos

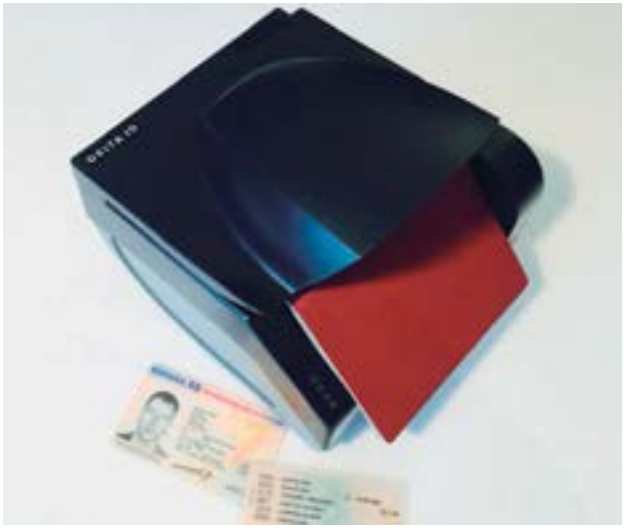
La empresa tecnológica Delta Informática ha lanzado recientemente un nuevo escáner de DNIs y pasaportes con capacidad para detectar documentos fraudulentos.

Se trata de un modelo de escáner fotográfico que además de adquirir la imagen del DNI con luz blanca, dispone de captura de imagen con luz infra roja y Ultravioleta. Con esta tecnología el sistema es capaz de identificar automáticamente las marcas de seguridad existentes en los documentos de identidad y pasaportes. Además el sistema va equipado con lector de chip de proximidad ( RFID ) compatible con el estándar para pasaporte electrónico ICAO9303. Esto permite lectura del chip existente en el pasaporte, así como en el nuevo DNI español 3.0, que también incluye esta tecnología.

El sistema DELTA ID compara la información impresa en el documento y obtenida a través de la imagen con la información biométrica codificada en el chip, detectando posibles alteraciones en la fotografía o los datos.

Como en modelos anteriores DELTA ID SmartCam reconoce y obtiene de forma automática los datos del documento de forma que agiliza la gestión de acreditaciones, control de accesos, procesos de check in o alta de clientes.

Con esta novedad, empresas de seguridad, administraciones públicas, banca, hoteles o retail no solo podrán agilizar sus procesos de atención al cliente sino que podrán tener la tranquilidad de saber que el documento escaneado es auténtico evitando posibles fraudes por suplantación de identidad.



# ATA98 Seguridad: nueva gama AHD 1080p, porque la definición lo es todo

ATA98 Seguridad S.L. ha presentado su nueva gama de producto basada en sistema de Alta Definición, con protocolo abierto AHD, a resoluciones de 1080p.

La nueva gama de producto a 1080p, irrumpe en el mercado alcanzando la mayor definición en grabación jamás pensada en sistemas basados sobre cableado coaxial.

Las cámaras con tecnología AHD 1080p, incluyen sensores de 1/2.8", lo que nos permitirá tener un ángulo de visión horizontal mucho mayor a lo que estábamos acostumbrados.

Implementan la última gama de tecnología led, garantizando una imagen de alta calidad en modo noche.

Sobre la gama de cámaras, podemos resaltar su modelo domo varifocal con lente motorizada y auto-foco, la cual podremos actuar sobre el motor de la lente desde el DVR, PC o APP de SmartPhone, realizando un zoom óptico con resolución 1080p sin perder el más mínimo detalle.

Los DVR´s, como marca toda la línea de ATA98 Seguridad S.L. son tríbridos, aceptando cámaras Analógicas, cámaras IP (ONVIF) y cámaras AHD (720p / 1080p), a parte, incorporan su ya conocido sistema de P2P basado en nube.

Dichos grabadores, amplían características a señalar como por ejemplo la opción «coaxial control», la cual nos permite poder configurar el menú interno de las cámaras 1080p desde el mismo grabador, cómodamente, sin necesidad de estar a pie de cámara.

Nuevamente, la marca española ATA98 Seguridad, muestra una nueva línea de producto que dará mucho que hablar en el sector de la seguridad.

# Samsung: minidomo SNV-6013 con conteo de personas


La última actualización del firmware del minidomo IP SNV-6013 permite hacer uso, de forma gratuita, de la funcionalidad de conteo de personas. Este minidomo IP antivándálico, especialmente diseñado para entornos comerciales, refuerza su potencial de uso con una aplicación incorporada en el chipset WiseNet III Open Platform de la cámara mediante una sencilla e intuitiva configuración. Aquellos usuarios que ya dispongan de este modelo de cámara, podrán descargarse el firmware en la siguiente dirección http://www.samsungsecurity.com/product/product_view.asp?idx=7056&cid=83&clvl=0#FL060000.

El minidomo antivandálico SNV-6013, con un diámetro inferior a los 113 mm y una altura de tan solo 64 mm, ofrece una resolución Full HD (1920 x 1080) de excelente calidad y, gracias a su nueva funcionalidad, permite a los propietarios de tiendas y locales comerciales mejorar la gestión y rendimiento de sus establecimientos.

Esta nueva funcionalidad se puede configurar para que muestre estadísticas relacionadas con el recuento de personas, en gráficos, ya sea diario, semanal o mensual. Y permite buscar las estadísticas de dichos datos respecto a un día, semana o mes. Además, permite mostrar estadísticas sobre zonas de ocupación, así como verificar la información sobre el recuento y zona con vídeo en tiempo real.

El minidomo SNV-6013 también es una excelente opción para los instaladores y usuarios que quieran instalar una cámara discreta con esta funcionalidad en oficinas, centros sanitarios, hoteles y transportes, así como en espacios reducidos como ascensores, vestíbulos y escaleras.

# Videofied: ningún daño... detecten antes de la intrusión¡

La cámara MotionViewer exterior OMVC es una cámara inalámbrica, que funciona con pilas, dispara por detección de movimiento en la cual está integrada una lente cortina.

Esta lente permite adaptar una protección fuera de su casa, una protección residencial exterior antes de una intrusión en su domicilio!

El OMVC lleva 4 leds infrarrojos permitiendo una visión nocturna optimizada, también una autoprotección en caso de extracción del detector cámara.

- Único sistema de alarma radio con videoverificación de color.
- Sistema desarrollado para un uso en exterior - IP65.
- Gama radio bidireccional en la banda de frecuencia europea 868 MHz.
- Autonomía de las pilas de 4 años.

Videofied, un sistema 100% disuasivo!

No esperen que los ladrones rompan su puerta o sus ventanas: el sistema Videofied protege y alerta antes de la intrusión!

En caso de un intento de intrusión por un patio, una terraza o bien por un jardín, las cámaras exteriores Videofied detectan la presencia, graban y alertan su CRA. Las sirenas y sirenas-flash exteriores hacen parte también de los elementos de disuasión del sistema de alarma. Su disparo disuade al intruso y alerta los vecinos. El potente flash de la sirena permite la localización visual de la alerta.

En caso de intrusión o de peligro real, las fuerzas del orden pueden intervenir rápidamente.

¡Una experiencia reconocida!

RSI Video Technologies desarrolla soluciones de seguridad anti-intrusión con un real avance tecnológico. Gracias a los productos Videofied, ponemos a su disposición un concepto innovador y único en el mundo!

Desde la concepción hasta la producción pasando por ventas, el equipo esta a disposición de los clientes. Más de 20 años de experiencia hace de que RSI Video Technologies sea un actor inevitable en el mercado. Los productos de Videofied están reconocidos con más de 500 000 sistemas instalados a día de hoy.

# ESET: nueva solución para entornos virtualizados

ESET, empresa pionera en la detección proactiva de malware desde hace más de dos décadas, ha anunciado el lanzamiento de ESET Virtualization Security. Este producto sin agente totalmente nuevo y basado en VMware vShield combina la appliance de ESET Virtualization Security con ESET Remote Administrator, cuya última versión acaba de ser lanzada al mercado con características como la administración de dispositivos iOS o la integración de ESET SysInspector. La herramienta de diagnóstico de ESET ha sido totalmente integrada en ESET Remote Administrator para ayudar a los administradores de seguridad a consultar las incidencias de seguridad y los cambios en el sistema de cada equipo.

El módulo ESET Mobile Device Management para iOS, por su parte, permite a los clientes implantar totalmente la política BYOD (Bring your Own Device, es decir, que facilita que los empleados usen sus propios dispositivos en el trabajo, minimizando los riesgos). Con la nueva versión, los administradores pueden configurar los ajustes de seguridad de los dispositivos con sistema iOS junto a otros dispositivos en la red de la empresa.

«La administración para dispositivos móviles para iOS es fácil de configurar y permite al departamento de sistemas administrar, configurar, bloquear o borrar remotamente todo el contenido de los dispositivos iOS», afirma Michal Jankech, responsable de productos para empresas en ESET. «Añadir esta característica a la consola de administración remota de ESET hace que se pueda evitar la interacción del usuario final, con lo que se consigue una mejor implantación de las directivas de la empresa y un mejor control de los dispositivos».


Contactos de empresas, p. 7.

# 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**

Antoñita Jiménez, 25
28019 Madrid
**ISO 9001**
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**

## COMUNICACIONES

**DYNASCAN** professional radio
**PIHERNZ**

Doctor Ramón Solanich
i Riera 13-15
08905 L'Hospitalet-BCN
Tel. 93 334 88 00*
comercial@pihernz.es
www.pihernz.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**

online
**SEGURPARKING**
Control de mandos por Internet

**Sistemas de seguridad para garajes comunitarios**

C Aragón 355 - 08009 Barcelona
T 934575026
info@segurparking.com
**www.segurparking-online.com**

# MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

**SKL** Smart Key & Lock
Ferrerías 2,
20500 MONDRAGÓN -SPAIN-

**+34 943 71 19 52**
**info@skl.es**
**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**

C/ Caballero, 81
08014 Barcelona
Tel. 93 247 88 00 • Fax 93 247 88 11
spec@specsa.com
**www.grupospec.com**

---

**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**

---



---

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**

---

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

---

**Soluciones integrales en control de Accesos y seguridad**

Carrer Esperança, 5
08500 Vic (Barcelona)
Tel.: 902 447 442
Fax.: 938 864 500

info@accesor.com
**www.accesor.com**

---

**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**
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**
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**

---



---

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, 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 S.A.**

C/ Barcelona 101
17003 Girona
T (+34) 972 203 300

**info@optimus.es**
**www.optimusaudio.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**

---

## PROTECCIÓN CONTRA INCENDIOS. ACTIVA

---

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**

# MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

# MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

## 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**

### 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

### dahua TECHNOLOGY

**Dahua Technology Co, Ltd.**

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

### 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**

### Canon

**Canon España, S.A**
Avenida de Europa 6
28108 Alcobendas
Madrid

Tel: +34915384500
www.canon.es
**camarasip@canon.es**

### BOSCH

**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**

## VIGILANCIA POR TELEVISIÓN

### VISIOTECH

**Visiotech**
Avenida del Sol, 22
28850, Torrejón de Ardoz (Madrid)
Tel.: 911 836 285 • Fax: 917 273 341
info@visiotech.es
www.visiotech.es

### ernitec

Professional Video Surveillance

**Ballerup, Dinamarca.**
**Tlf. +34 902 65 67 98**
**ventas@ernitec.com**
**www.ernitec.com**

### AXIS COMMUNICATIONS

**AXIS COMMUNICATIONS**
C/ Yunque, 9 - 1ºA
28760 Tres Cantos (Madrid)
Tel.: +34 918 034 643
Fax: +34 918 035 452
**www.axis.com**

### HIKVISION

**HIKVISION SPAIN**
C/ Almazara 9
28760- Tres Cantos (Madrid)
Tel. 917 371 655
Fax. 918 058 717
**info.es@hikvision.com**
**www.hikvision.com**

### LSB www.lsb.es

**Expertos en VIDEOVIGILANCIA**

LSB, S.L.
C./ Enero, 11 28022 Madrid
Tf: +34 913294835
info@lsb.es

### Dallmeier

**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**

### FF Videosistemas GEUTEBRÜCK

**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**

### SAMSUNG

**Samsung Techwin Europe Ltd**

P. E. Omega - Edificio Gamma
Avenida de Barajas, 24 Planta 5 Oficina 5
28108 Alcobendas (Madrid)
Tel.: 916 517 507

**STEsecurity@samsung.com**
**www.samsungcctv.com**

### EET SECURITY European Distributor

C/ Aragoneses, 15
28100 Alcobendas, Madrid
Tlf. 902 902 337

**seguridad@eeteuroparts.es**
**www.eeteuroparts.es**

### WD

A Western Digital® Company

**WD ESPAÑA**
4 boulevard des Iles
92130 Issy les Moulineaux · Francia
florence.perrin@wdc.com
Tel.: 00 331 70 74 46 27
www.wdc.com

### N2V

**N2V**
C/ Torrent Tortuguer, 7 - nave 4
Pol. Ind. Els Pinetons
08291 RIPOLLET (Barcelona)
Tel.: 93 580 50 16 - Fax: 93 580 36 58
**n2v@n2v.es**
**www.n2v.es**

# MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

## CERTIFICACIONES

**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**

**INSPECCIÓN Y CERTIFICACIÓN**

C/ Caleruega, 67, Planta 1
28033 Madrid
**Tel. 917663133**
**http://www.tuv-nord.es/**

**ASOCIACIÓN ESPAÑOLA DE INGENIEROS DE SEGURIDAD**

C/ San Delfín 4 (local 4 calle)
28019 MADRID
**aeinse@aeinse.org**
**www.aeinse.org**

**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**

Josep Estivill, 67-69
08027 Barcelona, Spain.
**www.ata98.com**
**info@ata98.com**
**Tel. +34 931 721 763**

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.

## ASOCIACIONES

C/ Viladomat 174
08015 Barcelona
Tel.: 93 454 48 11
Fax: 93 453 62 10
**acaes@acaes.net**
**www.acaes.net**

**ASOCIACION ESPAÑOLA DE EMPRESAS DE SEGURIDAD**
Alcalá, 99
28009 Madrid
Tel.: 915 765 225
Fax: 915 766 094

**ASOCIACIÓN DE EMPRESAS DE SEGURIDAD Y SERVICIOS DE ANDALUCIA**

C/ DOCTOR DUARTE ACOSTA Nº 7
11500 PUERTO DE SANTA MARIA · CADIZ
Tel. 677.401.811
Fax: 954.002.319
**gerencia@adessan.es**

**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**

**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**

## EVENTOS DE SEGURIDAD

**SECURITY FORUM**
Tel.: +34 91 476 80 00
Fax: +34 91 476 60 57
www.securityforum.es
info@securityforum.es

C/ Alcalá 99
28009 Madrid
Tel. 915765255
Fax. 915766094

**info@uaseguridad.es**
**www.uaseguridad.es**

**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**

**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

# MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

**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**

**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-ESPAÑA**
C/ Velázquez 53, 2º Izquierda
28001 Madrid
Tel.: 911 310 619
Fax: 915 777 190

**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

**FEDERACIÓN ESPAÑOLA DE SEGURIDAD**
Embajadores, 81
28012 Madrid
Tel.: 915 542 115 - Fax: 915 538 929
**fes@fes.es**
**C/C: comunicacion@fes.es**

**ASOCIACIÓN DE JEFES DE SEGURIDAD DE ESPAÑA**

Avd. Merididana 358. 4ºA.
08027 Barcelona
Tel. 93-3459682 Fax. 93-3453395
**www.ajse.es presidente@ajse.es**

**ASOCIACIÓN VASCA DE PROFESIONALES DE SEGURIDAD**
Parque tecnológico de Bizkaia
Ibaizabal Kalea, 101
**sae@sae-avps.com**
**www.sae-avps.com**

**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**

## FORMACIÓN DE SEGURIDAD

**TECNOSYSTEMS**
**Formación especializada en video IP**
**Avenida de Brasil 29, 28020 Madrid**

Telf.: 916 323 168
www.videoipformacion.es

**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

## 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**

## 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

**TECOSA**

Telecomunicación, Electrónica y Conmutación

**Grupo Siemens**
**Industry Sector**
División Building Technologies
Ronda de Europa, 5
28760 Tres Cantos - Madrid
Tel.: +34 91 514 75 00 - Fax: +34 91 514 70 30

## APLICACIONES INFORMÁTICAS

**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**

## INSTALACIÓN Y MANTENIMIENTO

**Techco Security**
C/ Barbadillo 7
28042 Madrid
+34 91 312 77 77
www.techcosecurity.com
tcs@techcosecurity.com

# MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

SEGURIDAD LEVANTE
Homologación de registro D.G.S.E. nº 432

**INSTALACIÓN Y MANTENIMIENTO**
INTRUSIÓN – CCTV – INCENDIO – ACCESOS
SUBCONTRATACIÓN
ALICANTE, VALENCIA, MURCIA, ALBACETE

www.seguridadlevante.com
**902 400 022**
info@seguridadlevante.com

## PUBLICACIONES WEB

## MATERIAL POLICIAL

GRUPO RMD SEGURIDAD, S.L.

**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

Telefónica Ingeniería de Seguridad

**TELEFÓNICA INGENIERÍA DE SEGURIDAD**
Don Ramón de la Cruz 82-84 4ª
28006 Madrid
Tel.: 917 244 022 • Fax: 917 244 052
**tis.clientes@telefonica.es**
**www.telefonica.es/ingenieriadeseguridad**

PUNTO SEGURIDAD.com

**PUNTOSEGURIDAD.COM**
TF: 91 476 80 00

**info@puntoseguridad.com**
**www.puntoseguridad.com**

SABORIT INTERNATIONAL
Importación y Distribución de Equipos para la Seguridad, Vigilancia y Defensa

**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**

## TRANSPORTE Y GESTIÓN DE EFECTIVO

AGÜERO Proyectos e Instalaciones, S.L.

**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



## VIGILANCIA Y CONTROL

LOOMIS

**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**

ambar SEGURIDAD Y ENERGÍA

**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**

INSTAL SEC

Avda. Manzanares, 196
28026 Madrid
Tel.: 914 768 000 - Fax: 914 766 057
**publi-seguridad@epeldano.com**
**www.instalsec.com**

SECURITAS

**SECURITAS SEGURIDAD ESPAÑA**
C/ Entrepeñas, 27
28051 Madrid
Tel.: 912 776 000
email: info@securitas.es
**www.securitas.es**

**¿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

# Sergio Picallo González

Secretario Sectorial de Seguridad y Servicios Auxiliares. UGT-FeS

# «La sociedad debe conocer y valorar el papel que desempeña el vigilante de seguridad»

Gemma G. Juanes

NO diría toda la verdad si afirmara que ésta ha sido una entrevista en toda regla de manual de periodismo: pregunta, respuesta, pregunta… Sí, fue un encuentro muy profesional, pero donde las respuestas se adelantaban veloces a las preguntas, y las preguntas se tachaban, indiscriminadamente, en el bloc del periodista. El hombre que ocupa desde no hace ni tan siquiera un año la Secretaría Sectorial de Seguridad y Servicios Auxiliares de UGT-FeS, Sergio Picallo, lo tiene muy claro, ha venido a hablar y, sobre todo, a reivindicar la profesión del vigilante de seguridad. Sus palabras tienen como escenario un despacho, que comparte con otros «compañeros», en una de las sedes del sindicato en Madrid. Allí habló, con el único límite marcado por una reunión posterior, sobre el presente y futuro de estos profesionales de la seguridad.

Estas líneas son un simple esbozo de una rápida narración apenas interrumpida donde la figura del vigilante adquiere un absoluto protagonismo. Sergio Picallo, vigilante de profesión desde hace más de 20 años, y con una amplia trayectoria sindical asumiendo diferentes cargos de responsabilidad, reconoce que el sector de la seguridad privada se ha ido adaptando a las necesidades actuales y reales, con unos trabajadores cada vez más preparados y cualificados, aunque matiza que «pese al esfuerzo y trabajo, carecen del reconocimiento profesional, económico y social que deberían tener».

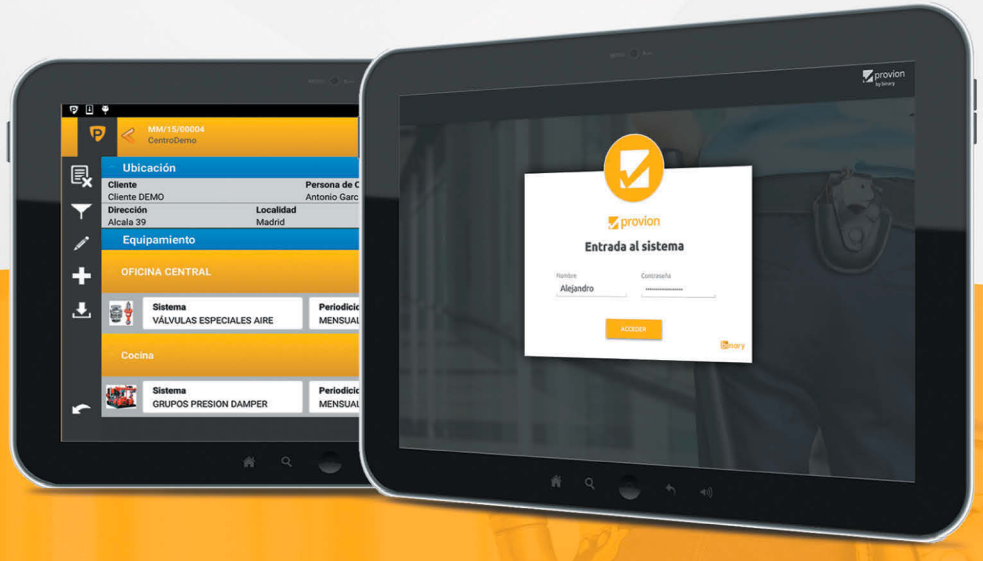
Fiel defensor de la formación y especialización, se queja de la ausencia de carrera profesional, como uno de los grandes obstáculos para el desarrollo y crecimiento laboral de los vigilantes. «Siempre hemos defendido una mayor exigencia en el acceso a la profesión, y dotar al sector de una carrera, donde el trabajador se pueda desarrollar y progresar; es así como conseguiremos el reconocimiento que no tenemos. Es fundamental que la sociedad conozca y valore el papel que desempeña el vigilante de seguridad. Nuestro futuro pasa por la implantación de una carrera profesional».

Especialización, reconocimiento, esfuerzo, mejoras laborales y sociales, nueva normativa…, Sergio Picallo, con contundentes afirmaciones, continúa analizando el momento que le ha tocado vivir al sector de la seguridad que, inmerso aún en un periodo de versatilidad e incertidumbre, demanda estabilidad y progreso. Mientras, en medio de esta reivindicativa conversación, no me resisto a entresacar otras cuestiones más personales. Aprovecha su tiempo libre para huir de la capital y perderse con su familia por Santander, cuna de sus orígenes. Dice ser de aquellos que se ajusta el mandil en la cocina para luego degustar suculentos platos acompañados de un buen vino. Hoy dedica sus horas de lectura a descubrir la historia de Corocotta, un guerrero cántabro –«El último soldurio», de Javier Lorenzo–, que luchó junto a Julio César, y que fue capaz de renunciar a la ciudadanía romana por conservar sus raíces. Lo dicho: no fue una entrevista en toda regla… pero, eso sí, al final quedó tiempo para un café. ●

binary
Soluciones Informáticas

# Software para la gestión eficaz de la información

Sector de Seguridad | Mantenimiento | Protección contra incendios | Gestión documental | Movilidad |




## protecnus

- Registro de centros e inventarios de equipamiento
- Geoposicionamiento de técnicos
- Planificación de mantenimientos preventivos y correctivos
- Plataforma de clientes
- Emisión de certificados e informes

www.protecnus.com

## provion

- Registro de documentación y partes de trabajo a tiempo real
- Envío de alertas por sms y mail
- Geolocalización de sus agentes
- Reporte de fotos y videos
- Análisis de datos y cuadros de mando
- Portal de clientes

www.provion.tech

**+ Info 91 184 76 00**
info@binary.es

www.binary.es
España · Chile · Argentina

binary
Soluciones Informáticas

# N° 1 EN TU SEGURIDAD

## Un Partner Sólido, Comprometido, Innovador, Fiable, Presente.

Hikvision lider mundial en el mercado de la seguridad, dispone de una completa gama de productos y soluciones adaptadas a las diferentes necesidades del mundo actual. Con más de 15.000 empleados y una constante apuesta por la innovación, Hikvision es la primera elección para los profesionales de la seguridad.

**Hikvision Spain**
C/ Almazara, 9
28760 Tres Cantos (Madrid)
T +34 91 7371655
F +34 91 8058717
info.es@hikvision.com

www.hikvision.com