# CUADERNOS DE SEGURIDAD

Núm. 318 • ENERO 2017 • 10 euros

PUNTOSEGURIDAD.com


## El sector ante 2017: retos de futuro

## RPAS y Seguridad

**Ciberseguridad:** las aerolíneas tampoco se libran del fraude

# Dahua Solución

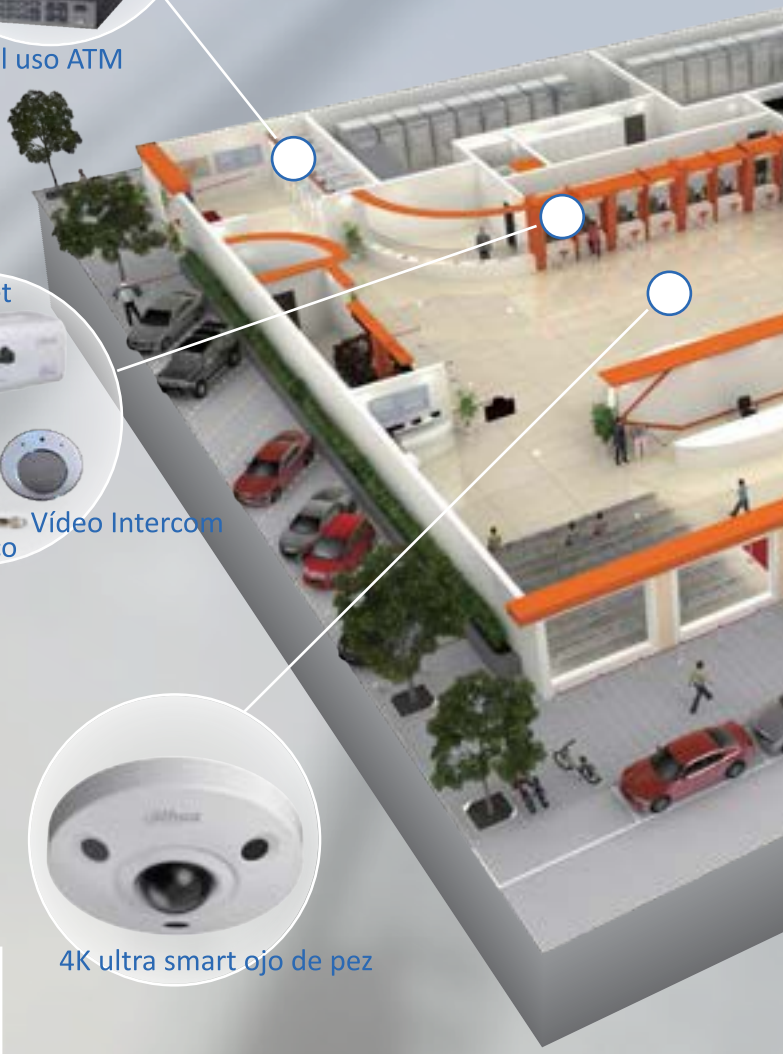
## Banca

### ATM

Evitar alto riesgo de seguridad de robos, atracos, incursiones.
Vigilar integralmente.
Grabación de videos.

2MP Cámara Pinhole

DVR del uso ATM



### Mostrador

Gran volumen de transacciones en efectivo, Imagen facial de alta-definición e información registrada de transacciones son necesarios para evitar peligro escondido.

Cámara Bullet

Botón de pánico

Vídeo Intercom

### Vestíbulo

Grandes áreas con un montón de gente requieren alta definición y sin puntos ciegos.



4K ultra smart ojo de pez

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

# Integrada de Seguridad

# y Finanzas

Video Wall

Plataforma de gestión de vídeo

## Centro de Seguridad

Seguridad de datos.
estabilidad y confiabilidad del sistema.
Abundante mecanismo de alarma.



Multi-lente Paronámica Cámara

## Outdoor

Entorno complicado, el rápido cambio de luz requieren alta-definición, ultra gran angular, Starlight tecnología.



Smart WDR IR Cámara

## Entrada

Imagen facial clara bajo la luz del sol, reconocimiento VIP mejora la experiencia del cliente.

España

Portugal

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

# ¿ESTÁS PREPARADO?

**CCIB**
Centro de Convenciones
Internacional de Barcelona

17 y 18 de mayo
BCN**2017**

Security FORUM
International Security Conference & Exhibition

www.securityforum.es

## SECTOR DE LA SEGURIDAD PRIVADA

# 2017, punto de partida de una nueva etapa

Traspasar la frontera de un año a otro siempre supone el punto de partida de una etapa para renovar ilusiones y esperanzas, motivarse y plantear buenos propósitos para afrontar los próximos 365 días con éxito. Doce meses donde lo más urgente es pasar a la acción para que, con unas previsiones económicas cada vez más optimistas, se generen mecanismos y herramientas que terminen con una etapa de crisis, revitalicen el tejido empresarial y social, y devuelvan a la sociedad, y al sector de la seguridad en particular, ilusiones de presente y futuro.

Y ese es el principal objetivo del sector de la Seguridad de nuestro país, que se abre paso con fuerza en busca de un futuro prometedor, en donde, de nuevo, el desarrollo reglamentario de la Ley de Seguridad Privada, Ley 5/2014 de 4 de abril, sigue siendo una necesidad apremiante.

Por ello, en este número que inaugura un recién estrenado 2017, acudimos un año más a los representantes de las distintas asociaciones sectoriales para que sean ellos los que expongan las expectativas y claves del sector de la Seguridad Privada, ante los nuevos retos y desafíos para 2017. La primera y más urgente, la publicación del Reglamento de Seguridad Privada, del que se espera recoja el «trabajo ya realizado por el sector desde la publicación de la Ley», y con el que se «disiparían algunas de las dudas que surgen respecto a determinadas previsones normativas, como la vigilancia en espacios públicos, la subcontratación, la videovigilancia,...», señala Anna Aisa, gerente de la Asociación Catalana de Empresas de Seguridad (ACAES).

Pero el sector no solo se prepara para estos futuros desarrollos normativos, sino que además se enfrenta a grandes desafíos actuales como es la protección de las infraestructuras críticas, «en la que es fundamental la cooperación público-privada entre las empresas y administraciones», explica Paloma Velasco, directora ejecutiva de la Asociación Española de la Empresas de Seguridad (AES), quien además hace hincapié en los desafíos futuros: «las telecomunicaciones, la trasformación digital, el Internet de la Cosas, el Big Data,..». El sector se muestra unánime en sus planteamientos de futuro, así lo han constatado en este número los representantes de las asociaciones, donde la tecnología sigue y seguirá jugando un papel fundamental.

Y en este inicio de año, ponemos el punto de mira en Security Forum 2017, que celebra ya su quinta edición los días 17 y 18 de mayo en Barcelona, y donde el equipo de Peldaño sigue trabajando en la elaboración de sus contenidos y novedades. También está en marcha el II Congreso Nacional de Jefes de Seguridad, que tendrá lugar también en Barcelona el próximo mes de abril. Un evento que cuenta con el respaldo de la Asociación de Jefes de Seguridad de España (AJSE), y que tiene entre sus objetivos profundizar en la figura del jefe de Seguridad y analizar su futuro profesional.

Citas de referencia imprescindibles para un sector que apuesta por la calidad en el servicio, la formación, la especialización y la innovación, en un año que comienza con buenas perspectivas y lleno de oportunidades.

CUADERNOS DE SEGURIDAD

www.puntoseguridad.com

Nº 318 • ENERO 2017

Peldaño

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

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

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

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

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





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

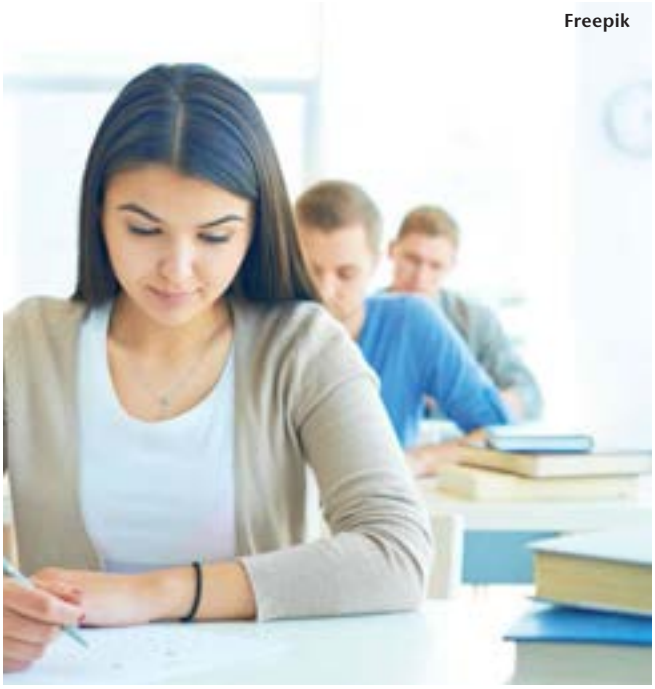
# FEBRERO 2017 - Nº 319

# EN PORTADA

## SEGURIDAD EN CENTROS UNIVERSITARIOS

La seguridad en los centros universitarios -englobamos tanto públicos como privados- se encuentra sujeta a una diversa normativa general que abarca todas las áreas en cuanto a seguridad se refiere. Edificios e instalaciones muy diversos, que con el paso de los años han ido cambiando su aspecto interno –en algunos casos hasta el externo–, y otros son de reciente construcción. Lugares en los que es preciso establecer medidas y medios de seguridad adecuados para garantizar la seguridad de sus trabajadores, así como la de sus alumnos, y personal externo. Y es que, quién no ha oido alguna vez hablar de robos, incendios, actos violentos, etc. en centros universitarios; instalaciones que cuentan -en la gran mayoría de los casos- con servicios y sistemas de seguridad actualizados y adaptados a las últimas tecnologías. Responsables y directores de Seguridad toman la palabra en este número para contar cómo gestionan la seguridad de los centros universitarios.

Freepik




Freepik

## SISTEMAS DE ANÁLISIS DE VÍDEO

Los sistemas de análisis de vídeo han ido potenciando y afianzando, desde su introducción en el ámbito de la seguridad, su utilidad, aplicación y valor añadido. De esta manera, se han ido convirtiendo en uno de los elementos principales y fundamentales de cualquier instalación.

Las tecnologías, además, también han hecho acto de presencia en este tipo de sistemas, y se han caracterizado por un permanente avance y mejora, lo que ha hecho posible que amplíen sus funciones y utilidades.

Y es que los sistemas de análisis de vídeo, al tratarse de un componente de una industria con un alto factor de desarrollo y necesidades funcionales, ha mantenido desde siempre un avance exigente y permanente en todos sus aspectos técnicos. Hoy en día ya podemos encontrar potentes sistemas, eficaces, fiables y aplicables a cualquier tipo de escenario.

**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 |
|---|---|---|---|
| ACG DRONE | 66 | 876500602 | www.acgdrone.com |
| AXIS COMMUNICATIONS | 47,84 | 918034643 | www.axis.com |
| AXXONSOFT | 82,83 | 934925729 | www.axxonsoft.com |
| CUEVAVALIENTE INGENIEROS | 79 | 918047364 | www.cuevavaliente.com |
| DAHUA | 2ª Cubierta, 3,74 | 917649862 | www.dahuasecurity.com |
| ELEVEN PATHS | 72 | 914830815 | www.11paths.com |
| EULEN SEGURIDAD | 60 | 902355366 | www.eulen.com/es/seguridad |
| FF VIDEOSISTEMAS | 92 | 902998440 | www.ffvideosistemas.com |
| GRUPO AGÜERO | 94 | 915655420 | www.grupoaguero.com |
| GRUPO ÁLAVA INGENIEROS | 56 | 915679700 | www.alava-ing.es |
| GRUPO VPS | 25,106 | 930047035 | www.vpsitex.es |
| HANWHA | 41 | 916517507 | www.hanwha-security.eu |
| HIKVISION | 4ª Cubierta,17,53 | 917371655 | www.hikvision.com |
| HOCHIKI | 19 | 441634260133 | www.hochikieurope.com |
| HOMSEC | 59 | 915945255 | www.homsec.es |
| II CONGRESO JEFES DE SEGURIDAD | 3ª Cubierta | 914768000 | www.congresojefesdeseguridad.com |
| MBC IURIS | 68 | 931702417 | www.mbciuris.com |
| OPTEX | 76 | | www.optexiberia.com |
| PACOM | 63 | 902052377 | www.pacom.com |
| PELCO By Schneider Electric | 37 | 916245617 | www.pelco.com |
| PYRONIX | 15 | 917371655 | www.pyronix.com |
| RPAS FORMACIÓN | 70 | 931733230 | www.tsacenter.com |
| SAFIRE | 29 | 911836285 | www.safirecctv.com |
| SETELSA | 21 | 942544354 | www.setelsa.net |
| TECOSA | 35 | 915147500 | www.tecosa.es |

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


## ÍNDICE DE ANUNCIANTES

**Andrés Sanz Coronado**
Coronel Jefe del Servicio de Protección y Seguridad (SEPROSE) de la Guardia Civil

# *«La seguridad privada tiene un papel fundamental en la sociedad para reforzar y complementar a la seguridad pública»*

«Convivimos con los profesionales de la Seguridad Privada no como elementos del paisaje sino como auténticos actores en el ámbito de la seguridad con funciones propias y con un reconocimiento cada vez mayor», así lo asegura Andrés Sanz Coronado, Coronel Jefe del Servicio de Protección y Seguridad (SEPROSE) de la Guardia Civil, quien además subraya en esta entrevista como prioritario potenciar mecanismos de colaboración y coordinación entre ambas seguridades, así como la necesidad de trabajar en la concienciación sobre una «cultura de seguridad integral y vigilancia para la detección temprana de las ciberamenazas».

**Meses después de ratificarse su nombramiento como jefe del Servicio de Protección y Seguridad (SEPROSE) de la Guardia Civil –cargo que ocupaba previamente como responsable interino–, ¿sobre qué pilares y objetivos ha asentado su nueva andadura profesional?**

— Los pilares para crecer o para avanzar en el periodo inicial al frente del Servicio son los que encontré cuando me hice cargo: un equipo humano reducido, pero muy comprometido con la misión; unos programas de colaboración público-privada consolidados, aunque con enorme potencial de mejora y de crecimiento; y una buena predisposición de todos los interlocutores fundamentales en el sector de la Seguridad Privada para colaborar con la Guardia Civil en general y conmigo en particular. Esos son los mimbres de la cesta.

Hacia donde he puesto la proa es hacia una mayor labor de apoyo y dirección del SEPROSE sobre las actividades que las Unidades de la Guardia Civil realizan en el ámbito de la seguridad corporativa, en el ámbito de la seguridad de las empresas y en el ámbito de la protección de infraestructuras críticas. Nos hemos dado cuenta de que las iniciativas que adoptamos a nivel central y las relaciones que establecemos con asociaciones, empresas y otros interlocutores precisan de seguimiento, continuidad, engrasamiento y engrosamiento en otros niveles de organización territorial. Por ello dedicaremos un importante esfuerzo durante 2017 a optimizar nuestra gestión interna dentro de la Guardia Civil.

Por otra parte, debo decir que ya hemos tomado varias decisiones de cierta importancia para tratar de reordenar el espacio de prestación de los servicios que corresponden a los guardas rurales, pues no ha sido suficientemente respetado por los contratantes de servicios de seguridad, entre los cuales a menudo hay que incluir a órganos de diferentes administraciones públicas. En este sentido, entendemos que deberemos realizar sobre todo labores

de información y concienciación más que de denuncia, pues se trata de un problema generalizado.

En otro orden de cosas, durante el año próximo tendré que implicarme de forma muy personal en la coordinación del sistema de protección de infraestructuras críticas en el ámbito de la Guardia Civil en relación con los numerosos cometidos atribuidos al SEPROSE, puesto que la implantación del Sistema de Protección en su conjunto y a nivel nacional está avanzando de modo muy acelerado y constantemente creciente, mientras que los recursos humanos de mi Servicio están sufriendo el proceso contrario. Cada vez cuento con menos oficiales a causa de nuestros procedimientos de gestión interna de los recursos humanos.

Finalmente, también estamos dando pasos importantes para establecer programas de colaboración para colectivos del Sector que tenían encaje en los ya creados. Ya tenemos definidas las líneas maestras de su caracterización y contenido, pero falta todavía su aprobación por parte de nuestra Dirección General. Dado que estamos en un momento de relevo en la cúpula institucional, quizá tengamos que esperar un cierto tiempo antes de poder ponerlos en funcionamiento puesto que son ciertamente novedosos y ambiciosos.

**—Existe una clara apuesta de la Guardia Civil por la Seguridad Privada plasmada en el Plan General de Colaboración, desarrollada a través de los Programas Coopera y Plus Ultra, ¿cómo se potenciarán en los próximos años estos programas de colaboración?**

—Estos programas de colaboración creados en 2010 y 2013, respectivamente, establecieron en su momento el marco para que se pueda desarrollar una colaboración institucional y operativa de tipo genérico. Ahora, tras


haber acumulado una considerable experiencia sobre los campos en los que la Seguridad Privada precisa de un modo más concreto del apoyo y el respaldo de la Seguridad Pública, nos disponemos a ir abordando paso a paso el dar respuestas específicas a problemáticas concretas. Conscientes del papel que nos corresponde como el mayor cuerpo policial de España, debemos responder a las demandas que se nos han planteado desde el Sector en aspectos operativos concretos, a menudo estratégicos y casi siempre trascendentes y de solución compleja. Por ello, estamos preparando en este momento tres protocolos operativos que esperamos que en su momento puedan incorporarse como Addendas del Programa «Coopera» para desarrollar la colaboración en ámbitos específicos de actuación y de intercambio de información relevante para la seguridad.

**—Con una visión general, ¿qué valoración haría de la situación actual en la que se encuentra el sector de la Seguridad Privada?**

— Quisiera ser muy prudente al contestar a esta pregunta, pues la percepción que tiene el SEPROSE del Sector no deja de ser la de un espectador externo. Por mucho que queramos acercarnos a sus verdaderos actores e interactuar con ellos, no podemos perder de vista que no formamos parte del Sector en sí mismo, y que nuestra perspectiva para analizar su evolución es muy distinta de la que pueden tener las personas que viven de, por y para la Seguridad Privada.

Dicho lo anterior, entiendo que el Sector se encuentra en un momento de transición que los diversos colectivos que lo integran viven de un modo diferente. Posiblemente haya en este momento una considerable mezcla de ilusión, confianza o desconfianza -según de quién se trate- e incertidumbre por las expectativas que cada cual pueda haberse creado ante la salida de la crisis, en relación con los cambios en la cúpula del Ministerio del Interior y los que ha habido y los que habrá en las estructuras de las direcciones generales de la Policía y de la Guardia Civil, respecto a la obligación de desarrollar reglamentariamente la Ley de Seguridad Privada y, en los casos en que sea de aplicación, con motivo de la implan-

tación del sistema de protección de las infraestructuras críticas. Estos cuatro factores impactan de un modo distinto en empresas proveedoras o usuarias de seguridad privada, en los guardas rurales autónomos, en los detectives privados, en los centros de formación, etc. Sacaríamos la incertidumbre como el denominador común.

**—Años después de la aprobación de la Ley de Seguridad Privada, es pregunta obligada por el Reglamento de desarrollo,¿2017 será el año en el que finalmente saldrá el documento?**

— Ojalá fuera así, pero no soy optimista al respecto. Sin duda, el nuevo Equipo Ministerial precisará de un cierto tiempo para hacerse con los mandos del timón, para dominar los gajes del oficio, para conocer a fondo las diversas problemáticas y establecer prioridades, etc. No creo que sacar adelante esta compleja norma reglamentaria se encuentre entre tales prioridades durante los primeros meses de su mandato.

Por otra parte, si bien se ha avanzado mucho en la elaboración de diversos borradores del Reglamento, en la Guardia Civil consideramos que ninguno de los borradores que han sido sometidos a nuestro estudio e informe responde realmente a las expectativas abiertas por la Ley. Desde nuestro punto de vista, sigue habiendo excesivo control administrativo en esos textos –incluso abarcando nuevos ámbitos a controlar e inspeccionar–, en tanto que se ofrecen pocas herramientas al personal de seguridad privada para que sea más eficiente en su trabajo. Por otra parte, tampoco se ha desarrollado lo que debería constituir el núcleo fundamental para que verdaderamente pueda predicarse de la Seguridad Privada que es una extensión de la Seguridad Pública, y para convertir en realidad la integración funcional de los servicios: el efectivo control operativo por parte del cuerpo policial competente en razón de las competencias territoriales y materiales que establece la Ley Orgánica de Fuerzas y Cuerpos de Seguridad. No tiene mucho sentido que se perpetúe la confusión y mezcla entre control administrativo y control operativo. Por ello, creemos que es necesario llevar a cabo un cambio radical de enfoque en ciertos aspectos, lo cual será difícil sin una implicación a fondo de la Secretaría de Estado de Seguridad una vez que el nuevo Equipo se haya asentado bien.

**—Hace más de cinco años que entró en vigor la Ley 8/2011, de 28 de abril, por la que se establecían las medidas para la protección de la Infraestructuras Críticas, ¿qué papel está desempeñando la Guardia Civil, a través del Servicio de Protección y Seguridad (SEPROSE), a la hora de proteger este tipo de instalaciones?**

—El SEPROSE tiene atribuidas en las normas internas un papel esencial con relación a este asunto. De hecho, la Instrucción de nuestro Mando de Operaciones sobre «la implantación del Sistema de Protección de Infraestructuras Críticas en la Guardia Civil», dictada en desarrollo y aplicación de otra similar del Secretario de Estado de Seguridad, asigna al Servicio de Protección y Seguridad, como no podría ser de otra manera, una función general de coordinación de su implantación y de elaboración de las directrices técnicas necesarias para su mejor desarrollo, así como cometidos concretos en relación con la supervisión de los planes de protección específicos (PPE,s) de todas y cada una de las infraestructuras críticas asignadas a la Guardia Civil (el conjunto más grande cuantitativa y cualitativamente) y de todos y cada uno de los planes de apoyo operativo (PAO,s) previamente a su aprobación por nuestro Mando de Operaciones para su remisión al Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC).

Como se podrá colegir, se trata de una enorme responsabilidad y de un trabajo ingente. Para que se pueda entender mejor lo que significa el párrafo anterior, baste con tener en cuenta que a principios de 2016 revisamos y supervisamos uno a uno 86 PPE,s de los primeros cuatro sectores afectados (Eléctrico, Gas, Hidrocarburos y Financiero) antes de devolverlos a las Delegaciones del Gobierno correspondientes para que a su vez los enviaran al CNPIC. Y en el mes de diciembre de 2016 revisamos y aprobamos, uno a uno, los 86 PAO,s elaborados por las Comandancias de la Guardia Civil con relación a esas mismas infraestructuras críticas. Y dentro de poco comenzaremos con los PPE,s de otros nuevos sectores...

Para llevar a cabo adecuadamente lo anterior, hemos adoptado diversas medidas organizativas como reunir en Madrid a todos los Jefes de Operaciones de las Zonas (las Jefaturas a nivel de Comunidad Autónoma) para tratar sobre este asunto, y hemos elaborado un modelo de PAO específico de la Guardia Civil que incluye todos los contenidos mínimos ordenados por la Secretaría de Estado de Seguridad, pero va más allá para asegurar un planeamiento más completo y coherente. También, como es lógico, hemos visitado todo tipo de infraestructuras para conocer mejor sus peculiaridades y nos hemos reunido con diversos interlocutores sectoriales. No paramos de aprender y de trabajar, porque es lo que toca ahora.

**—¿Qué papel juega y aporta hoy en día la Seguridad Privada a la sociedad?**

—Es una obviedad que la Seguridad Privada ha sido integrada en el modelo de seguridad español mediante una

norma con rango de Ley. Por algo será. Nadie discute ya que empleados privados puedan desempeñar funciones cuasi públicas en lugares como los aeropuertos, los centros penitenciarios o en los accesos a Ministerios y edificios públicos. Esto es indicador fehaciente de la naturalidad con que propios y extraños, 46 millones de españoles y los pronosticados 74 millones de turistas, convivimos con los profesionales de la seguridad privada no como elementos del paisaje sino como auténticos actores en el ámbito de la seguridad con funciones propias y con un reconocimiento cada vez mayor.

Consecuentemente con lo expuesto, podemos hablar de un papel fundamental de la Seguridad Privada en nuestra sociedad para reforzar, suplir o complementar a la Seguridad Pública en lugares, eventos o funciones concretas, bien de modo temporal o bien con carácter permanente, de propia iniciativa o bajo el mando y coordinación de las Fuerzas y Cuerpos de Seguridad. Esto configura un marco de relaciones matricial entre empresas proveedoras de servicios, personal profesional prestador de los servicios, empresas y organismos usuarios de los servicios, unidades policiales competentes para el control administrativo, y cuerpos y unidades policiales competentes para proveer la Seguridad Pública. Un buen lío que, afortunadamente, resulta «transparente» para los ciudadanos. Lo que importa es que gracias a la Seguridad Privada nuestros ciudadanos y visitantes se sienten más cómodos y seguros, y las empresas y organismos que contratan sus servicios ven mejor asegurada la normalidad y continuidad en el desarrollo de sus negocios, actividades o funciones.

No quiero dejar de mencionar que la Seguridad Privada está asumiendo progresivamente un cierto papel vertebrador e integrador en el tejido


empresarial e institucional sin pretenderlo. Abstraigámonos del día a día, elevémonos para ver más allá de las reglas de organización interna de cada entidad, y examinemos en conjunto los trasvases de personal, conocimiento, técnicas, experiencias y contactos entre entidades. Al hacerlo, nos daremos cuenta de que la movilidad de un director de seguridad de una empresa a otra entidad que lo contrate después, la contratación de diversos proveedores de servicios por parte de una misma entidad usuaria (y algunas contratan incluso a nueve empresas privadas de seguridad al mismo tiempo...), la subcontratación de unas empresas por parte de otras, la subrogación de unos mismos escoltas, vigilantes de seguridad o guardas rurales por parte de sucesivas empresas, la concurrencia en foros, jornadas, reuniones y seminarios, etc., son factores que aportan cohesión al Sector, enriquecen a todos y fomentan el trasvase de conocimiento entre sectores, entre profesionales, etc. En este sentido es especialmente merecedor de una reflexión el hecho de que las empresas ya no sólo establecen relaciones entre sus niveles de alta dirección (Presidente-Presidente o Director General-Director General) o entre sus departamentos operativos, comerciales o de marketing, sino también entre sus departamentos de seguridad. Y puede resultar que entre dos empresas de ámbitos productivos o de servicios muy distanciados puede que no haya apenas relaciones salvo quizá entre sus directores de Seguridad...

**—Hoy en día el sector apuesta por la convergencia de la seguridad como concepto integral, ¿está preparado el sector para asumir este nuevo reto?**

—Honestamente, creo que aún es pronto. Si fuera de otro modo, ni «Cuadernos de Seguridad» me habría formulado esta pregunta, ni proliferarían tanto las reuniones, convenciones, congresos, jornadas, seminarios, simposios y conferencias en que tratar sobre este asunto. Está de moda porque no deja de ser una asignatura pendiente.

Para alcanzar esa ansiada visión integral sobre riesgos, amenazas y obligaciones de cumplimiento e integradora de las di-

versas medidas organizativas, técnicas, normativas y materiales adoptadas para prevenirlas o hacerles frente, y así garantizar no sólo la protección y seguridad de personas y bienes sino también la resiliencia y la continuidad de la actividad o del negocio, aún falta mucho.

Posiblemente habrá que superar personalismos de directores de diverso perfil en algunos casos, convencer a altos directivos en otros, vencer resistencias de los departamentos financieros, legales o de prevención de riesgos laborales en ocasiones, complementar y reforzar la formación de casi todos los empleados de los departamentos afectados, etc. Y con toda seguridad será necesaria e imprescindible una actitud proactiva, generosidad, altura de miras e imaginación para poder ir dando los pasos de modo ordenado y seguro, sin provocar traumas ni desmotivar a nadie. Desde luego, habrá que dar tiempo al tiempo pues cada entidad tiene su propio ritmo y no parece razonable imponerle un cambio de estructura organizativa a una empresa para mejorar su seguridad en contra de los propios intereses y de la cultura de esa entidad, so pena de caer en un nuevo estilo de despotismo ilustrado. Si en algo será precisa mesura, proporcionalidad, racionalidad, prudencia al exigir el cumplimiento de la dura lex, sed lex, será en el tránsito desde las diversas situaciones de partida actuales hacia los diversos modelos posibles de seguridad integral.

**—El sector se desarrolla a la par que la sociedad en el ámbito de un nuevo mundo globalizado que tiene que hacer frente a nuevos riesgos y amenazas –ciberamenazas–. ¿Están preparadas empresas y profesionales del sector de la Seguridad ante estas nuevas amenazas?**

—Vaya... otra pregunta que podría responder casi con los mismos argumentos empleados para dar contestación a la anterior. ¿Quién está realmente preparado para hacer frente a las ciberamenazas? Ni siquiera lo están los Estados, y por ello se ha generalizado entre los países de la OTAN la creación de Mandos Conjuntos de Ciberdefensa, pues la red se ha configurado como un vector de ataque a la seguridad de los Estados... Es de pura lógica pensar que toda preparación por parte de los órganos de la Administración civil o de las empresas será siempre insuficiente. Pero no por ello hay que dejar de prepararse: todo lo contrario. Si bien la seguridad total no existe y menos aún frente a este tipo de amenazas, hay muchas cosas que se pueden hacer y muchas de ellas resultarán efectivas para prevenir o impedir ataques masivos indiscriminados, para reducir las posibilidades de que un empleado dañe consciente o inconscientemente los sistemas de la entidad, para minimizar las posibilidades de sufrir espionaje industrial, para asegurar la continuidad de la actividad mediante la implantación de plataformas redundantes, sistemas de respaldo, copias de seguridad de las aplicaciones y los datos, etc.

Por encima de todo, creemos que al final el mayor riesgo procede del error humano o de la maldad puntual del empleado desleal. Consecuentemente, con independencia de que toda inversión en sistemas y productos carísimos y buenísimos contribuirá a mejorar la seguridad corporativa, consideramos que es imprescindible trabajar en dos líneas con relación a los empleados y trabajadores: concienciación sobre una cultura de seguridad integral y... vigilancia para la detección temprana de posibles riesgos.

**—¿Qué elementos deben confluir para conseguir una adecuada coordinación y colaboración entre el sector público y privado?**

—Voluntad, buena voluntad, querer colaborar, dejarse coordinar, saber coordinar, saber colaborar. Como siempre, esto es cuestión de saber y querer. Si sólo concurre uno de los dos requisitos, la cosa fallará. Por eso todos conocemos casos de personas y entidades que hablan de coordinación y de colaboración, pero luego no logran materializarlo porque les pierde su ego, o porque anteponen siempre sus propios intereses personales o los intereses o la visión corporativa por delante de cualquier otra consideración.

Es que la colaboración sólo es posible desde la generosidad –difícilmente por vía de la mera imposición– y la coordinación nunca es espontánea, sino resultado de una buena planificación, de un correcto análisis metodológico de la situación de partida, del problema a resolver y de los medios y capacidades disponibles para afrontar la tarea, y de una clara asignación de cometidos, funciones y responsabilidades. Hay que saber: saber coordinar y saber dejarse coordinar. Y no quiero ir mucho más allá en este momento. Simplemente apunto que no basta con que la Ley establezca que dos personas, dos autoridades, dos cuerpos policiales o dos entidades de cualquier tipo deben colaborar y coordinarse para que eso se convierta en realidad. Por ello, en la parte que me afecta, me marco como objetivo no tanto cambiar a otras entidades (por ejemplo las empresas y los profesionales de la Seguridad Privada) para exigirles colaboración o para imponerles una coordinación cuanto mejorar la mentalización y las capacidades de las Unidades de la Guardia Civil, para propiciar una efectiva mejora de la colaboración y para que sepan llevar a cabo esa coordinación cuando sea necesaria. ●

*Texto y Fotos: Gemma G. Juanes*

# Detector Volumétrico de Exteriores de Triple Tecnología y Anti-masking

Pyronix
HIKVISION




# XDH10TT-AM

## Características

- Alcance 10m
- Tres frecuencias de microondas para anti-colisión
- Triple lógica de detección
- Triple tecnología de anti-masking
- Incluye lentes adicionales
- Fácil ajuste
- Tamper de tapa y de pared
- RFL para salidas de alarma, tamper y anti-masking
- Compensación digital de temperatura
- Regulación de alcance de microondas y anti-masking

Para recibir más información, regístrese aquí

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

# Security Forum 2017, un espacio para el desarrollo y la innovación

## Bajo el lema «Ver para Crear», el Congreso Security Forum se desglosará en dos sesiones diferenciadas: Global Day y Ciber Day

Inmersos ya en 2017 la quinta edición de Security Forum sigue avanzando en su organización. Las empresas continúan reservando su espacio en el área de exposición, los Premios Security Forum siguen recibiendo trabajos, y el área de conferencias, desglosado en dos sesiones diferenciadas : Global Day y Ciber Day, va gestando sus contenidos. Consolidado ya como un espacio de networking, esta nueva edición sigue apostando por la innovación y nuevos valores empresariales en el sector de la Seguridad.

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

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

### Global Day y Ciber Day

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

•Global Day: la primera jornada estará dedicada a la seguridad global. Los asistentes podrán descubrir desde una visión multidisciplinar aspectos y temáticas de gran interés como es la «Comunicación no verbal y análisis de conductas sospechosas como herramienta para el director de Seguridad» o «Realidad Virtual aplicada a Seguridad».

•Ciber Day: la segunda jornada se centrará en la ciberseguridad. Temas como «La coordinación estatal ante la Directiva NIS», o «Ponga un CISO en su empresa», centrarán el debate de esta edición.

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

### Ficha técnica

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

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

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

**Periodicidad:** Anual.

**Carácter:** Exclusivamente profesional.

**Organiza:** Peldaño.

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

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

DS-7600NI-E1/A
MONITOR CON NVR INTEGRADO

# ALL-IN-ONE
## SENCILLEZ Y VERSATILIDAD

Hikvision DS-7600NI-E1/A/1T All-in-One le proporciona la mejor manera de configurar un sistema de videovigilancia en red. Basta con conectar las cámaras IP para comenzar la grabación. Además de todas las caracteristicas ya existentes en los NVR de Hikvision, el NVR All-in-One se combina con un monitor de 22 pulgadas para videovigilancia. Funciona como grabador, pantalla y se conecta a otros dispositivos para crear un entorno de videovigilancia completo. De este modo se reduce significativamente el coste y el tiempo total de gestión, haciéndolo ideal para pequeños y medianos negocios como tiendas, hogares y oficinas ya que no requiere de avanzados conocimientos técnicos para su instalación.

- Todo en uno: Monitor de 22" con NVR de 8 canales integrado
- Capacidad de visualizar contenido de Vídeo / Audio
- Full HD con fines publicitarios - (Vía USB)
- Entrada HDMI/VGA adicional para fuentes externas y salida VGA
- Soporta hasta 8 cámaras IP
- Incluye 1 HDD 2.5" WD de 1TB preinstalado
- Soporta cámaras ONVIF

Hikvision Spain
Almazara 9
28760 Tres Cantos (Madrid)
T +34 917 371 655
info.es@hikvision.com

**ÁNGEL CÓRDOBA.** PRESIDENTE DE LA ASOCIACIÓN PROFESIONAL DE COMPAÑÍAS PRIVADAS DE SERVICIOS DE SEGURIDAD. APROSER

# Un sector ante **urgentes retos**

**El sector de la Seguridad Privada se enfrentará a nuevos retos, alguno de ellos fruto de las incertidumbres actuales**

EL sector de la Seguridad Privada se enfrentará a nuevos retos, alguno de ellos fruto de las incertidumbres actuales. Sin olvidar los retos presentes, aquellos que ocupan y condicionan nuestro día a día, hacer una valoración de lo que nos deparará 2017 obliga a hacer un pequeño parón y a echar la mirada atrás.

En esta reflexión sobre lo acontecido en 2016 para así centrar la vista en los retos de futuro, observamos un periodo marcado por distintos avances y retrocesos. En cuanto a los progresos, algunos discretos y otros más patentes, se identifica en primer lugar la adopción, por parte de diversas Comunidades Autónomas y Administraciones Locales, de diversas iniciativas relativas a la exigencia de aplicación del convenio colectivo como criterio de ejecución o como criterio de valoración en la adjudicación. Estas iniciativas se encuadran en una reflexión más amplia, relacionada con la inclusión de cláusulas sociales en la contratación pública, en la línea de lo que disponen las nuevas directivas europeas.

Otro paso adelante para la industria ha sido la sentencia dictada por el Tribunal Supremo sobre asunción de deuda salarial en las subrogaciones de contratos. La Sala de lo Social del Tribunal Supremo ha establecido en esta resolución la exoneración de responsabilidad a la empresa cesionaria frente a las deudas contraídas por la compañía cedente. Es decir, las empresas de seguridad privada que consigan un contrato prestado anteriormente por otra no tendrán que asumir las deudas salariales contraídas por esta última en caso de subrogación. Que esta interpretación se extienda al ámbito de la responsabilidad por impagos a la seguridad social, es capital para una clara determinación de los riesgos empresariales.

No podemos tampoco olvidar cómo, frente a la interpretación del Ministerio de Empleo y otras organizaciones empresariales, la Audiencia Nacional ha validado la modificación parcial del convenio colectivo de empresas de seguridad adoptada a finales de 2015. Dicha publicación implica la aplicación de una cláusula de penalidad del 50%, como consecuencia de un eventual impago de las tablas salariales del año 2016. También ratifica que, en los procesos de subrogación, el convenio sectorial prevalece temporalmente sobre un convenio de empresa que estuviese en vigor en la nueva adjudicataria de un contrato, hasta que esa empresa cesionaria no firme un nuevo convenio de empresa o el convenio secto-

rial pierda su vigencia, algo en absoluto baladí para nuestro sector. La no prioridad aplicativa de un Convenio Colectivo de ámbito inferior a la empresa frente al Convenio Colectivo sectorial es, sin duda, otra relevante resolución judicial para el sector.

Pero, al igual que se identifican los avances acontecidos, también se perciben los retos aún latentes propios del sector. Concretamente, y centrándonos en las tres prioridades que le afectan directamente, es menester apuntar muy especialmente a la necesidad de generar empleo de calidad, donde hay que reformular parcialmente el Estatuto de Trabajadores, modificando –por lo menos para los sectores intensivos de mano de obra como es el caso de la Seguridad Privada– la normativa actual relativa a los descuelgues salariales o la prioridad aplicativa de los convenios de empresa.

Otra prioridad, es la reformulación del papel de la Administración, de la que se esperan dos medidas urgentes; de un lado, que dote al sector de una seguridad jurídica que potencie las decisiones de inversión en el mismo, evitando inesperados Decretos Ley o facilitando la entrada en vigor del todavía pendiente desarrollo reglamentario de la Ley de Seguridad Privada.

Y como tercera necesidad, resulta esencial la trasposición de la nueva directiva europea de contratación pública. Las posibilidades abiertas por este instrumento comunitario deben ser incorporadas a la normativa nacional de contratación pública, concretamente la adjudicación de contratos que consideren también los criterios cualitativos y no exclusivamente el precio ofertado, entre otras medidas.

Somos una industria y por ello no debemos ni podemos obviar el contexto económico en que nos encontramos; un contexto determinado por la no resolución de estas prioridades enumeradas con anterioridad. Porque, aunque los resultados del balance económico 2015 del sector de la Seguridad Privada, presentado por APROSER en el mes de julio del pasado año, indican que hay una leve mejora en la industria materializada en un incremento del 2,87% en términos interanuales, el sector dista de haberse recuperado del enorme bache sufrido en los últimos años. Seguimos creciendo por debajo del conjunto de la economía y sigue avanzando la contracción de los márgenes comerciales. Y, lo que es más preocupante, las previsiones de cierre para 2016 pueden seguir viniendo marcadas por las diversas incertidumbres del entorno nacional e internacional.

Nos encontramos, en definitiva, frente a muy diversos retos. Retos urgentes cuya resolución es imprescindible para garantizar la sostenibilidad del sector a corto plazo. En ello confiamos.

Fotos: *Archivo*

**PALOMA VELASCO.** DIRECTORA EJECUTIVA DE LA ASOCIACIÓN ESPAÑOLA DE EMPRESAS DE SEGURIDAD. AES

# Un mercado dinámico, eficaz y abierto

UN año más, Cuadernos de Seguridad, y en concreto su redactora jefe, Gemma G. Juanes, me ha pedido la colaboración de AES en un artículo que defina los retos del sector, a los que nos referimos nosotros como industria, ante 2017.

Nuestra asociación, como la asociación de fabricantes, instaladores, mantenedores, centrales receptoras de alarma, laboratorios y proveedores de servicios para sistemas electrónicos de seguridad física y electrónica, apoya los objetivos de España y por ende de la Comisión Europea, participando activamente en las dos asociaciones sectoriales europeas de la industria, Euralarm y Eurosafe.

Ello nos lleva a secundar el objetivo del Gobierno español y de la Comisión de Fomento del Empleo, del Crecimiento y la Inversión. Estamos convencidos de que en el adecuado marco político, legislativo y regulador, nuestra industria puede desempeñar un papel importante en la consecución de dichos objetivos.

Por otro lado, apoyamos decididamente el fortalecimiento y profundización de un mercado europeo único –que comprenda las áreas de políticas y servicios digitales–, y perseguimos el crecimiento del tejido industrial español y europeo. Una prioridad clave de nuestra industria es un enfoque más eficaz de la normalización para asegurar un mercado único equitativo.

La Unión Europea necesita desarrollar y mantener acuerdos comerciales justos y equilibrados con la Asociación Europea del Libre Comercio, así como con otros países y regiones, consolidando su posición como piedra angular de la economía global.

## AES, un socio comprometido y constructivo

En todos estos objetivos, durante 2017, AES será un socio comprometido y constructivo, ayudando a las instituciones españolas y europeas a diseñar las políticas, leyes y disposiciones adecuadas que converjan en los mismos y que den forma a un mercado dinámico, eficaz y abierto.

Nos proponemos pues comunicar y sensibilizar a las instituciones españolas y europeas de la importancia e impacto del mercado español y de la seguridad física y electrónica, así como

las tendencias en mercados secundarios, a la hora de la implementación y desarrollo de sus políticas.

No olvidamos los desafíos actuales de la industria, como la protección de las infraestructuras críticas, en la que es fundamental la cooperación público-privada entre las empresas y las distintas administraciones públicas, de quien depende el correcto funcionamiento de dichas infraestructuras que gestionan los servicios esenciales de los ciudadanos.

Pero además ponemos la vista en los desafíos futuros, las telecomunicaciones, la transformación digital, el internet de las cosas, la industria 4.0, el big data, las ciudades inteligentes o la nube…

Cada vez es mayor la aplicación del internet de las cosas a las centrales receptoras de alarma, por ejemplo, y a los centros de control, por lo que tanto las unas como los otros tendrán que adecuarse y deberán actualizar sus sistemas de gestión a estas nuevas tecnologías.

Una de las mega tendencias mundiales es la urbanización y por ello las ciudades tendrán que ser más sostenibles e inteligentes, aplicando la tecnología a la ciudad y sus ciudadanos. Para ello es fundamental tener una plataforma que permita conectar todo.

## Ciudades inteligentes

Las iniciativas para ciudades inteligentes, y para las españolas en concreto, es un paso al que damos la bienvenida como necesario para asegurar que las nuevas tecnologías desempeñen su papel en el desarrollo de los entornos urbanos.

> «Apoyamos decididamente el fortalecimiento y profundización de un mercado europeo único y perseguimos el crecimiento del tejido industrial español y europeo»

No obstante, la iniciativa de nuestro Gobierno y de la Comisión Europea de 2011 debe ampliar su campo de aplicación, desde el transporte y la energía hasta otros ámbitos de la vida en áreas urbanas, incluida la seguridad física y electrónica.

AES busca sensibilizar sobre los aspectos de protección y seguridad de las Ciudades Inteligentes, y asegurarse de que aquellos desempeñan su papel en actividades futuras. Entre otras se incluyen un eficaz sistema de alarma y respuesta para emergencia pública, que pueda alertar a la población más allá de fronteras y asegurar que la respuesta ante los desastres naturales pueda ser la más eficaz posible.

En este sentido hemos escrito el Manifiesto AES 2016 a 2019, para una España y una Europa más seguras y protegidas, que presentamos en la Asamblea General de la Asociación, el 29 de noviembre, en la que celebramos también el 35 aniversario de AES, y que posteriormente haremos llegar a toda la industria, así como a las instituciones españolas y europeas, tanto públicas como privadas, para dar a conocer nuestra hoja de ruta para los próximos años.

Nos ponemos a ello, que como dijo Ralph Waldo Emerson, los retos hacen que la vida sea interesante. Superarlos es lo que hace que la vida tenga sentido. ●

Fotos: AES/Pixabay

**ANNA AISA BIARNÉS.** GERENTE DE LA ASOCIACIÓN CATALANA DE EMPRESAS DE SEGURIDAD. ACAES

# Seguridad Pública & Seguridad Privada, un **diálogo cada vez más fluido y constante**

HACE ahora aproximadamente un año reflexionábamos sobre la necesidad de la publicación del Reglamento de Seguridad Privada en desarrollo de la ya no tan reciente Ley de Seguridad Privada.

La atípica situación política que hemos vivido para nada ha ayudado a dicho desarrollo reglamentario. Y nos encontramos con que finalizamos este 2016 sin novedad legislativa al respecto, con una Ley que recogió muchas de las pretensiones del sector, que tiene multitud de remisiones, tanto expresas como implícitas, al futuro Reglamento, y que no han visto su concreción reglamentaria. Las circunstancias acaecidas han comportado la perpetuación, por el momento, de una situación un tanto contradictoria: aplicar una Ley de 2014 y un Reglamento de 1994. Esto es, veinte años separan a dichas normas, todo un universo si tenemos en cuenta la evolución que ha experimentado la tecnología en estos últimos años, y la integración de las «diferentes seguridades» (desde un punto de vista tradicional de las mismas) dentro del concepto de la seguridad integral, que además es la que ha de regir a la hora de interpretar las actividades, los servicios y las funciones contempladas en la Ley.

Finalmente tenemos Gobierno y en este sentido esperamos y pedimos que el nuevo Reglamento sea una de las prioridades del nuevo Ministro de Interior, que sin prisa pero sin pausa, ponga al órgano competente a trabajar para poder tener un proyecto sobre el que poder hacer las aportaciones correspondientes. Y que, recordemos, ya fueron elaboradas por el sector de la Seguridad Privada y presentadas al Ministerio el pasado mes de noviembre de 2014.

Por consiguiente, uno de los retos que esperamos ya se cumpla este año, es la tramitación del nuevo Reglamento de Seguridad Privada. El Ministerio, a pesar del cambio de titular habido, debe ser consciente del trabajo ya realizado por el sector desde la publicación de la Ley de Seguridad Privada hasta ahora, y tenerlo en cuenta a la hora de recogerlo en el que será el futuro Reglamento.

Con la publicación del Reglamento, seguramente se disiparan algunas de las dudas que surgen respecto a determinadas previsiones normativas, como la vigilancia en espacios públicos, la subcontratación, la videovigilancia, los requisitos para que se dé la protección de agente de la autoridad, y un etcéte-

ra un tanto extenso, que está pendiente de las previsiones que se contengan a nivel reglamentario.

Como ya hemos indicado, han pasado dos años desde la Ley de Seguridad Privada y en estos dos años la tecnología ha ido avanzando, las tendencias delincuenciales se han modificado, las necesidades de seguridad han variado, nuevos conceptos han sido incorporados a la seguridad integral, y todo ello, que quizás no quedó recogido en su momento en las propuestas presentadas al Ministerio, deberá ser tenido en cuenta a la hora de plasmar el desarrollo reglamentario requerido.

Por otra parte, algunos aspectos que deberá recoger el nuevo Reglamento son de gran importancia para el sector en sus relaciones con la Administración Pública. Desde el Observatorio de Seguridad Privada, la contratación pública es uno de los aspectos en los que se está trabajando de forma constante y contundente. A nivel de Cataluña, durante 2017 seguiremos trabajando, desde el Comité de Seguimiento, por una contratación pública que respete el convenio colectivo, que sea socialmente responsable, que no impida el acceso de las Pymes a la contratación, que no opte por subastas encubiertas donde sólo prime el precio del servicio, y donde, en definitiva, sólo tengan juego las empresas que cumplen con sus obligaciones y apuestan por una contratación responsable y de calidad.

El trabajo que desde ACAES estamos realizando en la contratación pública a nivel de ámbito autonómico, vamos a extenderlo también al ámbito municipal, para lo que estamos colaborando con el Sindico de Cataluña, con el Ayuntamiento de Barcelona y la Diputación de Barcelona, principalmente, aunque también trabajamos con otros Ayuntamientos, en aras a conseguir una contratación que respete la normativa (general y sectorial), y que tenga en cuenta la oferta económicamente más

ventajosa, entendida ésta como la que guarde la correcta proporción entre precio y calidad del servicio.

Ello requiere de un esfuerzo importante por parte de la asociación, pero es una de nuestras apuestas para el próximo año, en el que esperamos se consigan avances relevantes en este sentido, que acaben beneficiando al sector en general.

Y como bien dice el refrán, contra el vicio de pedir está la virtud de no dar, aprovechamos la ocasión que nos brinda Cuadernos de Seguridad para pedirle al nuevo Gobierno, que no olvide la asignatura que tiene pendiente relativa a la Ley contra la Morosidad. Como miembros de la Plataforma Multisectorial contra la Morosidad (PMcM), estuvimos presentes en el mes de octubre en el acto que tuvo lugar en el Congreso de los Diputados el año pasado, y en el que todos los grupos parlamentarios se comprometieron a elaborar un régimen sancionador para los incumplimientos de los plazos de pago legalmente establecidos. Esperamos que dicho régimen sancionador llegue y que no quede en una mera promesa sin más. Su publicación y entrada en vigor es necesaria, más aún en momentos como los actuales en los que la falta de liquidez acucia a las empresas.

Y por último, no quiero finalizar sin mencionar la relación público-privada que celebramos cada vez se está llevando a cabo en el ámbito de la colaboración. Las Fuerzas y Cuerpos de Seguridad están apostando, todavía más si cabe, por un diálogo más fluido, constante e intenso con el sector de la Seguridad Privada. Cada vez son más constantes las jornadas informativas que organizan y a las que invitan a los representantes del sector. Jornadas en las que la información facilitada es de gran relevancia para los profesionales asistentes, donde se intercambian conocimientos, experiencias, inquietudes y donde, entre todos, se consigue la consolidación de la confianza mutua entre Seguridad Pública y Seguridad Privada, que en definitiva trabajan ambas en aras a la seguridad ciudadana. ●

Fotos: *Archivo/Freepik*

**LUIS GONZÁLEZ HIDALGO.** SECRETARIO GENERAL DE LA FEDERACIÓN EMPRESARIAL ESPAÑOLA DE SEGURIDAD. FES

# Un futuro con **nuevas expectativas**

COMENZANDO el año 2017, la mayor preocupación actual de las empresas sigue siendo la crisis económica. Y a esta problemática, se le añaden otras como la incertidumbre normativa, pues aunque tras la publicación de la Ley de Seguridad Privada, el sector ha avanzado un poco más y ha permitido ofrecer una seguridad jurídica que en muchos aspectos carecía la anterior Ley, queda todavía otro camino por recorrer, que es su desarrollo reglamentario. El sector espera con cierta inquietud que el Reglamento de Seguridad Privada salga a la luz, pues muchas de las principales novedades que recoge la Ley, son de difícil aplicación hasta que no sean desarrolladas, y con el Reglamento vigente se ha producido un periodo transitorio que genera incertidumbre.

También, tras la composición del nuevo Gobierno, nos encontramos con la posibilidad de que se produzcan a lo largo de este primer año de legislatura, algunos cambios normativos desde el punto de vista laboral, fiscal, etc., que pueden afectar al tejido empresarial español en general. Por lo que es necesario que los empresarios cuenten con esta importante premisa.

A parte de estos aspectos normativos, cabe destacar otros a los que las empresas de seguridad deben afrontar, como las infraestructuras críticas y la ciberseguridad. Esta última, es un mecanismo de prevención y reacción frente a los riesgos y amenazas que pueden impactar en cualquiera de los recursos y activos del Estado, desde el ámbito de los sistemas y las redes de información como el ciberterrorismo o los ataques a servicios esenciales como las infraestructuras críticas. La excesiva dependencia de la sociedad respecto a las nuevas tecnologías, internet, móviles, etc., puede ser una fuente de colapsos del propio ciberespacio, de sistemas financieros, de servicios públicos, etc. Por ello, la ciberseguridad es una dimensión en la que la seguridad del Estado debe también concentrar sus esfuerzos, y en concreto las empresas de seguridad.

En definitiva, el sector debe seguir apostando por las nuevas tecnologías, que en muchas ocasiones sustituyen a la seguridad física. Por ejemplo en las CRA´s, que es una actividad que está revolucionando el sector y que todavía queda mucho terreno por recorrer.

También, no hay que olvidar que ha aumentado la demanda de ciertos servicios de vigilancia en centros comerciales, urbanizaciones, hospitales y lugares de internamiento, aunque la actividad de vigilancia sigue en tendencia negativa, con una competencia desleal de precios a la baja, con la amenaza del intrusismo, y con la impugnación de ciertos concursos.

Desde FES esperamos que el futuro incierto se convierta en un futuro con unas nuevas expectativas, que permitan mejorar la imagen del sector y que las pequeñas y medianas empresas de seguridad vean una luz en el horizonte. ●

Fotos: *Freepik/Archivo.*

VPS
PROTECT MANAGE MONITOR

# PROTEGE EL PATRIMONIO DE TUS CLIENTES Y SU ENTORNO

- **Coste directo por okupación:**
  **25.000€.** Por no alquilar o vender el inmueble, por reformas, por gastos legales.

- **Coste social por okupación:**
  Problemas de convivencia vecinal, vandalismo, efecto llamada para okupas, efecto expulsión para vecinos.

## SOLUCIÓN: PUERTAS ANTIOKUPA VPS

- **Reduzca el riesgo de intrusión.**
- **Reduzca el deterioro del inmueble.**
- **Evite problemas vecinales.**



**Protegemos lo que es tuyo**

Para más información:
spain@vpsitex.es

**JUAN MUÑOZ.** CPP CSMP CSYP. PRESIDENTE DE ASIS ESPAÑA

# 2017: AC-DC

EL contenido de esta columna no tiene nada que ver con lo que un lector potencial haya podido interpretar con la lectura del titular a primera vista. En este contexto, con el acrónimo AC-DC me refiero a un firme deseo para 2017: menos AC, autocomplacencia y autosuficiencia; y más Deber de Cuidado (DC) o Deber de Protección, en Inglés Duty of Care.

El diccionario de la RAE define autocomplacencia como «la satisfacción por los propios actos o por la propia condición o manera de ser», y la autosuficiencia como «estado o condición de quien se basta a sí mismo». Con ambas estamos familiarizados por muy diferentes razones. Por su parte, el Duty of Care es la doctrina –de adopción internacional– que determina que las empresas son responsables legales, fiduciarias y morales de la Seguridad de sus empleados, independientemente de donde se encuentren estos, lo que adquiere una dimensión muy especial cuando hablamos de expatriados y viajeros frecuentes, que operan en países con entornos bajo las circunstancias VUCA: alta volatilidad, elevada incertidumbre y complejidad, y ambigüedad. Y lo hace desde la perspectiva de las diferentes legislaciones de los países occidentales, pero también desde la perspectiva de la jurisprudencia o Common Law internacional. Este concepto de Seguridad engloba tanto el Safety (los que entendemos como Prevención o PRL) como el Security (lo que entendemos como Seguridad), que en el entorno internacional están profundamente interrelacionadas.

Es público que una parte crítica de los ingresos de las empresas del Ibex35 procede del exterior –cerca de un 60% de media– y que estos han sido claves para la actual situación económica española, que parece se encuentra en mejor estado que algunas de sus homólogas europeas. Pero esta no es una característica exclusiva. Algunos centenares de empresas más pequeñas están en una situación similar o todavía aún más dependiente con el componente internacional como único motor de su existencia. Por ejemplo, con el 80% de sus ingresos procedentes del exterior, en algún caso con decenas de trabajadores expatriados y centenares de viajes internacionales cada año, liderando proyectos millonarios pero sin un mínimo modelo de seguridad formal a pesar de operar en países con entornos complejos como Arabia Saudí, Bangladesh, Brasil, Filipinas y otros.

Y esta exposición no va a reducirse; todo lo contrario. Están en marcha

o próximos a su lanzamiento algunos proyectos internacionales de grandes dimensiones en los cuales se espera que estén presentes las empresas españolas. Por ejemplo, la construcción del nuevo aeropuerto de Ciudad de México, con un presupuesto cercano a los 10 mil millones de euros o varias obras de infraestructura en otros países de LATAM o de la Región MENA (Norte de África y Oriente Medio), donde se habla de proyectos potenciales por casi 350 mil millones. Según el informe «Talent Mobility 2020 and Beyond», publicado por la consultora Price Waterhouse and Cooper en 2010, para ese año se espera un incremento del 50% en el número de los expatriados que trabajan fuera de sus países de origen: en toda la década anterior lo habían hecho un 25%. Si se estiman en más de dos millones los españoles que viven y trabajan en el exterior, según fuentes oficiales, ¿como afectará el informe de PWC, si está más o menos acertado, a nuestro país? ¿Cómo están gestionando este escenario?

«Las empresas españolas deberían disponer de consistentes estrategias de seguridad en viaje y expatriación que sean ágiles, adaptables y en constante evolución»

## Empresas españolas

Resulta evidente que en base a lo anterior las empresas españolas deberían disponer de consistentes estrategias de seguridad en viaje y expatriación que sean agiles, adaptables y en constante evolución para satisfacer las necesidades de su fuerza laboral y también para limitar las posibles responsabilidades penales de sus administradores por negligencia y los posibles efectos en la reputación de las organizaciones. En este sentido es importante considerar las recientes noticias sobre el caso de un embajador español y una investigación iniciada por la AN en relación con un grave incidente con el resultado de dos muertes. Es cierto que las estrategias y las medidas de seguridad deben ser proporcionales al tamaño y los recursos de cada organización, pero las empresas españolas tienen que entender de una vez por todas que las operaciones internacionales requieren un coste del riesgo más elevado en seguros (transferencia del riesgo), seguridad (control del riesgo) y otras áreas. Al mismo tiempo que aceptan lo bueno (el incremento de ingresos y del beneficio derivado) deben hacerlo también con los costes adicionales agregados.

El Deber de Protección no es un evento sino un proceso continuo que requiere el respaldo del máximo nivel de las organizaciones para su implementación y desarrollo, y la asignación de los recursos necesarios, financieros, humanos y organizativos. Y su implementación –aunque mejorando– está alejada de lo que debería en relación con el tamaño de las operaciones internacionales de las empresas españolas si lo comparamos con otros países próximos. Pero de todos los riesgos a los que se enfrentan estas (terrorismo, crimen organizado, pandemias, desastres naturales, accidentes de tráfico, incidencias sanitarias, etc.), el mayor es en realidad el desconocimiento y la autosuficiencia.

Donald Rumsfeld, secretario de defensa de EEUU entre 1975 y 1977 y entre 2001 y 2006, definió muy bien los tipos de riesgos y su planteamiento ha sido adoptado internacionalmente. Drew Zavastsky en su artículo «La autosuficiencia, el mayor de los riesgos», publicado en 2016 por la revista RIMS, los resume y complementa desde una perspectiva

muy interesante. Para él existen cuatro tipos de riesgos: los sabidos y conocidos, que algunos prefieren ignorar; los sabidos pero desconocidos en su alcance y consecuencias; los desconocidos pero sabidos, porque sí existen datos sobre sus posibles consecuencias; y los ni sabidos ni conocidos, los más peligrosos de todos. Pero Zavatsky opina además que el mayor de los riesgos es la autosuficiencia, que desafortunadamente es muy común entre los humanos, y define esta «como la autosatisfacción acompañada del desconocimiento de los verdaderos peligros y deficiencias».

## Deber de Protección

Sólo poco más de tres años después de su ocurrencia, el incidente de In Amenas, que marcó un supuesto punto de inflexión para el Deber de Protección, es para la mayoría un caso aislado a pesar que más recientemente se hayan producido incidentes similares, aunque de dimensiones inferiores, por ejemplo, en Bangladesh cuando hace sólo unos meses un grupo de terroristas locales tomó un restaurante frecuentado por extranjeros y tras el asalto de las Fuerzas de Seguridad el balance resultó trágico: 29 muertos incluidos 24 rehenes de diferentes países. Para muchos analistas el modelo de acción-reacción no funciona. La situación de seguridad en México era la misma antes y después del terrible incidente que le costó recientemente la vida a una ciudadana española. Para el consenso de los analistas nada ha cambiado, sólo que algunas circunstancias determinadas se conjugaron y llevaron a ese fatal desenlace. El país estaba y está igual en términos de nivel de riesgo, pero sin embargo muchas organizaciones han elevado sus medidas de protección anteriores. ¿Qué criterios han seguido para hacerlo, aparte del componente psicológico? ¿Qué indicadores esperan para revisar estas medidas adicionales y retornar a la situación de partida?

En 35 años de práctica profesional he visto muchas cosas sorprendentes, pero en estos últimos quince, más concentrado en la seguridad internacional, he visto y veo cada día algunas que me cuesta comprender dada la dimensión de los riesgos y las posibles consecuencias de su materialización. No estamos hablando de desconocimiento sino de irresponsabilidad. Pero además, entre la esperanza de ver cómo algunas empresas y profesionales están haciendo bien sus deberes, no sin un gran esfuerzo y pueden ser utilizadas como modelo de referencia, se aprecia todavía mucha autosuficiencia y hay todavía muchas empresas que no están dispuestas a tomar siquiera las medidas más elementales de diligencia debida y hacerlo de una forma profesional. Sabemos que el desconocimiento no es un eximente para el cumplimiento de la ley, pero la no actuación u omisión después de conocer y haber sido informado de los potenciales riesgos y de las medidas necesarias tiene una clasificación diáfana. Hablamos de riesgos previsibles y de medidas razonables. Los riesgos que no se tratan tienen un muy grande y desconocido componente residual extremadamente difícil de manejar en un entorno de escenario de incertidumbre como el actual.

Por todo lo anterior espero que 2017 sea un año determinante para la consolidación del Deber de Protección como un componente básico de la estrategia de las empresas españolas que operan en el exterior, y que la cultura de la autosuficiencia comience su retirada progresiva como referente de gestión de la seguridad. ●

Fotos: Archivo/Pixabay

safire

# 3.0

## HD OVER COAX


- Grabadores 5n1
- Ultra HD 4Mpx
- H.264/H.264+
- Mayor distancia de transmisión

HD TVI HD CVI IP CVBS AHD

Distribuidores oficiales:

www.jmsystems.es

www.avantech.info

www.visiotech.es

SAFIRE
www.safirecctv.com
info@safirecctv.com

**VICENTE DELGADO.** PRESIDENTE DE LA ASOCIACIÓN PROFESIONAL DE DETECTIVES PRIVADOS DE ESPAÑA. APDPE

# El **detective privado** ante 2017

CON gran interés esperábamos por parte de los detectives privados este año 2016 que ya ha finalizado. Esperábamos, sobre todo, la salida del Reglamento de Seguridad Privada en el que se iban a zanjar cuestiones que, sin lugar a duda, mantenían en vilo a gran parte de la profesión. Cuestiones como qué tipo de medidas de seguridad deberíamos tener en nuestros despachos, avales, información sobre contratos de investigación suscritos en nuestros despachos, etc.

No cabe duda que la situación política vivida en nuestro país ha tenido una repercusión clara en que este Reglamento no haya visto la luz. Igualmente, las reuniones mantenidas con el fin de intentar un consenso entre lo establecido en la Ley y lo que el Reglamento finalmente pudiera contener, también han sido algo que ha dilatado la redacción final y publicación del mismo.

Sin duda este Reglamento y su futura redacción es uno de los principales retos a nivel legal del sector de los detectives privados para este 2017, pero no nos detenemos aquí.

2017 tiene que ser el año de la lucha contra el intrusismo profesional. Para ello necesitamos de un mayor esfuerzo por parte de las Fuerzas y Cuerpos de Seguridad en erradicar estas actuaciones por parte de personal no habilitado. Estamos convencidos de que así será. No se puede seguir permitiendo que en determinadas provincias haya tal nivel de intrusismo que impida que los detectives privados legalmente habilitados puedan trabajar. Por parte de nuestra asociación, APDPE, vamos a usar todos los recursos a nuestro alcance para poner a disposición de las Jefaturas de Seguridad Privada todos los elementos de prueba necesarios para que, una vez comprobadas las situaciones irregulares por parte de estas Jefaturas, se realicen las correspondientes inspecciones y cierre de «sucursales» de detectives de otros países, sanción de «profesionales extranjeros» sin habilitación para trabajar en España, etc.

El intrusismo en nuestra profesión es una lacra que en este 2017 tiene que ser erradicada. En este punto cabe destacar que la Ley de Seguridad Privada 5/2014 sanciona tanto la realización de actividades o servicios de investigación privada por personal no habilitado como la contratación, a sabiendas, de estos servicios, por lo que es importante

la solicitud de la correspondiente habilitación (TIP) a la hora de contratar un detective privado. De hecho, los detectives estamos encantados de mostrar nuestra TIP a solicitud de nuestros clientes. Sin duda realizar las campañas necesarias a nivel estatal para que los jueces y magistrados, profesionales del derecho, empresarios y particulares exijan la correspondiente habilitación a la persona que se presente como detective en un Juzgado a testificar con su informe, es algo que debe ser prioritario para el conjunto de la profesión y sobre todo para las Asociaciones del Sector. Es algo en lo que todos tenemos que estar unidos.

## Concienciación de lo que puede aportar un detective privado a la sociedad

2017 tiene que ser por tanto el año de la concienciación por parte de la ciudadanía, instituciones, Fuerzas y Cuerpos de Seguridad del Estado, administraciones y resto de empresas y personal de Seguridad Privada de lo que un detective privado puede aportar a la sociedad, de cuáles son sus funciones, de la importancia de su testimonio en un juzgado, y en definitiva de lo necesario que es para una sociedad moderna la figura del detective.

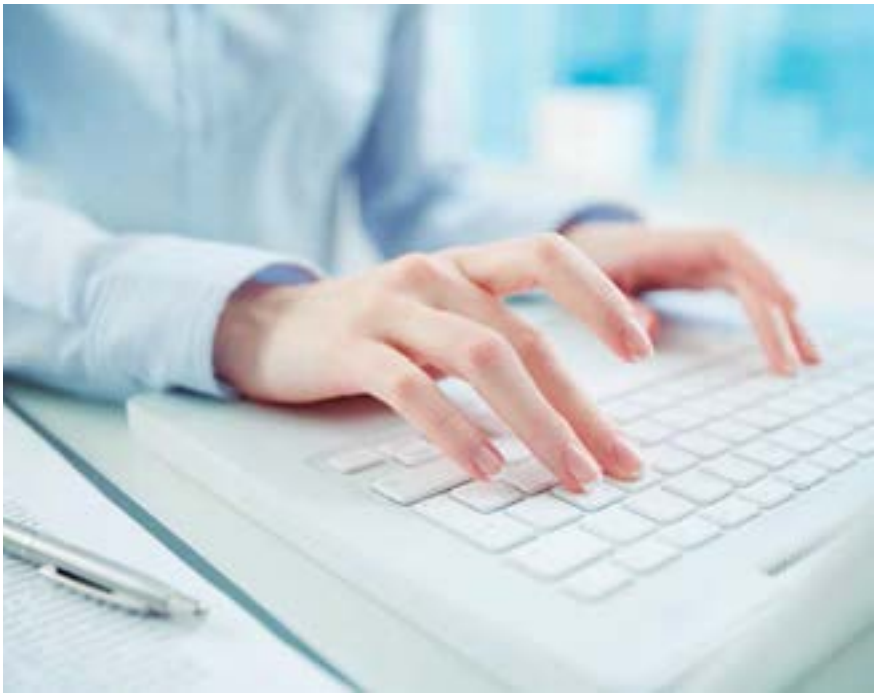
El detective privado que actualmente se encuentra ejerciendo su profesión en España es un profesional con formación universitaria. Muchos de ellos también se han especializado en campos como la informática forense o la ciberseguridad. La formación constante es una de las características profesionales de los detectives privados, ya que entendemos que nuestra profesión se encuentra en constante evolución y la forma en que se obtienen pruebas para nuestras investigaciones ha ido variando durante las últimas décadas, por lo que la obligación de estar al día es entendida como una necesidad. Otro reto prioritario para este 2017 será por tanto la continuidad en la formación de los detectives privados.

El futuro de nuestra profesión se torna apasionante conforme avanza el tiempo. Nuestras investigaciones ya no se realizan solo a nivel local, sino que nuestros acuerdos con otros profesionales, asociaciones internacionales, etc. nos permiten dar un servicio global a nuestros clientes. Ya no comienza y finaliza una investigación siempre en la misma ciudad. Las ramificaciones societarias de una empresa ya no terminan en España. Es fácil encontrarse con que un cliente precisa un servicio en otro país europeo. Incluso hay clientes que precisan informarse de un futuro proveedor cuya sede se encuentra en un país asiático. El detective privado de 2017 ya no es una persona dedicada solo a asuntos matrimoniales. El detective privado de 2017 está a la última en nuevas tecnologías, emplea las herramientas más punteras en obtención de pruebas, maximiza el rendimiento de sus servicios y minimiza los costes para el cliente. Y siempre respetando la legalidad vigente y bajo los principios de razonabilidad, necesidad, idoneidad y proporcionalidad.

Por último: nunca olvidar que el detective privado es el único profesional habilitado por la Ley de Seguridad Privada para investigar la vida privada de las personas, siempre fuera de sus domicilios u otros lugares reservados, obtener información para garantizar el normal desarrollo de actividades en ferias, hoteles, exposiciones, grandes superficies comerciales, etc. ●

> «El intrusismo en nuestra profesión es una lacra que este 2017 tiene que ser erradicada»

Fotos: Pixabay/ Freepik



**ANTONIO CEDENILLA GALERA.** PRESIDENTE DE LA ASOCIACIÓN DE JEFES DE SEGURIDAD DE ESPAÑA. AJSE

# Seguridad Privada, un **magnífico aliado**

¿CUÁNTO daño ha hecho y está haciendo esta larga crisis, y cuántas empresas más desaparecerán para el año 2017? Son preguntas que me hago cuando se o veo que una empresa de seguridad cierra.

Dejando a un lado las perspectivas del año pasado que parecía que iban a ser más halagüeñas, hemos sufrido un giro de 360º esperando una mejoría que no ha llegado; éstas no han sido todo lo positivas que cabría esperar, sino al contrario, han sido un claro ejemplo de pesimismo empresarial. Todo ello hace que tengamos que parar la maquinaria un momento y empecemos a reflexionar de nuevo, ya que el proceso sigue siendo muy pesimista; claro que siguen apareciendo nuevas empresas de Seguridad, al mismo tiempo que otras desaparecen, empresas con años de trabajo, y no pequeñas precisamente, empresas grandes y medianas, que han aportado mucho al sector, dejando una profunda herida en el panorama actual de la Seguridad Privada.

La realidad bajo un prisma lógico, es la de pintar un panorama pesimista en el sector de la Seguridad Privada, donde los empresarios y los emprendedores apuestan más por estar en otros sectores con menos riesgos, ya que los márgenes económicos de las empresas de seguridad son exiguos y ridículos. Nadie podría decir que hoy en día esto es un negocio rentable, empresas con gran prestigio o son compradas por tener pérdidas económicas y absorbidas, o realizan un cierre total creando así más paro en el sector de la Seguridad de este país.

Qué nos deparará el año 2017, y con esto no quiero que se me entienda como una persona pesimista con respecto a la creación de nuevas empresas, pero se presenta un año muy parecido a este que ya finaliza, creo que seguirán cerrando empresas, aguantando quien mejor esté preparada para los retos o mejor gestionadas, no pudiendo sostener servicios deficitarios y quedándose los que estén con mejores márgenes lógicos y rentables.

Tenemos claros ejemplos, como el reciente procedimiento de despido de las empresas nacionales de gran y mediano tamaño: Segur Ibérica, con casi 4.000 trabajadores, LPM, Punto y Control, etc., o absorciones como las de Ombus-Casesa.

La profesionalidad de estos hombre y mujeres que viven de este trabajo diario está estancada, pues se han paralizado muchas acciones formativas en este sector, y es de lo que se están quejando muchos centros de formación nacionales, asociaciones profesionales y sindicatos. La formación es un bien necesario para la seguridad de su personal, pues entre los riesgos profesionales está el más importante que es el riesgo personal que cada día se incrementa, pues entre este último hay un claro índice elevado de agresiones a Vigilantes de Seguridad sin poder repeler estas amenazas por falta de preparación y adecuación en los medios defensivos. En la actualidad tampoco se les dota de herramientas de defensa eficaces, por tanto, se le está haciendo caso omiso por parte de la administración o de las empresas del sector. Estas empresas que no están viendo los beneficios económicos esperados por motivos diferentes como, por ejemplo, un gasto innecesario (pérdida de horas de trabajo) en dos palabras, el sector está parado! Como decía en líneas anteriores los casos son: unos presupuestos ajustados o muy bajos, unos sueldos altos en las direcciones de las empresas, un sobrecoste de personal en oficinas, medios informáticos obsoletos, unas malas gestiones económicas de las empresas, beneficios ridículos, gastos en aumento, una competencia cada vez mayor, los impagos de clientes, el intrusismo de algunas empresas, etc., y seguramente me dejaré alguno, esto hace que el sector esté en la UCI.

Asociaciones empresariales y profesionales tenemos que hacer un replanteamiento a este y a muchos otros temas pendientes, para darles una bocanada de aire fresco y un empuje hacia adelante

¿Cómo veo el panorama para 2017? Francamente un poco oscuro, y soy realista porque no quiero errar con facilidad, aunque podemos sufrir ahora con

el nuevo Gobierno un aumento del negocio, también con el nuevo reglamento aún por llegar puede proporcionar un poco de alas a este aspecto. Me gustaría acertar y decir que espero un despegue positivo del sector, sobre todo no tanto en las empresas de Vigilantes, sino más en las empresas tecnológicas, ya que el futuro está en sus manos, «bajo mi humilde opinión», la robótica, la informática, los medios audiovisuales, el personal cualificado, etc.

Veo o espero ver un incremento en el aumento de la demanda de las Centrales de Alarmas (CRA), en las empresas instaladoras y en las nuevas tecnologías, por lo que las empresas de seguridad de Vigilancia tendrán que moverse en áreas hasta ahora no valoradas, menospreciadas o desconocidas. Un paso importante son las vigilancias de prisiones, las acudas por parte de empresas de Seguridad, donde hasta ahora unas pocas empresas se habían atrevido a poner sus ojos, metiéndose de lleno en este negocio con un alto índice de acierto; las poblaciones de menos de 100 habitantes que están desprotegidas sería un caso importante de negocio también, ya que estas poblaciones no tienen suficiente economía presupuestaria para tener sus propios agentes de seguridad (Policías Locales), pues son Ayuntamientos pobres y con dificultades de financiación; los desahucios de pisos ocupados ilegalmente también sería una muy buena solución. La Seguridad Privada es un magnífico aliado para dar una alta protección ante la delincuencia y la criminalidad de este país.

Este es un pequeño esbozo de ideas en las que se puede buscar negocio en la Seguridad Privada, eso sí, todo debidamente legislado y centralizado por los Cuerpos de Seguridad del Estado. Hay otras fuentes que están aún por estudiar, y creo que la Seguridad Privada se acerca poco a poco a estas nuevas ideas de negocio.

Hay luz en el camino, que los magníficos profesionales de este sector verán nuevas fórmulas para trabajar y no cerrarnos a una competencia desorbitada por los mismos servicios, cada vez más baratos; hay ideas aún por valorar, ideas que sacarán a este sector de la gran y profunda crisis que parece no terminar nunca de dañar a un sector ya muy dolido. ●

**Fotos: Freepik/Archivo.**

**RAÚL BELTRÁN.** PRESIDENTE DE LA ASOCIACIÓN PROFESIONAL DE GUARDAS JURADOS DE CAZA

# Gobiernos, **mercados y reglamentos**

FRECUENTEMENTE he recibido elogios por mi visión de futuro, y por «predecir» pequeñas cuestiones en mis colaboraciones con publicaciones; te tantean sobre algo que debemos conocer y con el tiempo suficiente para reflexionar y vertebrar un escrito, que repose en la editorial para luego publicarse y que se distribuya; y que aún así conserve algo de frescor y de razón, no es cosa fácil.

Prever algo para 2017 es, sin más, una auténtica temeridad, un imposible, un brindis al sol, y aún así en 2017 habrá que comer todos los días.

Las cosas en el campo para los guardas rurales no pintan muy diferentes que al resto de la seguridad; ya empieza el Cuerpo Nacional de Policía a tomar razón de los contratos de los guardas, de su forma de prestación de servicio; ya la Ley 5/2014 comienza a modular la actividad en el medio rural. Sustos, sofocones y ojos vueltos a un reglamento que no llega.

Buenas sensaciones trasmite el SEPROSE, parece haber reforzado su respaldo al colectivo, pero nada se sabe de los temas fundamentales, la reserva de la vigilancia en terreno rural para los Guardas, ¿o al final se volverán a llevar el gato al agua los vigilantes, con un sistema de vigilancia compartida? Todo queda en el limbo de un reglamento que no llega.

Lo que parece que ya es una realidad es el Gobierno, recientemente se han conocido los nombres de los responsables en Interior, Juristas, ¿cómo influirá esto en el deseado reglamento? Un reglamento que esperamos allane el camino para nuevos nichos de mercados, en los que el sector de la seguridad recobre márgenes y comience a producir esos beneficios que sirvan de revulsivo.

Un reglamento que clarifique límites y sea una herramienta eficaz contra el intrusismo que nos parasita hasta la extenuación, para poco a poco ir retomando un mercado, con costes justos, precios justos, pagos justos y beneficios, pues es en la consecución de beneficios en los que al fin se sustenta el desarrollo y la evolución, que en el caso del medio rural ha retrocedido alarmantemente.

Si ha sido frecuente que el Guarda contratado directamente por el usuario no tuviera unas condiciones laborales demasiado espléndidas, ha sido el Guarda en el régimen de Autónomos el que ha tenido que rebajar hasta límites de esclavitud sus emolumentos, entrando a competir en precio con el intruso, haciendo de la nómina que el convenio asigna al Guarda Rural, un lujo envidiado por todos, pero al alcance de muy pocos.

Mucho tiene que hacerse y asentarse en 2017; parcheado un Gobierno para salir del trance, veremos si podemos promover un reglamento que permita, en un deseable horizonte libre de crisis, vertebrar el mercado y el sector… que no sea otro año «huero». ●





# Innovación al servicio de la seguridad

- Equipos de inspección por rayos X
- Detectores de metales
- Equipos de inspección por ondas milimétricas

Excelencia en calidad y servicio post-venta.

**TECOSA, la empresa de seguridad del Grupo Siemens, contribuye con sus productos y soluciones a hacer del mundo un lugar más seguro.**

**TECOSA**

Telecomunicación,
Electrónica y Conmutación, S.A.
Grupo Siemens

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

**JORGE SALGUEIRO.** PRESIDENTE EJECUTIVO DE AECRA. JURISTA-ABOGADO

# Tecnología & Seguridad Privada

LOS nuevos desarrollos tecnológicos, la hiperconectividad y la globalización de la economía están planteando importantes oportunidades y retos a nuestra economía. La Seguridad Privada como ámbito empresarial también debe abordar estas oportunidades y retos, para evolucionar y posicionarse como un sector fuerte, competitivo y de referencia internacional.

Las principales limitaciones en su expansión internacional derivan de diferentes marcos regulatorios y de una falta de unidad de mercado. La previsible falta de armonización normativa en el marco de la Unión Europea no favorece en modo alguno una búsqueda de nuevos mercados.

Obviamente el modelo tradicional de la Seguridad Privada se va a ver alterado por una impregnación permanente de las nuevas tecnologías, determinando un cambio en los modelos de negocio de las empresas de seguridad.

Ya hemos observado durante el año 2016 un avance en el modelo de alianzas entre las empresas de seguridad y las empresas de telecomunicaciones en aras a dotar al usuario cliente de nuevas soluciones y servicios más amplios de seguridad, que garantizan la interacción con el mismo, no limitadas a una mera intervención policial justificada.

Por consiguiente la empresa de seguridad debe acelerar su crecimiento y adaptación a estas nuevas necesidades tecnológicas y de internet de las cosas planteadas por sus clientes, teniendo como elementos clave la innovación, la internacionalización, la comercialización, las habilidades directivas, la financiación, el desarrollo de nuevos productos y servicios, la estrategia empresarial y la escalabilidad del modelo de negocio. Hay que conocer de forma permanente las necesidades del cliente para proponer nuevas soluciones de seguridad cada vez más ligadas a su modelo de autoprotección, garantizando su participación y complicidad en la prevención del delito.


Freepik

Así hace falta que la empresa de seguridad se dote de forma permanente de las herramientas tecnológicas y la información necesaria, para poder llevar a cabo una reflexión estratégica e identificar los factores clave y de éxito en sus relaciones con los clientes usuarios de dichos servicios de seguridad.

La consecuencia de lo expuesto será que la empresa de seguridad logrará tener una hoja de ruta suficiente, una continuidad en el negocio frente a sus clientes, sabiendo adaptar su metodología a su resultado principal: satisfacer las necesidades subjetivas de seguridad de sus clientes.

Estas nuevas políticas de servicio afectan a los modelos de comercialización que deben adoptarse por las empresas de seguridad, con claro predominio de un modelo de contratación electrónica a distancia en las relaciones frente a los clientes de seguridad, así como en el desarrollo de los nuevos productos y servicios de seguridad, permitiéndose la obtención de un mercado más amplio.

Pelco™ by Schneider Electric™

# END-TO-END SOLUTIONS

PELCO™

by Schneider Electric

*Choose with Confidence.*

**ADRIÁN GÓMEZ.** PRESIDENTE DE TECNIFUEGO-AESPI

# El sector de SCI debe **aportar soluciones** ante los retos futuros

Junta Directiva Tecnifuego-Aespi.

EN estos momentos el sector debe protagonizar un cambio en la mentalidad de la sociedad en relación a la importancia de la Seguridad contra Incendios. Por un lado, la campaña debe ir dirigida a los usuarios profesionales en la elección adecuada de empresas certificadas y a la Administración, que dirija la actualización reglamentaria que lleva años paralizada por diversas causas.

En definitiva el sector de Seguridad contra Incendios tiene una serie de retos que afrontar, a los que TECNIFUEGO-AESPI intentará ofrecer las soluciones más convenientes en cada proceso.

Uno de los retos más inmediatos y urgentes es el de reducir muertes por incendio en vivienda. Vamos a liderar un cambio en la percepción de lo que significa la Seguridad contra Incendios. Debemos hacer que cale en las conciencias que los 164 muertos por incendio de hace un año, no se van a repetir.

Desde TECNIFUEGO-AESPI vamos a plantear de nuevo al Ministerio de Fomento la necesidad de exigir detección de incendios en vivienda como sucede en Francia o Portugal desde 2015. La detección de incendios debe ser una exigencia del Código Técnico de la Edificación en vivienda nueva y, además, se debe instalar en todas las viviendas de ciudadanos vulnerables (Tercera Edad, discapacidad, etc.), independientemente del año de construcción.

## Salvar vidas

Como expertos en la materia y a tenor de las estadísticas en otros países, sabemos que la detección de incendios y el resto de medidas de protección contra incendios salvan vidas. Este dato debemos trasladarlo a la sociedad y concienciar en esta línea. Por todo ello, continuaremos con esta iniciativa que vela por la seguridad de las personas hasta que consigamos que se recoja en la legislación vigente, llevándolo al Ministerio y también al Parlamento.

Esta será la punta de lanza del resto de acciones, por ejemplo, la mejora del sector de Seguridad contra Incendios (SCI). Mejora económica, normativa, de regularización y buen hacer profesional.

Debemos ser más competitivos, extremar la atención y servicio al cliente, explicar al usuario que en Seguridad contra Incendios la eficacia y la fiabilidad de la instalación y equipos de protección contra incendios van unidas a la profesionalidad de la empresa que instala, mantiene y fabrica.

## Invertir en formación

La competitividad también significa invertir en la formación del personal,

presentar innovaciones y soluciones para atender retos y problemas. Y poner como bandera sectorial la calidad, porque estamos hablando de vidas y bienes.

Pero la calidad no sirve si en el mercado existen empresas que operan otros utilizando malas prácticas empresariales. Empresas que por llevarse el contrato, ofertan instalaciones/mantenimientos/equipos a precios por debajo de coste. Estas malas prácticas, desencadenan instalaciones deficitarias, es decir, engañosas. Es imposible hacer un trabajo por debajo del coste. Esto en seguridad contra incendios pone en riesgo la vida, el negocio, el futuro…

Desde TECNIFUEGO-AESPI continuaremos trabajando para poner en marcha la actualización de los reglamentos tan necesarios para el desarrollo del sector. Así mismo, pedimos que activen programas de inspección y control del mercado y concienciación del usuario final. También pedimos a las aseguradoras que pongan las máximas exigencias a las instalaciones, etcétera.

Aunque es obvio, debemos recordar una y otra vez que los sistemas de Seguridad contra Incendios no entran en acción hasta que no se da una situación de incendio, y la única forma que garantiza su funcionalidad es que se sometan a los diversos mantenimientos según prescribe la normativa vigente (RPC, RIPCI, RSCIEI), etc. Por ello, es necesario contratar empresas inscritas oficialmente como instaladoras, mantenedoras autorizadas y fabricantes, con productos certificados, con amplia experiencia y referencias. Solicitar estos requisitos es una práctica muy recomendable para asegurar la correcta selección de productos e instalaciones de SCI. Siempre debemos exigir productos con marcado CE y exigir a los fabricantes la obligada Declaración de Prestaciones.


**Stand Tecnifuego-Aespi en Sicur.**

> «En estos momentos el sector debe protagonizar un cambio en la mentalidad de la sociedad en relación a la importancia de la Seguridad contra Incendios»

## Reglamentos que afectan al sector

Además, ahora que entramos en un nuevo ciclo, con un nuevo Gobierno, esperamos la aprobación y publicación de las adaptaciones de los reglamentos que afectan al sector. La Administración Pública debe dar un impulso a esa recuperación que se espera leve pero sostenida en el tiempo. La seguridad de las personas es una responsabilidad de todos, de los profesionales que la hacemos posible, de los usuarios que deben contratar lo que establece la legislación y preocuparse por mantener los sistemas operativos, y de la Administración que debe velar porque se cumpla la ley e inspeccionar las instalaciones. ●

**Fotos:** *Tecnifuego-Aespi*

**JON MICHELENA.** DIRECTOR GENERAL DE CEPREVEN

# La **esperanza** es lo último que se pierde

AL finalizar 2015 todos veíamos al 2016 como el año en el que todas nuestras esperanzas se verían hechas realidad: el mercado de la seguridad se reactivaría gracias a la recuperación económica y a la publicación de los reglamentos y códigos que, con su permiso, voy a denominar «los viajeros sordos». Sí, ha acertado. Me refiero a las nuevas versiones del reglamento de seguridad privada, del reglamento de instalaciones de protección contra incendios y al código técnico de la edificación en las partes que afectan a la seguridad contra incendios, uso y accesibilidad. La cualidad de sordos se la otorgo a todos ellos porque nunca responden cuando se les llama, son insensibles al clamor sectorial y no hacen acto de presencia a pesar de los múltiples coros que reclaman su presencia. Viajeros lo son, se les conocen numerosos desplazamientos con billete de ida y vuelta a Bruselas, pero después de cada viaje la fatiga del mismo les obliga a reposar en un cajón durante un tiempo indeterminado.

Pero volviendo al año que acaba, no parece que haya satisfecho esas expectativas que teníamos. Los reglamentos siguen descansando en sus cajones y un gobierno en minoría, obligado a buscar consensos en todas sus actuaciones, no parece que sea la mejor opción para su promulgación, más cuando no se ha hecho disfrutando de una mayoría absoluta. Seguiremos llamándoles por si se recuperan de su sordera.

Sin embargo, la incipiente recuperación que vivimos en 2015 se ha consolidado a nivel macroeconómico y también se ha reflejado en la disminución del número de parados. Sería injusto no reconocerlo. Vamos por buen camino, pero es un camino muy estrecho, y da la sensación de que en cualquier momento podemos caer por cualquiera de los precipicios que nos rodean. La globalización ha introducido infinidad de nuevas variables en las teorías económicas que se han utilizado hasta la fecha, con mayor o menor éxito, haciendo que muchas de ellas ya no sean de aplicación y que otras tengan una utilidad limitada. Mientras no aparezca un Einstein de la economía que sea capaz de integrar en una nueva teoría la totalidad de las variables, nos veremos obligados a seguir transitando por el estrecho camino de la recuperación, esperando que la situación geopolítica, el gobierno, el precio del petróleo, el terrorismo internacional o cualquier otra variable que surja, no nos haga caer por un precipicio que probablemente no tenga fin.

Y llega 2017 y, a pesar de todo, seguimos con la misma esperanza con la que finalizábamos 2015, y con las mismas ganas de superación que mostrábamos al iniciar 2016; al fin y al cabo, la esperanza es lo último que se pierde. ●

Fotos: Archivo

WISENET
SAMSUNG

# NOS MOVEMOS

Nos movemos para que Hanwha Techwin sea la marca de seguridad de su confianza.

Nos movemos con nuestro plazo de reparación de cinco días y hasta 3 años de garantía.

Nos movemos al ampliar nuestro centro de servicio al cliente y los equipos locales.

Nos movemos para ofrecer los más altos niveles de calidad en el soporte preventa y posventa. Somos Hanwha Techwin, y nos movemos juntos.

Hanwha-security.eu/we move

Hanwha
Techwin Europe

**DRA. MARÍA ANGUSTIAS CARACUEL RAYA.** PRESIDENTA DE LA ASOCIACIÓN DE DIPLOMADOS ESPAÑOLES EN SEGURIDAD Y DEFENSA. ADESYD; Y DIRECTORA DE SPANISH WOMEN IN INTERNATIONAL SECURITY. SWIIS

# #SomosADESyD

EL pasado 20 de septiembre de 2016, la Asociación de Diplomados Españoles en Seguridad y Defensa (ADESyD) celebró su quinto aniversario. Cinco años atrás, el escenario era muy delicado, debido a la crisis económica que atravesaba España con importantes ramificaciones en las esferas política, institucional y social. Entonces, un grupo de compañeros que compartíamos inquietudes en estos temas pensamos que había llegado el momento de ser innovadores y considerar la crisis como una oportunidad para pasar a la acción, comprometiéndonos aún más con nuestra sociedad en el fomento de una cultura de paz, seguridad y defensa, la tríada sobre la que se sustenta nuestro bienestar. Así fue cómo nos unimos bajo un mismo lema: «Si quieres paz y seguridad, defiéndelas», «Si vis pacem et securitatem, defende».

Hoy, 89 miembros del Consejo de Honor y 179 socios compartimos un conjunto de valores y de objetivos con el único fin de ser útiles a nuestra sociedad, fomentando el diálogo, la tolerancia y el entendimiento en temas relacionados con la paz, la seguridad y la defensa sobre la base del respeto, la libertad, la igualdad, la cooperación y la ayuda mutua para la consecución de nuestras metas.

Sin duda, todos y cada uno de nosotros, con su formación y experiencia, compartimos unos objetivos que no sólo redundan en hacer más sólida a nuestra Asociación, sino que los proyectamos fuera de nuestros respectivos ámbitos profesionales para llegar más lejos juntos. Somos académicos, diplomáticos, políticos, ingenieros, periodistas, funcionarios, abogados, científicos, cooperantes, militares, policías, guardias civiles y expertos del ámbito de la inteligencia y de la seguridad privada, entre otros, identificados plenamente con el artículo 30 de la Constitución Española y con una visión integral, inclusiva y multidimensional de la seguridad, como contempla la Estrategia de Seguridad Nacional de mayo de 2013. Pero también somos una Asociación abierta y receptiva a los diplomados extranjeros que han realizado cursos de posgrado en España y quieren contribuir con sus conocimientos a fomentar una cultura de seguridad, basada en el previo conocimiento, concienciación y sensibilización sobre estos temas. En particular, destacaría la inclusión de la perspectiva de género en todas nuestras actividades. Por ello, nació Spanish Women in International Security (SWIIS), integrada en la red WIIS-Global con sede en Washington DC, EEUU.

Entre las cuestiones que nos interesan como organización de la sociedad civil responsable y participativa, destacan los desafíos regionales que se plantean en distintos ámbitos geográficos (Europa, el Mediterráneo y Oriente Medio, las Américas, África y Asia-Pacífico), así como otros temas tan relevantes como la Agenda 2030 sobre el desarrollo sostenible; la superación de conflictos armados; la defensa de los derechos humanos; las misiones de las Fuerzas Armadas y Fuerzas y Cuerpos de Seguridad del Estado en el exterior; el control de armamento, el desarme y la no proliferación; las medidas de fomento de la confianza y la seguridad entre las naciones; el problema de los refugiados, los desplazados internos y la trata de personas; las consecuencias de las catástrofes naturales o de origen humano; las amenazas transnacionales, como el crimen organizado, el terrorismo y el extremismo violento; la seguridad cibernética, marítima y de la información, etc. Ante estos retos, contamos con importantes instrumentos del Estado y otras herramientas internacionales –proporcionadas por Organizaciones Internacionales a las que España pertenece– que trabajan día a día para prevenir, gestionar y responder, llegado el caso, a las amenazas compartidas que afectan a nuestra seguridad.

Ahora bien, existe un amplio consenso a nivel internacional de que ningún actor puede afrontar por sí mismo todos estos desafíos de seguridad. Por ello, desde ADESyD SWIIS sentimos la responsabilidad de sumar esfuerzos y unir nuestras voluntades a las de otros organismos gubernamentales, intergubernamentales y no gubernamentales que trabajan en estos campos. No en vano,

se trata de una responsabilidad compartida velar por los derechos de todos los ciudadanos; verdadero fundamento de nuestro progreso y desarrollo, y garantía de paz y estabilidad necesarias no solo para nuestro país sino también para otros pueblos, especialmente los que viven situaciones de conflicto.

Con este convencimiento y conscientes de que se precisa una labor constante de divulgación de estas cuestiones, que se apreciará a más largo plazo, durante estos cinco años hemos colaborado conjuntamente con instituciones públicas y privadas y de la sociedad civil, y con diversas organizaciones internacionales con las que compartimos intereses comunes, como la Organización de Estados Americanos (OEA), la UE, la OTAN y el Consejo de Europa, gracias al trabajo generoso y altruista de nuestros socios y su excelente disposición a compartir sus conocimientos e iniciativas.

Es más, siguiendo una máxima que se recoge en numerosos documentos de las NNUU, cada vez es más necesario el establecimiento de alianzas estratégicas para contribuir al logro de resultados tangibles en función de unos objetivos previamente marcados. Entre nuestros logros, destacaría cinco Cursos de Verano, tres Congresos nacionales, numerosos Foros de Debate, publicaciones, exposiciones fotográficas, vídeos y 87 Boletines informativos de difusión gratuita en nuestra web www.adesyd.es, en @ADESyD2011 @SWIIS2011 y en nuestro Canal de YouTube.

Con estas prácticas, vamos consiguiendo divulgar ampliamente la cultura de paz, seguridad y defensa con el ánimo de influir positivamente en la sociedad y en las instituciones que nos representan, favoreciendo la interconexión entre ellas. En este sentido, apostamos por una visión de liderazgo transformacional[1], que descansa en el establecimiento de normas de comportamiento inspiradas en la colaboración y la cooperación entre los ciudadanos, levantando la moral y reforzando sus aspiraciones mediante el reconocimiento de sus contribuciones y los logros en el ámbito de la seguridad. Se trata de un nuevo liderazgo basado en la interacción y el intercambio de conocimientos, predicando con el ejemplo en nuestra base social con el fin último de crear una verdadera comunidad de seguridad.

Retomo aquí las palabras de Radhika Coomaraswamy, quien lideró el estudio mundial sobre la resolución 1325 de NNUU sobre Mujeres, Paz y Seguridad, cuyo décimo sexto aniversario celebramos el pasado mes de octubre. Con estas acciones, «no hacemos lo correcto. Hacemos lo inteligente» –It is not the right thing to do… It is the smart thing to do– porque si contribuimos a divulgar estos temas en nuestra sociedad, ¡nos beneficiamos tod@s!

Fotos: AEDSyD/Freepik

[1]Sobre una definición de este concepto, véase Consejo Económico y Social de Naciones Unidas: Fomentar el liderazgo transformador y mejorar las competencias pertinentes de los funcionarios públicos, 25 de enero de 2016, E/C.16/2016/7, pág. 2!

**DANIEL LARGACHA.** DIRECTOR DEL CYBER SECURITY CENTRE DE ISMS FORUM Y GLOBAL CONTROL CENTER ASSISTANT DIRECTOR DE MAPFRE

# Situación y retos de la seguridad en 2017-2020

NADIE pone hoy en duda que la seguridad es uno de los pilares básicos de la sociedad del siglo XXI. La configuración actual de la sociedad se ha confeccionado gracias a la creación de servicios que están soportados ya sea directa o indirectamente en Tecnologías de la Información, a su vez en gran medida gestionadas por empresas privadas. Nos encontramos en un momento bastante disruptivo, pero a la vez bonito, en el que estamos cruzando el punto de inflexión que realmente nos ayude a darnos cuenta de que el cambio de era ha tenido finalmente lugar.

La seguridad está disfrutando de un momento de singularidad al calor del auge de la eclosión de la TI. Esta situación modifica por completo el escenario actual, ya que afecta tanto a las amenazas como a los riesgos. El cambio podría ser en una u otra dirección, pero lamentablemente si atendemos a los datos está siendo en el sentido más desfavorable. Según datos de PWC en el informe de 2015 el número de incidentes que habían sufrido las empresas en el último año se había incrementado en un 38%. Podríamos llegar a pensar que es algo de lo que nuestro país es ajeno, pero, según datos del CCN-CERT los ataques han crecido un 356% desde 2012 y tan sólo en el último año han crecido un 41%.

## El número de incidentes ha aumentado

El hecho de que el número de incidentes haya aumentado por sí sólo no tiene que significar que nos encontremos en una peor situación que en el pasado. Una posible hipótesis válida podría ser que ahora se contabiliza y registra aquellos que antes no se contabilizaba. Sin tratar de quitar la razón a esta hipótesis, que tiene su sentido, también es cierto que los incidentes son cada vez no sólo más comunes sino más costosos (aprox. 7 millones de € por incidente según el Ponemon Institute) y de mayor criticidad.

Nos podríamos preguntar sobre cómo hemos llegado a esta situación, incluso a una persona neófita se le pueden plantear dudas de cómo es posible que estemos en un momento tan precario. Sin embargo, no debemos de olvidar que tanto hoy como dentro de 20 años, el software es inherentemente vulnerable. Toda la tecnología toma vida con un fragmento de software, desde un ordenador con su sistema operativo, hasta una pequeña antena 4G/LTE que funciona con un firmware. Sin software no hay tecnología, y el software está desarrollado directa o indirectamente por seres humanos que no dejan de introducir cierta manualidad en el proceso de desarrollo.

Esta situación de vulnerabilidad se ve condicionada de forma negativa en tres dimensiones adicionales:

• El aumento de la presión regulatoria. Están surgiendo nuevas regulaciones de los distintos países con respecto a la privacidad que vuelven a complicar el escenario. Tenemos en Europa la nueva GDPR, que establece un nuevo tablero de juego para el tratamiento de los datos de los ciudadanos europeos (en definitiva los datos que realmente importan a las empresas), pero en otros países la tendencia es similar, ya que también están aflorando nuevas regulaciones muy restrictivas con respecto a los datos de sus ciudadanos (Rusia, China, Panamá, Ecuador, Colombia, etc). La seguridad y la privacidad se están empleando como el nuevo arancel utilizado por los países para la protección de sus mercados internos.

• La digitalización de procesos. Las empresas de hoy en día están abordando sus planes internos para que sus procesos internos recojan ese cambio digital que ya venimos recogiendo a nivel personal, como integrantes de la sociedad de hoy en día. Este proceso que tiene muchas ventajas, también tiene algún inconveniente, en particular en seguridad, aquellos procesos que no tenían un alto grado de digitalización estaban menos expuestos a los riesgos de seguridad, que una vez abordado el proceso de digitalización. Es una cuestión simple de grado de exposición.

• La aparición de nuevas tendencias de TI. Para terminar de confeccionar el panorama, no tenemos que olvidar que tendencias como el Cloud Computing, los nuevos dispositivos IoT, nuevos escenarios de movilidad (tanto B2B como B2C), y los entornos dinámicos que nos plantea la virtualización (con infraestructura de TI que se crea de manera temporal y a demanda, y dentro o fuera de las empresas), no ayudan particularmente a simplificar el panorama.


«La seguridad y la privacidad se están empleando como el nuevo arancel utilizado por los países para la protección de sus mercados internos»

Las empresas están observando cómo las estrategias de seguridad que venían implantando van perdiendo eficacia tornando el paradigma de la seguridad actual en altamente inefectivo. Por ello, las empresas se están planteando nuevas aproximaciones centradas en el ámbito reactivo, tratando de optimizar los costes, recursos y ganando en eficacia.

## Un aumento del riesgo

La situación actual ha puesto en una situación complicada a las empresas, pero estas han entendido que se ha producido un aumento del riesgo, tanto por su dependencia con las TI como el mayor peso que las TI han tomado y van a tomar. Además han terminado por aceptar que los ataques son inevitables, y que éstos cada vez son más sofisticados.

Posiblemente en los próximos años veremos pivotar la estrategia de seguridad de las empresas sobre estas cinco líneas de actividad:

• Aumento y mejora de las capacidades. Las empresas deben de poner el foco en mejorar su efectividad en entornos detectivos y reactivos, partiendo de la premisa «cuando vamos a tener un incidente de seguridad» y evolucionando a cómo mejorar en la respuesta. Así, las aproximaciones de colaboración público-privada y privada-privada tendrán un importante auge en los próximos años.

• Seguridad por defecto. Tanto las tradicionales como las nuevas tendencias de TI deben limitar su riesgo de exposición mediante la aplicación de medidas que sean por defecto, tratando de minimizar la exposición a las cre-

«La seguridad está disfrutando de un momento de singularidad al calor del auge de la eclosión de la TI»

cientes amenazas. Es la única manera de tratar de tornar en eficiente una estrategia de seguridad que cada vez ha de abarcar un escenario en crecimiento y evolución continua.

• Consolidación. La mejora de la eficiencia y reducción de costes pasa necesariamente porque las empresas fabricantes de tecnologías de seguridad integren y consoliden funcionalidades y tecnologías que actualmente están dispersas en soluciones independientes, reduciendo los TCO y ayudando en la eficiencia.

• Mejora de la visibilidad. En entornos que se encuentran fuera de los límites de la organización. El perímetro de la tecnología que queda dentro y fuera del ámbito de una empresa está completamente desdibujado. La regla de utilizar los firewalls para conocer aquellos sistemas que estaban dentro o fuera del ámbito de actuación de la empresa ha dejado de ser útil, y las empresas deben de definir e implantar estrategias y soluciones que les permitan controlar y actuar en ubicaciones fuera de su perímetro, allá donde se encuentre su información.

• Automatización. La mejora de la efectividad pasa irremediablemente por ir dejando en un segundo nivel las actuaciones de seguridad realizadas por personas, para ir aumentando en un primer nivel las actuaciones automatizadas de los sistemas de información de seguridad, permitiendo focalizarse principalmente en aquello que requiere un mayor nivel de dedicación humana.

## Mejorar la seguridad y privacidad

Desde la creación del ISMS las empresas asociadas vienen colaborando en estos ámbitos. El Cloud Security Alliance (CSA) trata de mejorar la seguridad y la privacidad en entornos cloud. El Centro de Estudios de Movilidad (CEM) abarca la seguridad tanto los nuevos entornos de movilidad como con los nuevos dispositivos IoT. El Cyber Security Center (CSC) desarrolla actividades dentro del ámbito de la ciber seguridad que ayuden a las empresas a estar mejor preparadas como la plataforma de compartición e intercambio de seguridad (IoCs) o los ejercicios de simulación de ciber crisis. Todas estas actividades están disponibles para las empresas asociadas al ISMS sin coste adicional alguno. ●

Fotos: Freepik

# Axis Solution Conference 2017

## ¡Nuevas soluciones que no se puede perder!

8 y 9 de marzo de 2017,
Hipódromo de la Zarzuela

- Ciudades Inteligentes y Seguras
- Infraestructuras Críticas e Industria
- Retail y Logística
- Plataformas de Integración: Vídeo, Control de accesos y Audio


No se pierda la II Edición del **Axis Solution Conference**. El evento de referencia del año, donde podrá conocer un mundo de soluciones sectoriales con demostraciones en vivo, exposiciones y conferencias, en un formato dinámico y visual. ¡Además le sorprenderemos con multitud de novedades!

Siga el evento en Twitter: #AxisSolution2017
Para más información:
http://www.axis.com/events/es/solution-conference-es-2017
**Axis Communications se reserva el derecho de admisión.*

AXIS COMMUNICATIONS

VAXTOR SYSTEMS · milestone · TechnoAware TECHNOLOGIES FOR AMBIENT INTELLIGENCE

Citilog · ngaro intelligent solutions · herta security · PACOM · COGNIMATICS

SeeTec An OnSSI Company · Allied Telesis · xtralis · ASSA ABLOY · prysm

**FRANCISCO JAVIER GONZÁLEZ GOSÁLBEZ.** PRESIDENTE DE EUROCLOUD ESPAÑA

# Cloud Computing: una realidad que ha venido para quedarse

HACE ya bastante tiempo que venimos hablando de cloud computing y sus bondades en todo tipo de empresas, como pago por uso, simplicidad o ahorro de costes. Muchos, atraídos por estos atractivos, se convirtieron en *early adopters* de esta tecnología a finales de la década anterior con experiencias de todo tipo.

Como sucede en el recorrido de maduración de cualquier nueva tecnología, ésta ha ido mejorando y se ha ido adaptando a las necesidades de los clientes en todos los aspectos, llegando a ofrecer características de personalización cada vez más completas, que nos permiten su despliegue con niveles de control muy similares hoy en día a los que venimos disfrutando normalmente en despliegues *on-premise*. A modo de ejemplo, en el ámbito de la seguridad informática, muchos proveedores permiten ya que las llaves de cifrado en nubes públicas sean generadas y gestionadas por el cliente. Algo que puede parecer simple pero que en los primeros momentos de difusión masiva de estos servicios echó para atrás a muchos potenciales consumidores, por no ser compatible con sus políticas de seguridad.

## Normativa

Más pronto que tarde, los proveedores adaptan sus tecnologías para cumplir con la normativa de cada país, las especialidades de los distintos tipos de empresa y las necesidades en general de todo tipo de consumidores, convirtiéndose así en una alternativa muy viable a la hora de desplegar un proyecto de cualquier tipo en la actualidad.

2016 ha sido un año muy intenso en España en lo que se refiere a tecnologías cloud. Como viene sucediendo en otros países desde hace ya bastante tiempo, no sólo el CIO compra servicios en la nube a día de hoy. Es muy común que un CSO adquiera un CRM por su cuenta o un CMO una aplicación de envío de correo electrónico masivo, ambas en la nube, sin tan siquiera conocer que están adquiriendo servicios cloud.

Esto ha provocado una proliferación importante en el mercado de software como servicio (*Software as a Service o SaaS*), la capa de mayor valor para el cliente, el que está llamado a ser el gran mercado dentro de tecnologías cloud.

Al mismo tiempo, los proveedores de Infraestructura como Servicio locales han interconectado sus plataformas con los grandes proveedores mundiales de cloud, y lo han hecho a través de puntos

de interconexión local, ofreciendo soluciones llave en mano multi-cloud con interlocutor en España, lo que ha facilitado el despliegue de todo tipo de soluciones con mayor eficiencia y seguridad, gracias al conocimiento normativo y a la especialización local de estos proveedores, permitiendo además la integración con los entornos *on-premise* de los clientes.

## Información en la nube

Todo esto no quiere decir que la nube sea la «panacea» y el camino a seguir en todos los casos. Los CISO no son ajenos a esta realidad, si bien su trabajo es garantizar que se cumplen unos requisitos de acceso seguro a la nube conforme a las políticas de la compañía, la normativa local y los estándares de mercado. La buena noticia es que cada vez disponen de más medios para garantizar el control que precisan sobre la información que se despliega en cloud, pudiendo por lo tanto garantizar que este despliegue se realiza con los parámetros de seguridad, información y monitorización requeridos.

> «Cloud Computing se está convirtiendo en una *commodity* donde cada vez nos centramos más en el uso práctico que es capaz de aportar»

En el entorno macro, estos movimientos han favorecido la proliferación de un fuerte ecosistema en torno al cloud computing, como Internet of Things (IoT), Big Data o Machine Learning, entre otras tecnologías, que pueden aportar mucho valor al negocio con un coste moderado gracias a la flexibilidad que ofrece la nube.

En 2017 lo esperable es que este movimiento de convergencia desde entornos *on-premise* a entornos cloud continúe con paso firme, al mismo tiempo que los proveedores ofrezcan todavía más flexibilidad y control sobre sus plataformas para que cualquier empresa pueda tomar decisiones sobre cómo desea utilizar la nube.

EuroCloud España, como representantes de la industria en nuestro país, realiza diversas acciones de apoyo y estandarización en torno a esta tecnología, como las iniciativas IoTrust o Big Data Lab, la creación de condiciones estándar de contratación en proveedores cloud, la elaboración del primer Estudio del Mercado del Cloud Computing en España que hemos encargado recientemente a IDC, o una participación muy activa en iniciativas públicas como la campaña de adopción de soluciones en la nube que ha lanzado con gran éxito RED.ES en 2016.

Todo sin olvidar la seguridad y el cumplimiento normativo, una de las preocupaciones más habituales a la hora de adoptar tecnologías en la nube en entornos corporativos. Nuestra Comisión de Seguridad reúne a expertos del sector con clientes finales de diferentes empresas y sectores con el objetivo de promover el desarrollo de buenas prácticas para la adopción segura de cloud computing en las empresas españolas, siendo una de las Comisiones más activas y más solicitadas de la Asociación.

Como en su momento sucedió con la electricidad, cloud computing se está convirtiendo en una *commodity,* donde cada vez nos preocupamos menos de la base tecnológica y nos centramos más en el uso práctico que es capaz de aportar, acercando la tecnología al usuario cada vez más, con los retos que esto supone para los responsables de ciberseguridad de las empresas. ●

**Fotos: Eurocloud/*Freepik***

**MIGUEL GARCÍA-MENÉNDEZ.** VICEPRESIDENTE DEL CENTRO DE CIBERSEGURIDAD INDUSTRIAL (@INFOR_CCI)

# Hacer de la **Ciberseguridad (Industrial)** un asunto de todos

## Desafío clave para 2017

LA afirmación «la ciberseguridad es un asunto de todos» acompaña, año tras año, a las diferentes campañas que promueven entidades como ENISA1 («una responsabilidad compartida»), ISACA2 («una responsabilidad de tod@s»), etc., dedicadas a la sensibilización en este terreno.

Sin entrar a valorar, a priori, la rotundidad con la que se realiza una afirmación como la que abre este artículo, permítame, simplemente, sugerirle que piense por un momento en el variado perfil de quienes asisten a conferencias, seminarios u otros eventos organizados por entidades como las citadas más arriba.

Sí, efectivamente, tiene Ud. razón: resulta que «el variado perfil», en realidad, no es tan variado. La experiencia indica que quienes asisten regularmente a esos eventos pertenecen, mayoritariamente, a un determinado colectivo profesional. Un colectivo de personas vinculadas al ámbito tecnológico; con unos antecedentes académicos y un nivel de formación medio-alto en ese mismo ámbito (o en campos afines); y, con intereses y/o experiencia en la ciberprotección de sus organizaciones (o las de sus clientes).

¡En definitiva, que siempre ve Ud. las mismas caras!

En esas condiciones, no es de extrañar que en un reciente –y concurrido– encuentro en el que se presentaba una guía de ciberseguridad dirigida a PYMEs no hubiese ninguna PYME. Ninguna, salvo varias del sector tecnológico surgidas a iniciativa de algunos emprendedores-autónomos presentes en la sala, esperanzados en poder llevar las recomendaciones de la guía, en una próxima visita, a algunos de sus clientes (todos ellos PYMEs).

Pero retomando la reflexión que acaba de hacer Ud. –por cierto, no se desilusione; a los congresos médicos, también asisten sólo los médicos–, para que la misma no desbarate por completo su confianza en los mensajes que revelan fuentes tan fiables como las citadas, quédese con la idea –menos osada– de que la ciberseguridad, si no de todos, es, al menos, un asunto de muchos.

## Un asunto de muchos...

¡Tome, como ejemplo, el macrosector industria!

Varios son los actores que conforman «el ecosistema industrial»; en par-

ticular, en lo relativo a los sistemas de control industrial (SCI). Por un lado, las empresas propietarias y/u operadoras de tales SCI en fábricas, plantas u otras instalaciones de corte industrial o similar. Por otro, cuantas entidades han venido ofreciendo a las primeras productos o servicios relativos a esas tecnologías de operación (TO), como fabricantes de bienes y equipos industriales, firmas de ingeniería u otras, especializadas en la integración de soluciones y sistemas diversos. Y, en tercer lugar, una serie de «nuevos» actores, originarios del mundo de las tecnologías de la información (TI), como fabricantes de TI, fabricantes de soluciones de ciberseguridad o firmas de consultoría, que han comenzado a adentrarse en el ámbito de las TO, conscientes de las oportunidades de negocio que les está ofreciendo la creciente conectividad y la ola digitalizadora, que en sus más variadas acepciones –Industria 4.0, Internet Industrial de las Cosas, fábricas inteligentes, tecnologías de operación inteligentes, etc.–, está permeando la actividad productiva industrial.

Adicionalmente, cabría mencionar otros grupos cuyos intereses bien podrían girar, también, en torno al sector industrial: los centros de investigación –especializados, tanto en TI, como en TO–; los centros de formación -reglada o no; universitaria u otra-; la propia Sociedad, como receptora de los bienes y/o servicios finales que ofrece la Industria; y, finalmente, la Administración, encargada de establecer las reglas de juego para unos y otros.

Todo este nutrido conjunto de grupos de interés ofrece una clara idea de los muchos a los que un asunto como la ciberseguridad –mejor dicho, la falta de ella– puede afectar, ante la materialización de cualquiera de los riesgos que, hoy, se ciernen sobre los sistemas de control que hacen posible los procesos productivos en las diferentes industrias.

Ese es el motivo por el que, desde entidades como el Centro de Ciberseguridad Industrial (CCI), se presta una atención preferente a dichos grupos. El último informe «Estado de la Ciberseguridad Industrial en España. Evolución y Futuro. Edición 2016»[3], publicado recientemente por el Centro, confirma el creciente interés por esta materia, materializado en una mayor participación en la encuesta, por parte de muchos más actores del ecosistema industrial que en ediciones anteriores. Actores procedentes, tanto del lado de la oferta, como del de la demanda de soluciones de ciberprotección.

El mismo informe destaca los muchos departamentos que, en mayor o menor medida, se están viendo implicados en atajar la problemática «ciber» que afecta a las organizaciones industriales. Destacan, entre ellos, sin duda, los departamentos de TI, muy por encima de los de TO, que quedan, incluso, en tercer lugar, tras las áreas de Seguridad Física de estas organizaciones. Y, al mismo tiempo llama la atención la baja implicación de los departamentos de Compras, cuya actividad en la cabecera del ciclo de vida de los sistemas de control con destino a este tipo de instalaciones, debería ser mucho más significativa de lo que es, por cuanto podrían hacer de filtro para aquellos productos (y proveedores) que no ofrezcan las mínimas garantías de confianza en lo tocante a su ciberrobustez.

Preguntados, igualmente, por los aspectos de responsabilidad, los participantes en el estudio han vuelto a dar idea de los muchos actores entre los que dicha responsabilidad parece estar repartida. Las áreas de TI, de TO y de Seguridad Física vuelven a tener valoraciones destacadas; pero, sin embargo, cabe subrayar el papel relevante que se asigna a las áreas de Operaciones (los usuarios de los SCI), a las que las empresas industriales colocan en el tercer puesto de la escala de responsabilidades, mientras que para los proveedores son los principales responsables. Una valoración que parece tener todo el sentido: la responsabilidad última sobre el uso, y las consecuencias de dicho uso, que se hace de los sistemas de control industrial que sustentan los procesos productivos ha de estar en manos de quienes están al frente de tales procesos, las áreas de Producción (Operación).

…pero de unos más que de otros.

Ciertamente, si hay algo que realmente ponga en tela de juicio la afirmación que abría estas reflexiones es el capítulo de responsabilidades.

Tras el asunto «TalkTalk» (2015), en el que la conocida operadora de telecomunicaciones británica sufrió un ciberataque –por cierto, acaba de sufrir otro (2016) mientras escribíamos estas líneas–, el Par-

«Sería un excelente propósito de Año Nuevo intentar promover en 2017 una cultura de ciberseguridad de todos y para todos»

lamento británico, por vía de su Comisión de Cultura, Medios y Deportes, elaboró un informe, «Ciberseguridad: La Protección de los Datos Personales En Línea»[4], el primero del curso político 2016-17, en el que sentenciaba que «la responsabilidad última sobre la ciberseguridad de una empresa recae sobre su consejero delegado». Por cierto, exonerando de toda responsabilidad al consejo de administración y a sus miembros.

El informe, de hecho, decía algo más; señalaba que a pesar de eso, el consejero delegado no tendría por qué dimitir en caso de producirse algún tipo de ciberincidente –muy probablemente los diputados británicos que elaboraron el informe desconocían los historiales profesionales de Randy Rademacher (ComAir, 2004), Satoru Nishibori (Mizuho Bank, 2011), Gregg Steinhaffel (Target, 2013), Amy Pascal (Sony Pictures Entertainment, 2014), Noel Biderman (Ashley Madison, 2015), Keith McNeil (NHS, 2015), Martin Winterkorn (Volkswagen, 2015), …; todos ellos exconsejeros delegados de las que fueron sus respectivas compañías–. Aun así, esos mismos diputados aconsejaban vincular, de algún modo, las remuneraciones de los consejeros delegados al hecho de que sus organizaciones no sufrieran ningún incidente de este tipo.

Finalmente, el informe apuntaba a la necesidad de contar con la figura de un responsable técnico/operativo, que se hiciese cargo de la ciberseguridad en el día a día; y a quien se pudiese sancionar debidamente, en caso de presentarse alguna situación indeseada.

La sensibilización de la dirección es, sin duda, una asignatura, aún, pendiente en muchos casos –a ella tratará de contribuir el que será próximo entregable de CCI, «Beneficios de la Ciberseguridad para las Empresas Industriales»–; pero, más allá de esa circunstancia concreta, lo que demuestran los ejemplos revisados a lo largo de este escrito es el todavía poco claro papel que TODOS, unos y otros, han de jugar en materia de Ciberseguridad.

Sería un excelente propósito de Año Nuevo intentar promover en 2017 una cultura de la ciberseguridad de TODOS y para TODOS, en la que comience a verse un público más generalista en los eventos del sector, en la que los departamentos de compras de las empresas industriales comiencen a exigir el cumplimiento de unos requisitos mínimos de ciberseguridad a sus proveedores, en la que los consejos de administración –y quienes los pueblan; no sólo los consejeros delegados– tomen conciencia de la responsabilidad que les corresponde en relación a la rendición de cuentas sobre el uso que se hace de «lo digital» en sus organizaciones, en la que los responsables técnicos de la ciberseguridad no sirvan únicamente de chivos expiatorios cuando las cosas vengan mal dadas, …

Una cultura en la que TODOS los afectados –TODOS nosotros– puedan (podamos) vernos identificados, de forma que, definitivamente, tenga todo el sentido hablar de la Ciberseguridad como «un asunto de TODOS»..

**Fotos: Archivo/Freepik.**

---

1. Agencia Europea para la Seguridad de la Información y de las Redes (www.enisa.europa.es).
2. Antigua Asociación para la Auditoría y el Control de los Sistemas de Información (www.isaca.org).
3. El informe «Estado de la Ciberseguridad Industrial en España, evolución y futuro. 2016» fue publicado, por CCI, el pasado 19 de octubre de 2016. URL: https://www.cci-es.org/web/cci/detalle-actividad/-/journal_content/56/10694/281015
4. El informe «Cyber Security: Protection of Personal Data Online», fue publicado, por el Parlamento británico, el pasado 20 de junio de 2016. URL:: https://www.publications.parliament.uk/pa/cm201617/cmselect/cmcumeds/148/148.pdf

## HIKVISION: TECNOLOGÍA DARKFIGHTER

# Por qué conformarse con el blanco y negro


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

Los innovadores productos Darkfighter Lite, utilizados en soluciones de seguridad y transporte urbano, ayudan a aportar a la escena el color y el detalle necesarios. Mediante la combinación de esta tecnología revolucionaria con funciones inteligentes integradas, ayudamos a las instituciones locales, a los responsables de seguridad industrial y a la industria del entretenimiento a hacerse con una solución de vigilancia adaptada a sus necesidades.

Hikvision, que posee el mayor departamento de I+D del sector, siente que es su responsabilidad ayudar a sus socios con los retos asociados al trabajo diario. Uno de los principales retos a los que se enfrenta la industria de la vigilancia es añadir color a las cámaras nocturnas. Nuestro departamento de I+D ha respondido con soluciones innovadoras para recuperar el color incluso en ambientes con poca luz.

Nuestras cámaras, que incorporan nuestra tecnología EXIR patentada, ofrecen grabaciones rectangulares revolucionarias con una iluminación IR uniforme, con lo que se solucionan los problemas con las lentes LED tradicionales, como la sobreexposición en el centro de la imagen y las zonas más oscuras en las esquinas. Gracias a la mayor potencia de la luz LED, la cámara Darkfighter Lite reduce el consumo de energía y el calor, y dura más tiempo.

Asimismo, hemos rediseñado la cámara domo y desarrollado una nueva tapa del obturador para evitar los efectos de distorsión de la imagen. Estos podrían deberse al reflejo de la luz (IR) por las malas condiciones meteorológicas, como la lluvia. Nuestro domo evita estos efectos y garantiza la claridad de la imagen en cualquier circunstancia.

Las Darkfighter Lite son las primeras cámaras del sector que incorporan estas innovaciones. La revolucionaria imagen a todo color, nuestra tecnología EXIR patentada y la nueva tapa del obturador hacen que esta cámara sea adecuada en cualquier circunstancia complicada de poca luz en interior o exterior. Como líderes mundiales en productos y soluciones de videovigilancia, nos ocupamos de su seguridad centrándonos en la innovación, la sostenibilidad y la calidad.

Para obtener más información sobre la amplia gama de productos y soluciones de Hikvision, visite www.hikvision.com


Contactos de empresas, p. 9.

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

# *«El futuro de los drones pasa por ser un **sector regulado**, que abogue por la seguridad y la **profesionalización**»*

**EN qué momento se encuentra el nuevo marco normativo que regulará la actividad de los drones los próximos años?**

—El pasado 22 de noviembre finalizó el plazo de Información Pública del proyecto de Real Decreto por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, y se modifica el Real Decreto 552/2014, de 27 de junio, por el que se desarrolla el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea y se modifica el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea. Ahora mismo se están analizando las observaciones y comentarios que se han realizado.

**—La Comisión de Transporte del Parlamento Europeo respaldó recientemente las nuevas normas que ha propuesto la Comisión Europea para garantizar la seguridad y privacidad en la UE en relación al uso de drones, ¿de qué manera afectará al marco regulador en nuestro país?**

—Toda la legislación en materia de seguridad aérea debe ser lo más homogénea posible a nivel internacional. Existen ya foros donde se trata de la homogenización normativa y de nuevas propuestas del sector, como OACI (Organización de Aviación Civil Internacional) o JARUS (Joint Authorities for Rulemaking on Unmanned Systems), en los que España está presente.

En función del formato que adopte la futura legislación a nivel europeo, reglamento o directiva, España en principio poco tendría que legislar al respecto, una vez que hemos participado en su elaboración junto con otros países que al igual que nosotros ya tienen norma, aunque dependerá de la versión final de la norma.

**—Las limitaciones de la Ley actual, aprobada en 2014, impiden el despegue de una industria, en la que se incluye el sector de la Seguridad Privada, ¿podría adelantarnos algunos aspectos que recogerá la nueva legislación?**

—El nuevo Real Decreto establece nuevos escenarios operacionales, tal como demanda el sector.

Los principales escenarios que se contemplan son:

- El sobrevuelo de zonas urbanas y aglomeraciones de personas, siempre que sea con un dron de menos de 10 kilos, a un máximo de 100 metros del piloto y de 120 metros de altura. Además, es necesario presentar un estudio de seguridad específico para cada tipo de operación y la autorización de AESA para la misma.
- Las operaciones nocturnas y los vuelos más allá del alcance visual del piloto con aeronaves de entre 2 y 25 kilos, en ambos casos es necesario un estudio de seguridad, la autorización de la Agencia y que el aparato tenga unos requisitos técnicos para cada caso.
- La norma también contempla la evolución tecnológica, por lo que prevé que cuando la tecnología lo permita se puedan realizar operaciones en espacio aéreo controlado, aunque en este caso, se requerirán requisitos de formación del personal y de los equipos, así como un estudio aeronáutico de segu-

ridad coordinado con el proveedor de servicios de tránsito aéreo y la previa autorización de AESA.

**—¿Podría ofrecernos datos actuales del sector de los RPA´s -número de operadores habilitados, escuelas autorizadas ATOS,...?**

—Más de 1.800 operadores habilitados en AESA.

• Más de 2.500 aeronaves registradas.
• Más de 2.700 pilotos registrados en AESA.
• Autorizados más de 1.000 vuelos de prueba demostración o investigación.
• 72 Escuelas ATOS que imparten cursos de piloto de drones.
• 89 organismos entre operadores y fabricantes que imparten formación práctica.

**—¿Cree que es necesaria la profesionalización del sector para potenciar y asegurar su crecimiento? ¿Qué acciones llevará a cabo AESA para potenciar este aspecto?**

—No podemos olvidar que el objetivo final es lograr un sector verdaderamente robusto y profesionalizado. Es necesario tener en cuenta que la mayor parte de los usuarios que trabajan ahora mismo en él y los que lo harán en el futuro no provienen del mundo de la aviación, por lo que les resulta ajeno un sector que está fuertemente reglado, por ello es importante que, si el sector de los drones quiere crecer de forma exponencial, tal como auguran todas las perspectivas, debe hacerlo de forma «fuerte y robusta» y, para ello, es imprescindible la seguridad y la profesionalidad de todo el sector. Cumplir la normativa para garantizar la seguridad de las personas y bienes en tierra, y la del resto de aeronaves que utilizan el espacio aéreo, es fundamental para que este sector tenga el desarrollo deseado. En definitiva, el futuro de los drones pasa por ser un sector regulado, como el español, que abogue por la seguridad y la profesionalización del sector, ya que ese es el único camino para asegurar un crecimiento fuerte y consistente de este prometedor sector.

Desde la Agencia trabajamos para ello, y además de participar en foros, habilitar una sección específica en nuestra web o tener un servicio de atención al ciudadano para este ámbito, hemos creado un grupo de trabajo interministerial y con representantes de la industria y el sector, que ayudará a seguir de cerca las necesidades y la evolución del mercado de los drones y por tanto de su profesionalización.

**—¿Qué papel debe jugar la seguridad para promover e impulsar el desarrollo de esta actividad?**

—Desde la Agencia Estatal de Seguridad Aérea venimos haciendo, desde 2011, un trabajo minucioso puesto que hay que prevenir todo tipo de situaciones y ver cuál es la mejor opción para cada caso.

Es necesario que la norma permita a todos trabajar con seguridad, porque todo este prometedor sector, no tendría ningún futuro sin ella. Y es ese, precisamente, el gran reto que tenemos por delante: permitir el desarrollo de este sector puntero, pero garantizando la seguridad de las personas y bienes en tierra, y del resto de las aeronaves.

Para lograrlo las Administraciones Públicas debemos trabajar en dos ámbitos paralelos. Por un lado, garantizando esa seguridad de las operaciones y la protección de personas y bienes; y por otro, facilitando el desarrollo de un sector llamado a ensanchar los límites de la aviación, a introducir mayor eficiencia en la actividad económica y a reducir el impacto de las operaciones aéreas sobre el medio ambiente.

Todo ello, junto con el generalizado abaratamiento de los equipos y su consecuente facilidad de adquisición, exigen a las Administraciones Públicas, si cabe, un mayor esfuerzo para disponer de una completa ordenación, orientada a cumplir esos dos grandes objetivos: garantizar la seguridad de las operaciones y facilitar el desarrollo del sector.

Podemos hablar de legislación, de la evolución tecnológica y de las múltiples aplicaciones de los drones, pero si no logramos un sector con un elevado grado de profesionalización, que vaya de la mano con la seguridad, y ésta depende de la evolución tecnológica, y si administración, operadores, fabricantes y usuarios no trabajamos juntos y no somos conscientes del reto y las responsabilidades que tenemos por delante, el futuro del sector no será el que todos esperamos. ●

*Fotos: AESA/ Pixabay*

**SERGIO GARCÍA FERNÁNDEZ.** JEFE DE PRODUCTO ÁREA IMAGEN & FOTÓNICA; **EDUARDO OLALLA.** DESARROLLO DE NEGOCIO ÁREA SEGURIDAD; Y **EDUARDO INZA.** INNOVACIÓN. GRUPO ÁLAVA INGENIEROS

# RPAS, un **mundo de posibilidades en seguridad**

«Es un pequeño paso para el hombre, pero un gran paso para la Humanidad». La célebre frase de 1969 no sólo comparte el ámbito de la ingeniería aeroespacial, también refleja perfectamente el cambio al que se enfrenta la sociedad con la llegada, para quedarse, de los drones. Día tras día, la tecnología que permite el uso de RPAS (Remotely Piloted Aircraft System o sistema de medios aéreos pilotados remotamente) en todo tipo de entornos y situaciones avanza de forma frenética y ofrece soluciones que mejoran y superan las limitaciones humanas.

SIN ir más lejos, los helicópteros de extinción de incendios que operan en España todos los veranos deben trabajar en entornos muy peligrosos –tanto para los aparatos como para los piloto– y se encuentran limitados por dos factores fundamentales: las partículas en suspensión que pueden afectar a las partes móviles o bloquear las salidas de gases y, por otro, los periodos de descanso de los pilotos, que deben seguirse a rajatabla.

De manera similar, los helicópteros y aviones guardacostas se enfrentan al reto de la localización de objetos flotantes y embarcaciones de la forma y tamaño más diverso, en medio de grandes superficies marinas. Sólo para España, esta superficie supera el millón de kilómetros cuadrados[1] y es equivalente a más del doble de la superficie terrestre total del país.

Los constantes avances en el desarrollo y la operación de medios aéreos no tripulados, la bajada de precios generalizada de la tecnología que los rodea (sistemas de posicionamiento, sensores de imagen, láser, escáner, radar, etc.) y los nuevos algoritmos inteligentes de visión artificial y *machine learning* ofrecen importantes ventajas en las situaciones descritas anteriormente.

## Proyectos de aplicación de RPAS

Se han puesto en marcha ya algunos proyectos reales que buscan la aplicación de RPAS para diferentes aplicaciones con diferentes cargas de pago y sistemas de control.

Uno de ellos es el proyecto ENJAMBRE. El objetivo del proyecto es poner en marcha un sistema de vuelo cooperativo que permita la operación conjunta de RPAS y aeronaves tripuladas en entornos de emergencias.

Misiones onshore, offshore, rescate

de personas o extinción de incendios son algunos de los ejemplos en los que el rápido despliegue y la calidad de la información que proporcionan son el elemento diferenciador. Por tanto, en el marco del proyecto se incluye el desarrollo de un dron con la tecnología más avanzada, que mejore la eficiencia del servicio y apoye las operaciones de las aeronaves tripuladas de mayor capacidad.

Por su parte, el proyecto ONTIME aborda el desarrollo de las tecnologías de captación, procesamiento y transmisión de la enorme cantidad de información que se genera durante el despliegue de RPAS en entornos de emergencias y vigilancia.

El objetivo general del proyecto es mejorar la eficiencia en la toma de decisiones en ese tipo de situaciones críticas, incrementar la fiabilidad de las transmisiones a los centros de control remotos y facilitar la disponibilidad de la información desde el origen, el dron.

Es indudable que a medio plazo, los RPAS incorporarán algoritmos para la toma de decisiones en tiempo real, sin ningún tipo de intervención humana. Pero también lo es que la gestión del Big Data plantea retos que requieren de nuevos desarrollos relacionados con la inteligencia artificial y los sistemas basados en redes neuronales artificiales. Todos estos retos son los que se están abordando en ONTIME.

En estos dos proyectos se empleará una sensórica muy avanzada, incluyendo cámaras de muy alta resolución, telémetros láser, sensores LIDAR, cámaras termográficas, multiespectrales e hiperespectrales, y sistemas de transmisión de la información que ofrecen un excelente equilibrio entre precisión, fiabilidad y accesibilidad.

Otro ejemplo del uso de estos sistemas no tripulados es el proyecto ICARUS. Después de los terremotos en L'Aquila, Haití y Japón, la Comisión Europea confirmó que existe una gran discrepancia entre la tecnología (robótica) desarrollada en laboratorio y el uso de dicha tecnología en el terreno para operaciones de búsqueda y salvamento (SAR) y gestión de emergencias.

El proyecto ICARUS nace precisamente con el objetivo de mejorar la gestión de una emergencia real y con ello reducir el riesgo y su impacto en la población. Para ello, se establece como principal vía de actuación el uso de dispositivos de búsqueda y salvamento no tripulados (terrestres, acuáticos y aéreos). Dichos dispositivos estarán integrados en las infraestructuras de comunicación existentes (GPRS, WiMAX, UHF, etc.), y ayudarán a la toma de decisiones críticas proporcionando información detallada, en tiempo real y de fácil entendimiento sobre la situación de emergencia.

El conjunto de plataformas y sensores propuestos informará al personal de emergencias sobre los peligros reales presentes en el terreno y, por lo tanto, mejorará su capacidad para resolver la situación. Sensores electro-ópticos IR para la detección de personas por diferencias de calor, sensores LIDAR para reconstrucción tri-dimensional de la zona y obtención de volúmenes de tierra desplazados, accesos, etc., o sensores acústicos direccionales para la «escucha» de posibles víctimas atrapadas son sólo algunos ejemplos de la tecnología necesaria para este tipo de actuaciones SAR.

> «La tecnología que permite el uso de RPAS en todo tipo de entornos y situaciones ofrece soluciones que mejoran y superan las limitaciones humanas»

Es indudable que la introducción de dispositivos de búsqueda y salvamento

no tripulados puede ofrecer una valiosa herramienta para salvar vidas humanas y acelerar el proceso SAR. Dichas plataformas no tripuladas pueden ser aéreas (UAV), terrestres (UGV) y marinos (ASV), pero es su interconexión y la toma de decisiones basada en redes neuronales e inteligencia artificial lo que verdaderamente marcará la diferencia.

Existe una vasta literatura sobre los esfuerzos de investigación para el desarrollo de herramientas de búsqueda y rescate sin tripulación. Pero la brecha entre la comunidad científica y la aplicación de sus avances con retornos para la sociedad se cierra cada vez más y empiezan a recogerse los primeros frutos.

Pero del mismo modo que los drones se utilizan para multitud de aplicaciones beneficiosas para el ser humano, el uso malintencionado o negligente de estos dispositivos puede suponer un serio problema para nuestra sociedad actual.

Algunas de estas amenazas son violación de la intimidad, crimen organizado, espionaje industrial, terrorismo, o simplemente la paralización de infraestructuras al sobrevolar su área de influencia. En la prensa podemos encontrar casos recientes de drones sobrevolando centrales nucleares, aeropuertos, infraestructuras militares, etc.

## Sistemas anti-dron

Existe por ello una necesidad operativa de un sistema que garantice la seguridad de las personas, un sistema anti-dron.

Este sistema anti dron debe integrar distintas etapas:

• Detección, identificación y seguimiento: Debe ser temprana para tener tiempo de reacción, con una identificación precisa y el menor número de falsas alarmas, y con un seguimiento automático de la intrusión.

• Denegación: Debemos evitar que el dron se acerque al objetivo.

• Neutralización o interceptación: En esta fase además de neutralizar al dron, debemos evitar o minimizar los daños colaterales que puedan afectar al entorno.

Para conseguir estos propósitos se deben combinar distintas tecnologías para que el sistema sea lo más eficiente posible. En fase de detección las tecnologías utilizadas hoy en día son principalmente sistemas radar, acústicos, electrópticos, lidar y antenas directivas.

Para realizar la denegación, la mayor parte de los esfuerzos se concentran actualmente en las comunicaciones, inhibiendo la señal. Técnicas de jamming, spoofing o incluso apropiación de las comunicaciones del dron (hacking).

La interceptación del dron es hoy en día la parte más compleja, porque en un entorno urbano, el derribo del dron puede causar daños. Las soluciones son variadas pero ninguna concluyente: drones cazadores de otros drones (drones con red), láser de alta potencia, águilas amaestradas y en última instancia, armas de fuego.

Las Fuerzas y Cuerpos de Seguridad del Estado (FFCC) investigan y trabajan desde hace años intensamente para conseguir el sistema antidron más eficiente posible, de forma que estos pequeños aparatos sean útiles a nuestra sociedad y no una seria amenaza.

Por tanto, queda de manifiesto que los drones son herramientas que encajan perfectamente en misiones críticas de seguridad, emergencias, vigilancia, etc. El uso eficiente de estas plataformas aportará indudables beneficios a la sociedad, pero también permitirá el acceso de capital privado a tecnologías que hasta ahora eran casi de exclusivo ámbito militar o a las que sólo tenían acceso grandes multinacionales. Definitivamente, avanzamos hacia un mundo mejor.

*Fotos: Grupo Álava*

[1].- Ministerio de Agricultura y Pesca, Alimentación y Medio Ambiente.

Contactos de empresas, p. 9.

# KEEP CALM AND

spain Homsec 2017

## 10 YEARS CONCERNED WITH THE INTERNATIONAL SECURITY & DEFENSE

### 6th International Exhibition
of Security & Defense Technologies

Conferences & Tech Days
International Delegations
National Authorities
Business Point
Product Presentations

March 14-16, 2017
Madrid, Spain

www.homsec.es/en
marketing@grupoateneasn.es

**VÍCTOR HERNÁNDEZ SEGOVIA.** DIRECTOR DE OPERACIONES DE EULEN SEGURIDAD

# Seguridad & **RPAS,** nuevos retos y oportunidades

En la actualidad están muy de moda los sistemas aéreos no tripulados, más conocidos como drones, aunque su origen proviene del acrónimo inglés RPAS –Remotely Piloted Aircraft Systems–. A pesar de que la mayor parte de la gente considera que estos sistemas son de reciente creación, la realidad es que no es así.

LOS orígenes de los drones comenzaron en el año 1916, con el diseño de una aeronave no tripulada para ser cargada de explosivos, por parte de un científico militar, con el fin de evitar el uso de los zepelines en sus bombardeos sobre el sur de Inglaterra, demostrando así que existía la posibilidad de controlar un pequeño y novedoso biplano a través de radio.

La versatilidad que otorgan estos dispositivos radica en el gran número de aplicaciones que existen en el mercado y su bajo coste, que los hacen perfectos para la realización de casi cualquier tipo de tarea, siempre que la normativa vigente lo permita.

La aplicación en el sector de la Seguridad Privada, donde su aplicación permite aumentar la eficiencia y eficacia de los servicios, abre un nuevo escenario de retos y oportunidades en el mercado de las tecnologías.

En este contexto, buscamos nuevos retos y con ello aportar soluciones que permitan conseguir una seguridad única e integral, revolucionando así el campo de la seguridad y la vigilancia con el uso de sistemas aéreos no tripulados.


Hemos desarrollado una serie de servicios que permiten cubrir cualquier sector empresarial, vigilando desde infraestructuras críticas a bienes e inmuebles, pasando por acuartelamientos militares, soporte y apoyo a las intervenciones convencionales de seguridad, a las tareas convergentes de seguridad y mantenimiento, monitorización y apoyo en caso de emergencias, localización, monitorización y soporte en incendios forestales, levantamientos de planos topográficos y cartografía, así como apoyo a los sistemas de comunicación.

## Cómo elegir una aeronave

A a la hora de elegir una aeronave, cuando se realiza una consultoría estratégica y de vigilancia integral, es clave conocer qué necesidades se tienen. Gracias a este estudio es posible identificar qué tipo de aeronave se ajusta mejor a cada situación, añadiendo a los dispositivos las capacidades tecnológicas imprescindibles para ofrecer un servicio de primera calidad.

Así, el servicio de aerovigilancia permite añadir valor a la seguridad convencional. La realización de patrullas de vigilancia con sistemas dotados de la última tecnología en cámaras que emiten imágenes en tiempo real a cualquier Centro de Control, permite salvaguardar las evidencias ante posibles actos de intrusión.

Los dispositivos que utilizamos poseen la inteligencia artificial necesaria para realizar sus misiones de manera autónoma, aunque para cumplir con la legislación vigente, se dota al servicio de un vigilante-piloto de seguridad, para tomar el control de la aeronave en caso de emergencia. Este servicio de aerovigilancia cuenta con capacidad de detección automática de intrusos, mediante el cual se recogen datos para su posterior análisis y medición. En el caso de intrusión real, se genera una alarma en el Centro de Control, donde se gestionan las imágenes.

Cabe destacar que es la Agencia Estatal de Seguridad Aérea –AESA-, adscrita al Ministerio de Fomento, el órgano encargado de la seguridad de la aviación civil en España y se encarga, por tanto, de regular las operaciones con RPAS, consideradas aeronaves a todos los efectos.

## Legislación a cumplir

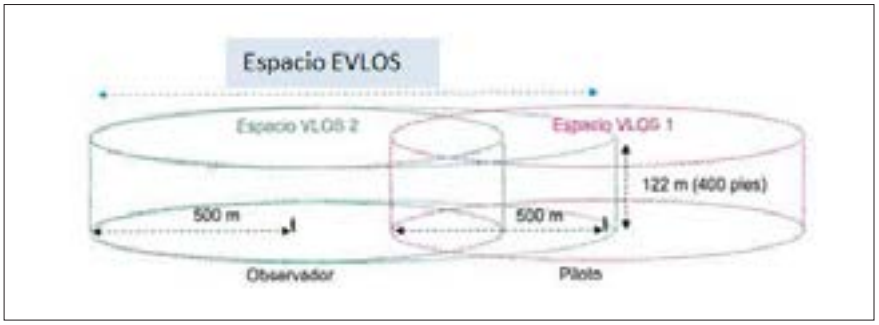
Actualmente, la legislación vigente que regula la utilización de los RPAS en España es la Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia, pero no es la única. Como la mayor parte de los drones que nos encontramos en el mercado están dotados con cámaras, es obligatorio que cumplan con la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Así mismo, deben cumplir con el Real Decreto 863/2008, de 23 de mayo, mediante el cual se aprueba el Reglamento de desarrollo de la Ley 32/2003, en lo relativo al uso del espacio radioeléctrico.

Los requisitos que un operador debe cumplir, para poder operar con drones, están recogidos en la normativa actual de RPAS, sólo para el ámbito profesional. La legislación no recoge los requisitos a cumplir para usos recreativos y deportivos de los multirrotores.

A continuación, se exponen las principales exigencias que debe cumplir el operador para trabajar con aeronaves cuya masa máxima al despegue no supere los 25 kg:

- El piloto debe ser mayor de edad.
- Debe estar en posesión de licencia de piloto de RPA o, en su defecto, acreditar que posee los conocimientos necesarios para poder pilotar.
- Sólo podrán operar en zonas fuera de aglomeraciones de edificios en ciudades, pueblos o lugares habitados o de reuniones de personas al aire libre, en espacio aéreo no controlado.
- La altura máxima de vuelo para los drones es de 120 m (400 pies).
- Los vuelos deben ser diurnos, en condiciones meteorológicas visuales.
- Todas las aeronaves civiles pilotadas por control remoto deberán llevar fijada a su estructura una placa de identificación en la que deberá constar, de forma legible, la identificación de la aeronave, mediante la designación específica del número de serie, nombre de la empresa operadora y los datos necesarios para ponerse en contacto con la misma.
- Por último, el vehículo aéreo no tripulado debe estar preparado para protegerse de interferencias ilícitas durante las operaciones.

De esta manera, la legislación deposita toda la responsabilidad sobre el operador del equipo. Aunque el aparato esté




diseñado para ser completamente autónomo, siempre debe existir la figura del piloto como responsable de la operación.

A pesar de las limitaciones que existen en la regulación actual, se prevé que la normativa se irá adaptando paulatinamente a las necesidades del mercado, favoreciendo la operación de los vuelos autónomos, y permitiendo aprovechar al máximo los avances tecnológicos de los sistemas integrados.

Actualmente se cuenta con el Proyecto de Real Decreto por el que se establecen nuevos escenarios operativos, entre otros:

• Se amplía el escenario de operación dentro de la línea visual del piloto (VLOS), introduciendo la figura del observador, creando el espacio EVLOS **(Ver figura 1)**.

• Más allá del alcance visual del piloto (BVLOS), cuando la aeronave cuente con sistemas certificados que permitan detectar y evitar a otros usuarios del espacio aéreo.

• La operación sobre aglomeraciones de edificios en ciudades o reuniones de personas al aire libre que se realice dentro del alcance visual del piloto (VLOS), podrán realizarse siempre que la masa máxima al despegue no sea superior a 10Kg y la distancia al piloto sea inferior a 100m.

• Podrán realizarse vuelos nocturnos con sujeción a las limitaciones y condiciones que establezca al efecto un estudio aeronáutico de seguridad realizado por el operador de la aeronave.

En EULEN Seguridad, gracias a la tipología de sus RPAS, ofrecemos agilidad de actuación, soporte y apoyo a las unidades de tierra, alta capacidad disuasoria, gestión de métricas e indicadores, así como visualización de imágenes de forma remota y en tiempo real, lo que nos permite aumentar considerablemente la seguridad de las instalaciones.

Los sistemas seguros y fiables que disponemos en EULEN Drone Security & Services, una nueva línea creada para potenciar los servicios de RPAS, nos permitirá realizar tareas de vigilancia y seguridad de forma casi automática. Un servicio de vigilancia constante en infraestructuras desatendidas o en instalaciones con grandes extensiones, en tiempo real, conociendo de primera mano lo que ocurre en ellas.

Además, la utilización de drones para realizar servicios de vigilancia industrial, permitirá aumentar tanto la seguridad física como operacional, lo que en inglés está claramente diferenciado con los conceptos safety & security, al evitar que los operadores de una instalación tengan que intervenir en situaciones que puedan poner en riesgo su propia integridad física.

La recepción constante de información a través del RPA, el operador puede determinar si es conveniente o no actuar en determinados momentos, evitando así situaciones de riesgo para el personal de la empresa.

*Fotos:* ***Eulen Seguridad***

Contactos de empresas, p. 9.

# PACOM OBTIENE LA CERTIFICACIÓN DE GRADO 3 PARA SU NUEVA CENTRAL DE SEGURIDAD 8003

El Controller (panel de alarmas) de Seguridad Inteligente 8003 ha sido concebido a partir de la tecnología Pacom-edge. Pacom-edge representa una nueva familia de dispositivos que ponen a disposición del usuario avanzadas prestaciones en materia de seguridad en toda la infraestructura Ethernet de su organización.

Heredero de la fiabilidad y prestaciones de la conocida 8002, de amplia implantación en entornos de alta seguridad, el panel 8003 ha sido diseñado para instalaciones de menor tamaño, pero en las que se requiere la integración de entradas, salidas e incluso sistemas de control de accesos.

Una sola placa, de tamaño reducido, pero potentes prestaciones es capaz de cubrir estas necesidades, aportando asimismo la certificación de seguridad en grado 3 que requiere la normativa.

Manteniendo el principal valor que caracteriza a los sistemas PACOM, la seguridad y la gestión de las comunicaciones IP, el panel 8003 dispone de un puerto RJ45 integrado para la conexión a la red de todos los elementos, que permite una inmediata transmisión de las alarmas, así como una perfecta comunicación bidireccional con numerosas aplicaciones automatizadas, tales como los mantenimientos remotos o las actualizaciones de firmware.

La posibilidad de utilizar una IP implica que se reducirá la necesidad de utilizar el cableado tradicional utilizado para un sistema de seguridad, lo cual garantiza una adecuada puesta en funcionamiento así como una amplia capacidad para cambiar sus dimensiones y adaptarse al entorno de trabajo.

El 8003 es un controller inteligente que está diseñado para aplicaciones de control de acceso y de alarmas avanzadas. Como dispositivo de control de acceso, puede utilizarse con un máximo de 2 puertas, cada una de ellas con un lector de ENTRADA y de SALIDA, cumpliendo así con las necesidades de aquellos entornos en los que el usuario pueda requerir la función antirretorno.

Como dispositivo de alarmas, el 8003 dispone de hasta 8 entradas configurables de 5 estados y de 8 salidas que incluyen 2 relés y 6 colectores abiertos. La cantidad de entradas puede ampliarse hasta 64 y, la de salidas, hasta 32 al añadir módulos de expansión integrados y/o dispositivos de E/S a distancia.

Asimismo, el 8003 puede funcionar de modo autónomo en entornos a distancia o de menores dimensiones, o incorporarse de forma sencilla como parte de un sistema de control de acceso y de alarmas completamente integrado en instalaciones de mayores dimensiones o en aplicaciones con múltiples sitios.

Su reducido tamaño, la facilidad de instalación y la incorporación en placa de entradas, salidas y controladores de puerta, hacen de la 8003 un candidato potente y de bajo coste en instalaciones pequeñas y medianas con altos requerimientos de seguridad.

**CARACTERÍSTICAS:**

- **Control de acceso y detección de intrusión integrada**
- **8 entradas supervisadas integradas (ampliable a 64)**
- **8 salidas integradas (ampliable a 32)**
- **Comunicación Ethernet Integrada en placa**
- **Tamaño estándar de 3U para montaje en bastidor o en caja**
- **Puede conectar 2 puertas, cada una de ellas con un lector de ENTRADA y de SALIDA**
- **Capacidad para 500.000 usuarios/tarjetas**
- **Capacidad de almacenamiento para 50.000 transacciones**
- **Niveles de acceso ilimitados**
- **Servidor web incorporado para facilitar las tareas de programación**
- **Actualizaciones de firmware en línea**

**SALVADOR BELLVER ESCRIHUELA.** ABOGADO EXPERTO EN TIC Y DRONES.
PRESIDENTE DE AEDRON

# La **normativa** del sector dron **alza el vuelo**

Los drones irrumpieron en el espacio aéreo, y han venido para quedarse, prueba de ello es el exponencial crecimiento de operadores y pilotos; a fecha actual existen en nuestro país más de 1.700 empresas operadoras y 10.000 pilotos de esta tecnología.

HASTA la publicación de la nueva normativa no se pemitiría realizar operaciones en los focos donde existía una mayor oportunidad de negocio: ciudad, nocturno, con lluvia, a más de 500 metros del piloto (con drones de más de 2 kg.)…, pero el escenario está cambiando, los actores del sector imploraban una nueva regulación, además, la tecnología evolucionó dotando de una mayor seguridad a estas aeronaves, ahora disponiendo de redundancia en sistemas de baterías o sensores anticolisión.

El nuevo real decreto es una evolución del anterior, aborda y desarrolla el sector, regulando muchos de los aspectos que anteriormente no se especificaban, entre ellos debería destacar:

**Placa identificativa:** Los drones cuya masa máxima al despegue no exceda de 25 kg. deberán llevar fijada a su estructura una placa de identificación ignífuga, en la que deberá constar la identificación de la aeronave, mediante su designación específica, incluyendo el nombre del fabricante, tipo, modelo y, en su caso, número de serie, así como el nombre del operador y los datos necesarios para ponerse en contacto con él.

**Radiocontrol:** El enlace de mando y control deberá cumplir con la normativa vigente en relación con el uso del espectro radioeléctrico, y utilizar frecuencias seleccionadas adecuadamente para reducir al mínimo la posibilidad de interferencia, voluntaria e involuntaria, que pueda afectar a la seguridad de las operaciones, sujeto a su autorización por el Ministerio de Industria, Energía y Turismo, cuando proceda conforme a la normativa de aplicación.

**Fabricantes de drones:** Se distingue entre las organizaciones de producción y fabricación. Los fabricantes de aeronaves pilotadas por control remoto serán responsables de las aeronaves que fabriquen. El fabricante o, en su caso, el titular de su certificado de tipo deberá elaborar y desarrollar un manual o conjunto de manuales que describan su funcionamiento, mantenimiento e inspección. Estos manuales deberán incluir directrices para realizar las tareas necesarias de inspección, mantenimiento y reparación a los niveles adecuados y específicos de la aeronave y sus sistemas asociados (RPAS), y deberán proporcionarse al operador junto con la aeronave.

**Mantenimiento:** El operador es responsable del mantenimiento y la conservación de la aeronavegabilidad, debiendo ser capaz de demostrar en todo momento que la aeronave pilotada por control remoto (RPA) y sus sistemas asociados conservan las condiciones de aeronavegabilidad con las que fueron fabricados. Además, el operador deberá cumplir con cualquier requisito de mantenimiento de la aeronavegabilidad declarado obligatorio por la Agencia Estatal de Seguridad Aérea.

**Entrenamiento y formación contínua del piloto a través de libro registro:** Al igual que ocurre en aeronaves tripuladas, se requiere que el piloto disponga de entrenamiento para realizar la operativa con seguridad, por ello, el operador deberá establecer un sistema de registro de los datos relativos a los vuelos realizados y el tiempo de vuelo, las deficiencias ocurridas antes de y durante los vuelos, para su análisis y resolución, los eventos significativos relacionados con la seguridad, y las inspecciones y acciones de mantenimiento y sustitución de piezas realizadas. Los pilotos que operen RPAS habrán de ejercer sus funciones de forma regular, de manera que en los últimos 3 meses se hayan realizado al menos 3 vuelos en cada categoría de aeronave en que se pretendan realizar operaciones, sean dichos vuelos de operación normal o específicos de entrenamiento. Parte de esa actividad podrá realizarse en sistemas sintéticos de entrenamiento. Además, se deberá realizar un entrenamiento anual específico en cada categoría de aeronave y para cada una de las actividades que se vayan a realizar. Para acreditar el cumplimiento de todo lo anterior, el piloto llevará un libro de vuelo en que se anotarán las actividades de vuelo y entrenamiento realizadas.

**Realización del mantenimiento:** El mantenimiento de las aeronaves pilotadas por control remoto (RPA) podrá realizarse por su fabricante y, en su caso, por el titular de su certificado de tipo, así como por aquellas otras organizaciones de mantenimiento que cumplan los requisitos que se establezcan por orden del Ministro de Fomento.

**Vuelo en zonas anteriormente no autorizadas:** Podrán realizarse operaciones aéreas especializadas sobre aglomeraciones de edificios en ciudades, pueblos o lugares habitados o reuniones de personas al aire libre, en espacio aéreo no controlado y fuera de una zona de información de vuelo (FIZ), únicamente por aeronaves pilotadas por control remoto (RPA) cuya masa máxima al despegue no exceda de 10 kg, dentro del alcance visual del piloto (VLOS), a una distancia horizontal máxima del piloto de 100 m, y a una altura máxima sobre el terreno no mayor de 400 pies (120 m) sobre el obstáculo más alto situado dentro de un radio de 600 m desde el drone. Se deberá acotar la zona, contando con el apoyo de la autoridad competente para limitar el paso de vehículos y personas ajenas a la operación.

**Área de protección y recuperación:** El operador deberá establecer un área de protección para el despegue y el aterrizaje, de manera que en un radio de 30 m no se encuentren personas que no estén bajo el control directo del operador.

**Registro de aeronaves vendidas**: En la comercialización de aeronaves pilotadas por control remoto, para cualesquiera usos, el vendedor está obligado a requerir el Documento Nacional de Identidad (DNI), Número de Identificación de Extranjeros (NIE) o documento o sistema de identificación equivalente que permita identificar al adquirente y, en su caso, el poder de representación mediante el que actúa, así como las autorizaciones o documentación complementaria que, en su caso, se establezca en la normativa de aplicación, y a consignar tales datos en los asientos de los libros o sistemas de registro del establecimiento junto con los identificativos de la aeronave, mediante su designación específica. En este caso, y recordando que vivimos en un mundo globalizado gracias a Internet, cabría destacar que la normativa no prevé un sistema de registro para los drones adquiridos fuera de nuestro país.

Con el cambio de paradigma provocado por esta evolución normativa, los operadores ya habilitados disponen de un plazo de tres meses para adaptarse a lo dispuesto.

No cabe duda que se trata de un importante avance y un paso firme, denotando la importancia y peso de un sector que está alzando un gran vuelo.

*Fotos: Aedron*

Contactos de empresas, p. 9.

**ANA PILAR CARRASCO.** RESPONSABLE DE MARKETING Y COMUNICACIÓN. ACG DRONE

# ¿Puede ser útil un dron en materia de seguridad?

Cuando oímos la palabra dron, todavía son muchos los que vinculan esta herramienta casi exclusivamente con el mundo recreativo. Como mucho, recordamos esas imágenes tan vistosas que nos muestran planos hasta ahora imposibles de alguna ciudad del mundo. Pero el universo RPA va mucho más allá del ocio o de la recolección de preciosas imágenes.

A DÍA de hoy, las posibilidades de actuación que tiene un dron alcanzan casi hasta donde llegue la imaginación. Hoy ya es posible su aplicación en sectores tan dispares como la agricultura, analizando multitud de factores en busca de la máxima productividad de un cultivo, el entorno industrial, realizando por ejemplo revisiones de estructuras de gran envergadura minimizando así la exposición de técnicos al riesgo; las emergencias, ayudando en labores de búsqueda de personas dada su facilidad para adentrarse en entornos poco accesibles como puede ser un rescate en alta montaña; o en la supervisión de incendios, inundaciones…, en general, zonas afectadas por una catástrofe. Todos estos supuestos están directamente relacionados con la seguridad porque de entrada están evitando que personal humano se exponga directamente al peligro.


Pero ¿puede ayudarnos un dron en otras facetas relacionadas con la seguridad? Rotundamente sí.

Gracias a la evolución de la tecnología, que ha hecho posible el desarrollo de cámaras y detectores de reducido tamaño y escaso peso, un dron puede ser equipado con dispositivos de última generación para realizar por ejemplo tareas de vigilancia. Casi a diario recibimos noticias de nuevos sistemas ideados para la supervisión de espacios. De hecho, hace pocas semanas se presentaba un sistema de vigilancia pensado para atender situaciones peligrosas y realizado por drones autónomos. La navegación de estos drones se lleva a cabo a través de un software que contiene la ruta a seguir y el calendario, y que puede ser activado desde un ordenador de control sin tener que depender de una señal GPS.

## Localización y visionado de personas

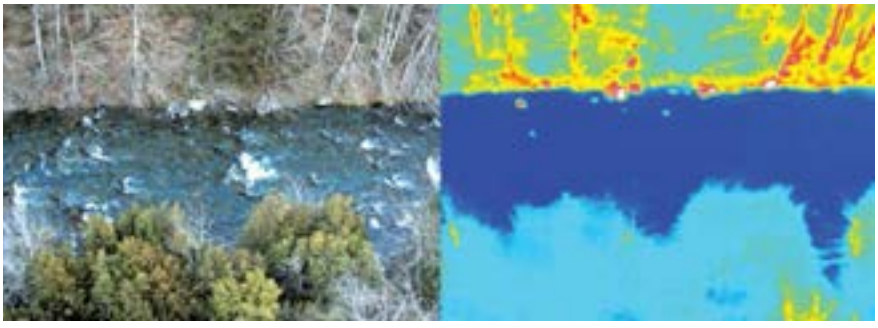
Otra de las grandes aplicaciones en desarrollo de los drones para las que se augura un buen futuro, es la localización y visionado del estado de personas que necesiten de una vigilancia frecuente. Para hacerlo posible, la persona a vigilar lleva consigo una pulsera con localizador. Gracias a esta pulsera, cuando se solicite un dron podrá colocarse en la ubicación de la persona y comenzar a emitir imágenes en tiempo real.

Sistemas de este tipo integrados en un RPA pueden convertirse en un gran avance para localizar y ver el estado de salud en personas con Alzhéimer, para localizar a personas que hayan sido secuestradas, o simplemente que se hayan desorientado y perdido.

## Rondas de vigilancia

Emplear drones para realizar rondas de vigilancia por ejemplo en polígonos industriales, es otro de los servicios más demandados en la actualidad. Se pueden llevar a cabo programando con antelación la ruta que debe seguir el dron, de manera que el piloto puede permanecer en el cuarto de vigilancia visualizando las imágenes que el RPA va recogiendo durante su ronda. Este método es también aplicable por ejemplo a entornos rurales, donde los robos de ganados y destrozos en cultivos están por desgracia a la orden del día. Podría decirse en tono figurado que sería una manera de «poner» puertas al campo en momentos delicados como pueden serlo las temporadas en las que el fruto está a punto para la recogida.

No podemos esconder que la normativa vigente en la actualidad, impide en buena medida el vuelo en muchas zonas, pero parece que por fin está a punto de actualizarse el marco regulatorio que afecta a los drones, estando prevista la apertura de la normativa en algunos puntos como la autorización de vuelos nocturnos –importantísimo dado que permite las rondas de vigilancia en grandes extensiones–, y el vuelo sobre zonas urbanas bajo condiciones específicas.



Hasta la fecha, hacer esto no era posible de una manera legal.

Los vehículos aéreos no tripulados han llegado a nuestra vida y parece que lo han hecho para quedarse. Debemos apelar a la responsabilidad de todo aquel que quiera hacer uso de una herramienta tan útil como esta, porque manejada de manera correcta, nos puede ayudar en muchos aspectos y facilitarnos la vida en buena medida.

*Fotos: ACG Drone*

Contactos de empresas, p. 9.

**IVÁN BAYO.** ABOGADO. DIRECTOR DEL DEPARTAMENTO DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS DE MBC IURIS.

# Protección de Datos & RPAS

## La evaluación de impacto en la protección de datos personales y su obligatoriedad (o conveniencia) en los Servicios de Vigilancia prestados por medio de aeronaves no tripuladas

En la actualidad, una de las principales preocupaciones de las empresas de seguridad es, sin duda alguna, la protección de la privacidad y de los datos personales tanto de sus clientes como de terceras personas. El fundamento de tal preocupación viene determinado por el Derecho Fundamental a la Protección de Datos que deriva de los artículos 10 y 18.4 de nuestra Constitución y que, tal y como ya manifestó el Tribunal Constitucional en su Sentencia 292/2000, de 30 de noviembre, tiene como objeto garantizar y proteger, las libertades públicas y los derechos fundamentales de las personas físicas y, especialmente, su honor e intimidad personal y familiar.

A NIVEL normativo no podemos pasar por alto que el régimen jurídico de la protección de los datos en España viene determinado, en términos generales, por la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD), así como su Reglamento de desarrollo (Real Decreto 1720/2007, de 20 de diciembre). Ambas normas se encuentran actualmente en vigor y resultan de aplicación tanto a los particulares como a las empresas conviviendo, de forma temporal, con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD), en vigor desde el pasado 5 de mayo de 2016 y que resultará de aplicación directa a todos los Estados de la Unión Europea, a partir del día 25 de mayo de 2018 quedando, a partir de entonces, derogada la LOPD.

La referida norma comunitaria, en cuyo análisis pormenorizado no nos detendremos por razones obvias, supone un cambio de paradigma en la protección de datos personales ya que introduce importantes novedades destacando, entre otras, el establecimiento de una Evaluación de Impacto en la Protección de Datos Personales (EIPD) regulada en el artículo 35 del RGPD.

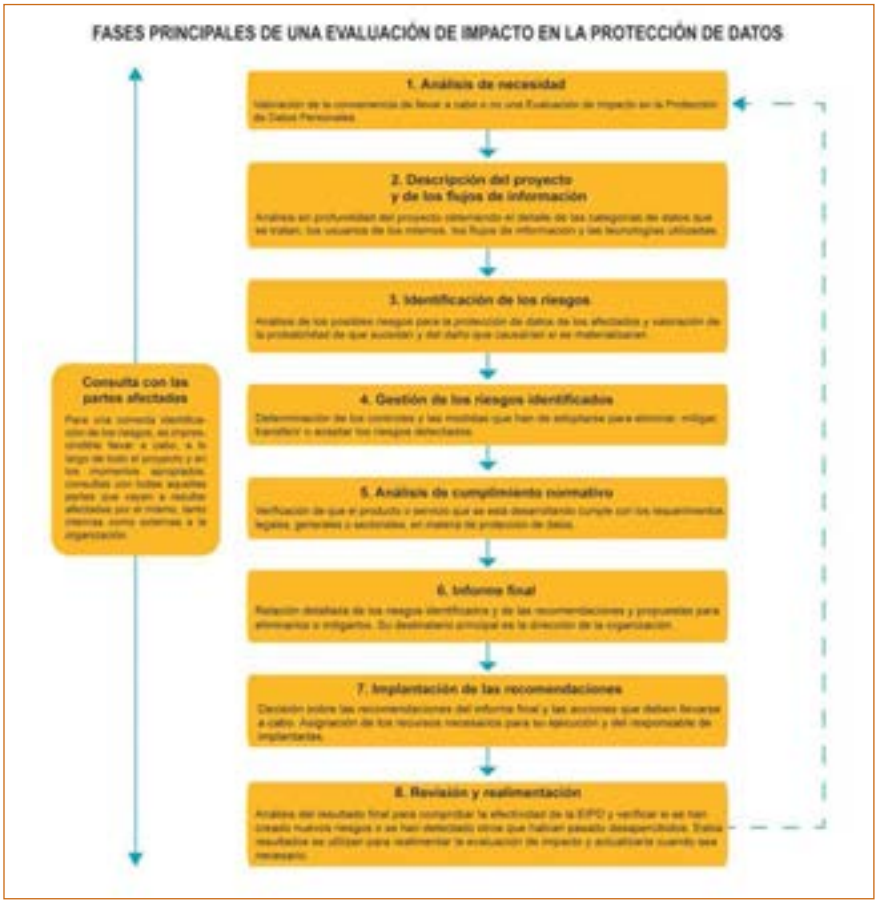
Las EIPD se configuran como un análisis de los riesgos que un producto o servicio puede entrañar para la protección de datos de los afectados y, como consecuencia de ese análisis, la gestión de dichos riesgos mediante la adopción de las medidas necesarias para eliminarlos o mitigarlos. De este modo, las EIPD son herramientas que van más allá de una evaluación de cum-

plimiento normativo –aunque, obviamente, la verificación de dicho cumplimiento formará necesariamente parte de las mismas–, ya que se adentran tanto en las expectativas de privacidad que tienen las personas ante cualquier tratamiento de sus datos personales como en las percepciones generales de la sociedad o, concretamente, de los colectivos más afectados por el tratamiento del que se trate.

## Evaluación de impacto en la Protección de Datos Personales

A la vista de lo anterior, seguramente nos estaremos preguntando ¿en qué situaciones se tendrá que realizar una EIPD? Pues bien, La respuesta a tal interrogante podría venir determinada por el contenido del artículo 35.3 del RGPD, teniendo en cuenta que si bien, a día de hoy, no existe ningún listado específico de tratamientos que requieran de una EIPD, lo cierto es que la Agencia Española de Protección de Datos ( AEPD) ha señalado que sería aconsejable realizar tal evaluación en aquellos casos en los que se utilicen tecnologías consideradas especialmente invasivas con la privacidad como la videovigilancia a gran escala o la utilización de aeronaves no tripuladas[1].

A lo anterior se le ha de sumar el hecho de que la utilización de aeronaves no tripuladas para la prestación de servicios de vigilancia implicará, por regla general, la observación sistemática y a gran escala de zonas de acceso público, generando importantes riesgos para la privacidad de las personas y, por tal razón, resulta altamente aconsejable ( por no decir necesario) que todas aquellas empresas que se dediquen total o parcialmente a esta actividad cuenten con la correspondiente EIPD, con el objetivo de identificar y determinar la entidad de los riesgos inherentes a tal actividad y, lo que es más importante, adoptar las medidas necesarias para eliminarlos o mitigarlos, quedando así a salvo de sanciones y daño reputacional con las pérdidas económicas y de clientes que ello conllevaría.




Apuntado lo anterior, es el momento de referirnos a dos cuestiones que, por su importancia, no pueden ser obviadas. Son las siguientes:

a) El Delegado de Protección de Datos será el encargado de asesorar al responsable del tratamiento durante la realización de la EIPD, y también podrá asumir el rol de coordinador del equipo encargado de su elaboración.

b) De conformidad con lo señalado por el artículo 36 del RGPD, el responsable del tratamiento deberá de formular una consulta previa a la Autoridad de Control antes de proceder a tratar los datos cuando, a la vista del resultado de la EIPD, se muestre que dicho tratamiento entrañará un alto riesgo si no se toman medidas para mitigarlo.

En definitiva, y como conclusión, la vigilancia mediante el uso de Drones puede resultar altamente efectiva y eficaz tanto para los usuarios como para las empresas de seguridad y, con toda probabilidad, conllevará una importante reducción de costes para las últimas, aunque ello no permite ignorar el hecho de que, el uso de esta tecnología, resulta particularmente invasivo con la privacidad de las personas y, por lo tanto, es muy aconsejable que las empresas de seguridad, que pretendan prestar tales servicios, se vayan adaptando a las disposiciones del RGPD, siendo un paso inicial la elaboración de la EIPD. ●

*Foto: Feeepik*

[1].- Guía para una evaluación de impacto en la protección de datos personales. AEPD 2014

Contactos de empresas, p. 9.

**TONI CABALLERO.** CEO RPAS FORMACIÓN

# Una apuesta por la **profesionalización**

Desde la regulación del sector a mediados del año 2014, el sector de los RPAS (aeronaves controladas remotamente) o más conocidas coloquialmente como drones, ha experimentado un cambio y avance sin precedentes. Con un crecimiento del sector vertiginoso, que ha situado las cifras de creación de operadores profesionales en las 1.830 altas, según datos de la Agencia Estatal de Seguridad Aérea.

NO obstante, cabe reconocer que este crecimiento de operadores censados se ha estabilizado en el último semestre, experimentando un aumento mucho más comedido y dejando atrás las cifras del pasado año, que fueron superlativas. Crecimiento que se ha pausado debido a diversos factores, como lo podrían ser la carencia de una legislación que permita realizar operativas en lugares tan necesarios e importantes como entornos poblacionales o urbanos, la posibilidad de realizar vuelos sobre determinados grupos de personas, o la posibilidad de volar en zonas de espacio aéreo controlado; todo derivado de una legislación «definitiva» que está por venir y que lleva en standby un importante número de meses, debido a la falta de gobierno en nuestro país. Si además le sumamos el incremento de control e inspección de cada uno de los operadores por parte de la Agencia Estatal de Seguridad Aérea, en base a unos requisitos normativos que ya deben empezar a cumplirse a rajatabla y que burocráticamente suponen una labor bastante tediosa para los operadores, que en la mayoría de los casos nada sabían de aeronáutica, operaciones aéreas y conceptos de seguridad al respecto, pues nos plantamos en un escenario que no requiere sino otra cosa que la profesionalización.


Por otro lado, a pesar de estas posibles trabas comentadas en última instancia en el párrafo anterior, el sector está creciendo y lo hace cada vez más con una coherencia y actitud muy determinante. Aquellos que se han embarcado o lo pretenden hacer en un futuro inmediato en este apasionante mundo de las operaciones aéreas mediante el uso de RPAS, están tomando decisiones y llevando a cabo actuaciones cada vez más completas y bien planteadas. Están realizando mejores y mayores planificaciones de sus proyectos empresariales y se está llevando a cabo una interesante y potente fusión entre proyectos altamente creativos,

de fuerte carga de I+D+i, con meticulosos y estudiados planes de negocio que auguran cifras más que tangibles a medio y largo plazo. Pero no obstante, volvemos al mismo punto que sigue siendo un freno para el sector, las trabas legislativas momentáneas impiden llegar más allá y hasta que no salga a la luz ese futuro marco regulatorio, los operadores, así como los futuribles, no pueden hacer otra cosa que ir preparándose para lo que está por venir.

En base a todo lo expuesto anteriormente es cuando entran en juego los centros de formación. Ya que se hace imprescindible una correcta e incipiente instrucción de todos los pilotos y resto de actores participantes en las operativas aeronáuticas llevadas a cabo con RPAS. Y mucho más si el futuro marco regulatorio va a abrir las puertas a realizar actuaciones profesionales en entornos mucho más sensibles a nivel de seguridad. A tal efecto, de buen grado serán necesarios cambios a su vez en esta importante parte de este sector, ya que este tipo de operativas requerirán de coordinaciones mucho mayores con distintos estamentos y todo el mundo deberá estar perfectamente preparado y capacitado para ello.

Por otro lado, el aumento del abanico de opciones posibles para realizar trabajos aéreos de muy distinta índole, abre las puertas a la generación, cada vez más, de cursos específicos que utilizan los RPAS como herramientas más que excepcionales para llevarlos a cabo. Operativas, por ejemplo, relacionadas con la seguridad y rescate en costas, áreas montañosas, espacios turísticos al aire libre, infraestructuras críticas, control y vigilancia de zonas residenciales, etc. Y las cuales precisan de una formación mucho más concreta y que enseñe al alumnado una serie de protocolos que les ayuden tanto a la realización segura y eficaz de la operativa, así como a trabajar de forma correcta y en plena consonancia con el cumplimiento del actual marco regulatorio. Porque no nos olvidemos de que un operador de RPAS debe estar atento, en la elaboración de sus planes de vuelo, a elementos como la proximidad de aeropuertos, helipuertos y aeródromos, proximidad a entornos urbanos, paso de personas, espacios naturales protegidos, zonas restringidas al vuelo fotográfico y videográfico, áreas influenciadas por campos electromagnéticos, condiciones meteorológicas previstas y un largo etc., que sí o sí requieren de la adquisición de estos conocimientos a través de correctos planes formativos.

El número de escuelas ha aumentado en los últimos meses y el abanico de posibilidades ha crecido en consonancia y de forma muy diversa, pudiendo encontrar desde cursos más clásicos como el de filmación y fotografía, pasando por cursos de mecánica de drones, análisis de imágenes (fotogrametría, agricultura de precisión, inspección de infraestructuras); a cursos más vanguardistas como lo son el de montaje de drones de carreras, curso de

emergencias y salvamento, o el curso de creación de un negocio de drones. Todo con la simple y llana intencionalidad de especializar y profesionalizar aún más un sector para el cual ya no hay marcha atrás. ●

*Fotos: RPAS Formación*

Contactos de empresas, p. 9.

**YAIZA RUBIO.** ANALISTA DE INTELIGENCIA. ELEVEN PATHS

# El sector de las **aerolíneas** tampoco se libra del **fraude**

Las aerolíneas y las empresas de viajes son también objetivo del cibercrimen. A pesar de que el tipo de fraude en este sector es difícil de detectar, ya que es necesario involucrar a jurisdicciones de diferentes países, ya se han llevado a cabo al menos tres grandes operaciones por parte de organismos policiales como Europol o Interpol. Sin embargo, una variable que sin duda está acentuando su crecimiento es el conocimiento cada día mayor de la existencia de markets en la deep web, como los que se pueden encontrar a través de la red anónima Tor o el uso de Bitcoin para la compra-venta de billetes fraudulentos.

El uso de tarjetas y puntos de fidelidad robados son los métodos más utilizados. Ambos suelen obtenerse mediante el compromiso de ordenadores personales mediante malware, además de otros métodos más sofisticados, como el caso del clonado de las tarjetas. En el caso del carding, con el fin de dificultar el rastreo, siempre suelen realizarse las compras a través de webs de agencias de viajes online y en países distintos al origen y destino del viaje. En cambio, en el caso de la adquisición de billetes haciendo uso de las millas de fidelidad de las aerolíneas, la detección del fraude suele llevar más tiempo, ya que gran parte de los usuarios no consultan con frecuencia su estado de puntos.

Por otro lado, se han identificado otros tipos de fraude menos utilizados pero también más difíciles de detectar. Se trata de la estafa a los seguros en el que las agencias de viajes con cierto volumen de ventas están involucradas y en donde estas incluyen algunas ventas fraudulentas. Otros están relacionados con los empleados de aerolíneas en donde éstos suelen revender los billetes que han conseguido de forma gratuita o con fuertes descuentos. Asimismo, otro tipo de fraude sería el llamado fraude de créditos corporativos en donde, tras atacar a compañías que suelen realizar una gran cantidad de viajes, se hacen compras camufladas dentro de todos los viajes que realizan.

## ¿Quiénes están involucrados?

De forma simplificada, el proceso para materializar el fraude podría traducirse de la siguiente manera. El defraudador llega a hacerse con billetes, ya sea mediante el pago con tarjetas o puntos de recompensa robados o a través de otros métodos más sofisticados, y los ofrece en black markets

con el fin de ponerse en contacto con potenciales compradores. Éstos ponen en conocimiento de los vendedores los detalles del vuelo que les interesa, y el comprador le verifica si puede proveer dicha venta junto con el precio final acordado. Una vez que ambas partes se ponen de acuerdo, el comprador formaliza la compra al market que actuaría como árbitro, pero nunca al vendedor directamente. Sin embargo, en este punto es cuando se puede diferenciar a los distintos tipos de vendedores. Los menos profesionalizados suelen retirar el dinero una vez que el comprador llega al destino o ha hecho el check-in con el fin de ganar confianza con los compradores. Otros suelen exigir que el pago se libere una vez que el comprador compruebe con las aerolíneas que se trata de un billete válido. Sin embargo, existen otros vendedores con más experiencia que suelen ser más flexibles, permitiendo la liberación del dinero de 24 a 48 horas antes de vuelo.

> «Las aerolíneas y las empresas de viajes son también objetivo del cibercrimen, a pesar de que el tipo de fraude en este sector es difícil de detectar»

## Otros tipos de ciberataques

Ya se han detectado casos de familias de malware, campañas de phishing, vulnerabilidades o aplicaciones móviles con el objetivo de engañar al usuario final tratando de suplantar la imagen de las compañías.

Del mismo modo, existen otras amenazas a las que se encuentran expuestos que podrían producir la parálisis de su actividad y, por tanto, el malestar de sus pasajeros. Los ataques hacktivistas o activistas y las filtraciones de bases de datos de clientes pueden tener como resultado elevadas compensaciones económicas. Por ello, para minimizar los riesgos de estas compañías, las medidas a implantar se deberían orientar hacia la modelización de transacciones fraudulentas para una detección precoz de forma automatizada, junto con un servicio de vigilancia de internet focalizado en aquellas otras amenazas procedentes del exterior. ●

*Fotos: Pixabay*

Contactos de empresas, p. 9.

DAHUA TECHNOLOGY

# Haz tu ciudad **más segura**

## Dahua Technology, fabricante y proveedor mundial de productos de videovigilancia con sede central en Hangzhou, China, ha lanzado una solución precisa y eficiente para ciudades seguras, Dahua Safe City Solution

Recientemente, el rápido desarrollo económico y urbano ha generado grandes retos en los centros urbanos. Estos desafíos son la delincuencia, las amenazas terroristas, la gestión del tráfico y hasta los desastres naturales. La insuficiencia de mano de obra y la capacidad del sistema para proteger a las ciudades de estos retos suponen una gran dificultad. Por lo tanto, encontrar una solución útil y segura para controlar y gestionar estas amenazas es importante para que una ciudad funcione correctamente.

DAHUA ha creado una solución avanzada de ciudad segura para permitir que policías, autoridades de tráfico u otros departamentos puedan hacer frente a las amenazas de seguridad utilizando menos fuerza policial, ofreciendo una respuesta más rápida. La solución ofrece de principio a fin cámaras confiables, plataforma integrada y tecnologías inteligentes para asegurar que las ciudades estén bien protegidas y funcionen eficientemente.

**Dahua Safe City Solution está diseñada atendiendo a cuatro aspectos esenciales.**

• Prevención fiable a través de tecnología de reconocimiento facial elaborada con el algoritmo de reconocimiento de cara Nº1 en el último resultado de LFW (Labeled Faces in the Wild). El reconocimiento facial Dahua puede identificar de forma efectiva a los sospechosos en áreas clave de la ciudad como el centro, centros de transporte, fronteras de alto riesgo e infraestructuras restringidas instantáneamente. De hecho, más de 100 equipos de cámaras de reconocimiento facial ya se han desplegado para cubrir los centros de transporte más importantes de Hangzhou durante la Cumbre del G20.

• Respuesta en tiempo real a través de la plataforma integrada. La plataforma integrada se encarga del comando unificado y del almacenamiento centralizado de datos para proporcionar una respuesta rápida de emergencia y un intercambio de información entre sistemas o entre departamentos. Gracias a la colaboración entre departamentos, la plataforma integrada garantiza la respuesta a incidentes en tiempo real y una mejor gestión de recursos policiales. Además, la aplicación móvil y la preparación para emergencias permiten que esta solución sea más eficiente cuando ocurre una emergencia.

• Investigación eficaz mediante potente sinopsis de vídeo. La sinopsis de vídeo es una típica herramienta analítica inteligente que permite una investigación de delitos más rápida y precisa. Proporciona un breve resumen que incluye todos los objetos en movimiento de un vídeo largo, y admite el movimiento del objeto en función de diferentes características como tamaño, color, dirección y velocidad. A través de esta gran herramienta analítica de da-

tos, los usuarios son capaces de identificar sospechosos en un tiempo muy corto.

• Mantenimiento del sistema más sencillo a través de la plataforma de mantenimiento automático.

Debido a los entornos de trabajo complejos, la calidad de vídeo de los dispositivos puede deteriorarse después de mucho tiempo de funcionamiento. Los trabajos de mantenimiento para mantener la calidad del vídeo y la calidad del almacenamiento se convertirán en un gran problema. Con la ayuda de un diagnóstico inteligente, la detección de mal funcionamiento del equipo puede realizarse mediante plataforma de mantenimiento automático. Ayuda a reducir las interrupciones del servicio OPEX y el servicio significativamente.

Utilizando tecnología avanzada (cámara de 4K de alta resolución, detección térmica, reconocimiento de matrículas, reconocimiento de rostros, detección de conductas, etc.), la solución Dahua proporciona una imagen de vídeo de buena calidad y una detección inteligente en cualquier condición climática. Después de ser utilizado extensamente en muchas ciudades, la Safe City Solution de Dahua se ha demostrado eficientemente y eficazmente en la protección de la ciudad. Además, gracias a su innovación y arquitectura de sistema personalizada, esta solución es flexible para adaptarse al cambio tecnológico y expandirse con el crecimiento de la infraestructura de la ciudad.

**Modelos recomendados:**

**Reconocimiento facial IVS-F7200**

- Tasa de detección de la cara ≥ 98%.
- Tasa de reconocimiento de rostros ≥ 90%.
- Reconocimiento completo en no más de 3s.
- Reconocimiento facial, consulta, lista negra.


**Sinopsis de vídeo IVS-S7200**

- Proporciona un resumen de todos los objetos en movimiento a partir de datos de vídeo sin procesar.
- Soporte para buscar objetos por tipo, tamaño, color, dirección y velocidad en el resumen de vídeo.
- Alto rendimiento de procesamiento.
- Alta eficiencia de extracción.

**Plataforma de gestión urbana segura - DSS**

- Gestión centralizada.
- Fuerte fiabilidad y estabilidad.
- Alta apertura y capacidad de expansión.
- Soporte de aplicaciones abundantes.

**Plataforma de mantenimiento automático - NMS8100**

- Capacidad para diagnosticar la calidad del canal de vídeo en línea / canal de vídeo / calidad de almacenamiento.
- Flujo de trabajo profesional para el procedimiento de mantenimiento normalizado
- Alta apertura, integración perfecta con los principales productos.
- Proporciona una serie de informes para optimizar el funcionamiento del sistema. ●

*Fotos: Dahua Technology*


Contactos de empresas, p. 9.

**MARK COSGRAVE.** EUROPEAN SALES MANAGER, OPTEX (EMEA)

# *«En Optex vislumbramos que los **sensores son la llave** de una lista interminable de **aplicaciones posibles**»*

«Cada vez vemos más aplicaciones para nuestros sensores que no solo están relacionadas con la seguridad, sino también con la utilidad, como alertar al usuario de la hora a la que llegan sus hijos al colegior o reducir la huella de carbono, adaptando el aire acondicionado para adaptarlo al nivel de ocupación del edificio», así lo asegura Mark Cosgrave, European Sales Manager, Optex (EMEA), quien además destaca en la entrevista, entre otros aspectos, que ha sido la aplicación de tecnología digital el principal avance en el campo de los detectores PIR de uso interior y exterior.

**OPTEX lleva más de 35 años dedicada a la fabricación de sensores de detección de intrusos. ¿De qué avances tecnológicos clave ha sido testigo?**

—En el ámbito de los detectores PIR de uso interior y exterior, el principal avance ha sido aprovechar la tecnología digital. De hecho, la mayoría de nuestros sensores de detección de intrusos incluye ahora un microprocesador capaz de medir digitalmente la frecuencia de las señales. Este microprocesador incorpora en su memoria rangos de frecuencias que cubren una amplia variedad de escenarios, lo cual dota al sensor de la inteligencia necesaria para diferenciar entre lo que puede o no ser un motivo real de alarma. Este microprocesador lleva incorporados, por decirlo de algún modo, muchos años de conocimientos y experiencia en el sector, que contribuyen a mejorar su capacidad para tomar decisiones más inteligentes. Le hemos enseñado a reconocer a un ser humano y a distinguir sonidos como el de encender una luz o el de poner en marcha un equipo de aire acondicionado, por lo que ahora es capaz de diferenciar entre estas señales.

También, nuestro sensor PIR interior de

puerta de entrada posee una «Plataforma central» digital que identifica las fuentes de calor, como una unidad de aire acondicionado o de calefacción, con el fin de reducir eficazmente la probabilidad de activar falsas alarmas.
Además de los avances en el campo de los detectores PIR, también hemos desarrollado tecnologías de sensor láser capaces de detectar el tamaño, la distancia y la velocidad de un objeto. Esta precisión ha abierto las puertas a toda una gama de áreas y aplicaciones nuevas, que permiten personalizar al detalle las zonas de detección y el tipo de elementos a identificar, como puede ser un objeto pequeño escondido en una zona controlada o una persona atravesando de forma no autorizada el perímetro.

**—¿Sigue prevaleciendo el uso de la tecnología de infrarrojos pasivos en los sensores de detección de intrusos?**

—En términos de volumen sí, la tecnología de infrarrojos pasivos sigue predominando por encima de las demás, sobre todo en el campo de las aplicaciones residenciales y comerciales. Ofrece detección volumétrica, muy eficaz para la protección interior y de aproximación a los edificios. Utilizados en combinación con circuitos de cámaras CCTV, proporcionan esta primera alerta para el sistema de seguridad y ayudan a rastrear a los intrusos dentro de una zona activando ajustes predefinidos de las cámaras. Sin embargo, en muchas ocasiones es necesario complementar la detección volumétrica con protección perimetral o de accesos, lo cual se consigue mediante la integración de otro tipo de tecnologías de detección: infrarrojos activos, láser o fibra óptica. Las barreras de infrarrojos crean un perímetro virtual «punto a punto», que es útil para asegurar sitios abiertos o para reforzar la seguridad de

recintos vallados. La tecnología láser crea un muro virtual en forma de panel sólido que puede llegar a alcanzar una altura de 15 m; el tamaño del objetivo puede definirse mediante el software de gestión del dispositivo. Otra forma de proteger perímetros vallados y de detectar si hay personas intentando cortar o saltar las vallas, consiste en fijar sensores de fibra óptica en la red o material de la propia valla.
Cuanto más complejo o sensible es un recinto, más probabilidades hay de implantar una variedad de tecnologías de detección de intrusos.

**—Ha mencionado el uso de sensores en los sistemas CCTV. ¿Cómo coexisten los sensores físicos con los dispositivos de vídeo detección de movimiento o las cámaras inteligentes?**

—Algunos expertos del sector consideran que ambos tipos de dispositivos compiten entre sí, pero nosotros pensamos que sus funciones son complementarias. Como hemos dicho antes, la mayoría de los sensores físicos son inteligentes y pueden analizar la señal que están detectando para diferenciar si su origen es un ser humano, una fuente de aire caliente, vegetación, etc., y cada vez son más inteligentes y más enfocados en una tarea: detectar intrusos o presencias, sean cuales sean las condiciones de iluminación y meteorológicas. Su limitación es que al no ser una tecnología de vídeo, este tipo de sensor nunca será capaz de proporcionar la información adicional

que ofrecen los análisis de vídeo, como clasificación de personas, niños/adultos, sexo, matrícula o reconocimiento facial, escenario dentro de la escena, etc. No obstante, debido a que los sensores no se basan en los cambios de pixelación (sino en los análisis de frecuencia), resultan extremadamente fiables para detectar presencias o movimientos, reduciendo así el nivel de falsas alarmas al mínimo y la cantidad de alarmas no detectadas casi a cero.

Cada vez vemos más y más casos de conexión directa de nuestros sensores a cámaras IP para activar ese primer evento, algo de vital importancia para los sistemas de seguridad condicionados a eventos, ya que primero permite dirigir la cámara al lugar exacto de la intrusión, y después la inteligencia de la cámara toma el control para añadir una capa adicional de información y definición del escenario.

**—¿Cuál es el siguiente paso para los sensores OPTEX?**

—Mejorar la conectividad y facilitar la integración son nuestros objetivos permanentes. Queremos seguir mejorando la conectividad de nuestros sensores, aprovechando los desarrollos de estos últimos cinco años de trabajo en conectividad inalámbrica para paneles de alarma y conectividad e integración IP con plataformas de Video Management Software (VMS) para aplicaciones CCTV.

La siguiente fase es integrarlos en una amplia gama de sistemas diferentes, como la gestión de edificios, la automatización de hogares y el control de accesos, entre otros muchos. De hecho, cada vez vemos más aplicaciones para nuestros sensores que no solo están relacionadas con la seguridad, sino también con la utilidad, como alertar al usuario de la hora a la que llegan sus hijos del colegio, o reducir la huella de carbono, adaptando el aire acondicionado para adaptarlo al nivel de ocupación del edificio.

Además, creemos que nuestros sensores láser también tienen un amplio campo de desarrollos potenciales por delante. Acabamos de lanzar la última generación que ofrece un nivel de velocidad y precisión de detección con capacidad para detectar incluso objetos de solo 2 cm, con lo que superar a nuestro sensor sería como batir un nuevo récord mundial de los 100 metros. A ángulos de 30 grados, es posible incluso detectar a personas corriendo a una velocidad de hasta 45 km/h.

**—¿Contemplan nuevos mercados o aplicaciones para los sensores físicos?**

—Por supuesto que sí, sobre todo para nuestros sensores de tecnología láser. Dado nuestro nivel de precisión y de personalización, cada vez recibimos más solicitudes para co-desarrollar sistemas de seguridad. Esto incluye la detección de personas atrapadas en pasos a nivel con las barreras bajadas, una solución que ya se ha implantado en más de 100 pasos a nivel en el Reino Unido, y que está despertando gran interés en los principales operadores ferroviarios de Europa. Nuestro sistema también ha demostrado una alta capacidad para detectar la caída de personas a las vías del metro o del tren. Otras aplicaciones son capaces de detectar a personas incluso saltando de un puente. En muchos casos es necesario desarrollar un software a medida para adaptarse y cumplir los requisitos específicos de determinados clientes, pero tenemos la capacidad de hacerlo. Por eso, en el futuro nuestro objetivo pasa por desarrollar nuevos algoritmos que se adapten a estos requisitos individuales.

Como hemos comentado anteriormente, también prevemos muchas oportunidades en las aplicaciones de gestión de edificios, donde nuestros sensores contadores de personas permitirían gestionar los servicios del edificio de la manera más eficiente posible.

En Optex vislumbramos que los sensores son la llave de una lista interminable de aplicaciones posibles, que seguirá aumentando a medida que sigan creciendo las necesidades de las personas. ●

*Fotos: OPTEX*

Contactos de empresas, p. 9.

**ENRIQUE BILBAO LÁZARO.** CUEVAVALIENTE INGENIEROS

# Análisis de riesgos para un **departamento de Seguridad**

En una sociedad como la actual, los ciudadanos del primer mundo asumimos como ciertas y «normales» algunas cuestiones que históricamente no lo han sido tanto: nuestro entorno es relativamente seguro y predecible. Podemos llevar a cabo nuestro trabajo, desplazarnos, adquirir productos, disfrutar de nuestras propiedades, etc. El Estado, como agente directo o como regulador de otros agentes (empresas de Seguridad, entidades aseguradoras, etc.), asegura el sistema, poniendo a nuestra disposición servicios y una estructura de relaciones entre las personas y el resto de entidades que la componen, las cuales hacen posible disfrutar de esta burbuja de Seguridad.

NATURALMENTE, la realidad es mucho más compleja que esta mera percepción, y la incertidumbre, los errores y las malas intenciones de terceros llevan a tener que considerar desviaciones respecto a nuestra percepción de Seguridad.

Por otro lado, el concepto de Seguridad tiene un fuerte componente subjetivo, que atiende principalmente a la consideración de seguro como una percepción o sensación más que como un estado absoluto.

Aunque la toma de decisiones sobre inversiones pueda justificarse en percepciones o en sensaciones para un consumidor (me siento inseguro ergo invierto en mi seguridad), difícilmente puede sostenerse esta manera de actuar en un responsable de una empresa, a quien habitualmente se le requiere una justificación razonada y objetiva (dentro de lo posible) para la toma de decisiones.

La principal herramienta para medir la Seguridad y los riesgos que deben afrontarse es el Análisis de Riesgos. Se trata de una herramienta que pretende valorar la posibilidad o contingencia de que una acción (amenaza) se produzca sobre un activo (bien, área, persona, información…), y las previsibles consecuencias que esto supondría. Con ello, se pretende analizar acciones previsibles, y cuantificar a priori los efectos de éstas. Si la herramienta permite considerar en su proceso de análisis el efecto de incluir o no ciertas medidas de Seguridad, es evidente el alto valor que la misma puede tener para justificar la inversión en Seguridad.

## Análisis de riesgos útil para el responsable de Seguridad actual

Naturalmente, a lo largo de los años han surgido múltiples metodologías de análisis de riesgos, adaptadas a las necesidades del momento y del sector al que se dirigían. No es objeto de este artículo analizar las más extendidas en España ni compararlas, ya que se trata de una tarea ingente y evidentemente subjetiva.

En lugar de esto, el artículo pretende compartir una reflexión sobre qué debe incluir un análisis de riesgos que pueda ser útil para un responsable de Seguridad.

La primera consideración a tener en cuenta es el contexto: amenazas y activos afectados que van a considerarse. Este contexto variará evidentemente en cada caso, debiendo cubrir los principales alcances y enfoques del departamento de Seguridad de que se trate. **Ver Grafico 1.**

Independientemente de los algoritmos de cálculo que se consideren, y que varían enormemente de acuerdo con la metodología estudiada, parece fundamental considerar al menos, de

cara a valorar las inversiones a considerar, el resultado del análisis de riesgos antes y después de implementar ciertas medidas de Seguridad. Una consideración habitual es la consideración de riesgos con y sin medidas de Seguridad:

- Riesgo inherente: sin considerar medidas de Seguridad.
- Riesgo residual: considerando medidas de Seguridad.

Para facilitar esta operación es conveniente que la metodología de análisis de riesgos esté ligada una propuesta, más o menos automática, de medidas de seguridad a implementar para paliar sus efectos. Esto permitirá comparar las medidas necesarias con las existentes y configurar un plan de acción tendente a disminuir los niveles de riesgo.

Para aquellos departamentos que han asumido un modelo de mejora continua en la gestión de sus riesgos, el análisis de riesgos es parte del proceso repetitivo en su fase de planificación. La evolución de sus riesgos se planifica mediante análisis de riesgos periódicos, los cuales suelen partir de un análisis de riesgos inicial en el que se consideran los riesgos inherentes y residuales, complementándose periódicamente con evaluaciones de las nuevas medidas de Seguridad que modifiquen los riesgos residuales.

Otra consideración fundamental es cómo se evalúa el impacto y sobre qué aspectos. Aunque existen diversas aproximaciones, es necesario tener en cuenta los intereses de cada responsabilidad de cada área de la empresa. Por ello, es frecuente analizar simultáneamente impactos económicos sobre la salud de las personas, al medioambiente, al patrimonio, legales, a la imagen de la empresa, etc. Todo ello, intentando encontrar escalas equivalentes comparativas entre diversos impactos (¿A cuántos heridos «equivale» una pérdida de 1 millón de euros?); y lo más objetivas posibles, lo que asegurará la coherencia de los análisis de riesgos en diversas instalaciones y momentos temporales.

Otro aspecto importante a tener en cuenta es que las medidas de Seguridad que se analizan (también denominadas controles cuando se habla de seguridad de la información), tengan en cuenta todas las alternativas a disposición de los responsables de Seguridad para disminuir los riesgos:

- Medidas Técnicas.
- Medidas Operativas.
- Medidas Organizativas.

Finalmente, es importante destacar que la metodología empleada sea acorde con normativa internacional de reconocido prestigio como, por ejemplo, las normas ISO 31000, ISO 27001, ISO 27002, MAGERIT II, AS/NZS 4360, ISO/TR 17944:2002.

## Adaptación y aprovechamiento de análisis de riesgos existentes

Las empresas, independientemente de su ámbito de actuación, están cada día más acostumbradas a considerar la gestión de sus riesgos como parte de su propio negocio. Los riesgos políticos, económicos, etc., son analizados por diversas áreas.

Asimismo, es frecuente que diversos ámbitos de Seguridad (seguridad laboral, seguridad de la información, seguridad antisocial) de una empresa dispongan de análisis de riesgos independientes con información valiosa que debe aprovecharse.

Por este motivo, es importante, a la hora de abordar un nuevo análisis de riesgos, considerar la necesidad de adaptar o integrar los análisis existentes y buscar el modo en que toda esta información pueda aprovecharse.

Otra consideración que puede llevar a tener que asumir esta adaptación es la existencia de metodologías o de enfoques de obligado cumplimiento, que marquen ciertas pautas a considerar en los análisis de riesgos. Estas obligaciones de Compliance son frecuentes en ámbitos regulados, así como en lo concerniente a las Infraestructuras Críticas.

**Grafico 1. Activos y Amenazas a considerar según el alcance del área de Seguridad.**


## Análisis de riesgos de Operadores Críticos

Los análisis de riesgos de las Infraestructuras Críticas están regulados por la legisla-

ción y reglamento correspondientes (Ley 8/2011 y Real Decreto 704/2011 que aprueba su Reglamento), así como por los manuales de mejores prácticas y de contenidos mínimos de los documentos que deben entregar los operadores (Plan de Seguridad del Operador, PSO y Plan de Protección Específico, PPE). Pese a que los operadores tienen libertad en cuanto a metodología a emplear, hay algunos puntos básicos que deben asumir en sus Análisis de Riesgos:

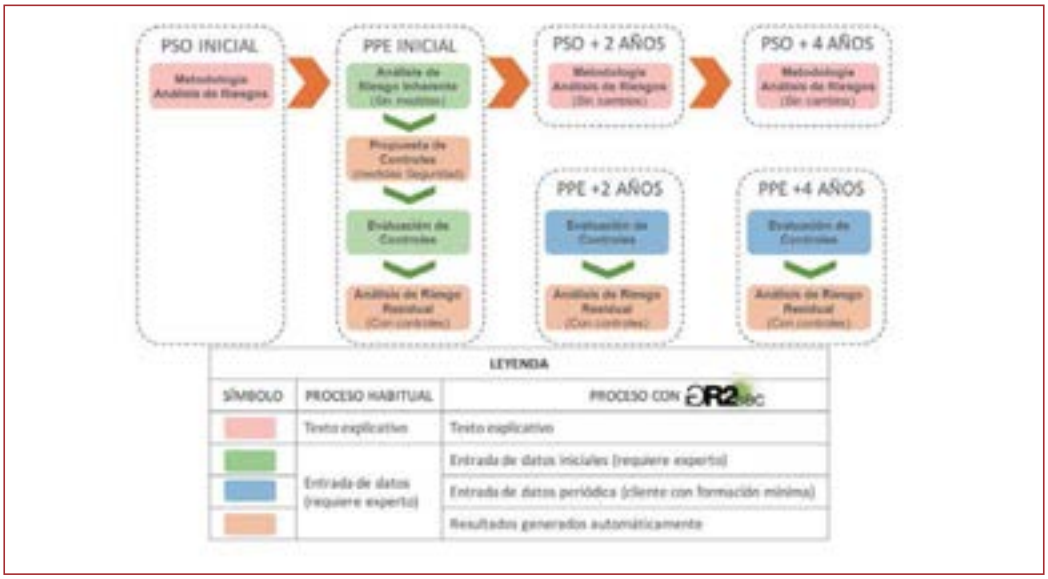



**Grafico 2. Diferencia del proceso de análisis de riesgos para un operador crítico usando GR2Sec.**

- Definición de la metodología de análisis de riesgos en el PSO.
- Realización de un análisis de riesgos de cada infraestructura crítica en su correspondiente PPE, debiéndose repetir cada dos años con la revisión del documento.
- Listado de amenazas consideradas, incluyendo aquellas facilitadas por el CNPIC a cada operador.
- Consideración de amenazas y activos físicos y lógicos, indiferentemente.
- Controles existentes para la mitigación del riesgo.
- Propuesta de controles (medidas de Seguridad) técnicos, operativos y organizativos, de acuerdo al análisis de riesgos, y estructurados como Plan de Acción
- Consideración de controles permanentes y temporales para adaptarse a diversos Niveles de Amenaza Antiterrorista (NAA).
- Consideración en la metodología de los conceptos probabilidad e impacto
- Consideración exclusivamente de los 4 criterios horizontales indicados en la citada Ley 8/2011 (daño a personas, al medioambiente, a la economía nacional y al servicio prestado), para la valoración de los impactos de cada amenaza sobre cada activo.

Debe destacarse, en este último punto, que los análisis de riesgos a incluir en los PPEs consideran el impacto como el daño que sufre la Sociedad, independientemente del que pueda sufrir la empresa. Esto supone que los análisis de riesgos realizados para los PPEs no son completos a nivel empresarial para la toma de decisiones de un departamento de Seguridad, ya que gran parte de las consecuencias no son analizadas.

## Nivel de detalle y complejidad en el desarrollo del Análisis de Riesgos

Por último, es necesario tener en cuenta que gestionar los riesgos de un elevado número de activos con la realización de un análisis de riesgo muy detallado de los mismos puede ser impracticable, especialmente cuando los recursos son limitados. La toma de datos, en especial cuando existe una gran dispersión de activos, suele recaer en personal no especializado en análisis de riesgos o en evaluación de controles existentes, lo que también puede suponer una limitación en cuanto a qué metodología y variables pueden ser las más adecuadas.

En lo referente a estos últimos aspectos, nuestra experiencia desde Cuevavaliente Ingenieros, como empresa enfocada y especializada en análisis de riesgos de Seguridad de todo tipo, nos hace concluir que deben elegirse metodologías y niveles de detalle con posibilidades de adecuación a cada circunstancia.

En este sentido, ponemos a disposición de nuestros clientes nuestra amplia experiencia en análisis de riesgos, incluyendo los de infraestructuras críticas de todos los sectores, así como una metodología y herramienta de gestión de riesgos de desarrollo propio ampliamente utilizada denominada GR2Sec de la que puede obtenerse información detallada en www.gr2sec.com.

Esta herramienta genera automáticamente datos del proceso de análisis de riesgos, pudiendo ser explotada por personal con una formación específica mínima, no necesariamente un consultor. En el gráfico 2 se muestra este proceso para el análisis de riesgos de PSOs y PPEs. ●

*Fotos: Cuevavaliente Ingenieros*

Contactos de empresas, p. 9.

# OFFLINE ANALYTICS - BÚSQUEDA INTELIGENTE EN VIDEOS DESDE CUALQUIER SISTEMA

**Axxon Next 4** presenta la nueva función Offline Analytics, que le permite importar videos de cualquier fuente externa y utilizar herramientas de última generación para buscar a través de ellas. Esta función es especialmente interesante para sistemas de videovigilancia avanzados que no cuentan con herramientas de análisis rápido para grabaciones de video.

Por ejemplo, este tipo de búsqueda puede ser de vital importancia para los cuerpos de la policía. Cuando ocurre un delito, normalmente se tiene conocimiento de la ubicación del incidente, con lo que queda claro qué cámaras podrían contener imágenes de los sospechosos implicados. Estas cámaras podrían ser cámaras especializadas controladas por la policía o cámaras de videovigilancia normales, instaladas, por ejemplo, en tiendas cercanas. Normalmente, se conoce la hora de un incidente en un plazo que va desde unas cuantas horas a varios días. Con esta información, la policía necesita averiguar quién estaba implicado en el delito y tratar de identificar a los sospechosos en el menor tiempo posible, ya que la rapidez es fundamental para resolver un caso.

Axxon Next 4 ofrece un extenso arsenal de herramientas de búsqueda rápidas y precisas para grabaciones de video y, gracias a Offline Analytics, no estará limitado a usarlas con las grabaciones de su propio sistema – sino que, además, puede utilizar estas herramientas con cualquier otro video.

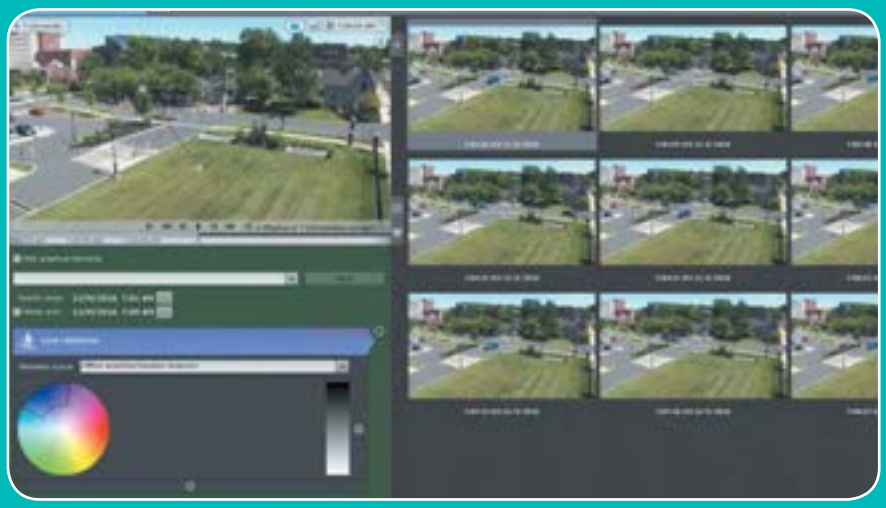
Para conseguir esto, se importa un video de un archivo externo (por ejemplo, con una extensión .avi) al archivo interno de Axxon Next 4. Durante la importación, el programa genera metadatos para el video que después se utilizan para realizar las búsquedas. Es importante señalar que no necesita amplios recursos del servidor por dos razones: el procesamiento no ocurre a tiempo real, y sólo se procesan los fragmentos verdaderamente relevantes.

Después de la importación, todas las funciones de búsqueda desarrolladas en Axxon Next 4 estarán disponibles:

## MomentQuest.

Búsqueda forense por trayectoria (cruce de línea, movimiento entre dos zonas poligonales, movimiento o merodeo dentro de una zona).

A este tipo de búsqueda los siguientes criterios complementarios pueden ser aplicados: color, tamaño (mínimo o máximo) o tipo de objeto. Entre tipos de objetos se diferencian: personas, grupo de personas o vehículos.

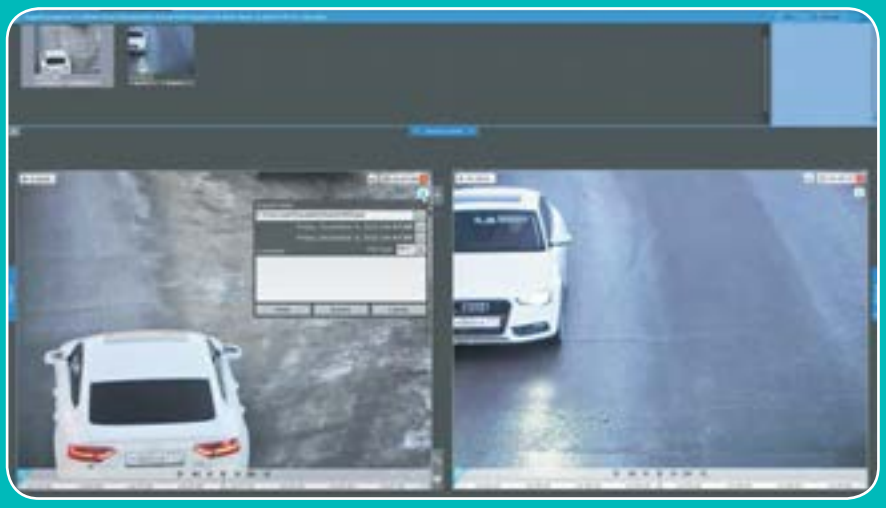


## TimeCompressor.

Búsqueda visual rápida en grabaciones de video (visualizando incidencias sin reproducción rápida)

## Face search.

Búsqueda de caras
en grabaciones de video.

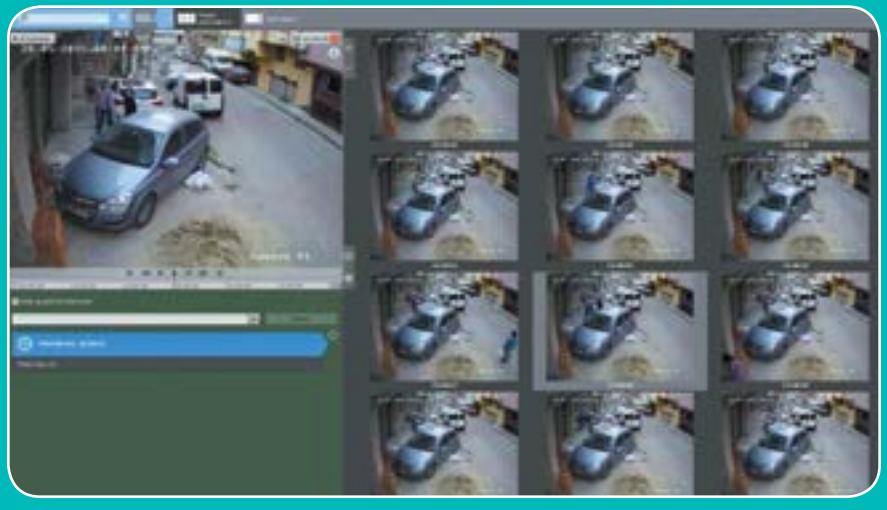


## LPR search.

Búsqueda por matrículas
(coincidencia completa
o parcial).

## TimeSlice.

Búsqueda de una incidencia
cuando se conoce
la hora aproximada.



**En la práctica, el uso de Offline Analytics por las agencias de orden público ha mostrado que estas funciones de búsqueda forense son altamente efectivas.**

axxon
Experience The Next®

**Axxon es una de las principales empresas de desarrollo de software que ofrece soluciones completas para sistemas de seguridad física**

**Más información: www.axxonsoft.com/sp**

**Localice su Partner**

**ALBERTO ALONSO.** BUSINESS DEVELOPMENT MANAGER. AXIS COMMUNICATIONS


# Instalar un sistema de control de accesos

La utilización de sistemas de control de accesos electrónicos es creciente aunque aún lejos de los niveles de implantación que se observan en otros países de nuestro entorno. Esta diferencia puede deberse a cuestiones culturales, pero también sin duda a otros factores tales como la barrera que los costes de instalación y la complejidad de los sistemas pueden suponer.

Si bien el mercado ofrece multitud de alternativas tecnológicas para adecuarse a los diferentes niveles de exigencia y de presupuesto, un factor importante es el de los costes de instalación. A diferencia de otros sistemas de seguridad, el control de accesos tiene un impacto en la actividad de los usuarios que es crítico, ya que afecta a la capacidad de acceder a los lugares de trabajo de un modo ágil y sin dificultar la operación habitual. Por ello, la instalación de estos sistemas debe ser lo más rápida posible, y su configuración sencilla y rápida también, para asegurar un funcionamiento óptimo de un equipamiento que será sometido a una carga de trabajo diaria y exigente. Cualquiera que se haya enfrentado a la instalación de estos sistemas, entiende perfectamente a qué nos referimos, y la complejidad que conlleva este tipo de instalaciones.

Colocar un sencillo controlador autónomo electrónico para leer credenciales (tarjetas, huellas dactilares u otros métodos de identificación) en una puerta de acceso, siendo una tarea especializada, puede ser relativamente simple. El problema se agranda cuando se trata de varios accesos, y necesitamos un sistema interconectado y flexible. Habitualmente esto se consigue con concentradores o controladores multipuerta, a los que se conectan todos los dispositivos de control (lector, sensor de puerta, cerradura, etc.) de cada puerta, con la complejidad de cableado que esto supone y la dificultad para comprobar una vez instalado que la configuración responde a lo requerido por el cliente, y que no se han cometido errores de cableado que conduzcan a comportamientos no deseados.

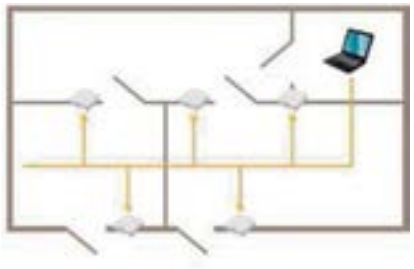
El concepto de controladores de puerta conectados a red Ethernet viene a minimizar esta complejidad y ayudar en la reducción de costes de instalación, especialmente aquellos derivados de los trabajos en el lugar de la instalación que representan mayor inconveniente para el cliente, menor facilidad para desempeñarlos, mayor riesgo de errores, y como consecuencia mayores costes de instalación. Los controladores de puerta en red Ethernet (IP) están pensados para colocar la electrónica de control justo adyacente a la puerta, reduciendo todo el cableado de sensor de puerta, lector, pulsador de salida,

cerradura, etc., a una corta distancia hasta una pequeña caja situada sobre la puerta, junto a ella o incluso en el falso techo. Sin duda esta arquitectura representa un gran ahorro de tiempo y cables, ya que hablamos de conexiones a muy corta distancia (1-3 mts). Otro de los factores que complican y encarecen la instalación es la alimentación de las cerraduras. En una puerta que no ha tenido nunca control electrónico, será difícil que dispongamos de una fuente de alimentación próxima. Los controladores de puerta en red trabajan con alimentación PoE, esto es, que toman la alimentación del único cable que los comunica, el de red Ethernet (Cat 5/6). Con esa alimentación son capaces de alimentar a su vez cerraduras de hasta 0,5 A, lo que supone que pueden alimentar los típicos cerraderos de resbalón que se utilizan en la mayoría de las puertas, así como cerraduras electromagnéticas de media potencia. De nuevo, pensemos en la ventaja de no tener que disponer de fuentes de alimentación específicas, y tendidos de cable calculados para compensar las caídas de tensión asociadas a la longitud de los cableados.

Una vez enumeradas las ventajas respecto al cableado, veamos cómo facilitan la instalación y configuración. Los controladores de puerta en red, pueden configurarse de acuerdo a cómo estarán funcionando en el lugar de instalación antes de desplazarse al mismo. Esto es, podemos hacer toda la configuración en nuestro laboratorio y obtener el esquema de cableado de forma impresa, de modo que el instalador una vez en el lugar del acceso tenga solo que conectar los cables de forma rápida y con un código de colores que minimice las posibilidades de error. La configuración realizada en el laboratorio (lector, cerradura, sensor, pulsador, etc.) no se perderá aunque desconectemos el controlador de la energía para transportarlo a su lugar de instalación.

Finalmente tenemos la parte del software de gestión, que habitualmente se instala en un ordenador a través del cual se gestionarán las acciones de altas, bajas, configuración de grupos, perfiles de acceso, horarios, etc. La utilización de un ordenador representa de nuevo una dificultad. Hay que seleccionar el ordenador adecuado o ver si alguno ya en uso por parte del cliente se adecúa a las necesidades del sistema de control de acceso. En cualquier caso siempre será un equipo asignado para estas funciones y por tanto un operador (recepcionista, centro de seguridad, recursos humanos, etc.) encargado en exclusiva para realizarlas. En el caso de los controladores en red, un software sencillo de control de accesos que permita todas las funciones básicas mencionadas, así como el acceso a los datos y alertas del sistema y sus interacciones con otros sistemas puede estar alojado directamente en la misma unidad. Se trata de un software embebido en las unidades y gestionable desde cualquier ordenador (tablet, etc.) que se conecte a la red (incluso Wireless) en modo cliente web. Esto elimina la necesidad de dedicar un único equipo a la gestión, y por tanto un solo operador bastará con acceder a las unidades e identificarse mediante contraseña para acceder a la administración del sistema. No será preciso que ese equipo de administración esté siempre conectado a la red del sistema ya que todas las acciones y automatizaciones programadas se ejecutan según el programa que

**«La utilización de sistemas de control de accesos electrónicos es creciente aunque aún lejos de los niveles de implantación que se observan en otros países de nuestro entorno»**



se encuentra en cada controlador. Además, en el caso de las bases de datos de usuarios, tarjetas, horarios, etc., es suficiente conectarse a uno cualquiera de los controladores y administrar desde él todas las unidades del sistema, ya que el software se encargará de actualizar los demás controladores de la red. Esto significa que si por algún motivo una vez programados los controladores la red no funcionase, las operaciones de control de accesos se seguirán ejecutando correctamente como si de equipos autónomos se tratase. Por otro lado, la flexibilidad es tal que si se desea añadir otro controlador (puerta / acceso) en cualquier momento, basta con instalarlo y conectarlo a la red, declararlo parte del sistema y automáticamente recibirá todas las bases de datos necesarias para funcionar. Esto último sería imposible si se tratase realmente de controladores autónomos no conectados entre sí.

En el caso de que fuera preciso acceder a funciones de control de accesos más complejas (anti pass back, gestión de visitas, etc.) no contempladas en el software embebido en los controladores, siempre es posible (tanto inicialmente como a posteriori) aprovechar la compatibilidad de plataforma abierta (tanto ONVIF como mediante API) para mantener el hardware (controladores de puerta) con la arquitectura mencionada que tantas ventajas aporta, y hacerlo funcionar con aplicaciones disponibles en el mercado, ya sean específicas de control de accesos o del tipo PSIM (plataformas de integración de seguridad), con lo que la inversión del cliente se ve protegida frente a una eventual evolución del sistema.


En definitiva, los controladores de puerta en red minimizan los costes de instalación mediante una simplificación del cableado y una facilidad para el instalador. Aportan flexibilidad al sistema facilitando incluso la instalación de los mismos vía wireless (especialmente útil en accesos tipo barrera de vehículos de difícil cableado) y ofreciendo una gestión sencilla y con reducidos requisitos de hardware adicional. Aprovechan la infraestructura de red existente o la implantación de una nueva red con todas las opciones que el mercado de las TI ofrece. Además su carácter abierto los hace idóneos en los casos en que sea necesaria la integración del control de accesos con otros subsistemas de seguridad (intrusión, CCTV, etc).

Parecería que en control de accesos todas las soluciones son similares, pero a la hora de instalar, algunas como las que se apoyan en las redes Ethernet suponen una evolución de gran valor tanto en la contención de los costes de implantación como en la de los futuros costes de adecuación y modificación para necesidades no contempladas inicialmente. Un valor que el instalador apreciará de inmediato y que se reflejará sin duda en el Coste Total de Propiedad (CTP) al que hará frente el cliente final a lo largo de la vida del sistema. ●

*Fotos: Axis Communications*

Contactos de empresas, p. 9.

SE CELEBRÓ LA TERCERA EDICIÓN

# CONGRESO ADESyD "Compartiendo (visiones de) Seguridad"

## El evento se presenta como una oportunidad para el análisis y para la presentación de propuestas rigurosamente elaboradas

La Asociación de Diplomados Españoles en Seguridad y Defensa (ADESyD), celebró en Madrid, el pasado 29 de noviembre, el "III Congreso ADESyD", manteniendo el lema de las dos ediciones anteriores: "Compartiendo (visiones de) Seguridad".

El "III Congreso ADESyD" pretende ser un foro para compartir visiones, tanto del contexto presente como del uso de los recursos disponibles para construir el futuro.

Los acontecimientos políticos y militares vividos en los últimos meses a nivel mundial incrementan la incertidumbre sobre el porvenir, pero también abren la puerta a nuevas oportunidades.

La bienvenida a los asistentes consistió en unas palabras de Jesús Alonso Martín, Director de Desarrollo de negocio, ISDEFE; María Angustias Caracuel Raya, Presidenta de ADESyD y Directora de Spanish Women in International Security (SWIIS); y José Díaz Toribio, Coordinador General del Congreso ADESyD. La inauguración estuvo a cargo de Josep Piqué, economista, exministro de Asuntos Exteriores y miembro del Consejo de Honor de ADESyD.

A continuación comenzaron las ponencias, que es estructuraron en cuatro paneles. El primero sobre Seguridad Nacional; el segundo y el tercero sobre Seguridad Internacional; y el cuarto sobre el tercero sobre Seguridad público-privada. Se trataron temas como los desafíos en la vigilancia de fronteras, la estrategia de seguridad aeroespacial, la seguridad en el discurso del gobierno británico tras el Brexit, la ciberdefensa, la Inteligencia aplicada a la lucha contra el terrorismo, la formación del personal de seguridad privada en España o la colaboración público-privada como mecanismo clave en la lucha contra el terrorismo yihadista, entre otros.

De la clausura se encargó José María Barreda, Presidente de la Comisión de Defensa del Congreso de los Diputados. ●

*Fotos: ADESyD.*

LA ASOCIACIÓN ESPAÑOLA DE EMPRESAS DE SEGURIDAD CELEBRA SU 35 ANIVERSARIO

# 35 años **dinamizando la industria de la Seguridad**

Bajo el lema «35 años dinamizando la industria de la Seguridad» la Asociación Española de Empresas de Seguridad, AES, celebró su trigésimo quinto aniversario en un encuentro celebrado el pasado 29 de noviembre en Madrid en el que reunió a asociados, profesionales del sector de la seguridad y medios de comunicación. Durante el evento, que contó con la intervención del Mago More, se procedió a la entrega de los reconocimientos AES 2016.

EL encuentro comenzó con la exposición de los informes de la Asamblea que incluyeron el informe de gestión, así como el «Documento de Recomendaciones para el diseño de medidas de Seguridad Física y Electrónica a incluir en los planes de protección específica en IC». Previamente, Antonio Escamilla, vicepresidente de AES, presentó el «Manifiesto de AES de 2016 a 2019», hoja de ruta para los próximos años, en los que, entre otros aspectos, la asociación potenciará y apoyará un sistema normativo europeo para el impulso del mercado válido para los consumidores y la industria del sector; un enfoque de mercado único para el ensayo, auditoría y certificación en la industria de la seguridad privada; un sistema válido en toda Europa para reconocimiento de capacitaciones y cualificaciones; un mercado único para la prestación de Servicios de Sistemas de Seguridad; así como apelará al Gobierno de España para que incluya los aspectos de seguridad como parte de sus trabajos en el futuro relativo a las ciudades inteligentes.

**Un momento del 35 aniversario de la Asociación Española de Empresas de Seguridad (AES).**

Posteriormente el Mago More ofreció una amena exposición sobre «Cambio positivo y oportunidades de negocio» donde destacó que vivimos en un «mundo pleno donde no hay fronteras» y en constante cambio, al que las empresas deben adaptarse y saber encontrar las oportunidades y apostar por la innovación. Tras poner ejemplos de empresas que han sabido reinventarse y adaptarse a las necesidades de los nuevos clientes –«el cambio más radical es el cliente», matizó–, More hizo hincapié en que son las personas que están en las empresas «aquellas que son realmente innovadoras».

La última de las intervenciones corrió a cargo de Joao Saint-Aubyn, de Roland Berger, quien abordó Seguridad 4.0, analizando la transformación digital en las empresas, y de manera concreta en el ámbito de España.

Durante el encuentro se procedió a la entrega de los «Reconocimientos AES 2016», que este año recayeron en María Valcarce, directora de Sicur; Javier García, director de Normalización de AENOR; Antonio Manzanaro, ex miembro de la Junta Directiva de AES; y José Antonio Martínez Ortuño, ex secretario de AES.

Además, durante el acto se procedió a la entrega de sendos reconocimientos a Carlos Alonso, Gerente de Grandes Cuentas de Bosch Security Systems, fallecido el pasado año, por parte de AES y la Unidad Central de Seguridad Privada, que fueron recogidos por su viuda.

*Texto y Fotos: AES/Gemma G. Juanes.*

Vista general del 35 aniversario de AES.

La viuda de Carlos Alonso, recoge el reconocimiento de la AES de manos de Antonio Pérez, presidente, y Antonio Escamilla, vicepresidente, respectivamente de la Asociación; así como de un representante de la Unidad Central de Seguridad Privada.

Reconocimiento AES a Javier García, director de Normalización de AENOR.

Mago More en un momento de su intervención.

Reconocimiento AES a Antonio Manzanaro, ex miembro de la Junta Directiva de AES.

Reconocimiento AES a María Valcarce, directora de Sicur.

Antonio Escamilla, vicepresidente de AES, durante su intervención en el 35 aniversario de AES.

Antonio Pérez, presidente; Francisco Ramos, tesorero; y Julio Pérez, secretario de la Junta Directiva, de AES.

**LA ASOCIACIÓN DE DIRECTIVOS DE SEGURIDAD INTEGRAL (ADSI) CELEBRÓ SU 20 ANIVERSARIO**

# Cena Anual **ADSI 2016**

La Asociación de Directivos de Seguridad Integral, ADSI, celebró en Barcelona su Cena Anual ADSI 2016, en el transcurso de la que se procedió a la entrega de los Premios ADSI 2016, que pretenden el reconocimiento público de aquellas personas o entidades, privadas o públicas, nacionales o internacionales, relacionadas con la Seguridad Privada o Pública, cuya actuación se haya hecho merecedora de dicha distinción.

EN el marco de la Cena Anual 2016, se llevó a cabo la entrega de los Premios ADSI 2016, que en esta ocasión han recaído en:

—Premio ADSI en «Agradecimiento a la tarea en favor de la seguridad», que esta edición recayó en Eligio Landín López, Facultativo Jurídico del CNP desde 1990, adscrito al Departamento Jurídico de Seguridad Privada de la Jefatura Superior de Policía de Cataluña.

—Premio ADSI 2016 en «Reconocimiento a la trayectoria profesional», otorgado a José María Vilamajó, presidente de Winterman, por su trayectoria de más de 43 años trabajado para la buena reputación del sector de la Seguridad Privada y más específicamente en el de los detectives privados.

—Premio ADSI 2016, «A los Valores Humanos relacionados con la Seguridad», que recayó en la Guardia Civil Mónica Alborés Noya, que poniendo su vida en peligro, evitó que un ciudadano pusiera fin a su vida lanzándose al vacío desde un puente el día 4 de julio de 2016, en la carretera AC-550 a la altura del puente de Ceilán, del término municipal de Outes provincia de A Coruña, cuando circulaba con su vehículo particular.

—Premio ADSI 2016 «A los Valores Humanos relacionados con la Seguridad», otorgado al Inspector de la Policía Nacional Sebastián García Oliver, por su actuación en el accidente de tráfico en el que intervinieron dos vehículos y un camión, ocurrido el día 24 de agosto de 2016, en la autovía A7 dirección Murcia, en el que puso su vida en peligro al introducirse por la ventanilla de uno de los coches accidentados, que estaba ardiendo, para extraer al ocupante que estaba inconsciente en su interior.

—Premio ADSI 2016 «A los Valores Humanos relacionados con la Seguridad», al Caporal de la Policia de la Generalitat Mossos d'Esquadra David Villarejo Estebanell, por su decidida actuación en un incendio detectado durante un servicio en un edificio de la localidad de Terrassa, la noche del día 10 de julio de 2016, desalojándolo en su totalidad y con ello salvando la vida de sus ocupantes.

—La Junta Directiva de ADSI otorgó el «Premio Especial 2016 a la Intervención de Armas de la Comandancia de la Guardia Civil de Barcelona» sección de Seguridad Privada, por su actuación a lo largo de años de Servicio a la ciudadanía y especialmente al sector de la Seguridad Privada. Recogió el premio el Capitán Interventor, Don Miguel Ángel Quesada Olmos.

—La Junta Directiva de ADSI decidió otorgar un «Premio Especial 20 Aniversario a: la revista Seguritecnia.

Miembros de la Junta Directiva de ADSI junto con algunos socios.

Galardonados con los Premios ADSI 2016.

Francisco Poley, presidente de ADSI, junto a los expresidentes Eduard Zamora (a la dcha.) y Juan Vilanova.


Contactos de empresas, p. 9.

EL ENCUENTRO SE CELEBRÓ EN MADRID

# FF Videosistemas: Apostando por la innovación y tecnología

## Durante el encuentro se procedió a la presentación del nuevo software GStatus-Net

Bajo el lema «Apostando por la Innovación y Tecnología» FF Videosistemas organizó el pasado 23 de noviembre, en colaboración con la Asociación Española de Ingenieros de Seguridad (AEINSE), un encuentro donde los profesionales tuvieron la oportunidad de conocer de primera mano el software de gestión G-SIM y el lanzamiento del nuevo software GStatus-Net, único en el mercado, que monitoriza el estado de mantenimiento de una instalación.

La presentación del acto, que tuvo lugar en el Hotel Sefutbol, en Las Rozas (Madrid), contó con la participación del presidente de AEINSE, Pedro Carpintero, quien realizó una breve presentación de la asociación y sus objetivos, entre los que destacó potenciar la figura del ingeniero de seguridad como figura indispensable en las instalaciones de sistemas de seguridad.

Posteriormente, Francisco Férez, director gerente de F.F. Videosistemas, agradeció a los profesionales congregados su asistencia y la confianza depositada desde hace más de 20 años hasta convertirse en una compañía referente en el sector de la seguridad. Y Fernando Blanchart, técnico de márketing de la empresa, hizo un repaso de la trayectoria de la compañía.

Francisco Férez, director gerente de F.F. Videosistemas en un momento de su intervención.

A continuación tomó la palabra Javier Tallón, director comercial de F.F. Videosistemas, para presentar la historia y evolución del Software de Gestión Geutebrück Security Information Management. G-SIM es una aplicación totalmente escalable desde su origen que permite una potencia sin precedentes: un único servidor puede operar sin límite de cámaras ni grabadores.

Posteriormente, tomaron la palabra Ana Mazo, project manager de F.F. Videosistemas, y Alberto Ruano, director de Marketing de F.F. Videosistemas, para realizar una demostración en directo de la plataforma G-SIM, donde los asistentes pudieron poner a prueba todas las funcionalidades y la facilidad de gestión del sistema.

Se trata de una herramienta construida pensando en los usuarios, con una interfaz flexible y personalizable. Permite configurar la pantalla y colocar visores de cámara, tours, mapas, con la sencillez de arrastrar y soltar sobre la pantalla todos los elementos de forma intuitiva y siempre en tiempo real.

A su vez es un potente gestor de alarmas, pudiendo establecer proce-

Asistentes a la jornada en el Hotel SEFutbol.

Alberto Ruano, director de Marketing de F.F. Videosistemas, y Ana Mazo, Project Manager de F.F. Videosistemas, durante la presentación Demo de G-SIM

dimientos claros, asignando procesos en forma de checklists, cambiar automáticamente la presentación del usuario para verificar la alarma y transferir una alarma específica para un usuario o grupo de usuarios en caso de alarmas de máxima seguridad.

G-SIM proporciona el nivel más alto de disponibilidad en el control y solución de incidencias del mercado. Permite la continuidad de todos los procesos en caso de fallo del servidor mediante un sistema de failOver. G-SIM regula automáticamente todos los procesos para que el usuario pueda continuar con total normalidad.

El software incluye un sistema de auditoría capaz de registrar todos los procesos de los usuarios y las acciones realizadas, y la posibilidad de generar informes de actividad en diferentes formatos de exportación (PDF, Excel, CSV) y enviar fácilmente por correo electrónico, si se requiere. Igualmente G-SIM facilita la colaboración entre todos los usuarios facilitando el envío de tareas, alarmas y mantener conversaciones mediante mensajería interna.

A continuación, Óscar Sacristán, responsable técnico de F.F. Videosistemas, presentó el lanzamiento del nuevo software GStatus-Net. Este software es una potente herramienta de control de instalaciones que facilita la posibilidad de poder controlar de forma efectiva todas las instalaciones sin importar distancia o número de ubicaciones.

Gstatus-Net permite auditar los errores, pudiendo analizar en profundidad el motivo de la avería para poder actuar.

El sistema controla todas las instalaciones desde un único sistema, permitiendo una sencilla identificación de errores para posteriormente asignar un grado de importancia y procedimiento adecuado de actuación.

Finalizado el acto, los asistentes tuvieron la oportunidad de participar en una visita al museo de la Real Federación Española de Fútbol y pudieron contemplar, entre otros trofeos conseguidos, la histórica copa del mundo conseguida en el mundial de Sudáfrica en el año 2010. ●

*Texto y Fotos: Redacción.*

Javier Tallón, director comercial de F.F. Videosistemas, explicando la historia del software G-SIM


Oscar Sacristan, responsable técnico de F.F. Videosistemas comenzando la presentación del nuevo software GStatus-Net.


Contactos de empresas, p. 9.

EL ACTO TUVO LUGAR EL 17 DE NOVIEMBRE EN MADRID

# Grupo AGÜERO conmemora su 50 aniversario

Más de 100 personas acudieron el pasado 17 de noviembre al acto organizado por Grupo Agüero, encuentro en el que se reconoció la trayectoria profesional del fundador de la compañía Mariano Agüero.

Gustavo Agüero, director técnico de Grupo Agüero, acompañado de su hermano Fernando, relató los inicios de la organización, fruto de la ilusión y la pasión por la electrónica y la seguridad de su fundador. Siempre al servicio de sus clientes y desde la humildad de sus orígenes, gracias a su constancia y adaptación a las distintas realidades y cambios del sector, Grupo Agüero se ha convertido en referente en el sector de la Seguridad en España. Posteriormente, hicieron entrega de una placa conmemorativa.

A continuación, tomó la palabra Mariano Agüero quien agradeció la presencia de todos los asistentes al evento. «Es para mí un placer contar con todos vosotros en una ocasión tan especial, como es el 50 aniversario de esta compañía».

Empleados, proveedores, clientes y amigos compartieron una agradable velada –el evento se celebró en el restaurante El Faro de El Pardo–, en la que además tuvieron la oportunidad de recordar anécdotas y buenos momentos.

Desde Cuadernos de Seguridad, queremos sumarnos a las felicitaciones por su 50 aniversario, deseándoles como mínimo otros 50 años de éxitos.

EL ENCUENTRO SE CELEBRÓ EN MADRID

# Asamblea anual del **Capítulo 143 (España) ASIS International**

## Posterior a la reunión se procedió a la entrega de diferentes premios y reconocimientos a destacados profesionales del sector

El Capítulo 143 (España) de ASIS International celebró el pasado 28 de noviembre su Asamblea anual de socios. Posteriormente, y en el transcurso de un cóctel al que asistieron cerca de un centenar de socios e invitados, se procedió a la entrega de diferentes premios y reconocimientos a destacados profesionales del sector.

Durante la celebración de la Asambleas se efectuaron las votaciones para la elección de la Junta Directiva del Capítulo 143 (España) de ASIS International para 2017. Con la totalidad de los votos de asistentes y representados el equipo elegido para dirigir la organización es prácticamente el mismo que lo ha hecho desde 2013. Este está formado por:

- Juan Muñoz CPP CSMP CSyP, presidente.
- Alfonso Castaño, vicepresidente.
- Nieves Beitia-Lluva, secretario.
- Fernando Andrade, tesorero.

Como vocales fueron elegidos Luis Morte, Ignacio Carrasco, José Gil, Esther Muela, Ignacio Botella, Joan Roda, Pedro Sebastián, Juan Carlos Martin y Carlos Bachmaier.

Como parte del acto se procedió a la entrega de diferentes premios que en esta ocasión recayeron en:

- Juan Gros y Jorge Quintana, vocales desde 2013 hasta 2016.
- Juan Amorós CPP, socio español con residencia en Andorra.
- Fernando Carrillo Cremades CPP, Eduardo González CPP y José Luis Bolaños CPP, que se incorporan al Quater Century Club, formado por los socios que han cumplido 25 años en ASIS International.
- Francisco Javier Sandoval y José Luis Nieto, por la difusión de ASIS España a través de los medios y su lealtad al Capítulo 143, respectivamente.

### Reconocimientos especiales

Los reconocimientos especiales fueron para:

- El comisario principal Esteban Gándara, jefe de la Unidad Central de Seguridad Privada.
- Francisco Muñoz Usano, doctor en derecho, presidente de la Sociedad Española del Derecho de la Seguridad.
- José Luis Bolaños CPP, presidente de ASIS España de 1996 a 1998 y Chief Security Officer de Gas Natural, que recibió el premio Carlos Sánchez Casalderrey, el más importante concedido por ASIS España.

*Texto y Fotos: Asis España*

19º CONGRESO AECOC DE PREVENCIÓN DE LA PÉRDIDA

# Prevenir es ganar

**Durante el encuentro se presentó el último estudio anual sobre el impacto de la denominada pérdida desconocida bajo el título «La pérdida en la gran distribución comercial 2016»**

AECOC reunió en Madrid el pasado 17 de noviembre a cerca de 200 destacados profesionales de las áreas de seguridad y prevención de la pérdida de las principales compañías del país en su 19º Congreso AECOC de Prevención de la Pérdida; un Punto de Encuentro que sirvió para tomar el pulso al sector, así como para compartir aprendizajes y experiencias que ayuden a solucionar un problema que afecta a toda la cadena de valor.

Representantes de empresas de distribución líderes analizaron los desafíos y las tendencias de futuro de las áreas de prevención de pérdida en una mesa debate. En concreto, el debate estuvo protagonizado por el director de Seguridad de DIA, Álvaro Martín; el director de Control de Stock de Mango, Oscar Molins; y el auditor interno de grupo Pyrénées, Manuel Garruta, quienes participaron en una mesa moderada por el responsable del Área de Seguridad de Eroski, Javier Uriarte.

En este sentido, el director de Stock de Mango precisó que «a la plantilla de trabajadores debemos pedirle que venda y no que vigile el producto, pero es verdad que mediante campañas de comunicación y de cierta profundidad se consigue que los propios trabajadores sientan la necesidad de proteger el producto».


Las empresas deben adaptarse al entorno cambiante y las áreas de prevención y pérdida de las compañías no están exentas de esta adaptación. El nuevo contexto legal, los avances tecnológicos, los nuevos formatos de tienda y la venta online y sus implicaciones logísticas son algunos de los cambios que obligan a las áreas de prevención a modificar su estructura y sus procedimientos.

## Reforma del Código Penal

Entre las ponencias destacaron también la del doctor en Derecho y profesor de derecho procesal en la Universidad Complutense de Madrid y en el Colegio Universitario de Estudios Financieros, Jesús Zarzalejos, quien realizó un balance de la reciente reforma del Código Penal. Tras un año de aplicación de la reforma, Zarzalejos analizó las principales consecuencias en la respuesta penal al hurto en el comercio, así como una proyección de nuevas iniciativas planteadas por AECOC para facilitar su correcta implantación.

Zarzalejos explicó que «el objetivo de la reforma no es meter gente en la cárcel, sino evitar que entren a robar en las tiendas», y destacó dos cambios introducidos por la reforma del Código Penal en este sentido: «la agrava-

ción por rotura o manipulación de los sistemas anti-hurto y la sanción especial por multirreincidencia y pertenencia a grupo criminal».

El 19ª Congreso AECOC de Prevención de la Pérdida contó también con una mesa redonda en la que se analizaron los cambios percibidos por las empresas después de esta reforma del código penal, especialmente en las denuncias, la preparación de los juicios, en las pruebas que se presentan y en las sentencias, así como las medidas de seguridad impuestas con la condena. La mesa redonda contó con la participación del jefe de área y responsable de Seguridad de la Agencia Española de Protección de Datos, Andrés Calvo; del Alférez de la Unidad Técnica de la Policía judicial de la Guardia Civil, Daniel Zorzo; y de la Fiscal Decana de la Fiscalía Provincial de Madrid, Patricia Alonso-Majagranzas, entre otros.

Además, el encuentro profesional contó con la participación de destacados responsables del sector en instituciones y empresas de ámbito nacional e internacional. Entre los ponentes se encontraron el profesor de Criminología de la Universidad de Leicester, Adrian Beck; el Senior Loss Prevention manager de Guess, Jerome Bertrume; el auditor interno de AKI, Javier Iglesias; el director de Proyectos Punto de Venta de Covirán, Germán Castillo; el responsable de Pérdida Desconocida de El Corte Inglés, Diego Pilares; la expresidenta y miembro de la Asociación Profesional de Detectives Privados en España, Eva Grueso; y la directora de Seguridad para España y Portugal de H&M, Sonia Guamis. Durante el transcurso del congreso, los ponentes coincidieron y pusieron de manifiesto la necesidad de formar a los trabajadores en materia de seguridad para prevenir las pérdidas.

Durante el congreso se presentó el último estudio anual sobre el impacto de la denominada pérdida desconocida (hurtos comerciales y errores administrativos), titulado «La pérdida en la

gran distribución comercial 2016», que actualiza el índice de la pérdida, profundiza en los criterios para utilizar estos indicadores y evalúa el impacto de la reforma del código penal. La presentación corrió a cargo del responsable de Prevención de Pérdida de AECOC, Javier Blanco, y el Business development director de Consumer Products & Retail en EY, Manuel Fernández. ●

*Texto y Fotos: Redacción/AECOC*

## Estudio «La pérdida en la gran distribución comercial 2016»

Durante la celebración del encuentro se presentó el estudio «La pérdida en la gran distribución comercial 2016», elaborado por AECOC en colaboración con EY, que analiza el estado de un problema que ha supuesto pérdidas de más de 1.778 millones de euros al sector en 2015 entre hurtos comerciales y errores administrativos, lo que representa el 0,84% de todas sus ventas.

En términos de cómo se distribuye la pérdida desconocida, los hurtos comerciales representan el 84% del total y los errores administrativos suponen el 16% restante. Así, los hurtos comerciales en su conjunto –externo e interno– ocasionaron pérdidas de un total de 1.493 millones de euros a las empresas de gran consumo durante el 2015.

El mayor índice de pérdida desconocida se observa en empresas del sector ferretería y bazar con un 1.32%, lo que supone un notable incremento al año anterior, seguido por el sector del textil con un 1.01%, la perfumería con un 0.75%, la electrónica de consumo con un 0.57% y el gran consumo en general con 0.72%.

El ranking de productos más sustraídos se mantiene similar al del año anterior y muestra que el material eléctrico y de iluminación, el maquillaje y las bebidas alcohólicas son los tres productos más hurtados, según las respuestas de los distribuidores. Las empresas continúan enfocándose en combatir el hurto externo invirtiendo, principalmente, en videovigilancia y sistemas anti-hurto, ambos utilizados por casi todas las empresas.

Por otro lado, los servicios de vigilancia se utilizan por el 63% de las empresas y el porcentaje medio de empresas con vigilante alcanza el 27%. Adicionalmente se presentan otros avances tecnológicos como Radiofrecuencia de Identificación (RFID), entre otros.

En lo referente al hurto interno, el estudio muestra un interés creciente en los sistemas de detección del fraude en el punto de venta, utilizado actualmente por el 52% de las empresas, un 44% mediante alertas en caso de que algún tipo de sustracción supere un determinado umbral, y un 8% que utiliza sistemas inteligentes más avanzados de detección de patrones.

**APROSER PRESENTA LOS RESULTADOS DEL ESTUDIO SOBRE «LA PERCEPCIÓN DE LA SEGURIDAD PRIVADA EN ESPAÑA»**

# El 64% de los ciudadanos ve adecuada una mayor presecia **de vigilantes en calles y zonas comerciales**

Cuatro de cada cinco españoles se siente más seguro en los lugares en los que hay presencia de vigilantes de seguridad privada, así se desprende del estudio sobre «La percepción de la Seguridad Privada en España» presentado por la Asociación Profesional de Compañías Privadas de Servicios de Seguridad (APROSER), que ahonda aspectos esenciales que inciden sobre la seguridad privada en nuestro país como son la percepción y valoración del cometido de los vigilantes, los lugares en los que la Seguridad Privada debería consolidar o incrementar su presencia o la protección jurídica y el reconocimiento social de los profesionales.

EL encuentro con los medios de comunicación contó con la presencia de Gonzalo Herrero, CEO de Canal Sondeo, empresa que ha realizado el estudio; Ángel Córdoba, presidente, y Eduardo Cobas, secretario general, de APROSER.

En la encuesta los consultados se pronuncian sobre en qué lugares incrementar la presencia de los vigilantes de seguridad. En concreto, el 64% de los encuestados considera adecuada una mayor presencia de vigilantes en calles y zonas comerciales, priorizando su asistencia en horario comercial, el 48%. Por otro lado, el 45% opta por solicitar mayor presencia de Vigilantes en calles de ciudades en general, y el 43% en las calles y barrios en los que residen.También valorarían positivamente que hubiera vigilantes de seguridad en otros espacios como centros escolares (colegios, institutos y universidades) y en parques y jardines.


En este sentido, España cuenta con una media de un vigilante por cada 600 habitantes, mientras que en Europa es uno por cada 250 habitantes. Ante estos datos, el 72% de los perfiles contrastados cree que no hay suficientes vigilantes por habitante en España y que es necesario asemejar el dato a la media europea. «A este respecto, más de la mitad de los encuestados, el 57%, no sustituiría a los Vigilantes por personal de las Fuerzas y Cuerpos de Seguridad del Estado en determinadas funciones como los controles de acceso», destacó Eduardo Cobas durante la presentación que realizó del estudio.

Con respecto a la percepción que tiene el ciudadano sobre el Vigilante de Seguridad Privada, cabe destacar que el 62% valora como buena o muy buena esta figura, mientras que sólo el 5,7% manifiesta una opinión negativa. Además, aunque para la gran mayoría de los encuestados, el 69%, su percepción no ha cambiado, el 16% recono-

ce que ha mejorado. En este sentido, el 24% señala el factor «sensación de seguridad» como la característica mejor valorada de los vigilantes de seguridad.

Otros motivos que aportan valor al desempeño de las labores de estos profesionales son que las tres cuartas partes, el 75% de los españoles, considera como algo necesario la función del Vigilante de Seguridad, seguido de su contribución a aumentar la seguridad ciudadana en general, el 71%, y por considerarlo una ayuda para la sociedad, el 69%.

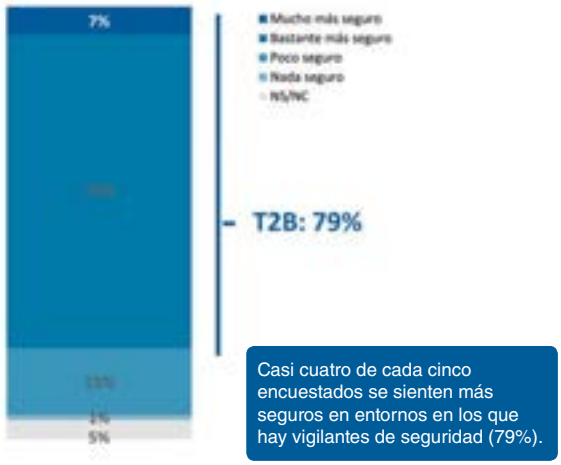
Además, según el estudio, el 66% considera que la profesión de vigilante de seguridad es dura y el 64% indica que está poco valorada. Del mismo modo, el 52% piensa que los vigilantes de seguridad complementan adecuadamente las labores de la Policía y la Guardia Civil.

En cuanto a la protección jurídica, Cobas destacó que el informe recoge que «el 53% intuye que la ley no protege lo suficiente a los vigilantes de seguridad, y el mismo porcentaje percibe que la ley ampara más a los presuntos delincuentes que a los vigilantes de seguridad en el desempeño de sus funciones».

Ante la actual amenaza terrorista internacional, el 72% coincide en dedicar un mayor número de vigilantes en las infraestructuras críticas como son el transporte o las centrales nucleares entre otras.

**SENSACIÓN DE SEGURIDAD EN ENTORNOS CON VIGILANTES DE SEGURIDAD**

Cuando vas a un sitio en el que hay vigilantes de seguridad, ¿en qué medida te sientes más seguro? (Respuesta única) | Base:900




Casi cuatro de cada cinco encuestados se sienten más seguros en entornos en los que hay vigilantes de seguridad (79%).

## El sector de la Seguridad Privada, clave en la economía y sociedad de nuestro país

La Seguridad Privada es un sector que contribuye al PIB nacional y proporciona trabajo a más de 100.000 profesionales, entre los cuales el 90% dispone de contrato indefinido.

En este sentido, y tal y como arroja el estudio, nueve de cada diez encuestados desconoce la aportación del sector de la Seguridad Privada a la sociedad.

Con respecto al reconocimiento social del vigilante de seguridad, continúa siendo un tema pendiente, ya que el 73% de los encuestados cree que esta profesión no tiene el reconocimiento social adecuado.

Durante la presentación del estudio, Ángel Córdoba, presidente de APROSER, recordó aquellos retos que sin duda inciden de forma directa en la percepción de la Seguridad Privada en España. A este respecto, destacó las siguientes cinco prioridades; la necesidad de acometer la trasposición de la nueva Directiva Europea de Contratación Pública, el ajuste del Estatuto de los Trabajadores para un tratamiento más adecuado de las condiciones laborales de los trabajadores en sectores intensivos en mano de obra, la responsabilidad social y subsidiaria de la Administración como licitador y contratante de servicios de seguridad, la finalización y entrada en vigor del reglamento de desarrollo de la Ley de Seguridad Privada 5/2014, y el desarrollo de un modelo de formación profesional para que los futuros profesionales del sector puedan contar con las capacidades y habilidades necesarias, tal como se establece en la nueva Ley como vía complementaria de acceso a la profesión. ●

**LUGARES / SITUACIONES EN LAS QUE DEBERÍA HABER SEGURIDAD**

¿En qué lugares o situaciones en los que actualmente no hay vigilantes de seguridad, te gustaría que los hubiera? (Respuesta abierta) | Base:900


Sólo se muestran los literales mayores del 3%
Pregunta espontánea y posibilidad de respuesta múltiple por lo que la suma de porcentajes puede ser superior al 100%.

A los encuestados les gustaría que hubiera seguridad en las calles, en centros escolares (colegios, institutos y universidades) y en parques y jardines.

*Texto y Fotos: Redacción/Aproser.*

EL ENCUENTRO FUE ORGANIZADO EN COLABORACIÓN CON ISMS FORUM SPAIN

# VI Encuentro de **Cloud Security Alliance España**

El capítulo español de Cloud Security Alliance celebró su sexto encuentro anual el pasado 14 de noviembre en el IE Business School de Madrid, organizado en colaboración con ISMS Forum Spain, con la participación de más de 160 profesionales de la seguridad y la privacidad en cloud computing.

EL presidente de Cloud Security Alliance España, Luis Buezo, y el Chief Academic Officer (School of Human Sciences and Technologies) del IE Business School, Manuel De Villalta, fueron los encargados de dar comienzo a una jornada en la que la Nube, a diferencia de los comienzos de la iniciativa allá por 2010, es ya una realidad en las organizaciones, y la seguridad una cuestión inherente.

La ponencia inaugural correspondió a Eduardo Di Monte, director de Seguridad y Continuidad de Negocio de AGBAR, que planteó su presentación sobre la Nube como un problema y a la vez como una solución. En sus palabras: «Cloud es una realidad que ha llegado para quedarse y que habilita un mundo de oportunidades que permite utilizar datos, analizarlos y, por tanto, hacer uso de los mismos para proteger nuestros sistemas». Di Monte recordaba las cifras de algunos informes del sector, que ponen de manifiesto que el 91% de las organizaciones quiere introducirse en el ámbito Cloud. Pero también hizo referencia a los aspectos problemáticos a tener en cuenta, haciendo hincapié en que, en el desarrollo de nuevas tecnologías ligadas a la Nube, a nivel de diseño no se contempla la seguridad. Por ello, finalizaba su intervención insistiendo en que «lo importante es aprender a utilizar correctamente las tecnologías que operan en la Nube por medio de tres claves: integración, orquestación y automatización».


Marcos Gómez, subdirector de Servicios de Ciberseguridad de INCIBE y miembro de Cloud Security Alliance España y de ISMS Forum, habló de la confiabilidad y la seguridad en la Nube desde el punto de vista de prestador de servicios públicos. La Nube como tendencia, sobre todo a través del móvil como dispositivo conectado, apuntaba Marcos, supone ya la «hiperconexión» de usuarios y, cada vez, de mayor número de empresas cuyos empleados comparten información. «Más del 40% del tejido empresarial y la Administración Pública ya está usando servicios en la Nube», destacaba Marcos.

El mismo desarrollo de servicios en la Nube, señaló Marcos, también supone nuevos riesgos y amenazas, como es el caso de los últimos ataques de denegación de servicio que han sufrido algunos de los principales proveedores de telecomunicaciones.

Como perspectivas y consideraciones a tener en cuenta a la hora de incorporarse a la Nube, Marcos recordaba la Directiva NIS que, entre otras, incluirá la obligación de establecer una estrategia que garantice la seguridad de los proveedores y operadores de servicios esenciales. Seguridad, privacidad, escalabilidad y disponibilidad, serán criterios básicos para la contratación de

servicios en la Nube; también tendrán que considerarse las transferencias internacionales de datos, la confidencialidad de los datos almacenados o la transacción de datos, entre otros.

Uno de los puntos clave del encuentro lo constituyó el análisis del estado de la adopción empresarial y seguridad de los servicios en la Nube, con la presentación de las principales conclusiones de la cuarta edición del Estudio sobre el Estado de la Seguridad en la Nube, informe desarrollado por ISMS Forum, Cloud Security Alliance España, los Capítulos peruano y argentino de Cloud Security Alliance, e ISACA Madrid y Perú.

El estudio consolida las tendencias identificadas en años anteriores respecto de las expectativas sobre la Nube, los requisitos que se exigen a estos servicios y la satisfacción final con los servicios recibidos. Así, las expectativas de seguridad sobre la Nube son muy altas (aunque con un leve descenso), y siguen siendo más altas que los requisitos que se piden (que se mantienen), y más altas aún que la satisfacción final de los usuarios de los servicios de Nube, que también se mantienen.

Las conclusiones del estudio dieron paso a un debate sobre la evolución de la adopción de soluciones y servicios en la Nube, desde una perspectiva centrada en la seguridad de la información, de los datos y de los servicios corporativos, analizando su influencia en la forma en la que se adoptan o no servicios en la Nube. Formaron parte del debate Raúl Pérez, Global Presales Manager de Panda Security; Federico Dios, Service Line Manager de Akamai; Félix Martín, EMEA Security Consulting Lead de HPE; y José Ramón Monleón, Chief Information Security Officer y miembro de la Junta Directiva de ISMS Forum. Como principales conclusiones destacaron la importancia del crecimiento de las expectativas en la Nube, la heterogeneidad de servicios y tecnologías, como por ejemplo la aplicación a Big Data para analizar con mayor precisión las amenazas, y la aplicación del nuevo Reglamento Europeo de Protección de Datos. Respecto al Shadow IT, continúa siendo un problema derivado de la agilidad del uso de soluciones gratuitas, por lo que la solución supone establecer sistemas de control.

Una mesa redonda formada por CISOs estableció un controvertido debate sobre si la Nube, especialmente en su vertiente de seguridad, supone para la Industria uno de los principales ejes para asegurar el éxito de su transformación digital. Participaron, Gianluca D'Antonio, Chief Information Officer de FCC y presidente de ISMS Forum; Manuel Martínez, responsable de Control de Seguridad de Gas Natural Fenosa; Rafael Hernández, responsable de Seguridad de la Información de Cepsa; Miguel Suárez, Jefe de Estrategia de Seguridad de Symantec + Blue Coat; y Javier Santiago, responsable de Ciberseguridad y Network Defense de Trend Micro. Concluyeron que la Nube juega un papel fundamental para la Transformación Digital y, aunque la seguridad no sea el objetivo principal por el que las organizaciones operan en la Nube, en un momento como el actual se convierte en estrategia, con nuevas capacidades y posibilidades con un gran potencial que trasladan la seguridad al rendimiento del negocio.

El profesor Dr. José Luis Piñar, Catedrático de Derecho Administrativo y Vicerector de Relaciones Internacionales de la Universidad San Pablo-CEU, y ex director de la Agencia Española de Protección de Datos, centró su ponencia en los nuevos retos para la protección de datos que supone la Nube. Ilustró su presentación con un ejemplo práctico, en el que evidenció el diseño seguro de automóviles, mientras que mostró que no parece ser igual cuando hablamos de datos de carácter personal, puesto que no nos preguntamos si existe un tratamiento de datos de carácter personal cuando participamos en redes sociales, cuando fabricamos drones o cuando incorporamos nuevas tecnologías. Piñar señaló que con el nuevo marco regulatorio europeo pasaremos de la gestión de los datos al gobierno responsable de la información con principios que van a imperar como el accountability, es decir, la responsabilidad proactiva que dejará en manos de los encargados la toma de medidas, la privacidad por defecto y la privacidad desde el diseño.

La sesión finalizó con la presentación del caso de éxito de Cloubity, startup dedicada a la movilización de aplicaciones para PYMEs y cuyo modelo se basa exclusivamente en la Nube. Manuel Martín, Chief Executive Officer de Cloubity, y su socio, Jordi Rodríguez, fueron los encargados de explicar las ventajas de la evolución de un modelo on premise a un modelo basado en cloud. ●

*Texto y Fotos: ISMS Forum*

CENTRO CRIPTOLÓGICO NACIONAL

# El CCN-CERT resuelve más de 19.000 ataques en 2016

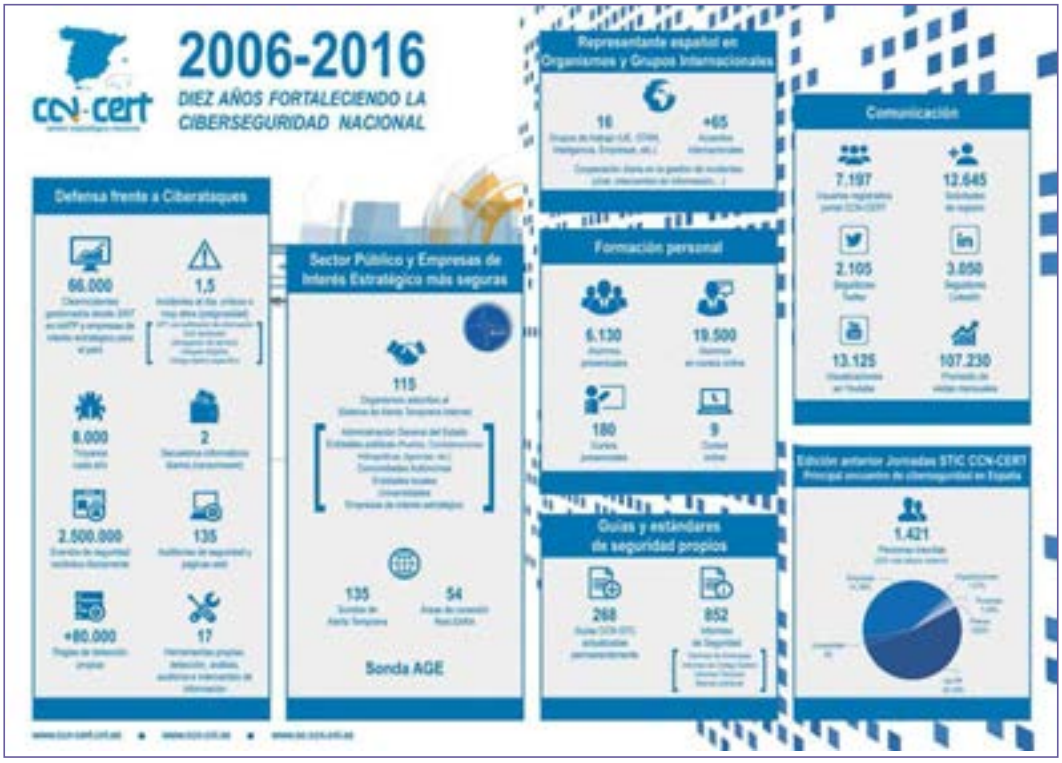
## A sistemas pertenecientes al sector público y empresas de interés estratégico

El CCN-CERT, del Centro Criptológico Nacional (CCN), organismo adscrito al Centro Nacional de Inteligencia (CNI), prevé concluir este año 2016 –datos ofrecidos al cierre de esta edición– con más de 19.000 ciberincidentes gestionados, frente a los 18.232 de 2015. De ellos, más del 3,5% fueron considerados de peligrosidad muy alta o crítica, en base a diversos parámetros (tipo de amenaza, origen, perfil de usuario afectado, número o tipología de sistemas afectados, impacto...).

Estos datos, facilitados a finales de noviembre de 2016, fueron ofrecidos en un encuentro ante los medios de comunicación, que contó con las intervenciones de Luis Jiménez, subdirector general adjunto del CCN, y Javier Candau, jefe de Ciberseguridad del Centro Criptológico Nacional.

El incremento constante del robo y secuestro de información, los ataques sofisticados con herramientas «ad hoc» y los dirigidos contra la disponibilidad de un servicio; la intrusión en todo tipo de dispositivos, con especial hincapié en los equipos móviles; el robo y suplantación de identidad, el sabotaje o la infección por código dañino distribuido a través de correo electrónico, páginas web o redes sociales, son algunas de las principales amenazas observadas en 2016. Así, tal y como explicaron, las causas de este incremento en los ciberincidentes gestionados son:


- Falta de concienciación de los usuarios y desconocimiento de los métodos seguidos por los ataques de ingeniería social y del intento de manipulación que, frecuentemente, acompañan a los ciberataques y que buscan siempre las debilidades del eslabón más débil de la cadena (factor humano).
- La inadecuada gestión de actualizaciones de los programas y aplicaciones en ordenadores, dispositivos móviles o servidores centrales. Las numerosas vulnerabilidades de día-cero descubiertas en 2016 y la rápida explotación de tales vulnerabilidades, ponen de manifiesto la necesidad de implementar una gestión de actualizaciones de seguridad (parches) rápida y completa.
- La mayor superficie de exposición: redes sociales, dispositivos móviles, servicios en la nube, BYOD, etc.
- El aumento del número de muestras de código dañino detectadas, tanto para equipos fijos como, en particular, para las plataformas móviles. En este sentido, los mensajes de correo dirigido («spear phishing») siguen siendo una fuente clave de este tipo de infecciones.




• La profesionalización de los atacantes, con independencia de sus objetivos, que provoca una sofisticación creciente de las amenazas.

• Organizaciones poco proclives a comunicar incidentes por cuestiones de prestigio, reputación online, etc.

• Poco personal dedicado a la seguridad y con la formación suficiente, con escasa vigilancia de los sistemas y equipos, siendo fácil para un atacante el movimiento lateral por las redes internas de las organizaciones.

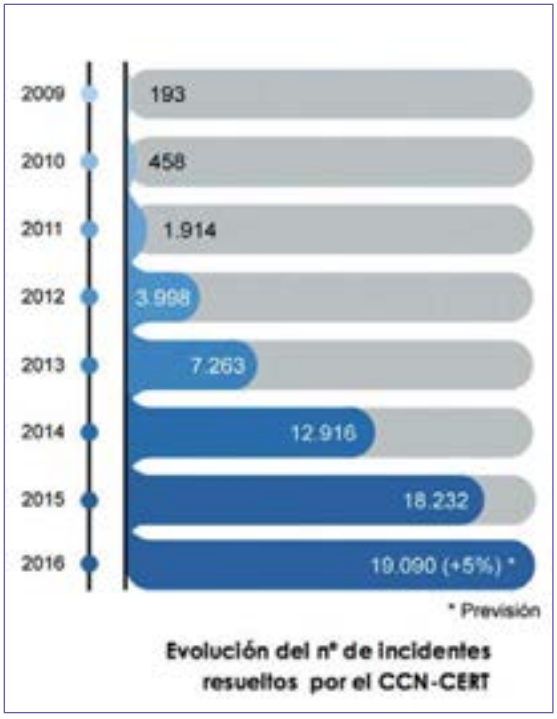
• Dificultad para atribuir el ataque y, por tanto, para perseguir al agresor. La mayoría de los ataques detectados muestran que en su ejecución se han incluido técnicas que dificultan la limpieza total de los sistemas comprometidos, facilitando su reinfección; asimismo, incorporan procedimientos que obstaculizan su investigación, o que ocultan el origen, las infraestructuras utilizadas, los tiempos de permanencia, los accesos alcanzados, la información sustraída, etc.

En este sentido, desde su creación en el año 2002, y avalado por diversa normativa, el CCN ha ido adecuándose y, en la medida de lo posible, ha mitigado las ciberamenazas cuyos principales agentes son: el denominado ciberespionaje (tanto político como industrial promovido por Estados o por organizaciones privadas), la ciberdelincuencia organizada, el ciberterrorismo, el hacktivismo o la nueva amenaza a considerar que puede suponer el ciberyihadismo, que ponen en riesgo el normal funcionamiento de nuestra sociedad, de su economía y de su desarrollo futuro, siendo la amenaza más importante para los intereses nacionales y la seguridad nacional.

El reto más importante para el CCN-CERT sigue siendo, por tanto, detectar estas amenazas cuanto antes y proceder a su neutralización, reforzando la capacidad de prevención y protección en todas las instancias del Estado, desplegando y coordinando sistemas de alerta que mejoren la facultad de detección y vigilancia. En este sentido, y durante 2017, centrará su actividad en la protección frente al ciberespionaje, frente a los ataques de Denegación de Servicio y la salvaguardia de los Sistemas de Control Industrial que están detrás de servicios públicos como Puertos, Confederaciones Hidrográficas u Hospitales.

Al mismo tiempo, está reforzando las capacidades de inteligencia para la identificación de los atacantes, determinación de sus objetivos, y la difusión y compartición de la información obtenida entre todas las organizaciones, públicas y privadas, que colaboran con el Equipo generando la confianza necesaria para contrarrestar a la amenaza. ●

*Texto y Fotos: Redacción/CCN-CERT.*



**JORNADA ORGANIZADA POR LA ASOCIACIÓN DE EMPRESAS DE ELECTRÓNICA, TECNOLOGÍAS DE LA INFORMACIÓN, TELECOMUNICACIONES Y CONTENIDOS DIGITALES (AMETIC)**

# Ciberseguridad en los entornos de **Infraestructuras Críticas**

La Comisión de Seguridad y Confianza de AMETIC celebró el pasado 22 de noviembre la jornada «Ciberseguridad en los entornos de infraestructuras críticas», con el objetivo de facilitar que los operadores de infraestructuras críticas y las empresas proveedoras del sector de la ciberseguridad pudieran exponer e intercambiar su visión, experiencia y soluciones al respecto, así como el impacto de la Directiva NIS recientemente aprobada.

La apertura de la jornada corrió a cargo de Antonio Cimorra, director de Tecnologías de la Información, Desarrollo de la Economía Digital y Estudios de AMETIC, quien destacó el papel de la Comisión de Seguridad y Confianza de AMETIC como interlocutor y voz autorizada de la industria de la ciberseguridad, para pasar a destacar que lo que hace que una infraestructura sea considerada como crítica es la importancia del servicio que presta. Asimismo, recalcó que hoy en día la ciberseguridad cobra especial importancia en cualquier infraestructura, y para hacer frente a las amenazas que evolucionan, crecen y traspasan fronteras, es muy importante la labor de actualización y coordinación que realiza el CNPIC.


El evento continuó con la intervención de Fernando Sánchez, director del Centro Nacional de Protección de Infraestructuras Críticas CNPIC, que comenzó su ponencia con un mensaje tranquilizador sobre la Directiva NIS, indicando que su transposición a la legislación nacional se hará buscando el menor impacto posible en las empresas del sector y contando con la opinión de la industria. También indicó que la transposición se basará en la legislación existente que, de hecho, ya reconoce las figuras de infraestructura crítica y de servicio esencial.

A la pregunta de los asistentes sobre las obligaciones de reporte Fernando Sánchez indicó que la idea de una «ventanilla única» ante la que informar es muy procedente, pero más importante es que cada actor sepa exactamente a quién y cómo reportar, sin necesidad de que esa ventanilla única lo sea para todos los sectores.

## Regulación de Protección de IC

A continuación, tuvo lugar la mesa redonda sobre el impacto de las regulaciones de protección de infraestructuras críticas y la Directiva NIS en los sectores de la energía y de las infraestructuras de transporte. El moderador de esta mesa fue Mariano José Benito, coordinador del Grupo de Trabajo de Seguimiento Legislativo de la Comisión de Seguridad y Confianza de AMETIC,

y como ponentes asistieron Luis Dorda, subdirector de Seguridad de Proyectos Internacional de ADIF; Cándido Arregui, jefe Departamento de Seguridad TIC/CISO de AENA; Andreu Bravo, Information Security & Cibersecurity/CIS de Gas Natural Fenosa; y Elena Matilla, responsable de la gestión de la Seguridad TI de REE. Ambas regulaciones son vistas con optimismo por parte de los operadores representados. Según las intervenciones, ha servido para concienciar a los altos cargos de la dirección de las empresas afectadas, y además puede ser muy positiva al favorecer la homogeneización de políticas en Europa.

Los ponentes mostraron acuerdo en la importancia de integrar todos los tipos de seguridad (física, ciberseguridad, ante accidentes, etc.) y evitar efectos «de silo», algo que no se consigue en el mismo grado en todas las compañías. Asimismo, las organizaciones han podido aprovechar el impulso derivado de estas regulaciones para la realización de proyectos de mejora.

## Impacto de la Directiva NIS

La segunda mesa redonda versó sobre el impacto de la Directiva NIS en el sector de la banca. El moderador fue Julián Inza, coordinador del Grupo de Trabajo de Prestadores de Servicios de Confianza Digital de la Comisión de Seguridad y Confianza de AMETIC, y participaron Jorge Blanco, Head of Global Forensics & Threat Intelligence del Grupo BBVA, y Andrés García, director Corporativo - Control de Riesgo Tecnológico y Fraude del Banco Santander. Ambos responsables coincidieron en que la aplicación de la Directiva NIS no debería presentar complicación para el sector bancario, muy adaptado a la ciberseguridad por la importancia que tiene en su negocio. Sí que puede ser algo más preocupante, para aquellas compañías que tienen carácter multinacional, la diferencia entre las distintas transposiciones que se realicen en cada Estado. También coincidieron en que la Directiva se recibe con incertidumbre, por un lado, y con cierto optimismo en la esperanza de que sirva para aumentar la concienciación sobre la ciberseguridad y la visibilidad de los asuntos que aborda. Sobre la notificación de incidentes, para este sector se comentó que no es algo novedoso ya que actualmente ya deben realizarlas ante el Banco Central Europeo, pero sí parece preocupante que no puedan converger en un mismo organismo las diferentes obligaciones de notificación. En su opinión, las actividades de notificación deberían abordarse más desde un punto voluntarista y de colaboración, que desde la obligación literal y la sanción.


La jornada fue clausurada por el presidente de la Comisión de Seguridad y Confianza de AMETIC, Juan Carlos Batanero. Tras realizar una breve síntesis de lo expuesto durante la mañana, agradeció la asistencia de los organizadores, los ponentes y el público en general, y expresó su deseo de volver a verles en futuras jornadas similares que puedan organizarse desde la Comisión. ●

*Texto y Fotos: AMETIC*

# Alberto Hernández, nombrado director general de INCIBE

EL Consejo de Administración del Instituto Nacional de Ciberseguridad (INCIBE) nombró el pasado mes de octubre a Alberto Hernández Moreno nuevo Director General de INCIBE, después de que Miguel Rego cesara en sus funciones en el puesto. Alberto Hernández desempeñaba hasta el momento y desde febrero de 2014 las funciones de Director de Operaciones del Instituto.

Es Ingeniero Superior de Telecomunicaciones por la Escuela Técnica Superior de Ingenieros de Telecomunicaciones de la Universidad Politécnica de Madrid y Director de Seguridad por el Ministerio del Interior. Como Director de Operaciones de INCIBE ha sido responsable en este periodo de la puesta en marcha de los servicios, tecnologías y actividades de apoyo a la industria, la I+D+i y el talento lanzados desde INCIBE, y ha venido participando, como experto internacional, en misiones de la Organización de Estados Americanos (OEA) para el desarrollo de las estrategias nacionales de ciberseguridad en varios países Latinoamericanos.

Previa incorporación a INCIBE como Director de Operaciones y como Jefe de Área de Ciberdefensa de ISDEFE, formó parte del equipo responsable del diseño y puesta en marcha del Mando Conjunto de Ciberdefensa de las Fuerzas Armadas.

# Grupo VPS: saber proteger inmuebles deshabitados

Llegaron a España en 2011, y desde entonces no han dejado de crecer. Grupo VPS es una multinacional británica pionera en Europa en incorporar los llamados «Sistemas antiokupa». Puertas y ventanas de seguridad que se alquilan durante el tiempo que el inmueble está vacío y que son capaces de repeler más de 90% de las okupaciones. Según Oscar Aragón, Managing Director de Grupo VPS asegura que «Nuestros sistemas se instalan sin dañar la estructura del inmueble y funcionan como elemento disuasorio a la vez que permiten a nuestros clientes a seguir con su actividad de comercialización o reforma de su inmueble».

El éxito de los sistemas y el aumento de casos de okupación ilegal en España ha hecho que la demanda se multiplique. En el último año, la actividad de Grupo VPS ha crecido un 300 por ciento. «En España existen más de 3 millones de inmuebles vacíos y la preocupación de todos los propietarios es protegerlos hasta venderlos alquilarlos. Desde que llegamos a España hemos protegido más de 10.000 inmuebles. De hecho somos el grupo líder en Europa con más de 80.000 inmuebles protegidos» Asegura Oscar Aragón.

El crecimiento de Grupo VPS ha hecho que, actualmente cuenten con cuatro delegaciones en España, con una red de instaladores profesionales con la que abarcan toda la península. Entre sus planes de expansión está el establecer delegaciones en las Islas.

La innovación permanente en el campo de la seguridad es una obligación. Grupo VPS está innovando también en las denominadas «Smart Tower». Una nueva solución de seguridad para vídeo vigilancia móvil a través de unas torres con cámaras. «Cada vez más clientes buscan soluciones complementarias a las tradicionales con vigilantes de seguridad, y es justo ahí donde nosotros les ofrecemos un valor real y un ahorro de costes», finaliza Oscar Aragón.

Contactos de empresas, p. 9.

# 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**

## CONTROL DE ACCESOS ACTIVO

**TALLERES DE ESCORIAZA, S. A. U.**
Barrio de Ventas, 35
E-20305 Irún • SPAIN
Tel.: +34 943 669 100
Fax: +34 943 633 221
**tesalocks@tesa.es • www.tesa.es**

**Líderes en Gestión de Horarios y Accesos desde 1978**
**SKL** Smart Key & Lock
Ferrerías 2,
20500 MONDRAGÓN -SPAIN-
**+34 943 71 19 52**
**spec@grupospec.com**
**www.skl.es**

**CONTROL DE ACCESO, HORARIO, TIEMPO Y PRESENCIA**
C/Samonta 21
08970 Sant Joan Despi
Tel.: +34 934774770
info@primion-digitek.es
www.digitek.es

**GRUPO SPEC**
Líderes en Gestión de Horarios y Accesos desde 1978
C/ Caballero, 81
08014 Barcelona
Tel. 93 247 88 00 • Fax 93 247 88 11
spec@grupospec.com
**www.grupospec.com**

# MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

**BIOSYS**
**(Sistemas de Tecnología Aplicada)**

C/ Cinca, 102-104
08030 BARCELONA
Tel. 93 476 45 70
Fax. 93 476 45 71
**comercial@biosys.es - www.biosys.es**




San Fructuoso, 50-56 - 08004 **Barcelona**
Tel.: 934 254 960* - Fax: 934 261 904
**Madrid:** Matamorosa, 1 - 28017 Madrid
Tel.: 917 544 804* - Fax: 917 544 853
**Sevilla:** Tel.: 954 689 190* - Fax: 954 692 625
**Canarias:** Tel.: 928 426 323* - Fax: 928 417 077
**Portugal**
Rua Ilha da Madeira, 13 A
Olival Basto 2620-045 Odivelas (Lisboa)
Tel.: 219 388 186* - Fax: 219 388 188
**www.bydemes.com**


**RISTER**
**PRESENTCO®**

Avda. Roma, 97
08029 BARCELONA
Tel.: 93 439 92 44 • Fax: 93 419 76 73

**Delegación Zona Centro:**
Sebastián Elcano, 32
28012 Madrid
Tel.: 902 92 93 84

**accesor**

**Soluciones integrales en control de Accesos y seguridad**

DDS

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**

**TECOSA**

Telecomunicación, Electrónica y Conmutación

**Grupo Siemens**
**Infraestructure & Cities Sector**
División Building Technologies
Ronda de Europa, 5
28760 Tres Cantos - Madrid
Tel.: +34 91 514 75 00
Asistencia Técnica: 902 199 029
www.tecosa.es

**TARGET TECNOLOGIA, 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**

## PROTECCIÓN CONTRA INCENDIOS. ACTIVA

**detnov**

C/ Alguer nº8 08830 Sant Boi de Llobregat (Barcelona)

Tel: +34 93 371 60 25
Fax:+34 93 640 10 84

**www.detnov.com**
**info@detnov.com**


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**


**GRUPO AGUILERA**

**FABRICANTES DE SOLUCIONES PCI**
**DETECCIÓN Y EXTINCIÓN DE INCENDIOS**

**SEDE CENTRAL**
C/ Julián Camarillo, 26 28037 MADRID
Tel. 91 754 55 11 • Fax: 91 754 50 98
www.aguilera.es

**Delegaciones en:**

| | | |
|---|---|---|
| Galicia: | Tel. 98 114 02 42 • | Fax: 98 114 24 62 |
| Cataluña: | Tel. 93 381 08 04 • | Fax: 93 381 07 58 |
| Levante: | Tel. 96 119 96 06 • | Fax: 96 119 96 01 |
| Andalucía: | Tel. 95 465 65 88 • | Fax: 95 465 71 71 |
| Canarias: | Tel. 928 24 45 80 • | Fax: 928 24 65 72 |
| Portugal: | Tel. +351 213 563 295 • | Fax: +351 213 563 295 |

**Factoría de tratamiento de gases**
Av. Alfonso Peña Boeuf, 6. P. I. Fin de Semana
28022 MADRID
Tel. 91 312 16 56 • Fax: 91 329 58 20

**Soluciones y sistemas:**
** DETECCIÓN **
Algorítmica • Analógica • Aspiración • Convencional • Monóxido • Oxyreduct® • Autónomos • Detección Lineal
** EXTINCIÓN **
Agua nebulizada • Fe-13™ • Hfc-227ea • $Co_2$

**PEFIPRESA, S. A. U**

**INSTALACIÓN Y MANTENIMIENTO DE SISTEMAS DE SEGURIDAD Y CONTRA INCENDIOS**

**www.pefipresa.com**

**Oficinas en:** A Coruña, Algeciras, Barcelona, Bilbao, Madrid, Murcia, Santa Cruz de Tenerife, Sevilla, Valencia y Lisboa.

**Atención al cliente: 902 362 921**
info.madrid@pefipresa.com


**¿No cree...**
**... que debería estar aquí?**

**El directorio es la zona más consultada de nuestra revista.**

**Módulo: 660€/año***

**Más información:**
**Tel.: 91 476 80 00**
**e-mail: publi-seguridad@epeldano.com**

* Tarifa vigente 2017

# MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

## PROTECCIÓN CONTRA INCENDIOS. PASIVA

### solexin

Calle Alberto Alcocer, 28, 1º A
28036 Madrid
Tel. 913 685 120

**info@solexin.es**
**www.solexin.es**

### DICTATOR Española

**DICTATOR ESPAÑOLA**
Mogoda, 20-24 • P. I. Can Salvatella
08210 Barberá del Vallés (Barcelona)
Tel.: 937 191 314 • Fax: 937 182 509
**www.dictator.es**
**dictator@dictator.es**

## PROTECCIÓN CONTRA INTRUSIÓN. ACTIVA

### bydemes

avanzando juntos hacia el futuro

San Fructuoso, 50-56 - 08004 **Barcelona**
Tel.: 934 254 960* - Fax: 934 261 904
**Madrid:** Matamorosa, 1 - 28017 Madrid
Tel.: 917 544 804* - Fax: 917 544 853
**Sevilla:** Tel.: 954 689 190* - Fax: 954 692 625
**Canarias:** Tel.: 928 426 323* - Fax: 928 417 077
**Portugal**
Rua Ilha da Madeira, 13 A
Olival Basto 2620-045 Odivelas (Lisboa)
Tel.: 219 388 186* - Fax: 219 388 188
**www.bydemes.com**

### DAITEM

**ATRAL SISTEMAS**
C/ Miguel Yuste, 16 5ª Planta.
28037- Madrid
www.daitem.es

### RISCO GROUP

Creating Security Solutions

**RISCO Group Iberia**
San Rafael, 1
28108 Alcobendas (Madrid)
Tel.: +34 914 902 133
Fax: +34 914 902 134
**sales-es@riscogroup.com**
**www.riscogroup.es**

### Honeywell

**Honeywell Security España S. A.**
**Soluciones integradas de intrusión, vídeo y control de accesos**
Avenida de Italia, 7
C. T. Coslada
28821 Coslada
Madrid
Tel.: 902 667 800 - Fax: 902 932 503
**seguridad@honeywell.com**
**www.honeywell.com/security/es**

### Tecnoalarm

Hi-Tech Security Systems

**TECNOALARM ESPAÑA**

C/ Vapor, 18 • 08850 Gavà (Barcelona)
Tel.: +34 936 62 24 17
Fax: +34 936 62 24 38
www.tecnoalarm.com
tecnoalarm@tecnoalarm.es

### VANDERBILT

**VANDERBILT ESPAÑA Y PORTUGAL**

Avenida de Monteclaro s/n
Edificio Panatec
CP 28223, Pozuelo de Alarcón, Madrid
Teléfono +34 91 179 97 70
Fax +34 91 179 07 75
**info.es@vanderbiltindustries.com**
**www.vanderbiltindustries.com**

## PROTECCIÓN CONTRA ROBO Y ATRACO. PASIVA

### AGA

LA INDUSTRIA DE LA CERRAJERÍA

Talleres AGA, S.A.
C/ Notario Etxegibel, 6
20500 Arrasate-Mondragón (Gipuzkoa)
Tel.: +34 943 79 09 22
tallereselaga@aga.es www.aga.es

### diid

**Diid Seguridad Gestión y Logística**
Pol. Ind. Mies de Molladar D3
39311 CARTES – CANTABRIA
Tlfno.: 902565733 – FAX: 902565884
**administracion@diid.es**
**www.diid.es**

## TELECOMUNICACIONES

### Alai Secure

**La solución de seguridad M2M definitiva para las comunicaciones de su CRA**

Condesa de Venadito 1, planta 11
28027 Madrid
T. 902.095.196 • F. 902.095.196
**comercial@alai.es • www.alaisecure.com**

## VIGILANCIA POR TELEVISIÓN

### HIKVISION

**HIKVISION SPAIN**
C/ Almazara 9
28760- Tres Cantos (Madrid)
Tel. 917 371 655
**info.es@hikvision.com**
**www.hikvision.com**

### SAMSUNG WISENET

**Hanwha Techwin Europe Ltd**
Avda. De Barajas, 24, Planta Baja, Oficina 1
28108 Alcobendas (Madrid)España(Spain)
Tel.: +34 916 517 507

**www.hanwha-security.eu**
**hte.spain@hanwha.com**

### GRUPO IPTECNO

Tel. 902 502 035 - Fax 902 502 036
iptecno@iptecno.com - www.iptecno.com
SEDE BARCELONA
**IPTECNO Videovigilancia S.L.**
C. Pla del Ramassar, 52, Nave 19
08402 Granollers
SEDE MADRID
**IPTECNO Seguridad S.L.**
Avda. Tenerife, 2 - Blq. 2, Pta. 3
28703 S. S. de los Reyes

### dahua TECHNOLOGY

**DAHUA IBERIA**
C/ Juan Esplandiú 15 1-B. 28007
Madrid

Tel: +34 917649862
**sales.iberia@global.dahuatech.com**
**www.dahuasecurity.com**

# MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

**Visiotech**
Avenida del Sol, 22
28850, Torrejón de Ardoz (Madrid)
Tel.: 911 836 285 • Fax: 917 273 341
info@visiotech.es
www.visiotech.es

**Expertos en VIDEOVIGILANCIA**

LSB, S.L.
C./ Enero, 11 28022 Madrid
Tf: +34 913294835
info@lsb.es

C/ Aragoneses, 15
28100 Alcobendas, Madrid
Tlf. 902 902 337

**seguridad@eeteuroparts.es**
**www.eeteuroparts.es**

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

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**

**Ballerup, Dinamarca.**
**Tlf. +34 902 65 67 98**
**ventas@ernitec.com**
**www.ernitec.com**



**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

A Western Digital® Company

**WD ESPAÑA**
4 boulevard des Iles
92130 Issy les Moulineaux · Francia
florence.perrin@wdc.com
Tel.: 615 235 013
www.wdc.com

**Canon España, S.A**
Avenida de Europa 6
28108 Alcobendas
Madrid

Tel: +34915384500
www.canon.es
**camarasip@canon.es**

**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**

**AXIS COMMUNICATIONS**
C/ Yunque, 9 - 1ºA
28760 Tres Cantos (Madrid)
Tel.: +34 918 034 643
Fax: +34 918 035 452
**www.axis.com**

**GEUTEBRÜCK ESPAÑA**
Edificio Ceudas
Camino de las Ceudas, 2 Bis
28230 Las Rozas (Madrid)
Tel.: 902 998 440
Fax: 917 104 920
**ffvideo@ffvideosistemas.com**
**www.geutebruckspain.com**

**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**

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.

**PELCO by Schneider Electric**
C/ Valgrande 6
28108, Alcobendas, Madrid
Tel.: +34 911 234 206
**pelco.iberia@schneider-electric.com**
**www.pelco.com**

**¿No cree...**
**... que debería estar aquí?**

**El directorio es la zona más consultada de nuestra revista.**

**Módulo: 660€/año***

**Más información:**
**Tel.: 91 476 80 00**
**e-mail: publi-seguridad@epeldano.com**
* Tarifa vigente 2017

EVENTOS DE SEGURIDAD

**SECURITY FORUM**
Tel.: +34 91 476 80 00
Fax: +34 91 476 60 57
www.securityforum.es
info@securityforum.es

## ASOCIACIONES

UAS

C/ Alcalá 99
28009 Madrid
Tel. 915765255
Fax. 915766094

**info@uaseguridad.es**
**www.uaseguridad.es**



AECRA
Asociación Europea de Profesionales para el conocimiento y regulación de actividades de Seguridad Ciudadana

C/ Emiliano Barral, 43
28043 Madrid
Tel 91 564 7884 • Fax 91 564 7829

**www.aecra.org**

AEINSE
Asociación Española de Ingenieros de Seguridad

**ASOCIACIÓN ESPAÑOLA DE INGENIEROS DE SEGURIDAD**

C/ San Delfín 4 (local 4 calle)
28019 MADRID
**aeinse@aeinse.org**
**www.aeinse.org**

ACAES

C/ Viladomat 174
08015 Barcelona
Tel.: 93 454 48 11
Fax: 93 453 62 10
**acaes@acaes.net**
**www.acaes.net**



tecnifuego AESPI

**ASOCIACION ESPAÑOLA DE SOCIEDADES DE PROTECCION CONTRA INCENDIOS**
C/ Doctor Esquerdo, 55. 1º F.
28007 Madrid
Tel.: 914 361 419 - Fax: 915 759 635
**www.tecnifuego-aespi.org**

**ASOCIACION ESPAÑOLA DE DIRECTORES DE SEGURIDAD (AEDS)**
Rey Francisco, 4 - 28008 Madrid
Tel.: 916 611 477 - Fax: 916 624 285
**aeds@directorseguridad.org**
**www.directorseguridad.org**

anpasp

**ANPASP**
**Asociación Nacional de Profesores Acreditados de Seguridad Privada**
C/ Anabel Segura, 11 - Edificio A - Planta 1ª
28108 Alcobendas (MADRID)
**info@anpasp.com • www.anpasp.com**

ADSI

**ADSI - Asociación de Directivos de Seguridad Integral**
Gran Via de Les Corts Catalanes, 373 - 385
4ª planta (local B2)
Centro Comercial **Arenas de Barcelona**
08015 Barcelona
**info@adsi.pro • www.adsi.pro**

AES

**ASOCIACION ESPAÑOLA DE EMPRESAS DE SEGURIDAD**
Alcalá, 99
28009 Madrid
Tel.: 915 765 225
Fax: 915 766 094

aproser

**ASOCIACIÓN PROFESIONAL DE COMPAÑÍAS PRIVADAS DE SERVICIOS DE SEGURIDAD**
Marqués de Urquijo, 5 - 2ºA
28008 Madrid
Tel.: 914 540 000 - Fax: 915 411 090
**www.aproser.org**

ASELF
Asociación Española de Lucha Contra el Fuego

**ASOCIACION ESPAÑOLA DE LUCHA CONTRA EL FUEGO**
Calle Escalona nº 61 - Planta 1
Puerta 13-14 28024 Madrid
Tel.: 915 216 964
Fax: 911 791 859

**¿No cree... ... que debería estar aquí?**

**El directorio es la zona más consultada de nuestra revista.**

**Módulo: 660€/año***

**Más información:**
**Tel.: 91 476 80 00**
**e-mail: publi-seguridad@epeldano.com**
*** Tarifa vigente 2017**

apdpe

**APDPE**
Asociación Profesional de Detectives de España
Marqués de Urquijo, 6, 1ºB
28008 - Madrid
Tel.: +34 917 581 399
Fax: +34 917 581 426
**info@apdpe.es • www.apdpe.es**

ASEPAL

**ASOCIACIÓN DE EMPRESAS DE EQUIPOS DE PROTECCION PERSONAL**
Alcalá, 119 - 4º izda.
28009 Madrid
Tel.: 914 316 298 - Fax: 914 351 640
**www.asepal.es**

ASIS INTERNATIONAL
*Advancing Security Worldwide™*
CAPITULO 143 – ESPAÑA
143 CHAPTER - SPAIN

**ASIS-ESPAÑA**
C/ Velázquez 53, 2º Izquierda
28001 Madrid
Tel.: 911 310 619
Fax: 915 777 190

cepreven

**ASOCIACIÓN DE INVESTIGACIÓN PARA LA SEGURIDAD DE VIDAS Y BIENES CENTRO NACIONAL DE PREVENCIÓN DE DAÑOS Y PÉRDIDAS**
Av. del General Perón, 27
28020 Madrid
Tel.: 914 457 566 - Fax: 914 457 136

FES

**FEDERACIÓN ESPAÑOLA DE SEGURIDAD**
Embajadores, 81
28012 Madrid
Tel.: 915 542 115 - Fax: 915 538 929
**fes@fes.es**
**C/C: comunicacion@fes.es**

# MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

## FORMACIÓN DE SEGURIDAD

**ASOCIACIÓN DE JEFES DE SEGURIDAD DE ESPAÑA**

Avd. Meridiana 358. 4ºA.
08027 Barcelona
Tel. 93-3459682 Fax. 93-3453395
**www.ajse.es presidente@ajse.es**

**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**

**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



## INSTALACIÓN Y MANTENIMIENTO

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



**Techco Security**
C/ Barbadillo 7
28042 Madrid
+34 91 312 77 77
www.techcosecurity.com
tcs@techcosecurity.com

**INSTALACIÓN Y MANTENIMIENTO**
INTRUSIÓN – CCTV – INCENDIO – ACCESOS
SUBCONTRATACIÓN
ALICANTE, VALENCIA, MURCIA, ALBACETE
www.seguridadlevante.com
**902 400 022**
info@seguridadlevante.com

## PUBLICACIONES WEB

**PUNTOSEGURIDAD.COM**
TF: 91 476 80 00

**info@puntoseguridad.com**
**www.puntoseguridad.com**

**INSTALACIÓN Y MANTENIMIENTO**

Avda. Manzanares, 196
28026 Madrid
Tel.: 914 768 000 - Fax: 914 766 057
**publi-seguridad@epeldano.com**
**www.instalsec.com**

# MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

## MATERIAL POLICIAL

**SABORIT INTERNATIONAL**
Avda. Somosierra, 22 Nave 4D
28709 S. Sebastián de los Reyes (Madrid)
Tel.: 913 831 920
Fax: 916 638 205
**www.saborit.com**

## VIGILANCIA Y CONTROL

**SECURITAS SEGURIDAD ESPAÑA**
C/ Entrepeñas, 27
28051 Madrid
Tel.: 912 776 000
email: info@securitas.es
**www.securitas.es**

**Grupo RMD**
Autorizada por la D.G.P. con el nº. 729
Avda de Olivares 17 – Plg. Industrial PIBO
41110 Bollullos de la Mitación (Sevilla)
Tlfno. 902194814 – 954108887
Fax. 954002319
gerencia@gruporomade.com
SERVICIOS EN TODA ESPAÑA



## TRANSPORTE Y GESTIÓN DE EFECTIVO

**LOOMIS SPAIN S. A.**
C/ Ahumaos, 35-37
Poligono Industrial La Dehesa de Vicálvaro
28052 Madrid
Tlf: 917438900
Fax: 914 685 241
**www.loomis.com**

# Miguel Ángel Gallego

Director de Seguridad de la Estación Sur de Autobuses de Madrid

Gemma G. Juanes

# «La vida me ha enseñado a no rendirme nunca»

Va la carrera pero no transmite prisa. Por eso nos regala parte de su tiempo, para que entrevista y fotos se hagan con la pausa necesaria para convertir una tranquila mañana de invierno en el epílogo de una vida llena de peripecias profesionales, sueños de adulto y reencuentros con la infancia. Cuando uno asoma la cabeza por la Estación Sur de Autobuses de Madrid –instalación que recibe 20 millones de personas al año– los avisos por megafonía se entremezclan con el rumor de las conversaciones y el traqueteo de las maletas arrastradas por los viajeros. Este bullicioso entorno obliga a la primera pregunta: ¿cómo es posible garantizar la seguridad de un recinto de más de 33.000 $m^2$, que incluye, además, una zona comercial y de servicios, y está operativo los 365 días del año? Miguel Ángel Gallego, director de Seguridad de la instalación, tan correcto en el fondo como en la forma, responde serio, rotundo y conciso: prevención, protocolos de actuación…, y trabajo, mucho trabajo. «Mi objetivo es que cuando alguien entre lo primero que perciba sea seguridad; que sienta que no le va a pasar nada», subraya.

Minutos antes –y posterior a un café donde templar unos incipientes nervios– Gallego cuenta, entre intermitentes llamadas al móvil, que fue en Canarias donde tuvo su primera incursión con el mundo de la seguridad privada. Desde allí inició un periplo de idas y venidas a la Península para gestar una trayectoria profesional que comenzó como vigilante de seguridad y continuó como jefe de servicios, delegado, gerente,... en diferentes compañías de servicios de seguridad. Una larga etapa de duro trabajo y variopinta formación –Dirección de seguridad, recursos humanos, habilidades directivas…– le llevarían 20 años después a ser el artífice de la puesta en marcha del departamento de Seguridad de la Estación Sur de Autobuses de Madrid. «Fue un gran reto implementar el Área de Seguridad –explica– en una empresa donde casi no existía cultura de seguridad. Somos un gran equipo: el director, los vigilantes y el personal de la estación, todos trabajamos para que los usuarios se sientan seguros. La colaboración y coordinación es clave para conseguirlo».

Simpático, irónico, y amable conversador, Miguel Ángel Gallego salta cómodo a su mundo más íntimo para confesar, entre bromas, que siempre tuvo la suerte de dormir en la litera de arriba –«¡y eso que era el pequeño de ocho hermanos!»–, y que soñaba con despertarse el día de Reyes Magos con un muñeco Geyperman entre sus manos. Cariñosos recuerdos en el seno de una familia numerosa donde sus padres «hicieron lo imposible, con muy poco, para sacarnos adelante –explica–, enseñándonos a ser independientes».

Hombre inquieto, decidido, y con gran espíritu solidario, pone su granito de arena desde varias ONGS, Miguel Ángel Gallego presume de estar hecho un auténtico chef –«cocidos, paellas..., me salen de rechupete»–. Las calorías luego las quema practicando running y natación. De playa y montaña, música clásica y rock, dice acostarse temprano, ver poca televisión y leer novela histórica. Y que aún le quedan muchas cosas por hacer, pero sin fecha concreta, como tirarse en paracaídas. Unos segundos de silencio dejan paso a una reflexión: «La vida me ha enseñado a no rendirme nunca».●

# II CONGRESO NACIONAL DE JEFES DE SEGURIDAD

## BARCELONA

Abril 2017

AJSE
Asociación de Jefes de Seguridad de España

Peldaño

Más información e inscripciones:

www.congresojefesdeseguridad.com info@congresojefesdeseguridad.com +34 914 768 000

## UN PARTNER SÓLIDO, COMPROMETIDO, INNOVADOR, FIABLE, PRESENTE.

El valor de un partner tecnológico se mide por su capacidad de generar ventaja competitiva, así como por su actitud y el poder de transmitir determinación, entusiasmo, y motivaciones siempre nuevas. Hikvision garantiza profesionalidad, solidez empresarial, compromiso, fiabilidad tecnológica, innovación continua y un alcance global con presencia local.

**Hikvision Spain**
C/ Almazara, 9
28760 Tres Cantos (Madrid)
T +34 91 7371655
F +34 91 8058717
info.es@hikvision.com

www.hikvision.com