CUADERNOS DE SEGURIDAD

Núm. 307 • ENERO 2016 • 10 euros

PUNTOSEGURIDAD.com

Ciberseguridad

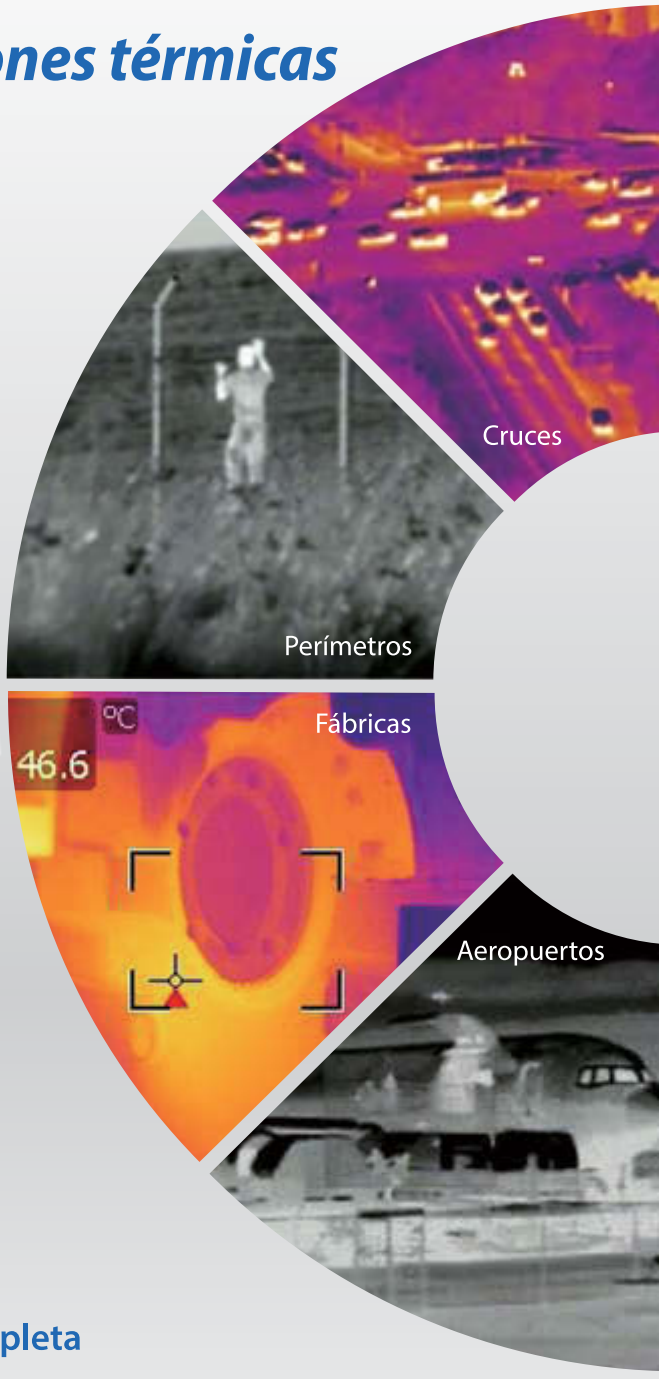
El sector ante 2016: retos de futuro

Actualidad: equipos y sistemas, acuerdos, jornadas...

dahua TECHNOLOGY

Detección en Oscuridad Total

— Soluciones térmicas



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

España

Portugal

CE FC 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

International Security, Safety and Fire Exhibition
23-26 Feb, 2016 Feria de Madrid
Booth:10D18

TECNOLOGÍA, ESPECIALIZACIÓN E INNOVACIÓN

Un año lleno de oportunidades

Empezar un nuevo año casi siempre implica elaborar una lista de propósitos y deseos, pero también es un buen momento para reflexionar sobre todo lo que se ha hecho y lo que ha quedado por hacer. Cada año que finaliza es un ciclo que se cierra para dar permiso a otro; es el momento de renovar ilusiones y esperanzas, de motivarse y hacer buenos propósitos para abordar los próximos 365 días con éxito.

Doce meses en los que el sector de la Seguridad buscará mecanismos y herramientas a adoptar, sobre la base de la calidad en el servicio, la especialización, la formación y la innovación tecnológica, para abordar un prometedor futuro, donde el desarrollo reglamentario de la Ley de Seguridad Privada, Ley 5/2014 de 4 abril, es una necesidad apremiante.

Por ello, en este número que abre sus páginas a un recién estrenado 2016, hemos querido que sean los representantes de las distintas asociaciones sectoriales los que expongan las expectativas y claves de futuro. La primera, y más urgente, la publicación del Reglamento de Seguridad Privada. Luis González Hidalgo, secretario general de la Federación Empresarial Española de Seguridad (FES), puntualiza que ante la publicación de la Ley de Seguridad Privada, «el sector ha avanzado un poco más y ha permitido ofrecer una seguridad jurídica, de la que en muchos aspectos carecía la anterior Ley. Sin embargo, queda 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». Para Anna Aisa, gerente de la Asociación Catalana de Empresas de Seguridad (ACAES), la situación en la que nos encontramos «no es la deseable, ya que se está aplicando una norma de 2014 y un Reglamento de 1994 que desarrolla la antigua Ley de 1992. Por ello, esperamos que 2016 sea el año de la publicación del Reglamento y que en él se contemplen las propuestas que desde el sector se elaboraron».

Desarrollo normativo al margen, los representantes de las asociaciones se muestran unánimes en sus planteamientos de futuro, donde la tecnología juega un pilar fundamental. «Tenemos muchos retos en el horizonte y mucha labor que desarrollar en el campo tecnológico y en el impulso de la industria de la seguridad», señala Paloma Velasco, directora ejecutiva de la Asociación Española de Empresas de Seguridad (AES). Estas y otras opiniones que publicamos en este número, serán la base de un trabajo común.

Y a este trabajo en equipo, un año más Peldaño también quiere aportar su granito de arena. Manteniendo su objetivo de servicio al sector, el próximo 4 de febrero los profesionales de la seguridad tienen una cita en Madrid, en la I Jornada Técnica de RPAS y Seguridad Privada, donde se analizarán las últimas novedades en materia legislativa aplicada a esta tecnología, así como los retos y oportunidades que puede ofrecer al sector de la Seguridad Privada. Además, a cuatro meses de su celebración, la organización sigue avanzando en los contenidos y la planificación de la cuarta edición de Security Forum, que tendrá lugar el 25 y 26 de mayo en Barcelona. Un innovador espacio que atiende a las necesidades e intereses de un sector que apuesta por un próspero año lleno de oportunidades.

CUADERNOS DE SEGURIDAD

www.puntoseguridad.es

Nº 307 • ENERO 2016

Peldaño

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

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

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

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

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

FIPP
conectia
EUROPEAN PRESS NETWORK fire prevention division
EUROPEAN PRESS NETWORK Security division
AEEPP

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

FEBRERO 2016 - Nº 308

EN PORTADA

SICUR 2016

Una nueva edición del Salón Internacional de la Seguridad está en marcha. En efecto, entre los días 23 al 26 de febrero, SICUR 2016 volverá a convertirse en el gran referente internacional en España de la seguridad integral en Feria de Madrid. De nuevo, este Salón, organizado por IFEMA, volverá a reunir a empresas, asociaciones, profesionales y usuarios de seguridad en torno a un escenario de alta representación sectorial, tanto desde el punto de vista de oferta como de demanda. Así lo confirman los datos registrados en la pasada edición que congregó a 1.300 empresas participantes y 38.963 visitantes de 74 países, convirtiendo a SICUR en la plataforma por excelencia de esta industria, así como en el espacio donde tomar el pulso al mercado y conocer las novedades de vanguardia en materia de protección y prevención.

DIFERENTES ÁREAS MONOGRÁFICAS

Como es habitual, la oferta de SICUR se presentará en distintas áreas monográficas representativas de la Seguridad Contra Incendios y Emergencias, en la que se enmarcan las empresas especializadas en la protección activa y pasiva contra el fuego, así como en las soluciones para mejorar la respuesta en situaciones de emergencia; la Seguridad Privada y Pública, en el sector Security y un contenido fuertemente marcado por el avance tecnológico al

servicio de la protección de bienes y vidas; la Seguridad Laboral, en SICUR Prolabor, con lo último en Equipos de Protección Individual –EPIs–, así como en medidas de prevención y salud laboral, y el sector de Defensa, que acogerá a las empresas suministradoras de productos para el ámbito naval, aeronáutico, espacial, armamento, soluciones electrónicas e informáticas, vehículos terrestres, industria auxiliar, así como otros desarrollos realizados para el mercado civil adaptados al ámbito de Defensa.

En este sentido, y al margen del gran atractivo que despierta la oferta del Salón, la feria contará también con un ambicioso programa de jornadas técnicas que, en el marco de FORO SICUR, abordará temas transversales de interés para los usuarios de la seguridad de todos los sectores de la actividad, con un formato muy dinámico y orientado al debate.

MÚLTIPLES ACTIVIDADES

SICUR se completará con el desarrollo de múltiples actividades con contenidos divulgativos, exposiciones, exhibiciones, demostraciones operativas, etc., que ofrecerán un contexto de gran dinamismo e interacción profesional. Entre ellas la Galería de Nuevos Productos, una muestra de la labor de investigación y desarrollo sectoriales; un programa de presentaciones de producto y de experiencias diversas, así como distintas exhibiciones, supuestos de intervención en situaciones de emergencia.

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
Amimon	76	14084904686	www.amimon.com
Arquero	3ª Cubierta	902544504	www.arquero.es
Axis	55	918034643	www.axis.com
Bosch Security Systems	103	902121497	www.boschsecurity.es
By Demes	41	934254960	www.bydemes.com
Cyrasa	27	902194749	www.cyrasa.com
Dahua	2ª Cubierta, 103	865718768883	www.dahuasecurity.com
Digitek	21	934774770	www.digitek.es
Diode	100	914568100	www.diode.es
Dorlet	37	945298790	www.dorlet.com
GMV	66	918072100	www.gmv.com
Grupo Eulen	62, 99, 101	916310800	www.eulen.com
Hikvision	4ª Cubierta,11,13	917371655	www.hikvision.com
Hochiki	101	4401634260133	www. hochikieurope.com
I Jornada RPAS y Seg. Priv.	9	914768000	www.dronesyseguridad.com
IBM España	64	913976611	www.ibm.com/es
Iptecno	49	902502035	www.iptecno.com
Mnemo	58	914176776	www.mnemo.com
Saborit International	19	913831920	www.saborit.com
Samsung Techwin	105	916517507	www.samsungsecurity.co.uk
Scati Labs	104	902116095	www.scati.com
Secure&IT	54, 100	911196995	www.secureit.es
Security Forum	29	914768000	www.securityforum.es
Setelsa	83	942544354	www.setelsa.net
Sicur	79	902221515	www.sicur.ifema.es
SKL	53	943711952	www.skl.es
Synology	104	886225521814	www.synology
Talleres Aga	102	943790922	www.aga.es
Tecosa	23	915147500	www.tecosa.es
TESA	99	943669100	www.tesa.es
Trend Micro	61-70	913697030	www.trendmicro.com
Tüv Nord	80	917663133	www.tuv-nord.es
Tyco IF&S	74, 102	916313999	www.tyco.es
Visiotech	35	911883611	www.visiotech.es
Vivotek	105	886282455282	www.vivotek.com
Western Digital	57	33170744627	www.wdc.com

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

ÍNDICE DE ANUNCIANTES

ENCUENTRO PROFESIONAL QUE SE CELEBRARÁ EL 4 DE FEBRERO EN MADRID

I Jornada Técnica **RPAS y Seguridad Privada**

El evento, organizado por PELDAÑO, cuenta con el apoyo y colaboración de la Federación Empresarial Española de Seguridad (FES) y la revista Cuadernos de Seguridad

MADRID será escenario el próximo 4 de febrero de la I Jornada Técnica sobre RPAS y Seguridad Privada. Un encuentro organizado por Peldaño, que contará con el apoyo y colaboración de la revista Cuadernos de Seguridad y la Federación Empresarial Española de Seguridad (FES).

El objetivo de la jornada es establecer un foro que reúna al sector de la Seguridad en un encuentro en el que se analicen las últimas novedades en materia legislativa aplicada a esta tecnología, así como debatir los retos y oportunidades que puede ofrecer al sector de la Seguridad Privada.

Revolución tecnológica

Vivimos una era de revolución tecnológica que está cambiando no solo nuestra forma de ver el mundo, sino incluso la forma en la que trabajan las empresas, que cambian métodos, se adaptan y ofrecen a sus clientes tanto nuevas plataformas tecnológicas de comunicación, como sistemas de última generación capaces de aumentar nuestro control sobre el entorno. Los RPAS conocidos popularmente como drones, están cambiando la metodología de muchas empresas, emergiendo como uno de los sectores de mayor crecimiento y proyección futura. Fruto de esta necesidad constante en adaptar sistemas, servicios y metodologías para poder ofrecer las mejores soluciones y medidas de protección y seguridad, el sector de la Seguridad Privada no es ajeno a la revolución tecnológica que ofrecerán estos equipos.

Panel de ponencias

Durante el encuentro, dirigido a directores y gestores de la seguridad en entidades públicas y privadas, profesionales de empresas de seguridad y profesionales de empresas de RPAS y centros de formación, se abordarán, entre otros, los siguientes temas: «Tipología de RPAS y su adaptación a servicios de Seguridad Privada»; «Utilización de RPAS con fines de Seguridad Privada en entornos autorizados»; o la «Utilización de RPAS como nuevo modelo de negocio para el sector de la Seguridad Privada».

I Jornada Técnica
RPAS y Seguridad Privada

MADRID

4 DE FEBRERO 2016

AUDITORIO CECABANK

Más información e inscripciones:

www.dronesyseguridad.com info@dronesyseguridad.com +34 914 768 000

Con la colaboración de: CUADERNOS DE SEGURIDAD FES

Organiza: Peldaño

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

Security Forum 2016, un espacio para el desarrollo y la innovación

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

Inmersos ya en 2016, la cuarta edición de Security Forum sigue avanzando en su organización. Las empresas continúan reservando su espacio en el área de exposición, los Premios Security Forum empiezan a recibir trabajos, y el área de conferencias se desglosa en dos sesiones diferenciadas : Global Day y Ciber Day. Consolidado ya como un espacio de networking, esta nueva edición sigue apostando por la innovación y los nuevos valores empresariales en el sector de la Seguridad.

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 2016, 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 perfiles de gran interés como son los *insiders*, el nuevo perfil del delincuente o las últimas tendencias en *coaching* para departamentos de Seguridad.
- **Ciber Day:** la segunda jornada se centrará en la ciberseguridad. Temas como la protección de la información, los delitos informáticos y los nuevos retos y amenazas en la protección de infraestructuras centrarán el debate de esta edición.

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

Ficha técnica

Fechas: 25 y 26 de mayo de 2016.

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

Lugar: Centro de Convenciones Internacional (CCIB).
Pza de Willy Brandt, 11-14.
0819 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

smart

HIKVISION

sicur

Visítanos en el pabellón: 10 stand D-11

COVERT CAMERA

SE ADAPTA A CUALQUIER LUGAR

TODO LO VE

LAS NUEVAS CÁMARAS IP DE HIKVISION CON ÓPTICA PINHOLE, PARA ESPACIOS DONDE LA DISCRECIÓN ES IMPORTANTE

Las nuevas cámaras Pinhole Covert de Hikvision están estableciendo nuevos estándares en el mercado de la videovigilancia, al reunir en un solo dispositivo: Tecnología de última generación, funciones Smart, efectividad y gran facilidad de uso. A pesar de su pequeño tamaño, son capaces de generar una calidad de imagen excepcional. Esta nueva gama de cámaras ocultas aporta una gran flexibilidad y facilidad de instalación, especialmente en lugares con un espacio muy limitado, siendo la solución ideal para aplicaciones de vigilancia discreta como cajeros automáticos, controles de accesos y centros comerciales.

First Choice for Security Professionals

HIKVISION SPAIN - C/ Almazara, 9 - 28760 Tres Cantos (Madrid) - Spain. Tel. +34 917371655 - Fax +34 918058717
info.es@hikvision.com - www.hikvision.com

TECNOLOGÍA, FORMACIÓN, NORMATIVA...

2016, año clave para el desarrollo del sector

Presidentes y representantes de asociaciones explican las claves y perspectivas de futuro del sector

Parece que arranca 2016 con buenas perspectivas de mejora, a nivel general y, en particular, en el sector de la Seguridad Privada, pese a que aún espera ansioso el nuevo Reglamento de Seguridad Privada. ¿Qué deparará este nuevo año a la industria y mercado del sector? ¿Se hará realidad el desarrollo reglamentario de la Ley de Seguridad Privada? Muchos de los profesionales de la seguridad seguro que se han planteado a lo largo de 2015 éstas y otras muchas preguntas, así como qué pasará, en los primeros meses de 2016. Por ello, en este primer número del año –un clásico ya de nuestra publicación– hemos querido pulsar la opinión de las asociaciones más representativas del sector que muestran su valoración sobre un tema de absoluta actualidad: el futuro del sector y... el desarrollo reglamentario de la Ley de Seguridad Privada. Unas pinceladas donde desvelan algunas de las claves de futuro para el sector. Ellos tienen en este número la palabra.

Y es que tal y como señalan algunos de estos responsables «tenemos muchos retos en el horizonte y mucha labor que desarrollar en el campo tecnológico y en el impulso de la industria de la seguridad», apunta Paloma Velasco, directora ejecutiva de la Asociación Española de Empresas de Seguridad (AES).

Por su parte, Anna Aisa, gerente de la Asociación Catalana de Empresas de Seguridad (ACAES), explica que «Creemos en la calidad del servicio, que va unida a la formación y a la innovación, es fundamental. El sector debe evolucionar hacia el desarrollo y aplicación de las nuevas tecnologías».

HIKVISION

sicur

Visítanos en el pabellón: 10 stand D-11

smart

FISHeye

VISIÓN DE 360°

APLICACIONES DE 360°

Obtenga una visión completa y detallada de toda la escena reduciendo el número de cámaras convencionales a instalar. Las cámaras Fisheye de Hikvision cuentan con un elegante y discreto diseño, adecuadas para instalaciones de interior y exterior. Son la mejor opción para profesionales de la seguridad en aeropuertos, centro comerciales, parkings, oficinas, restaurantes, zonas públicas, etc...

First Choice for Security Professionals

HIKVISION SPAIN - C/ Almazara, 9 - 28760 Tres Cantos (Madrid) - Spain. Tel. +34 917371655 - Fax +34 918058717
info.es@hikvision.com - www.hikvision.com

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

La industria de la **Seguridad Privada** ante 2016

Necesidades, perspectivas, y futuro

TODOS los indicadores invitan a pensar en una lenta reactivación de la economía global. En el caso de la Seguridad Privada, que fue un sector que llegó más tarde a la crisis económica, lo lógico es pensar que saldrá más tarde de ella.

Así, la previsión de cierre para 2015 sigue siendo negativa en el área de la vigilancia, parte muy importante del negocio, en tanto que el conjunto del sector podría estabilizarse e incluso comenzar una muy tímida recuperación.

En los volúmenes de facturación lo verdaderamente importante son los márgenes comerciales que han seguido contrayéndose. Además, conviene recordar que la procedencia del negocio viene, en gran medida, de la Administración, por lo que otro tema a tener en cuenta es la capacidad adquisitiva de ésta, como también el cumplimiento de sus plazos de pago, así como el cumplimiento de los plazos de pago de las grandes compañías que, según un reciente informe de la Plataforma Multisectorial contra la Morosidad (PMcM), ha empeorado de 2013 a 2014.

Desde la Plataforma se han presentado recientemente varias propuestas para acabar con este grave problema, como son la agilización de la recuperación del IVA, el sistema que detectaría automáticamente a las empresas morosas, el régimen sancionador (que actualmente no existe), que multaría a los que no cumplieran los plazos y que sería obligatorio para las Administraciones Públicas, o el contrato a compañías que tengan al día sus pagos a proveedores. Del análisis del cruce de los datos de pago con los de cobro se obtiene el periodo medio de financiación comercial neta, que evidencia la trágica realidad: las pymes financian a sus clientes frente a las grandes compañías que se financian a costa de sus proveedores.

Durante 2014, según este informe, el plazo medio de pago del sector privado aumentó un 5% respecto al año anterior, pasando de 85 días en 2013 a 89 en 2014, frente a los 60 días que marca la ley.

Tendencias de futuro

Lógicamente esta problemática afecta tremendamente a nuestras empresas que, en muchos casos, han tenido que cerrar.

En cuanto a las tendencias futuras, que tendrán un amplio desarrollo en 2016, serán tres fundamentalmente para las empresas que, como las que engloba AES, son tecnológicas: la protección de infraestructuras críticas, la conectividad de los diferentes dominios y el internet de las cosas y de los servicios (IoTS).

Protección de Infraestructuras Críticas

Con respecto a la protección de Infraestructuras Críticas, se continúa en la actualidad con la implementación de la Ley de Infraestructuras Críticas. En palabras del Secretario de Estado de Seguridad, Francisco Martínez, el pasado 21 de octubre en León, durante la inauguración de la Conferencia Meridian 2015, es fundamental la cooperación público-privada entre las empresas y las distintas administraciones públicas de quien depende el correcto funcionamiento de las diferentes Infraestructuras Críticas, que gestionan los servicios esenciales para que los ciudadanos puedan tener calefacción o agua caliente en sus hogares, coger un avión o un tren o ser atendidos en un hospital. Esta colaboración abre un amplio espectro de posibilidades para las empresas de seguridad privada, que ya se están preparando para poder prestar esta protección. Existen 12 sectores críticos en España. El más importante, el TIC, porque es transversal a todos los demás. En la actualidad, se han aprobado ya los planes estratégicos sectoriales de la electricidad, gas, petróleo, nuclear y financiero en una primera fase. En una segunda fase se aprobaron los planes estratégicos sectoriales del transporte y el agua. Estamos en la tercera fase. Es una oportunidad importante para la seguridad. El número de operadores críticos en la actualidad asciende a 93.

Internet de las cosas

Por otro lado, cada vez es mayor la aplicación del internet de las cosas a las Centrales Receptoras de Alarma 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.

Sobre esta última tendencia, el internet de las cosas, su importancia será enorme en poco tiempo, con entre 20 y 50 mil millones de dispositivos conectados. Existen más cosas que conectar en el mundo que seres humanos. Lo que supondría económicamente utilizar el internet de las cosas, sería como añadir una economía de Estados Unidos al mundo. En este campo destacan los sectores de salud y de industria de fabricación. Todo se puede conectar.

Dentro de las smart cities, consiste en aplicar la tecnología a la ciudad. Es importante adaptarse al cambio, ya que si las ciudades no son inteligentes (smart), se quedarán fuera de juego. Para ello es fundamental el tener una plataforma que permita conectar todo.

Tenemos pues muchos retos en el horizonte y mucha labor que desarrollar en el campo tecnológico y en el impulso de la industria de la Seguridad Privada en 2016. Lo afrontaremos con optimismo, ya que, como decía Winston Churchill, «el optimista ve oportunidad en cada peligro; el pesimista ve peligro en cada oportunidad». ●

Fotos: *Archivo/ Designed by Freepik*

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

Un sector con ganas de **avanzar y progresar**

«La situación en la que nos encontramos no es la deseable ya que se está aplicando una norma de 2014 y un Reglamento de 1994 que desarrolla la antigua Ley de 1992»

HACE pocos meses aparecía en prensa y redes sociales que se cumplía el futuro: en Regreso al Futuro II Marty Macfly viajaba al 21 de octubre de 2015 y se cumplía dicha fecha. La visión que en 1989 podía tener el director de la película de lo que sería la vida en el año 2015 se ha cumplido en algunos de sus aspectos y en otros no, pero lo cierto es que me ha hecho reflexionar sobre el sector de la Seguridad Privada y mirarlo con perspectiva en el tiempo.

En el mundo de la Seguridad Privada, qué ha sucedido, en qué punto nos encontramos.

Pues bien, hace ya bastantes años que reclamábamos una nueva normativa que permitiera dar respuesta a la cambiante realidad, a las necesidades de la sociedad y a la evolución tecnológica. Finalmente en 2014 se publicó la nueva Ley de Seguridad Privada, que en breve cumplirá el segundo aniversario de su publicación.

La entrada en vigor de la Ley fue celebrada y aplaudida por el sector, que empezó a trabajar de inmediato en las propuestas para el que tenía que ser el Reglamento que desarrollara dicha norma.

Por primera vez, el sector de la Seguridad Privada, entendiendo por éste a todos los agentes afectados o implicados en el mismo, se organizó en grupos de trabajo y, como digo, por primera vez, se elaboró un documento de propuestas consensuado por todos los agentes (empresas, personal de seguridad privada, usuarios, establecimientos obligados, centros de formación, …) .

Ciertamente el sector de la Seguridad Privada había dejado constancia de su madurez, de sus ganas de avanzar y progresar. Sin embargo, este esfuerzo no ha visto de momento sus frutos. Todavía no hemos podido disponer de un primer borrador del que tendría

que ser el nuevo Reglamento de Seguridad Privada.

La situación en la que nos encontramos no es la deseable ya que se está aplicando una norma de 2014 y un Reglamento de 1994 que desarrolla la antigua Ley de 1992. Más aún cuando la Ley en su propio articulado hace en innumerables ocasiones remisión expresa al desarrollo reglamentario.

Por lo expuesto, es obvio que de 2016 esperamos que sea el año de publicación del Reglamento y que en él se contemplen las propuestas que desde el sector se elaboraron a tal efecto.

Sin perjuicio del aspecto normativo, que en un sector como el nuestro es muy importante por ser un sector extremadamente regulado, otras cuestiones son relevantes de cara a 2016.

Nos encontramos con que la sociedad evoluciona con una rapidez extrema, el tiempo no corre sino vuela y la seguridad no puede ser ajena al ritmo que llevamos.

Nuestro sector está en constante evolución. Observa nuevas tendencias, nuevos modos operandi, y aprovecha las nuevas tecnologías para aplicarlas en pro de la calidad del servicio. Calidad que entendemos desde ACAES que es el elemento clave para que nuestras empresas tengan ese elemento diferencial que las haga imprescindibles.

Creemos que la calidad del servicio, que va unida a la formación y a la innovación, es fundamental. El sector debe evolucionar hacia el desarrollo y aplicación de las nuevas tecnologías.

En este sentido, desde ACAES seguimos trabajando conjuntamente con la Generalitat de Cataluña para que en la contratación pública se incluyan indicadores de todos los ítems referidos, y el esfuerzo realizado se ha visto recompensando por cuanto que hemos avanzado muy favorablemente. Ello va unido a la apuesta firme de ACAES por la lucha contra el intrusismo, que nos lleva a denunciar todas aquellas conductas contrarias a la legislación vigente, y exigir una actuación contundente por parte de la autoridad competente.

A tal efecto, es importante la evolución positiva que ha experimentado la colaboración público-privada. El diálogo con las Fuerzas y Cuerpos de Seguridad y con las Administraciones competentes es cada vez más fluido, bilateral y constante. Los canales de comunicación habilitados son ahora más dinámicos y ágiles, y se han creado plataformas que los fomentan y les sacan provecho. Tenemos el total convencimiento que durante 2016 esta comunicación, esta colaboración, será más estrecha y se seguirá trabajando para que crezca y se consolide la confianza mutua entre la Seguridad Privada y la Seguridad Pública.

Llegados a este punto no queremos pasar por alto los plazos de pago que afectan de forma importante a nuestras empresas. 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, 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 electoral. Su publicación y entrada en vigor ayudará en gran medida a las empresas, ya que la falta de liquidez es una de las causas de cierre de las mismas.

Finalizando, como miembro de UAS, durante el año 2016 seguiremos trabajando desde la Unión para y por el sector y, entre otros aspectos, apostamos por un papel más activo del Observatorio Sectorial de Seguridad Privada, que debe ser el instrumento idóneo para luchar por la dignificación de nuestro sector. ●

Fotos: *Archivo/Freepik.*

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

Un desarrollo **reglamentario** fundamental

«Precisamos de un Reglamento que desarrolle los nuevos servicios que podemos prestar a la sociedad»

TANTO en las épocas de bonanza como en la profunda crisis que ha atravesado nuestro sector –que ha reducido las cifras de facturación a las que le definían hace una década–, la Seguridad Privada debe encontrar nuevas palancas que permitan su paulatina recuperación a medio plazo.

Ninguno de los vectores de crecimiento del mercado de la Seguridad Privada a nivel mundial, definidos por los analistas internacionales, son aplicables a la situación española. En un futuro próximo, ni España ni Europa se van a caracterizar por un crecimiento de las clases medias, ni estaremos sometidos a fenómenos de urbanización. Es más, probablemente, ocurrirá todo lo contrario.

Al mismo tiempo, afortunadamente, todos los estudios reflejan que en nuestro país la sociedad tiene una percepción positiva con respecto a la seguridad y muestran una gran confianza hacia las políticas de Seguridad Públicas.

Son especialmente relevantes las estrategias, adoptadas a nivel empresarial –que apuesten decididamente por proyectos de especialización y que combinen de forma eficaz los medios humanos y tecnológicos, para ofrecer un servicio integrado de máxima calidad y definido de acuerdo con las auténticas necesidades de cada usuario–, las que pueden permitir avanzar en la demanda de servicios, en la cifra de negocios y, especialmente, en la rentabilidad de las empresas. Una realidad que afecta sobre todo en sectores que, como el nuestro, cuentan con una gran capacidad de generación de empleo. Esto es, volver a hacer atractivo invertir en nuestro sector.

Y para ello, el marco regulatorio adquiere una importancia decisiva. A nivel general, es necesario dotar al sector de una seguridad jurídica (en especial la referida a obligaciones tributarias), que no se vea continuamente vulnerada por la aplicación de decretos ley con un único objetivo recaudatorio, tal y como ha sido la tónica general en los últimos años.

A esto hay que sumarle que la regulación laboral necesita ya urgentemente, una vez superadas las posiblemente necesarias medidas de choque, establecer diferencias entre el sector industrial y los sectores intensivos en mano de obra, introduciendo, entre otras medidas más obvias, un concepto más amplio y actual del tratamien-

to de la responsabilidad subsidiaria en determinados procesos administrativos y, particularmente, en los de contratación pública.

Dentro del marco específico de nuestra actividad, la nueva Ley de Seguridad Privada ha asentado principios importantes, como la necesaria adaptación de la norma a las necesidades de seguridad definidas en cada contexto histórico por la sociedad, y la adecuación de los requisitos imprescindibles de control a la reducción máxima de las cargas burocráticas.

Consideramos que el desarrollo reglamentario es fundamental. Precisamos un reglamento que desarrolle los nuevos servicios que podemos prestar sin que se ahonde en estrictos requisitos que limiten las posibilidades abiertas, dejando éstos para actividades de especial relevancia para la seguridad pública y la seguridad nacional.

En resumen, necesitamos un reglamento que combata eficazmente las prácticas de competencia desleal e intrusismo, que controle eficazmente el sector dada su naturaleza complementaria con la de la Seguridad Pública, pero que no merme las potencialidades de desarrollo de las empresas hacia nuevas funciones y actividades que está, y seguirá, demandando continuamente la sociedad.

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

Un futuro con nuevas expectativas

COMENZANDO el año 2016, la mayor preocupación actual de las empresas sigue siendo sin lugar a dudas la crisis económica. Y a esta problemática, se le añaden otras que son aún más antiguas, como son la estabilidad en el mercado, la lucha contra el intrusismo, la profesionalidad del sector, la concienciación del cliente sobre el producto seguridad, la morosidad, la inviable aplicación del convenio colectivo y la incertidumbre normativa, entre otras.

De las enumeradas, me gustaría concretar las dos últimas. Respecto a la inviabilidad del convenio colectivo, cabe destacar que nos encontramos ante un acuerdo que tiene varios aspectos que ponen en duda su aplicación: por una parte no ha sido avalado por la organización empresarial que representa a las pequeñas y medianas empresas, y, por otra parte, ha sido impugnado por varias organizaciones sindicales y empresariales. Lo que pone en duda su viabilidad.

> «El sector espera con cierta inquietud que el Reglamento de Seguridad Privada salga a la luz»

Incertidumbre normativa

Y respecto a la incertidumbre normativa, es necesario puntualizar que ante 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. Sin embargo, queda 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.

Apuesta por las nuevas tecnologías

También, tras las elecciones generales del 20 de diciembre, 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.

Sin embargo, y aun teniendo en

cuenta estos aspectos, y otros muchos que deben afrontar las empresas de seguridad, el sector va hacia una dirección muy clara, apostando por las nuevas tecnologías y haciéndose hueco con nuevos ámbitos de mercado, como el de las Infraestructuras Críticas y la ciberseguridad, pues éstas siguen buscando renovadas fórmulas para abordar todas estas trabas. Aunque también no hay que olvidar que ha aumentado la demanda de servicios de vigilancia en centros comerciales, urbanizaciones, hospitales y lugares de internamiento.

Además, desde FES, en defensa de las pequeñas y medianas empresas, afrontamos el nuevo año con una perspectiva positiva, luchando para que los intereses de las pymes se vean representados en todos los ámbitos, como en la negociación del próximo convenio 2017; reorientación en la composición y actividades del Observatorio sectorial; y colaboración en el desarrollo reglamentario.

«El sector va hacia una dirección muy clara, apostando por las nuevas tecnologías y haciéndose hueco con nuevos ámbitos de mercado»

De esta forma, desde FES esperamos que el futuro incierto se convierta en un futuro con unas nuevas expectativas, que hagan ver la luz en esta oscuridad actual. ●

Fotos: *Archivo.*

EVA GRUESO. PRESIDENTA DE LA ASOCIACIÓN PROFESIONAL DE DETECTIVES PRIVADOS DE ESPAÑA. APDPE

Los **detectives** ante 2016

ES habitual, cuando el final del año se aproxima, que comencemos a hacer balance del año que se acaba y, como no, que surjan los nuevos planteamientos de cara al que en breve comenzará.

No es frecuente, en el caso de los Detectives, que esperemos grandes cambios que modifiquen sustancialmente nuestro trabajo pues, aun siendo cierto que los servicios que ofrecemos han ido cambiando paulatinamente, en función de las necesidades de nuestros clientes, no es menos cierto que esas modificaciones se producen de forma muy pausada, no existen grandes innovaciones con respecto a los asuntos que se llevaban a cabo desde hace unos cuantos años.

Incertidumbre e inquietud

Sin embargo, me atrevería a decir que, en esta ocasión, aguardamos con ansiedad la publicación del Reglamento de Seguridad Privada pues la incertidumbre, el desconcierto y la inquietud entre el colectivo es evidente. La Ley 5/2014 ha cambiado completamente los esquemas de funcionamiento, organizativos, de los Detectives Privados; no tanto en el trabajo del día a día, que no difiere de lo hecho hasta el momento de su promulgación, pero sí, por un lado, en la carga burocrática, tremendamente incrementada; por otro, en la forma de ofrecer nuestros servicios y, por último, el coste económico adicional que, se espera, tendremos en un futuro próximo.

En cuanto a los trámites administrativos, sólo pedimos que, los que quedan por ser regulados, se adecuen realmente a nuestra forma de trabajar. En ocasiones, teniendo las «comodidades» de poder trabajar en una oficina no somos conscientes que, en otros momentos, el hecho de enviar un sencillo email se convierte en toda una odisea imposible de llevar a cabo (poblaciones sin cobertura, baterías sin carga, etc.). La inmediatez en la que nos vemos inmersos en nuestra cotidianidad está bien para las redes sociales, pero no parece ser una necesidad cuando del trabajo bien hecho se está hablando.

Sobre la forma de ofrecer nuestros servicios es, quizás, el cambio más radical que hemos sufrido, por la asunción de conceptos que ha supuesto. Es coherente que los servicios de investigación privada sean ofrecidos a través de los despachos de detectives pero ¿qué es un despacho y quiénes somos un despacho? Nuestra adaptación a la Ley 23/92 había hecho que mantuviéramos una organización profesional que dista mucho de la planteada en la actualidad por lo que, nuevamente, tendremos que adecuarnos a la legislación. Pero, vinculado con este hecho, se encuentra el innegable desembolso económico al que vamos a tener que estar sometidos, pues ya la Ley apunta en este sentido.

Esclarecer las dudas

Exigencias relacionadas con la seguridad física, con la seguridad informática, con la tenencia de aval o seguro de caución, con seguro de responsabilidad civil, etc., harán, de no ser extremadamente moderados, que los costes se disparen y no pocos detectives deban plantearse la imposibilidad de continuar con sus negocios. Pero, infinitamente más negativo es para aquél que quiere ejercer la profesión de Detective Privado por primera vez, todo ello incrementado por la incomprensión que se genera al ver cómo una profesión liberal se ve completamente encorsetada con una desmesurada regulación.

Por todo lo expuesto, sería de agradecer que pudiéramos esclarecer todas estas dudas, aunque el momento político actual añade aún más incertidumbre, si cabe, sobre el momento en que el futuro Reglamento de Seguridad Privada verá la luz. ●

Fotos: *Archivo.*

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

JUAN MUÑOZ. CPP CSMP CSYP. PRESIDENTE DE ASIS ESPAÑA

Bajo un contexto de **incertidumbre**

TODO parece indicar que el sector, tanto en su vertiente de Seguridad Privada (los prestatarios de servicios y algunos aspectos de los usuarios) como en el de la Seguridad Corporativa (los usuarios), se enfrenta a importantes eventos y retos en 2016, y que posiblemente lo va a hacer bajo una gran carga de incertidumbre y con agendas, calendarios y momentums diferentes.

Desde la perspectiva de la Seguridad Privada en España, la aprobación del nuevo reglamento que desarrolla la Ley 5/2014 quizás constituya la piedra angular. Una pieza legislativa que el sector espera desde hace meses, y que la actualidad y la evolución de las circunstancias están afectando a su posible contenido desde incluso antes de su publicación. No cabe duda de que se trata de un documento altamente complejo, que seguramente quiere incluir muchas cosas, en base a la ley que desarrolla, pero que no debería tardar mucho en ver la luz. Combinar diferentes tipos de seguridad en base a su naturaleza no se antoja una tarea fácil, sobre todo en el caso de la seguridad lógica, que no tiene fronteras y se mueve en parámetros muy diferentes a los de la seguridad física.

En este sentido no cabe ninguna duda de que el Ministerio del Interior español es quien marca el ritmo y los tiempos, aún a pesar de que posibles demoras podrían afectar al ámbito, el alcance y la eficacia del propio reglamento. También parece que 2016 puede representar un hito muy importante para las infraestructuras críticas y la ciberseguridad, a pesar de la complejidad de los numerosos grupos de interés involucrados.

Pero quizás sea en la vertiente de la Seguridad Corporativa donde la preocupación absorba el centro de gravedad, no sólo del sector sino de la sociedad en general, y donde la agenda no esté bajo el control deseado. La compleja situación internacional, de la cual los recientes atentados de París son sólo un reflejo tras un largo proceso de deterioro y emisión de indicadores, tiene todos los síntomas de protagonizar en gran medida la agenda de seguridad a nivel global… y también nacional. Y lo va a hacer en unas circunstancias donde la capacidad de ejecución y la libertad de acción están repartidas al menos entre los dos bandos, suponiendo que sólo haya dos, lo que es mucho suponer. Espero sinceramente que no

suceda lo mismo con la voluntad de vencer. Los tres constituyen los principios fundamentales del arte de la guerra, situación en la que algunos analistas consideran que nos encontramos, aunque esta sea de naturaleza híbrida y asimétrica.

Los últimos movimientos del Daesh no solo han provocado el aumento de los presupuestos de Interior de varios países, también la revisión de los de Defensa de EEUU, Francia y Reino Unido, por mencionar a algunos.

La imagen de las calles de Bruselas, la capital de Europa, desiertas y sin actividad comercial y patrulladas por equipos conjuntos de militares y policías resulta desoladora. Y no es por la presencia física de estas Fuerzas de Seguridad sino por la imagen de incertidumbre e impotencia que transmiten hacia un enemigo extremadamente complejo (Al Qaeda y Daesh, tanto monta, monta tanto), que en sólo unos meses ha cambiado radicalmente su modus operandi, de los lobos solitarios a los ataques múltiples y simultáneos, y parece disponer de unas capacidades nunca antes imaginadas. Ahora todo parece indicar que el foco de la atención de la prevención está proyectado hacia las amplias comunidades musulmanas de algunos países europeos, que pueden actuar como polo de atracción y cobertura para el nacimiento y ejecución de acciones locales de terrorismo yihadista. Para una economía como la española, que depende en gran medida de su actividad exterior, y sobre todo en países complejos, la incertidumbre y los nuevos riesgos y amenazas representan un factor adicional de preocupación muy importante.

Y es precisamente en este entorno turbulento y complejo donde el concepto de resiliencia alcanza su máximo valor. Muchos empiezan ahora a comprender su sentido. Debemos estar preparados, no sólo para prever y prevenir incidentes de diferente naturaleza (atentados terroristas, desastres naturales, ataques de piratas informáticos, etc.), sino también estar preparados para reponernos y recuperar el estado inicial después de ser víctimas de algunos de estos incidentes, que no hayan podido ser previstos, detectados, prevenidos o incluso minimizados.

> «Debemos estar preparados, no solo para prever y prevenir incidentes de diferente naturaleza, sino también para reponernos y recuperar el estado inicial»

El ataque terrorista de In Amenas, que sucedió en enero de 2013, está actuando finalmente como un catalizador para que la seguridad se vaya transformando en un componente fundamental de la estrategia de las organizaciones y empresas que operan en el exterior y especialmente en los llamados entornos complejos. Todavía queda un largo camino por recorrer, pero el próximo año se anuncia capital en la seguridad corporativa de las empresas españolas –grandes, medianas y también pequeñas, en adecuada proporción–, y por lo tanto en el área de Seguridad Privada, cuyas trayectorias son convergentes. Algunas están revisando sus modelos, otras implementándolos por primera vez.

La globalización y la liberación de los mercados han incrementado las oportunidades de las empresas multinacionales, bien para entrar en nuevos países o para extender sus operaciones. Pero aunque los retornos financieros positivos potenciales son muy significantes, hay también una serie de riesgos inherentes con estas acciones que deben ser apropiadamente identificados, tratados y controlados.

A pesar de todo, como ha pasado en otras ocasiones, confío en que nos creceremos ante las dificultades y situaciones adversas, las cuales actuarán una vez más como un impulso para aumentar nuestra profesionalidad, dedicación y eficacia. ●

Fotos: Designed by Freepik/*Archivo.*

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

Apostar por la **innovación, investigación y desarrollo**

El cambio en el sector tiene que llegar y está llegando ya, dando pasos acertados y colaborando con todos sus medios

En corto periodo de tiempo la imagen de la Seguridad Privada está subiendo a niveles de profesionalidad y de calidad en todos sus servicios con la sociedad en general y como hace años no hemos visto, creo que era un nota discordante con lo que en realidad hacíamos hasta ahora. Bajo el punto de vista de las personas ajenas a este sector, se trata de un sector con falta de recursos y de profesionalidad, donde podía entrar cualquier persona con un bajo nivel cultural y de un pasado algo dudoso, la mediocridad era lo que se podía ver entre la gente de la calle. El resultado de todo esto, incluido el personal de Dirección de las empresas, son las malísimas gestiones económicas de algunas empresas de este sector, las estructuraras operativas y administrativas sobredimensionadas que son un lastre económico. Estamos cambiando nuestras ideas, buscando buenos y mejores profesionales para este sector, que junto con las nuevas tecnologías y la creación de nuevos departamentos de Seguridad, dentro de las propias empresas de seguridad y dando una mayor aportación de medios y de servicios al cliente final, hacen que este sector vuelva a ser un sector dinámico, capaz de generar empleo profesional; la desaparición de algunas empresas hace que queden unas pocas mejor gestionadas y con mayores recursos internos.

La Ley de Seguridad Privada y el nuevo Reglamento

La Seguridad Privada para el año 2016, con la nueva ley 5/2014 y el próximo Reglamento, tiene que apostar más por su colaboración con los Cuerpos de Seguridad del Estado, el intercambio de informaciones, que a la larga es un importante medio de focalización y control de la delincuencia organizada o la criminalidad.

La profesionalización de estas empresas radica principalmente en sus elementos humanos y en sus medios electrónicos, pero siempre hay nuevas formas de combatir a la delincuencia o la criminalidad, ya que estas se reinventan constantemente, y es por ello que los medios de combatir sean en todas sus formas, con ayuda de una ley y un reglamento que den apoyo, incluimos el intrusismo, puesto que hace un daño tremendo a medio y corto plazo a las

CYRASA

ALQUILER DE EQUIPAMIENTOS PARA EVENTOS

Alquiler de equipos por días-mes-año

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

✓ Cobertura nacional

ESPECIALISTAS

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

ABSOLUTO COMPROMISO

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

OTROS SERVICIOS:

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

¡¡Contacte con nosotros!!

cyrasa@cyrasa.com

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

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

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

«La profesionalización de las empresas radica principalmente en sus medios humanos y electrónicos»

empresas que reglamentan y pagan sus contribuciones religiosamente.

Las perspectivas durante 2016 suelen ser optimistas, la robótica ayudará en un futuro no muy lejano a dar mayores medios de detección, los nuevos drones están ahí, aportando medios más rápidos y técnicos; las nuevas tecnologías incluyen nuevos programas informáticos de control y eficacia; la telefonía y sus medios aportan mayores medios de comunicación para estar bajo un mejor control y seguridad, entre nuestro personal de Seguridad Privada. Se está apostando por una fuerte implantación y por un cambio de mentalidad en este sector, naturalmente no podemos olvidar los nuevos medios en cámaras de alta resolución, las cámaras con infra-rojos, las alarmas sin cableados aptas para evitar robos en domicilios y empresas, las altas tecnologías y medios para discriminar un animal u objeto de una persona, mediante barridos de ondas electrónicas o de microondas, evitando las falsas alarmas y los inhibidores; la inclusión de armas no lesivas entre el personal de Seguridad Privada para evitar las agresiones a estos profesionales y reducción de delincuentes, esto es una pequeña parte de las aportaciones por las que está apostando seriamente nuestro sector, con innovación, investigación y desarrollo.

¿Cómo veo el futuro 2016 en nuestro sector?

Veo claras tendencias a mejorar, a desligarnos de lo hasta ahora visto, a la profesionalidad entre su personal, con centros de formación homologados con una visión de futuro, incluidos cursos de alto grado de conocimientos, universidades apostando por incluir las carreras de Ciencias de la Seguridad, donde sean incluidos todos los medios y conocimientos de todas las formas de Seguridad conocidas «que hay muchas y poco utilizadas». Esto es una profesión de futuro, de conocimientos y altísima preparación y no olvidemos que no podemos vender estos servicios en costes mediocres, pues la inversión puede ser muy importante y las empresas tienen que tener unas ciertas ganancias económicas, como tampoco podemos olvidar que esto es un negocio con ánimo de lucro, el mismo nombre lo indica: Seguridad Privada.

Departamentos de Seguridad dentro de las empresas

Por último creo seriamente en dar Servicios de Seguridad a clientes finales, mediante la creación de departamentos de Seguridad dentro de las empresas de Seguridad, donde se reflejen las auditorías, peritajes, asesoramientos y consultorías.

Es así como veo el futuro de la seguridad, en 2016 o en 2017, pero el cambio tiene que llegar y está llegando ya, dando pasos acertados y colaborando con todos sus medios. ●

Fotos:Archivo/Designed by Freepik

Security FORUM

International Security Conference & Exhibition

CCIB
Centro de Convenciones Internacional de Barcelona

25 y 26 de mayo
BCN2016

VER PARA CREAR

#SecurityForumBCN2016

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

IBERIA renfe

Peldaño

RAÚL BELTRÁN. PRESIDENTE DEL CONSEJO NACIONAL DEL GUARDERÍO

Y el 15 trae al **16**

«Debería disponer el Reglamento que todo Guarda que se ponga el uniforme, tenga garantizado el respaldo sobre su responsabilidad civil, sobre su adecuada formación...»

Y es una novedad bastante grata, poder expresarnos por primera vez a través de Cuadernos de Seguridad –a quien agradecemos la posibilidad– y dar el «bienhallados» a los lectores de esta casa, con el mensaje que las circunstancias obligan; todo fluye a su ritmo.

Y es que tras 22 años de Ley 23/92, muerta por obsolescencia y por el interés nacional de poder aprovechar –en lugar de controlar y subyugar– el potencial que la Seguridad Privada puede representar, concurrimos a un apasionante tiempo –aguas rápidas– en el que parecía que todo cambiaba, y en esto la Ley se hizo y en esto el Reglamento... bueno, que parece encauzado, más que el Reglamento –que debe estarlo– el fluir de la situación en el cauce de un río, que en cuarenta años de democracia no ha presentando trazado más desconocido.

Si bien algunos presumen de haber estado en despachos donde ya han podido leer el texto reglamentario (390 Art. y 7 anexos), azul sobre blanco, parece que en lo que interesa a los Guardas si quiera se ha podido presentar al Ministerio, es decir que pudiera ser que lo que un día la Guardia Civil comunicó en reunión a las asociaciones del sector –carta otorgada– todavía no está incluso ni consensuado en el Reglamento. ¿Será entonces el de los Guardas un octavo códice del Reglamento, colándonos otra vez de rondón en la norma?

Si miramos para atrás, solo para coger impulso, veremos que este sistema de «carta otorgada» ha sido constante –para nuestro colectivo– en el cambio legislativo del 14, donde si bien es cierto la figura profesional del Guarda obtuvo un importante refuerzo en competencias, responsabilidades y facultades, no es menos cierto que su sistema laboral sufrió un importantísimo revés al aumentar los hándicaps a los autónomos, auténtico corazón del colectivo hasta la fecha.

La cuestión es que no hemos tenido fácil –mas allá de los 20 años y cinco archivadores de consultas al Seprose, que algo habrán influido en el conocimiento de los problemas– presentar inquietudes y alternativas, que han sido dadas por conocidas y en lo que interesó reflejadas (¿?); no obstante, el fluir de las cosas hace que sean –dentro de las mismas FF y CC de Seguridad– otros distintos los encargados de defender o impulsar la cuestión reglamentaria y lo que ahora vemos hace despertar nuestra ilusión.

A la concepción de los padres de este Reglamento hay que añadir la que pudiera tener el nuevo jefe del Seprose, y el partener que le toque en Policía, cuyas visiones y percepciones aún pueden matizar, al menos en nuestro caso muchas de las incógnitas que la nueva Ley ha dejado respecto de los Guardas Rurales.

Creemos saber, porque la Ley lo di-

ce, que recuperaremos muchos servicios que hasta ahora realizaban «nuestros primos», Vigilantes de Seguridad, por estos campos; también que muchos de nuestros hermanos guardas que los ocupen lo deberán hacer en empresas de seguridad; dentro de ellas concurriremos a los servicios de acuda y videovigilancia con tanta profusión, como el reglamento determine, todo está en el aire pues.

Como colectivo debemos arropar al Seprose para que tenga como antaño esa especial sensibilidad con los Guardas, no podemos permitirnos «guardas de segunda» y eso requiere un esfuerzo, también reglamentario; no puede existir un guarda bien formado, uniformado, reciclado y arropado por una empresa de seguridad como acreedor del mejor servicio y trato y, a la vez, un guarda abandonado a la suerte de su contratista o empleador, como hasta ahora, sin reciclaje, uniformidad, garantías de material o de respaldo, un pobre Azarías al fin.

Debería disponer el Reglamento que todo Guarda que se ponga el uniforme, tenga garantizado el respaldo sobre su responsabilidad civil, sobre su adecuada formación y reciclaje respecto de las materias de interés profesional, de la dignidad y eficiencia del material que para su servicio precisa, de que las líneas de colaboración con las FF y CC de Seguridad sean expeditas, tanto si trabaja en una empresa de seguridad, directamente para el propietario de una explotación o como autónomo, y todo ello bajo un control administrativo que hasta la fecha nos ha sido ajeno.

Solo pidiendo este rigor en nuestro control podemos ayudar a luchar contra la lacra del intrusismo, en nuestras carnes más lacerante, pues son en muchas ocasiones las propias Administraciones las que lo promueven, confundiendo a quienes –empleados por un particular– tienen una competencia para «celar» por determinadas especialidades del medio ambiente, para que dando un paso en el aire realicen las funciones que la Ley nos reserva a los Guardas, cuando no son personas sin ningún tipo de habilitación los que no hacen otra cosa sino vigilar, pero parecen que son perdonados por el mero hecho de no poder abandonar ese servicio y vivir dentro de él.

Otro riesgo es que la Habilitación de Guarda se está convirtiendo en una habilitación «florero», un ítem curricular más, en un motivo de fanfarroneo de quien saliendo al campo la tiene pero no ejerce, o un brindis al sol de quien, en un colectivo cuya facilidad en el ingreso y en el intento de la aventura «empresarial» no requiere absolutamente de ninguna inversión ni garantía, se erige en el Torrente de turno que «apatrulla» sin contrato ni encargo de ningún tipo, luciendo atractivos uniformes, siendo la envidia de su grupo de frikis y la confusión del cliente novel, la verdad es que con todo esto se hace difícil «ver el grano entre la parva».

En fin, que el fluir actual no es, ni está, como para abandonarse, muy al revés, habrá que estar atentos y dispuestos, ya veremos que ocurre con el cauce tras «la lotería». ●

Fotos: *Guarderio*

JORGE SALGUEIRO RODRÍGUEZ. PRESIDENTE EJECUTIVO DE LA ASOCIACIÓN EUROPEA DE PROFESIONALES PARA CONOCIMIENTO Y REGULACIÓN DE ACTIVIDADES DE SEGURIDAD CIUDADANA. AECRA. JURISTA ABOGADO

Seguridad Privada y **nuevas tecnologías**

TRAS el cierre del año 2015, una vez transcurrido más de un año de la entrada en vigor de un nuevo marco legal en las actividades y servicios de la Seguridad Privada, una primera consecuencia a extraer son bajo mi punto de vista los pocos cambios materiales y reales producidos en el sector, y ello porque sin duda alguna la crisis económica y el descenso en el nivel de contratación de los servicios de seguridad, ha marcado las inversiones que debieran producirse a nivel empresarial sectorial.

Sin embargo, sí que ha existido una clara percepción por parte del sector empresarial de la Seguridad Privada, de las nuevas amenazas y riesgos que amenazan a la seguridad y, particularmente, la clara implicación de las nuevas tecnologías que lo impregnan todo.

Dicho conocimiento no se ha traducido en un cambio importante en las ofertas de los contenidos de los servicios de Seguridad Privada, aprovechando las oportunidades de negocio planteadas por la nueva Ley de Seguridad Privada.

Por supuesto que el mercado de la Seguridad Privada es un mercado de servicios, que no ha experimentado una profunda transformación, porque el modelo de desarrollo de la Seguridad Privada tiene un carácter de complemento y de subordinación frente a la Seguridad Pública, sobre el cual no debe operar el fenómeno de la desregulación y de la liberalización que se vienen registrando en otras actividades de libre ejercicio, tanto a nivel nacional como internacional.

Claro que el progreso tecnológico propiciado por los operadores de telecomunicaciones, sí que considero ha afectado al sector de servicios de la Seguridad Privada, al provocar la aparición de nuevas formas de organización y de distribución comercial en el sector de las empresas de Seguridad Privada.

Antes de producirse la crisis económica en España, la expansión de los servicios de Seguridad Privada a nivel de contratación estimo que provino del propio desarrollo económico, del aumento de la renta y niveles de consumo o bienestar social por los usuarios de dichos servicios, y no propiamente

de un aumento en los índices de delito que afectaron a la Seguridad Ciudadana.

La dimensión de las empresas de la Seguridad Privada compuesta básicamente por pequeñas y medianas empresas, se ha visto determinada por últimos factores:

- El grado de regulación de dicho mercado.
- Las características de la tecnología aplicada a dicho ámbito.
- La necesidad de proximidad de los centros de servicios a los usuarios finales.

Estos dos últimos elementos favorecieron, en general, la presencia de grandes empresas de seguridad autorizadas para las actividades de vigilancia y protección de bienes y transporte de fondos, donde predominan las economías de escala, y donde no es necesaria la proximidad entre prestadores y consumidores de dichos servicios con mayor complejidad.

Por el contrario, en los servicios de gestión de alarmas, instalación y mantenimiento de sistemas de seguridad e investigación privada, la naturaleza y contenido de dichos servicios, ha exigido menor complejidad y nivel de exigencia frente al destinatario de este tipo de servicios.

Por consiguiente la presencia de empresas de pequeña dimensión en estas últimas actividades es elevada, y ello no ha constituido necesariamente un síntoma de la existencia de un grado de competencia elevado, que absorban una cuota importante del mercado. Dichas empresas de Seguridad Privada sí se han visto claramente influenciadas y dependientes de otros sectores como el de servicios de telecomunicaciones. Como consecuencia de dicha proximidad e influencia del sector de las telecomunicaciones, las empresas de Centrales Receptoras de Alarmas y las empresas Instaladoras y Mantenedoras de sistemas de seguridad se han visto condicionadas por la apertura de delegaciones o sucursales próximos a su clientela.

La inversión que pueda producirse los próximos años por parte de las empresas de telecomunicaciones, con participación en sus ofertas de servicios a través de sus plataformas, de este tipo de servicios de Seguridad Privada, con el importante añadido de la seguridad informática, va a delimitar el incremento o permanencia de los usuarios contratistas en el ámbito de la Seguridad Privada.

No obstante, la innovación y participación de las nuevas tecnologías en las actividades y servicios de Seguridad Privada más tradicionales, será menor y sin embargo se verá más ligada a la introducción de cambios en los procesos organizativos o en la forma de distribución comercial, así como en las relaciones con el cliente.

Así pues, este tipo de empresas de Seguridad Privada habrán de formalizar acuerdos de cooperación con otras empresas de servicios, orientados a la fidelización u orientación al cliente, por cuanto éstos permiten compartir los riesgos y beneficios asociados a estos proyectos o planes de seguridad integrales conjuntos, como por ejemplo en el ámbito de las Infraestructuras Críticas.

Así, por lo que se refiere al grado de formación, el empleo probablemente más cualificado se producirá en las actividades de Seguridad Privada más vinculados a las nuevas tecnologías y mercados de las comunicaciones, que no constituyen específicamente el conocido como personal de seguridad privada.

La creación de una Seguridad Privada europea con eficacia y eficiencia frente a las nuevas amenazas y riesgos, provendrá claramente de una apuesta por la Comisión en búsqueda de la armonización de los régimen normativo de la Seguridad Privada existentes en cada Estado de la Unión Europa.

Y por supuesto, esta armonización no consiste específicamente en la eliminación de las barreras al comercio de bienes y a los flujos de capitales a nivel comunitario, y sí de los avances aplicados en la tecnología de la información en la protección de la Seguridad Ciudadana a nivel intracomunitario. ●

Fotos: *Archivo/Freepik.*

JON MICHELENA. DIRECTOR GENERAL DE CEPREVEN

Otro **año** que se **va...**

SE han publicado múltiples teorías sobre la percepción del tiempo y la edad que intentan justificar científicamente por qué cada año nos parece que pasa más deprisa que el anterior, con razones neurológicas, sociológicas, psicológicas o simplemente matemáticas. Esta última es la que más me gusta, porque es la más sencilla de entender: cada nuevo año que vivimos ocupa un porcentaje de tiempo menor en nuestras vidas. Independientemente de la justificación que elijamos, lo cierto es que cada vez duran menos.

El 2015 nos deja con ansias de formar parte de los futuros libros de historia como el año en que se inició la recuperación de la profunda crisis vivida en gran parte del «primer mundo». Ojalá sea así y podamos contar a nuestros nietos batallitas sobre cómo conseguimos superarla.

Pero llega 2016, año de grandes expectativas y de grandes incertidumbres. A principios de año tendremos un nuevo gobierno. Es posible que cuando usted esté leyendo estas líneas probablemente se haya disipado parte de esa incertidumbre y ya conozca, al menos, quién será nuevo presidente de nuestro país.

La formación de un nuevo gobierno, la primera incertidumbre, no es un tema baladí para el sector de la Seguridad. Todos sabemos que en algunos cajones de determinados despachos de tres ministerios aguardan pacientemente tres documentos que aspiran a ser reglamentos: El nuevo Reglamento de Instalaciones de Protección contra Incendios, el deseado RIPCI, en el Ministerio de Industria; la nueva versión del documento básico de Seguridad contra Incendios, CTE-DB/SI, en el Ministerio de Fomento; así como el Reglamento de Seguridad Privada en el Ministerio de Interior. El nuevo gobierno tendrá tres opciones: mantenerlos donde están, rescatarlos y publicarlos para el regocijo de los sectores de la Protección contra Incendios y de la Seguridad Privada o reformarlos para adaptarlos a las nuevas necesidades de la sociedad española, visto desde el prisma de su imparcial ideología.

Como ya comentaba en un artículo similar en 2013, cuando el RICPI también estaba a punto de publicarse, «con reglamento o sin él, únicamente la ética profesional de fabricantes, diseñadores, instaladores y mantenedores y la concienciación del usuario final pueden conseguir que el futuro de la seguridad consiga llegar a un futuro próspero, mejor y más seguro.»

La otra gran inquietud que puede afectarnos es la cada vez menos oculta guerra contra el yihadismo. La inseguridad que provoca puede ser una triste oportunidad para el sector de la Seguridad Privada, pero sobre todo puede suponer un importante freno a la recuperación económica que tanto necesitamos.

Cuando acabe 2016 haremos balance de otro año, que también habrá sido más corto que el anterior. Espero con ilusión que para entonces 2015 ya haya conseguido su objetivo y se demuestre que fue el año del inicio de una nueva etapa de prosperidad que se consolidó a lo largo de 2016. ●

Fotos: *Designed by Freepik/Archivo*

Pyronix®

www.pyronix.com

Pyronix Cloud

Expande tu Negocio con el sistema inalámbrico ENFORCER y su potente Home Control+ APP

HomeControl+

Pyronix se complace en anunciar el acuerdo alcanzado con

VISIOTECH para la distribución de sus equipos

Regístrese en www.pyronix.com/espanol para participar en el sorteo de un kit Enforcer 32-WE.

El ganador será anunciado el 1 de Febrero del 2016.

VICENTE MANS. PRESIDENTE DE TECNIFUEGO-AESPI

La seguridad contra incendios, **un objetivo común**

LA seguridad contra incendios es el objetivo común que mueve a los miembros de la Asociación TECNIFUEGO-AESPI desde su creación. Para la consecución de la seguridad planificamos cada año qué temas deben ser trabajados con más intensidad.

Dentro de estos temas, durante 2015 hemos centrado la atención en la inspección. Así, en todos los foros, reuniones, jornadas técnicas programados estamos insistiendo en la importancia de que las autoridades competentes realicen puntualmente inspecciones periódicas como comprobante de que los equipos y soluciones de seguridad contra incendios están diseñados, instalados y mantenidos correctamente, y por tanto en el caso improbable de que tengan que accionarse debido a un incendio, cumplan su cometido con eficacia.

Además, tenemos otros proyectos en marcha que afectan a la mejora de la seguridad contra incendios. Uno de los más importantes es la puesta en marcha del Registro de Instaladores de Productos de Protección Pasiva. Estamos ultimando los procedimientos con una tercera parte, la certificadora, a fin de que el instalador de protección pasiva que avale su buen hacer, se pueda acoger al registro de TECNIFUEGO-AESPI. Esta certificación y registro acredita que la empresa registrada tiene medios y conocimiento para hacer correctamente la instalación. Es obviamente un registro voluntario, pero que sin duda contribuirá a una mejor calidad de las instalaciones.

Guía de Prevención y Actuación en Incendios de Interfaz Urbano-Forestal

Otro proyecto ambicioso y muy necesario es la elaboración de una Guía de Prevención y Actuación en Incendios de Interfaz Urbano Forestal. Estamos en una fase de presentación del proyecto en Europa para conseguir la financiación suficiente. Esta Guía, se va a elaborar en el seno del Foro de Seguridad contra Incendios en la Interfaz Urbano Forestal.

Esta Guía será una herramienta con-

sensuada para que las actuaciones en las áreas de competencia: Agricultura, Urbanismo, etc., tengan una misma base para elaborar unas disposiciones legales y que no entren en conflicto entre ellas, como sucede hoy en día y que dificultan mucho la prevención y actuación en estas zonas.

Tampoco descuidamos otros temas para llegar a esa mejora en el sector. Por ejemplo, trabajamos en concienciar al usuario de que la búsqueda del «mejor precio», no debe descuidar la profesionalidad y la calidad de la instalación. Y en los grupos de trabajo, en el seno de la Asociación, analizamos y aportamos nuestros conocimientos para la mejora de las normas de ensayo con que certificamos o calificamos nuestros productos, para que estén mejor definidas para que no sean «interpretables» y se eviten así problemas de competencia en el mercado. Este tema es común en la UE y estamos propiciando los caminos que mejoren esta situación.

En este sentido, una de las acciones más esperada, junto con AENOR, ha sido la creación de un nuevo sub comité en el CTN 23: Ingeniería para la seguridad contra incendios. Los nuevos materiales, las nuevas formas de diseño, etc., fuerzan más a menudo a aplicar la seguridad bajo el análisis prestacional. Ello supone fijar escenarios para el diseño, y esta fijación de escenarios no es un tema fácil y que

> «Uno de los proyectos más importantes es la puesta en marcha del Registro de Instaladores de Productos de Protección Pasiva»

conviene organizar. Este y otros temas serán seguro fuente de debate en este subcomité que sigue como espejo al recientemente creado en el seno del CEN/TC127.

Y finalmente señalar el apoyo e impulso dedicado a la actualización de la normativa vigente. El Reglamento de Instalaciones de Protección contra Incendios (RIPCI) tiene más de 20 años, todo un récord para estar hablando de seguridad y se traduce en que los avances tecnológicos habidos a través de I+D+i, el control de productos y sus certificados, es decir, que el avance y la actualización de la normativa no son exigibles, hoy por hoy. Por ello, urgimos a la publicación del nuevo RIPCI, tras pasar todos los requisitos administrativos. ●

Fotos: *Tecnifuego-Aespi/Freepik*

JESÚS ALCANTARILLA. PRESIDENTE DE LA ASOCIACIÓN PARA LA PROTECCIÓN DEL PATRIMONIO CULTURAL. PROTECTURI

El **reto** de plantear retos para la **seguridad** del patrimonio cultural

«El mayor de los peligros para la mayoría de nosotros no es que nuestro objetivo sea demasiado alto y no lo alcancemos, sino que sea demasiado bajo y lo logremos»

Michelangelo Buonarroti

¡QUÉ reto este de plantear retos! Cuando los amigos de Cuadernos de Seguridad me pidieron que presentase algunos de los que podrían plantearse durante 2016, pensé que lo más adecuado sería poner manos en el teclado tras la celebración del V Congreso de Protecturi (Asociación para la Protección del Patrimonio Cultural).

Y así he procedido. A nadie se le escapa que en tiempos como los que estamos viviendo, tan lábiles, tan líquidos en palabras del sociólogo y filósofo polaco Zygmunt Bauman, puede resultar temerario aventurarse a hacer una relación de retos, que puede quedar desfasada por la influencia de factores que aún puedan estar por formalizarse.

No obstante, y después de la magnífica experiencia vivida en la sede de la Real Casa de la Moneda, rodeado de profesionales de diversos sectores, todos ellos involucrados en la protección del patrimonio cultural, voy a arriesgarme a mencionar algunos retos ante los que, según mi humilde entender, los profesionales de la seguridad y la protección tendremos que mostrar profesionalidad, prudencia, pero también perspicacia, creatividad y atrevimiento.

Creo conveniente establecer dos tipologías de retos, los estratégicos, que tienen que ver con el marco conceptual de la seguridad, y los funcionales, más vinculados a nuestra labor cotidiana.

Diferentes escenarios de seguridad

En primer lugar, quiero plantear una obviedad pero que muy a menudo se ningunea. El sector de la Seguridad Privada plantea horizontes y escenarios que se escapan a la homogeneidad del café para todos. Y aquí aparece el primero de los retos. Aceptar, por parte de todos los agentes involucrados, la necesidad de realizar un mapa de los diferentes escenarios de seguridad y de las necesidades reales de cada uno de ellos. Sólo así, atendiendo a los contextos, diferenciados y dinámicos, podremos dar la respuesta adecuada y viable en cada caso. De ninguna manera supone desestimar los aspec-

tos comunes e irrenunciables que nos articulan como profesionales de la seguridad. Al contrario, significa reconocer la creciente complejidad con la integración de las nuevas tecnologías, la ciberseguridad, etc.

Establecido el mapa, el siguiente reto es, una vez más, establecer una diferencia que a menudo se confunde.Como profesionales de la protección del patrimonio, estamos sometidos, creo que sin excepción, al signo de los tiempos. A pesar de que según nos cuentan, los indicadores macroeconómicos han modificado de dirección descendente, mi experiencia sigue la misma tónica de los anteriores años. Recortes, reajustes, y más recortes. Más allá de estas circunstancias, sigo convencido de que la protección deber ser asumida como una inversión. Como un coste necesario. Nunca como un gasto.

Gasto o inversión

Hasta que todos, absolutamente todos los agentes del sector, no tengamos interiorizadas las consecuencias de optar por una u otra de las orillas de esta dicotomía, entre gasto e inversión, difícilmente podremos superar viejos modelos organizativos que impiden desplegar la seguridad como un factor estratégico en cualquier organización. El gasto nos enroca, nos minimiza, nos instrumentaliza, mientras que la inversión mostrará el verdadero papel de la seguridad en una organización del siglo XXI, en el que las amenazas son también articuladas desde espacios y realidades inimaginables hace apenas unos años.

Fe de ello da un factor que ha revolucionado nuestro mundo, la accesibilidad universal a las tecnologías de la información y el conocimiento. La vulnerabilidad de las redes informáticas, incluidas las más sofisticadas, es un filón para personas, grupos organizados, grupos criminales, etc., que pueden llegar al corazón estratégico de una organización. O el efecto dramático de la multipantalla, de quienes usan la destrucción de símbolos culturales como medio para amedrentar colectivamente a quienes consideran sus enemigos.

«Como profesionales de la protección del patrimonio estamos sometidos, creo que sin excepción, al signo de los tiempos»

Sin lugar a dudas, en el futuro inmediato deberemos hallar soluciones equilibradas para la inclusión de las nuevas tecnologías en un aspecto crítico en nuestras organizaciones: la protección de la propiedad intelectual y de la imagen de las colecciones, así como el prestigio de la marca de nuestros centros.

Este nuevo panorama es, sin lugar a dudas, uno de los retos de mayor calado al que nos enfrentamos no sólo los profesionales de la seguridad, sino el resto de profesionales y departamentos de nuestras instituciones. Ya nadie debería ver la seguridad como un ámbito finalista, sino como un eje transversal de cualquier organización cultural. El reto de ese cambio de paradigma también está en nuestras manos.

Para lograr ese cambio es necesario activar otro reto: el de la formación. A ningún profesional de la seguridad se le escapa que ésta ha de ser una de las piedras angulares del futuro de nuestra profesión. La formación tiene que dejar de ser una mera instrucción, para ser una vía de generación de técnicos y especialistas capaces de dar respuesta, cuando no de adelantarse, a las necesidades de una organización cultural. Será necesario no sólo adaptar metodologías y materias, sino incorporar los corpus teóricos y prácticos de los ámbitos de conocimiento afines a la protección de cualquier tipología de bienes culturales. Por tanto, la formación se extenderá a lo largo de toda la carrera profesional como un factor dife-

renciador. La continuidad de la formación debe estar, además, imbricada con los factores de los escenarios posibles de cada momento. Sin lugar a dudas, ello provocará un cambio de mentalidad entre todos los agentes comprometidos, directa o indirectamente, en la protección del patrimonio cultural.

Como Protecturi tenemos muy presente la necesidad de centrarnos en ayudar a los profesionales de la seguridad del patrimonio cultural en la complejidad de los diferentes entornos en los que desarrollamos nuestra labor. Por ello, hace un tiempo nos embarcamos en un proyecto que tenía como objetivo ayudar en la gestión de la seguridad y protección de cualquier equipamiento museístico. El Plan de Gestión de la Protección del Patrimonio Cultural, que hicimos público en nuestro IV Congreso, y que ya hemos presentado a los máximos responsables de los Cuerpos y Fuerzas de Seguridad, así como a representantes institucionales del mundo de la cultura, es una metodología escalable para garantizar la protección de los bienes, recintos y personas de cualquier centro o equipamiento que custodie obras de arte.

Sujetos obligados

Estamos en un momento muy interesante por los cambios que se aproximan en el sector. En concreto, estamos a la espera de que el futuro Reglamento de Seguridad Privada contemple la figura de sujetos obligados en las instituciones y equipamientos culturales de nuestro país. Así como del programa de medidas de seguridad obligatorias que le acompañará. Llegado ese momento, estaríamos frente a un gran reto. La entrada en vigor de la figura de sujetos obligados apremiará a los centros y a los profesionales a reformular la seguridad más allá de la funcionalidad. Estamos a la espera que el nuevo Reglamento de Seguridad Privada nos dé la melodía adecuada que esperamos, con ilusión, respeto, para potenciar el funcionamiento de los activos y actividades de nuestros centros.

Paso a enumerar algunos de los retos funcionales para los próximos tiempos:

a. Seguir colaborando con el Plan Nacional de Conservación Preventiva, en materia de seguridad.

b. La elaboración de una Red de Alerta Temprana de amenazas contra el patrimonio, de ayuda a los Cuerpos de Seguridad, Fiscalía, Jueces, actores culturales, etc.

c. Solicitar una mayor inversión estatal para cerrar el catálogo de bienes culturales y dotarlo de los recursos que garanticen su seguridad y conservación.

d. Insistir en la necesidad de mejorar la accesibilidad a los centros y actividades culturales para personas con necesidades especiales, tanto sensoriales, físicas como cognitivas.

e. Apoyar la demanda de un IVA reducido en la cultura.

f. Seguir con los acuerdos de colaboración con las instituciones, centros, entidades que tengan y persigan los mismos objetivos y fines que nuestra asociación.

Para concluir, quiero recordar que la «protección del patrimonio cultural» no es sólo un cometido de los profesionales de la seguridad, sino tarea de todos los profesionales involucrados. Así como un deber de las instituciones y un derecho de los ciudadanos. Sin lugar a dudas, un cometido, y un compromiso, transversal y multidisciplinar. ●

> «La protección del patrimonio cultural no es sólo un cometido de los responsables de la seguridad, sino tarea de todos los profesionales involucrados»

Fotos: Freepik/*Archivo*

HYUNDAI

HDTVI
HDCVI™

STARLIGHT®
NEXT GENERATION

1080P
Full HD

Visítenos en:
sicur
Pabellón 10
Stand 10D09

bydemes
San Fructuoso 50-56 08004 Barcelona
Tfls.: 934 254 960 / 934 269 111
Fax: 934 261 904
bydemes@bydemes.com
www.hyundai-security.es

HYUNDAI
Licensed by Hyundai Corporation, Korea

DR. JOSÉ DÍAZ TORIBIO. COORDINADOR GENERAL DEL CONGRESO ADESYD

Dos claves para 2016

El desarrollo del Sistema de Seguridad Nacional y el reto de explicarlo

EN medio de un contexto de complejidad general, desde el punto de vista de la Seguridad Nacional tres circunstancias determinarán el discurrir del próximo año 2016: el cambio de ciclo político; un escenario internacional complicado (inestabilidad en nuestra periferia, reconfiguraciones geoestratégicas y dudas en el proyecto europeo), y finalmente, una «Ley de Seguridad Nacional»*[1] recientemente aprobada que habrá que desarrollar para conseguir que sea efectiva.

Esto nos lleva a pensar en tres opciones para un futuro a medio plazo: la reforma del Sistema de Seguridad Nacional; la paralización del mismo, o su desarrollo tal y como está actualmente diseñado. Pero con los presupuestos ya aprobados, y con un nuevo gobierno que no será plenamente operativo a todos sus niveles hasta finales de primavera, es casi seguro que en 2016 nos mantendremos en las coordenadas del desarrollo del sistema actual[2] .

El desarrollo del sistema de Seguridad Nacional

En 2015 se ha materializado legalmente un sistema que se viene fraguando desde 2011, y que ha perseguido desde entonces la aplicación en España del concepto «Seguridad Nacional». La finalidad expresada de la nueva ley ha sido la búsqueda de la integración en torno al presidente del Gobierno de instrumentos dispersos en varios organismos de la Administración General del Estado, paralelamente se ha intentado dotar al gobierno de capacidad para coordinar al resto de administraciones y a los principales actores privados[3] .

No ha sido algo surgido de la nada. El cambio del contexto de seguridad, más la necesidad de responder a desafíos de carácter transversal, motivó el nacimiento del nuevo paradigma. Desde 2011 se han creado estructuras para coordinar las respuestas y racionalizarlas, aunque este empeño inicial no dejó de afectar a aspectos y funciones con sede en organismos no completamente conectados. La «Estrategia de Seguridad Nacional» de 2013[4], entre otros principios, trató de impulsar la Unidad de Acción del Estado y varias líneas de actuación estratégica que favorecieran la coordinación. La Ley 36/2015 ha tratado de conferir naturaleza legislativa a todo el proceso.

Dada la trascendencia de la nueva norma, el próximo año debería ser el de su desarrollo reglamentario, el del alineamiento de estrategias de diferentes sectores[5] y el de la elaboración de planes transversales.

Cuando hablamos de «Sistema de Seguridad Nacional» nos referimos a los organismos creados desde la aproba-

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

ción de la «Estrategia Española de Seguridad»[6], la primera de nuestra historia, que han tratado de aplicar por parte del Estado el propio concepto de «Seguridad Nacional». El proceso creativo de instituciones se ha prolongado durante estos años, ahora su actividad es la que aspira a ser organizada por la nueva ley. De manera que 2016 lo comenzaremos con un «Sistema de Seguridad Nacional» caracterizado por unas estructuras que empezaron a funcionar en 2012, una Estrategia de Seguridad Nacional redactada en 2013, y una norma legislativa que habrá que desarrollar durante el próximo ejercicio.

Algo que ha condicionado su naturaleza es que, al haber nacido en un momento de restricciones presupuestarias, ha crecido, prácticamente, sin contar con recursos propios. Esta dificultad la ha sorteado aprovechando las realizaciones anteriores más avanzadas[7] , así como buscando la coordinación de los actores implicados a través de planes transversales[8] .

En definitiva, tenemos un Sistema de Seguridad Nacional que, como la propia Ley de 2015 confirma, exigirá de sus gestores dotes pedagógicas y capacidad de liderazgo[9]. El intento de impedir un exceso de «securitización» del resto de actividades del Estado quizás haya deteriorado, en ese sentido, el principio de integración al que se aspiraba en un primer momento en beneficio de la coordinación.

En lo que respecta al núcleo del Sistema de Seguridad Nacional, durante 2016 se deberá desarrollar mediante Real Decreto la organización y funciones del Consejo de Seguridad Nacional, así como los reglamentos de los órganos de coordinación y apoyo del departamento de Seguridad Nacional, e incluso los mecanismos de enlace entre este último y los organismos del resto de las Administraciones Públicas. Aunque previamente a ello habrá de reunirse la «Conferencia Sectorial para Asuntos de Seguridad Nacional», que intentará definir las fórmulas de coordinación entre administraciones. De tal manera que, para finales de primavera, las Comunidades Autónomas deberán haber hecho los cambios normativos necesarios para adaptar los instrumentos de cooperación precisos con el Sistema de Seguridad Nacional.

Desde el punto de vista de la obtención de recursos se habrá de aprobar mediante Real Decreto la «Declaración de Recursos» para emplear en sectores de interés para la Seguridad Nacional[10] . Finalmente, antes del fin de 2016 se habrá de aprobar una Ley de Preparación y Disposición de la contribución de recursos a la Seguridad Nacional. De los pasos que vayamos viendo en la consecución de estos hitos podremos deducir el compromiso del nuevo gobierno el actual Sistema de Seguridad Nacional.

Junto a ello, y en lo que respecta a uno de los pilares fundamentales de la Seguridad Nacional, la Defensa[11], debemos mencionar, por ser proceso en marcha, la reorganización de las Fuerzas Armadas emprendida en 2014[12], continuada en 2015[13], y que como eje ha tenido la aplicación del concepto de «Fuerza Conjunta». El liderazgo de esta transformación se ha concedido al Jefe del Estado Mayor de la Defensa, que habrá de adaptar la doctrina militar durante el próximo año a los procesos de reorganización ya puestos en marcha, y además, deberá concluir la formación del Núcleo de la Fuerza Conjunta[14] . Está por ver el alcance y la fuerza transformadora que puede desplegarse, teniendo en cuenta que tiene instrucciones de que se haga a coste cero.

Consideramos previsible la aprobación de una nueva Directiva de Defensa Nacional[15], ya que la vigente, de 2012, es previa a la Estrategia de Seguridad Nacional. Deberá buscarse en el nuevo documento un alineamiento con el nuevo sistema de seguridad nacional, y además, prever una revisión estratégica de la Defensa, que finalmente no

«El Sistema de Seguridad Nacional está aún por consolidar y es complejo, parte de su éxito dependerá de la habilidad para hacerlo entender a la ciudadanía»

se ha realizado durante esta legislatura. Si algo ha sido transformador, y a la vez definitorio de la posición de España en el mundo, e incluso de su capacidad disuasoria, ha sido su participación en misiones internacionales. En 2015 se ha puesto fin a nuestra presencia en Afganistán. Durante 2016 España reintentará reasumir el mando de UNIFIL, al tiempo que habrá que tomarse decisiones sobre nuestro compromiso en misiones como ATALANTA, o EUTM MALI, coincidiendo con el final de su mandato. Lo que se haga en relación a ello tendrá influjo importante en nuestra política de seguridad, en lo que respecta a nuestro posicionamiento internacional y al desarrollo de capacidades.

Creemos que habrá otras cuestiones en las que focalizar esfuerzos. La Cumbre de la OTAN de Polonia, en junio, será una buena oportunidad para seguir atrayendo la atención sobre las amenazas y riesgos del Sur de Europa[16] , y al tiempo, de calibrar la capacidad de España para implicar en ello a socios atlánticos con intereses similares.

El mismo afán debería orientar nuestra política de seguridad en la Unión Europea. Pero en el ámbito continental, y ante la ralentización de la Política Común de Seguridad y Defensa, se podría intentar explotar la posibilidad de aplicar instrumentos financieros al desarrollo de proyectos de Industria de Defensa e Industria de Doble Uso, también habrá que continuar utilizando el paradigma «Pooling and Sharing» para ver qué otras capacidades podremos compartir y qué otros recursos podremos poner en común.

Campo en el que, desde nuestro punto de vista, no cabe esperar avances espectaculares será en el de la reestructuración de la Industria de Defensa. En vías de acabar el anterior ciclo inversor, los nuevos proyectos de desarrollo de las fragatas 110 y los vehículos 8x8 serán el núcleo de la demanda interna. Pero estamos en las fases iniciales, y la industria se encuentra en un momento crítico: con la demanda interna en la encrucijada y más competidores internacionales en liza. Frustrada la orientación europea, la reestructuración deberá emprenderse principalmente desde dentro, aunque compaginando la satisfacción de pedidos nacionales con la disposición a aprovechar los estímulos exteriores. La posible creación de una «Agencia de Adquisiciones» puede ayudar a consolidar y clarificar la demanda interna, pero en última instancia, la atención máxima de la Industria de Defensa deberá estar fijada en el desarrollo de capacidades (cuya priorización ya ha presentado Defensa[17]) y en los pasos que se puedan darse para la resolución del eterno «problema presupuestario»[18] .

El reto de explicar el Sistema de Seguridad Nacional

Para afrontar este desafío contamos con la comunicación y con la difusión de la cultura estratégica. Deberemos recurrir a ésta última para explicar en qué consiste el Sistema de Seguridad Nacional, el concepto y los principios en los que se inspira, los intereses na-

cionales que promueve, los derechos que protege, y además, cómo afecta al desarrollo de nuestra vida cotidiana la elección de una opción estratégica u otra. Y también será un reto explicar cómo ha de concebirse integrados en el mismo concepto la función de sectores de la administración tradicionalmente separados, como la Defensa, Seguridad Pública, Acción Exterior, etc.

Hasta hace muy poco el concepto dominante era el de «cultura de defensa»[19] . El conocimiento de lo que significa «seguridad nacional» ha llegado habitualmente a través de mensajes dispersos en diferentes medios, y sobre todo, a través de la comunicación en momentos de crisis[20] . La Ley de 2015 habla de «cultura de seguridad nacional» y de la obligación del gobierno de promoverla. Durante 2016 deberán ponerse en marcha acciones en dos líneas básicas de actuación: conocimiento y sensibilización.

Debería actuarse en coordinación con otras administraciones y aprovechar las sinergias de la participación privada[21]. El Sistema de Seguridad Nacional está aún por consolidar y es complejo, parte de su éxito dependerá de la habilidad para hacerlo entender a la ciudadanía. Esto nos lleva a una conclusión final: La Ley de Seguridad Nacional no consiguió mantener su identificación como legislación básica para el ejercicio de derechos fundamentales, dado que perdió el título de «Orgánica» durante su tramitación. A partir del año 2016, a través de una amplia participación, tendrá la oportunidad de recuperarla de facto en el proceso de su implementación. ●

[1] "Ley 36/2015, de 28 de septiembre, de Seguridad Nacional".

[2] Además, téngase en cuenta que la "Ley de Seguridad Nacional" aprobada en septiembre contó con un amplio respaldo parlamentario (en concreto de los grupos del PP, PSOE y UPyD).

[3] No debemos olvidar el otro gran pilar de la nueva ley: la gestión coordinada por el Gobierno de las denominadas "situaciones de interés para la Seguridad Nacional".

[4] "Estrategia de Seguridad Nacional. Un proyecto compartido". Aprobada en mayo de 2013 por el Consejo de Ministros.

[5] En una ponencia presentada en el I CONGRESO DE SEGURIDAD. COMPARTIENDO (VISIONES DE) SEGURIDAD, celebrado en Madrid el 27 de noviembre de 2014, el autor ya aconsejaba el alineamiento entre la "Estrategia de Acción Exterior" y la "Estrategia de Seguridad Nacional". La referencia bibliográfica es Morales Morales, Samuel, "La acción exterior del Estado como elemento de la Seguridad Nacional". En VVAA, "I CONGRESO ADESyD. COMPARTIENDO (VISIONES DE) SEGURIDAD". Madrid, 2015. Ed. ADESyD. Pags. 135-144.

[6] "Estrategia Española de Seguridad. Una responsabilidad de todos". Aprobada por el Consejos de Ministros en junio de 2011.

[7] Por ejemplo, en el área de "protección de infraestructuras críticas" se ha desarrollado lo previsto por la "Ley de Protección de Infraestructuras Críticas" de 2011, que tiene repercusiones también en la ciberseguridad.

[8] Se han elaborado planes para sectores tan importantes como el sistema financiero o la industria nuclear. En todos ellos se han implicado departamentos de diferentes ministerios: Economía, Industria, Interior, Asuntos Exteriores.

[9] No se olvide que aparte del Gobierno, implica a las Cortes Generales, al resto de administraciones y a actores privados.

[10] Pensando fundamentalmente en tener un listado de recursos disponibles en las "situaciones de interés especial para la Seguridad Nacional".

[11] Los otros dos que menciona la Ley 36/2015 son la Seguridad Pública y la Acción Exterior del Estado.

[12] El punto de partida fue la aprobación del "RD 872/2014 de 10 de octubre por el que se establece la organización básica de las Fuerzas Armadas".

[13] Junta al RD mencionado en la nota anterior deberemos tener en cuenta la implementación total de la "Orden DEF/166/2015, de 21 de enero, por la que se desarrolla la organización básica de las Fuerzas Armadas".

[14] Es en la formación del Núcleo de la Fuerza Conjunta donde parece haber más retrasos (compuesto por unos 27.000 efectivos, 12.000 para misiones interiores y 15.000 para exteriores).

[15] La que está en vigor, aprobada en 2012, lleva por título, "Directiva Defensa Nacional 2012. Por una defensa necesaria, por una defensa responsable".

[16] Habrá que aprovechar en ese sentido que España liderará desde el 1 de enero «la Fuerza Conjunta de Alta Disponibilidad» de la OTAN.

[17] En mayo de 2015 el Consejo de Ministros determinó las capacidades industriales esenciales para la Defensa y la Seguridad Nacional. A saber: C4I; Ciberdefensa; Vigilancia, reconocimiento y adquisición de objetivos (ISTAR); control de tráficos y de ayudas a la navegación; sistemas críticos embarcados en plataformas; sistemas espaciales, de tratamiento de datos y de misión; simulación de equipos y sistemas de armas para entrenamiento avanzado; sistemas de navegación, control guiado y carga de pago en misiones y municiones complejas; sistemas complejos integrados por otros sistemas de armas avanzados cuyos requisitos de integración están vinculados a intereses esenciales de defensa y seguridad.

[18] El Presupuesto de Defensa para 2016 perpetúa el sistema actual: dotación presupuestaria contenida; previsible crédito extraordinario una vez avanzado el ejercicio; asignación a programas de industria y a fondos de contingencia para misiones.

[19] De acuerdo con la "Ley Orgánica 5/2005, de 17 de noviembre, de Defensa Nacional".

[20] A veces con escasa coherencia y poca planificación. Así lo demostró D. Luis Romero Bartumeus en el "I CONGRESO ADESyD" ya mencionado anteriormente. La referencia bibliográfica es, Romero Bartumeus, Luis, "La comunicación pública y la seguridad nacional". VVAA, op, cit. Madrid, 2015. Pags. 59-70.

[21] Hay en España entidades y asociaciones privadas, como ADESyD, que comparten los fines de promover la cultura estratégica desde un enfoque integral.

MIGUEL ÁNGEL ABAD ARRANZ. JEFE DEL SERVICIO DE CIBERSEGURIDAD Y DE LA OCC. CNPIC

Desafíos de la ciberseguridad en España

El término «ciberseguridad» está siendo cada vez más utilizado en ámbitos no especializados, lo que no es más que un reflejo de la importancia que a esta actividad se le está prestando a todos los niveles, desde el político hasta el del usuario final que hace uso de las nuevas tecnologías. Y es fundamental que así sea, ya que la ciberseguridad, entendida como proceso que debe ser continuamente mejorado y pulido en base a los conocimientos adquiridos y errores cometidos, debe sustentarse en políticas que permitan su adecuado fomento y desarrollo.

EN España, la aprobación primero de una Estrategia de Seguridad Nacional que incluía como una de sus acciones prioritarias la mejora de la ciberseguridad, y posteriormente de una Estrategia de Ciberseguridad Nacional con la definición de las líneas de acción y objetivos que se deben acometer durante los próximos años, el panorama se ha clarificado, permitiendo identificar a todos los órganos que presentan algún tipo de responsabilidad en la materia. Todo ello con el objetivo fundamental de, como reza la Estrategia de Ciberseguridad Nacional, lograr que España haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección y respuesta a los ciberataques.

De este modo, si bien las mencionadas estrategias nacionales marcaron un punto de inflexión en lo que respecta al papel que los Estados deben jugar en la definición de políticas para el fomento de la ciberseguridad, quedan aún pendientes, en mi opinión, una serie de desafíos que se deben abordar de forma oportuna y que determinarán el éxito de la consecución de las actividades definidas en la Estrategia de Ciberseguridad Nacional de forma particular.

Formación especializada

A día de hoy es habitual que el personal especializado en materia de ciberseguridad haya obtenido los conocimientos técnicos necesarios como consecuencia de una labor autodidacta previa, basada generalmente en el interés que proporciona el conocer en detalle el funcionamiento de los dispositivos tecnológicos con los que nos desenvolvemos en nuestro día a día. De este modo, si bien el número de ofertas formativas especializadas ha ve-

nido aumentando en los últimos años, es difícil encontrar un esquema formativo que abarcando todas las materias de la ciberseguridad en una primera instancia permita una especialización en cualquiera de sus ramas.

Por tanto, creo que uno de los principales desafíos es el fomento de programas formativos que bien como estudios propios de ciberseguridad, o bien extendiendo los actuales programas universitarios oficiales permitan formar y capacitar a los jóvenes en esta materia.

Seguridad frente a funcionalidad

La implantación de medidas que fomentan la ciberseguridad suele venir acompañada de una pérdida de funcionalidad, al menos en lo que respecta a la facilidad de uso de las aplicaciones y sistemas tecnológicos afectados. En este sentido, es un desafío constante el lograr equiparar el grado de madurez en materia de ciberseguridad al nivel de madurez en funcionalidad y facilidad de uso. Es decir, se debe trabajar para minimizar el grado de desequilibrio que, desde mi punto de vista, siempre existirá entre la seguridad y la agilidad en el uso de sistemas de información y comunicaciones.

Con respecto a este desafío creo que se han producido avances considerables en lo que respecta a la autentificación de usuarios, si bien quedan otros aspectos en los que profundizar, como son aquellos relativos a la confidencialidad y a la integridad de la información almacenada o transmitida entre dispositivos tecnológicos.

Terminología común

El personal que trabaja en materia de ciberseguridad utiliza conceptos como «incidencia», «evidencia», «incidente», «evento» o «impacto», cuya definición es posible que varíe en función del entorno en el que se emplea. De este modo, pueden existir situaciones en las que se requiera (es lo más recomendable y la tendencia habitual) intercambiar información entre distintos profesionales especializados para la resolución de un caso. En este tipo de situaciones, puede suceder que ambos equipos hayan catalogado el suceso con una terminología distinta, queriendo decir lo mismo. O puede darse la situación contraria, es decir, que habiéndolo denominado de la misma forma esa denominación tenga connotaciones distintas en cada uno de los equipos técnicos involucrados en el asunto. Por ello es fundamental contar con un glosario de términos unificado, que facilite y agilice el intercambio de información entre las partes.

> «La ciberseguridad debe estar cada vez más presente como un elemento a tener en cuenta a la hora de actuar con nuevos dispositivos y sus aplicaciones»

Si bien a día de hoy en la Administración española se está un paso por delante en este aspecto, gracias a la disposición de glosarios, guías y esquemas específicos, queda como desafío el unificar estos criterios para aquellas comunicaciones que implican a sectores público y privado de forma conjunta.

Difusión a usuarios finales

En los núcleos más especializados, aquellos que trabajan en su día a día con la ciberseguridad, así como en

aquellos entornos que han tenido que lidiar alguna vez con algún incidente de este tipo, es habitual que se conozca la terminología empleada para describir el suceso, así como las técnicas, mecanismos o herramientas necesarias para su resolución. No obstante, debemos ser conscientes de que la gran mayoría de ciudadanos, a pesar de emplear en su día a día dispositivos tecnológicos, no conocen los riesgos a los que se enfrentan en cierta medida, porque los que tenemos algún tipo de responsabilidad en la materia no hemos sido capaces de explicar las cosas de una forma del todo sencilla.

Esto es así, desde mi punto de vista, porque muchas veces nos perdemos en términos que no permiten conocer el trasfondo de lo que pretenden representar, muy en línea con lo comentado anteriormente con respecto a la terminología común. De este modo, si a un ciudadano le preguntamos si ha sido víctima de un DDoS, si su equipo ha sido infectado por un malware, o por el contrario por un spyware, es fácil que nos enfrentemos a una situación de incertidumbre a la hora de elaborar su respuesta.

De este modo, creo que otro de los desafíos a los que nos enfrentamos en los próximos tiempos es el de conseguir que los ciudadanos no especializados en materia de ciberseguridad sean conscientes, al menos a grandes rasgos, de los riesgos a los que están expuestos. Y para ello, es fundamental disponer de una terminología común que permita describir esos riesgos de forma sencilla, es decir, que sea entendible. Pero también es necesario disponer de personal que con los conocimientos técnicos necesarios sea capaz de transmitir de forma simplificada las raíces de los problemas derivados del uso de las tecnologías. Todo ello sin alarmar y sin impactar al creciente uso de las tecnologías por parte de los usuarios finales; pero sí concienciando y poniendo ejemplos prácticos que garanticen que dichos usuarios harán un uso responsable tanto de los dispositivos como de las aplicaciones disponibles.

Conclusiones

El uso de las tecnologías avanza casi de forma exponencial, al igual que lo hace la aparición de nuevos dispositivos que facilitan nuestro desarrollo y nuestra convivencia como sociedad moderna que somos. Sin embargo, la ciberseguridad debe estar cada vez más presente como un elemento a tener en cuenta a la hora de actuar con dichos dispositivos y sus aplicaciones. Este artículo ha presentado cuatro desafíos que considero importantes de cara a fomentar la aplicación de la ciberseguridad en nuestro día a día de una forma natural, y no como un elemento que obstaculice o dificulte el uso de los sistemas de información y comunicaciones.

A pesar de que estos cuatro desafíos se han presentado de forma separada, entre todos ellos existe cierta dependencia, en el sentido de que la consecución de alguno de ellos repercutirá positivamente en los demás. El caso más paradigmático es el de la formación especializada, ya que ésta derivará en la existencia de personal que se integraría en el mercado laboral a medio plazo, lo que redundaría en un beneficio para la generación de nuevos mecanismos de seguridad más ágiles y de fácil implementación y uso; por otro lado, este personal sería capaz en muchos de los casos de llevar a cabo tareas de concienciación y simplificación terminológica, de cara a su difusión para los usuarios no especializados.

En cualquiera de los casos, creo que el abordar de forma óptima estos desafíos resultará en una mejora de las capacidades que en materia de ciberseguridad existen en España, facilitando asimismo la implementación de las medidas que se derivan de la Estrategia de Ciberseguridad Nacional. ●

*Fotos: **Freepik***

SÁCALE EL MÁXIMO PARTIDO A TUS GRABADORES

sicur
Salón Internacional de la Seguridad

Visita nuestro STAND en SICUR!
Del 23 al 26 de Febrero 2016
IFEMA - Feria de Madrid
Nº Stand: 10D20

IPTECNO SEGURIDAD S.L.
Avda. Tenerife, 2 - Blq. 2, Pta. 3
28703 S.S. de los Reyes (MADRID)

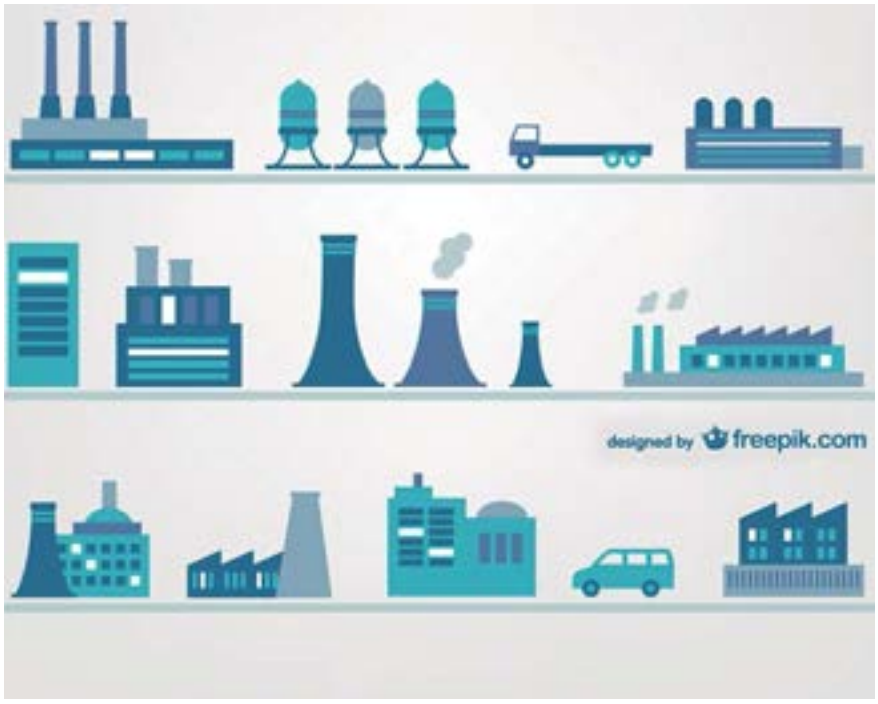
IPTECNO VIDEOVIGILANCIA S.L.
C. Pla del Ramassar, 52
08402 Granollers (BARCELONA)

iPTECNO
DISTRIBUIDOR OFICIAL DAHUA ESPAÑA
Tel. 902 502 035 - www.iptecno.com

MIGUEL GARCÍA-MENÉNDEZ. VICEPRESIDENTE. CENTRO DE CIBERSEGURIDAD INDUSTRIAL (CCI). miguel.garciamenendez@cci-es.org

Regulación de la **ciberseguridad industrial** en España

España lleva años soportando un grado de presión normativa y regulatoria superior a la media de los países que integran la Organización para la Cooperación y el Desarrollo Económico, tal y como recogía, hace ya una década, la propia OCDE en su informe de abril de 2005 sobre la materia [1]. En la misma línea se viene manifestando la Confederación Española de Organizaciones Empresariales (CEOE), cuyo reciente informe «Legislar menos, legislar mejor» [2], publicado este mismo año, ofrece una detallada visión de la capacidad legislativa nacional, autonómica, etc., lo que le ha valido a España el sobrenombre de «país de las cien mil normas».



SIN embargo, esa ingente cantidad de normas y regulaciones de diferente signo no parece quedar reflejada, en la misma y abundante medida, cuando del particular ámbito de la Ciberseguridad Industrial se trata.

Esa es, al menos, una de las principales conclusiones derivadas del estudio «Mapa Normativo de la Ciberseguridad Industrial en España» [3], que acaba de ver la luz de la mano del Centro de Ciberseguridad Industrial. A lo largo del documento, CCI repasa y referencia un notable número de normas, la mayoría de las cuales, sólo tangencialmente, se acercan a las problemáticas asociadas a la citada disciplina. Tal es el caso de la normativa de seguridad industrial vigente en España, cuya tradicional aproximación a la seguridad no ha contemplado la protección contra negligencias, fallos o ataques, de naturaleza cibernética, que puedan comprometer los sistemas de control de procesos que operan en las instalaciones españolas. A lo sumo, una interpretación generosa de dicha normativa puede llegar a incluir parcialmente dichos supuestos, siempre que deriven en un impacto material,

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

físico, sobre las personas, el patrimonio (incluido el cultural) o el medioambiente. Ello excluye automáticamente todo cuanto tenga que ver con acciones de ciberespionaje, ciberintrusiones, etc., por cuanto éstas no provocan –aparentemente– consecuencias físicas relevantes; al menos, a priori. [Naturalmente, estamos, en este punto, obviando el caso particular de los cibersabotajes].

Dividido en tres cuerpos, el estudio ofrece, en primer lugar –«Parte I: Panorama Normativo y Regulatorio Actual»– un repaso de las normas más relevantes en los ámbitos de la rendición de cuentas y el gobierno corporativo, con especial atención a la reforma del código penal y a las últimas recomendaciones sobre buen gobierno de las sociedades cotizadas, emitidas por la Comisión Nacional del Mercado de Valores. Dentro de este primer bloque, se hace un repaso a las políticas públicas, europeas y españolas, recogidas, entre otras, en las estrategias comunitarias y nacionales de seguridad y ciberseguridad. Asimismo, la referencia a normas generales de naturaleza jurídica como la Ley de Seguridad Nacional, la Ley de Seguridad Privada, la Ley General de Telecomunicaciones, la Ley de Servicios de la Sociedad de la Información y el Comercio Electrónico o la Ley Orgánica de Protección de Datos de carácter personal, entre otras, da paso al subapartado dedicado, de forma más específica, a la normativa reguladora de la actividad industrial y a aquella otra ligada a la protección de infraestructuras críticas. Así, se analizan la Ley de Industria, la futura Directiva europea para la Seguridad de la Información y las Redes (Directiva NIS), la Ley de Protección de Infraestructuras Críticas y los reglamentos y resoluciones que la desarrollan, el Esquema de Seguridad Nacional, amparado por la Ley de Acceso Electrónico de los ciudadanos a los servicios públicos y el futuro Esquema Nacional de Ciberseguridad Industrial (ENCI). Adicionalmente, el documento dedica una cierta atención a la normativa autonómica, sectorial e, incluso, voluntaria.

La «Parte II: Contexto de la Ciberseguridad Industrial» enumera los diferentes actores que constituyen el ecosistema industrial: negocio, mercado, clientes, organizaciones industriales e infraestructuras críticas, estudios de ingeniería, integradores y firmas de consultoría, fabricantes, Administración y otros, como asociaciones patronales o profesionales, organismos de normalización, centros de investigación, observatorios u otros centros de análisis, etc.

Ciberseguridad en el ecosistema industrial

Finalmente, el tercer y último bloque del documento –«Parte III»– muestra una propuesta de mapa regulatorio de la ciberseguridad en el ecosistema industrial español. El objetivo de dicho mapa es, por un lado, señalar el alcance de los textos normativos más relevantes contemplados en el estudio; y, paralelamente, identificar aquellos ámbitos en los que aún queda espacio para la actividad normativa. Tal vez, uno de ellos pueda ser el de los productos y/o soluciones aportados por los fabricantes.

El estudio concluye destacando dos nombres propios entre las referencias normativas analizadas: los de aquellas que actualmente tienen todo a su favor para convertirse, en el corto plazo, en los marcos de referencia para el sector industrial en materia de ciberprotección. Se trata, por un lado, del futuro, pero inminente, Esquema Nacional de Ciberseguridad Industrial (ENCI) y, por otro, de la largamente anunciada directiva europea para la Seguridad de las Redes y de la Información (Directiva NIS). Presumiblemente, serán ellos quienes marquen el camino de la Ciberseguridad Industrial, en un futuro muy próximo.

Y, por cierto, piense también que no todo ha de ser regulación. Las limitaciones impuestas a los fabricantes e integradores de sistemas de control industrial por el llamado «tiempo real», en el que han de operar estos sistemas, dificulta la introducción de mecanismos de protección en su software como antivirus, parches o actualizaciones. Es el lugar al que la normativa no llega y que, consecuentemente, invita a buscar un modelo en el que se vean contempladas tales limitaciones. ●

Fotos: CCI/Freepik

[1]-Conway, P.; Janod V. y G. Nicoletti. "Product Market Regulation in OECD Countries 1998-2003". OCDE, Working Paper n. 419. 1 de abril de 2005.
URL (a 2015.11.24): http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?doclanguage=en&cote=eco/wkp(2005)6.

[2]- CEOE. «Legislar menos, legislar mejor». OCDE, Working Paper n. 419. Enero de 2015.
URL (a 2015.11.24): http://www.ceoe.es/resources/image/legislar_menos_legislar_mejor.pdf.

[3]- CCI. «Mapa Normativo de la Ciberseguridad Industrial en España». CCI. 5 de noviembre de 2015.
URL (a 2015.11.24): https://www.cci-es.org/web/cci/detalle-actividad/-/journal_content/56/10694/190120

FRANCISCO JAVIER CARBAYO. MIEMBRO DEL COMITÉ OPERATIVO DEL DATA PRIVACY INSTITUTE. ISMS FORUM SPAIN *

Privacidad y protección de datos: el futuro es ahora

Los términos Privacidad, Protección de Datos, Datos Personales, Fuga de Datos, Seguridad de la Información, Ciberseguridad, etc., están cada vez más incorporados al debate público, a las portadas y primeras páginas o principales noticias de muchos medios de comunicación, y en general son una parte del debate ciudadano, en mayor o menor medida.

EN este sentido, los recientes atentados de París, han conllevado (en buena lógica) una intensificación de un debate que alcanza a ciudadanos, empresas y estados, y que es cómo hacer compatible una mayor Seguridad (en sentido amplio), sin menoscabar más allá de ciertos límites, derechos como pueden ser el relativo a Protección de Datos.

Con el Reglamento Europeo de Protección de Datos asomando en el horizonte, con la Sentencia del Tribunal de Justicia de la Unión Europea invalidando el sistema de Safe Harbor, con la Directiva NIS sobre la mesa, con las empresas y los estados buscando y requiriendo instrumentos no sólo técnicos sino también jurídicos contra ciberataques cada vez más frecuentes e intensos…

Retos de Privacidad y Protección de Datos

En este sentido, es posible que haya que identificar los importantes retos en Privacidad y Protección de Datos desde varios frentes, en función de los grupos de interés afectados. Así por ejemplo se podría hablar de:

- Consumidores. Tanto en el mundo analógico como sobre todo en el mundo digital, la toma de consciencia por los consumidores del gran volumen de tratamiento de datos personales que se realiza por diversos agentes, está derivando en que tales consumidores empiezan a valorar como factor de su toma de decisión tales factores vinculados a la Privacidad.
- Ciudadanos (probablemente los mismos sujetos del grupo anterior, pero desde un punto de vista diferente). Videovigilancia, control de las comunicaciones, creación de ficheros de perfiles (como el Fichero S en Francia), etc., someten al ciudadano a un escru-

tinio, continuo o puntual, por parte de los Estado. Sin duda por cuestiones de seguridad, pero que dan lugar a una reflexión como sociedad sobre los límites de dicha actividad, debate con muy diferentes bases en Europa y el mundo anglosajón, por ejemplo.

• Empresas. Este grupo de interés afronta riesgos en frentes variados, cambiantes y crecientes. Por un lado, las amenazas son cada vez mayores, más frecuentes, más persistentes y con mayor impacto. Por otro lado, su papel en la Seguridad como concepto global requiere de ellas una colaboración con Fuerzas y Cuerpos de Seguridad del Estado que requiere claridad de conceptos y recursos adecuados. Además, las pautas de cumplimiento, por parte de mercados y reguladores son cada vez más exigentes. Y por último, sin que esto sea una lista exhaustiva, han de auto-exigirse el convertir la Privacidad y Protección de Datos de mero requisito a elemento de creación de valor.

• Estados. La digitalización del ámbito sobre el que aplica la seguridad nacional, convierte a la ciberseguridad en un concepto que está sobre la mesa de las más altas instancias de los Gobiernos, en aspectos como la defensa de las infraestructuras críticas, la defensa frente a las amenazas de grupos criminales u otros Estados, en la configuración de una estrategia de defensa que tenga en cuenta los valores de la sociedad y las leyes pero sin menoscabar la capacidad de defensa, etc.

«Las amenazas son cada vez mayores, más frecuentes, más persistentes y con mayor impacto»

En definitiva, la importancia es incuestionable, los retos heterogéneos y la necesidad de trabajar con intensidad en estas materias indudable. ●

Fotos: Freepik

*Abogado. Asociado Senior y Gerente de Compliance en ECIX.

SONIA MARTÍN FERNÁNDEZ. DIRECTORA DE SERVICIOS PROFESIONALES DE SEGURIDAD. SECURE&IT

Ciberataques: uno de los mayores riesgos para las pymes españolas

El fuerte desarrollo de las TIC ha revolucionado en pocos años los hábitos de la sociedad y de las empresas. Desde los hábitos de consumo, hasta los trámites meramente burocráticos, pasando por el nacimiento de nuevas figuras delictivas, frecuentemente difíciles de encasillar en los tradicionales supuestos de hecho.

EL progreso de la tecnología en beneficio de todos se ha visto exponencialmente impulsado por el creciente uso de ésta tanto a nivel familiar como empresarial. Ello, ha traído la necesidad de adoptar medidas de seguridad que garanticen una protección óptima de nuestros derechos en la red.

Según un estudio publicado en el último trimestre de 2015 por Panda Security, 9 de cada 10 pymes españolas sufren ciberataques a diario. Estos ataques informáticos proceden, según dicho estudio, del acceso a webs poco seguras (39%); descargas de programas de la red (23%) y malware recibido por email (19%). Las prácticas que más problemas ocasionan a las empresas son el ciberespionaje, intrusiones en la red, los fallos de terceros o el fraude de empleados.

Por su parte un estudio de Kaspersky Lab y B2B Internacional indica que las pymes tienen pérdidas anuales de alrededor de 38.000 dolares de media a causa de los diferentes tipos de ciberataques durante 2015. Las grandes empresas necesitan 490.000 euros para recuperarse de un ciberataque y las pymes 33.700 euros.

«Las pymes sí están preparadas para abordar el reto de la ciberseguridad, pero deben apoyarse en los profesionales especializados en garantizar estos procesos, ya que de por sí resulta muy complejo contrarrestar las iniciativas de los cibercriminales», señala Francisco Valencia, director general de Secure&IT

Ataques cibernéticos

Durante el año 2014 España fue el tercer país del mundo que más ataques cibernéticos sufrió, con más de 70.000 incidentes. De ahí la importancia de profesionalizar y sistematizar las estrategias organizativas que han de velar por la seguridad de la información.

La seguridad de la información exige cumplimiento normativo, desarrollo de los procesos corporativos adecuados y seguridad de los sistemas. Y todo ello

AXIS COMMUNICATIONS

Innovando un mundo más inteligente, más seguro.

Axis ofrece un amplio portafolio de soluciones de seguridad inteligentes:

Codificadores de video

Cámaras de red

Control de acceso físico

Grabadores de video de red

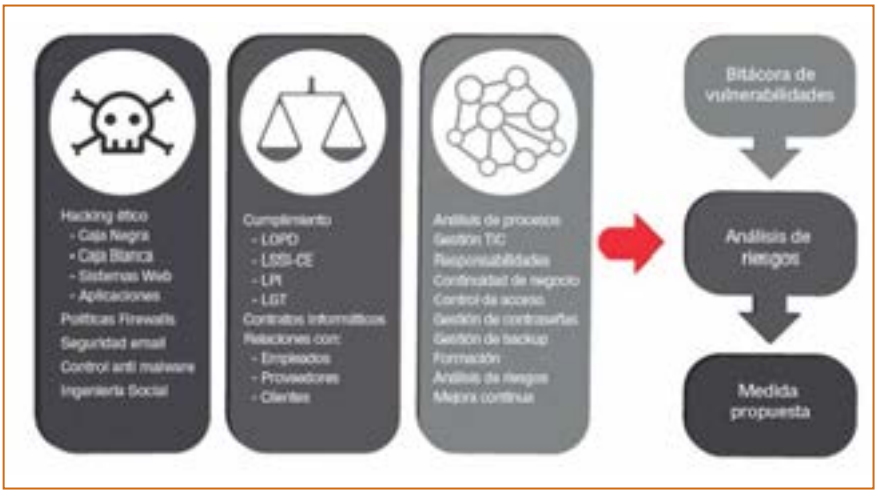
Software de gestión de video

Audio y accesorios

Visítenos en SICUR del 23 al 26 de Febrero en el Stand 10D02

Visita www.axis.com

implica una gestión estratégica, integral (aunando sinergias entre las diferentes áreas de la empresa o institución que se puedan ver implicadas), y planificación, para la puesta en práctica de las políticas de administración de la seguridad más adecuadas. Ello implica análisis de la situación, valoración de activos, procesos y riesgos, y con el fin último de generar un plan director que permita una actuación planificada, con monitorización permanente, prevención, respuesta en tiempo real, etc. Un modelo que Secure&IT considera imprescindible para que la seguridad de la información adquiera una dimensión estratégica en el desarrollo actual de las organizaciones.



«La prevención y la inversión previa en ciberseguridad son de vital importancia para la protección del negocio»

Crecimiento de las TIC

Tan frenético ha sido el crecimiento de las TIC en los últimos años, que de acuerdo con un informe publicado en el año 2013 por la agencia Lloyd´s e Ipsos (Global Risk Index 2013), los ciberataques, que para el año 2011 ocupaban el puesto número trece en la lista de preocupaciones para las compañías multinacionales, ascendieron al tercer puesto, seguido solo por la alta fiscalidad y la pérdida de clientes.

Otro dato que ilustra la importancia de este problema, es la posición que ocupan los ciberataques a gran escala en otro informe. Esta vez nos referimos al Global Risk 2014, un informe realizado por el World Economic Forum que estudió los mayores riesgos a los que se enfrentó la humanidad durante el año objeto de estudio. Los ciberataques a gran escala ocupan, ni más ni menos, que el quinto puesto del ránking del citado informe.

Diseñar una plataforma segura

El objetivo para evitar los ciberataques en pymes es diseñar una plataforma segura que proteja todas las aplicaciones críticas de las empresas con la implementación de las soluciones que necesita la entidad. Esto dependerá de las exigencias de cada empresa. La solución puede ir desde cableado, redes inalámbricas, comunicaciones unificadas, electrónica de red, etc.

La prevención y la inversión previa en ciberseguridad son de vital importancia para la protección del negocio y sobre todo contar con el partner adecuado que asegure una seguridad real.

Fotos: Secure & IT

Contactos de empresas, p. 7.

PURPLE para videovigilancia

Un disco para cada tarea.

wdc.com/purpose

2178-800116-B00 Agosto de 2015

JORGE CHRISTIAN DURÁN. DIRECTOR DE SEGURIDAD; E **INMACULADA PARRAS**. DESARROLLO DE NEGOCIO DE MNEMO

Ciberseguridad para todos...

Son continuos los mensajes que recibimos por todos los medios de comunicación y redes sociales sobre ciberataques.
Para quienes nos movemos en ese contexto la lectura de estos mensajes resulta tan cotidiana que a veces pierde su efecto.
Prevención, prudencia, inteligencia son adjetivos que aplicamos conscientes de su necesidad, pero la realidad nos lleva a un escenario muy diferente.

EL mundo conectado, los nuevos modelos de negocio, las relaciones sociales «digitales», la mensajería instantánea, todos los nuevos dispositivos que se engloban en el IoT (Internet of Thinks/Internet de las cosas), y más, nos arrastran a un mundo donde el cuidado, la atención, o la prevención quedan, sin querer, en un segundo plano.

Y todo lo anterior no queda circunscrito a la realidad doméstica, forma parte del día a día en las empresas, de cualquier tamaño o actividad.

En artículos anteriores reflexionábamos sobre la importancia de redefinir las necesidades en las empresas en términos de seguridad, así como los perfiles que las gestionan, debiéndose incorporar nuevas habilidades, conocimientos y responsabilidades. Este proceso, lejos de ser sencillo, aún tiene que encontrar su espacio.

La mayoría de las empresas tienen, de una u otra forma, la necesidad u obligación de cumplir con requisitos de seguridad que, dependiendo de su madurez tecnológica, está convenientemente resuelta, pero siempre quedan al descubierto algunos espacios que no pudieron ser cubiertos, por distintas razones, normalmente conocidas como limitado presupuesto, prioridades u otros factores.

Un empleado que en su Whatsapp alude a un viaje, genera conclusiones en terceros que pueden tener impacto en la organización. La falta de «información» o «instrucciones» a los empleados sobre la seguridad de la información (amén de la seguridad física)

cada vez se queda más corta, porque cada vez es más difícil poner puertas al campo.

Estos son casos muy sencillos, pero hay otros, por ejemplo, las políticas sobre ByoD (Bring your own device) que requieren políticas muy específicas. El control y monitorización de estos escenarios requiere de herramientas y recursos algo complejos, sin considerar las implicaciones legales.

Otro ejemplo se encuentra en los servicios en la nube. Las aplicaciones que utilizamos en modo servicio o las herramientas que utilizamos para compartir documentos. Dado el caso, documentar los hechos acaecidos en estos escenarios, cuando hablamos de fraude, extracción no autorizada de la información, etc., plantea serios problemas que, incluso, a nivel legal tienen difícil gestión.

Y aun siendo conscientes de todas estas cuestiones, aún hay más, ¿Qué ocurre en escenarios como la compra on line? Para particulares y para empresas.

Los particulares acceden a páginas no siempre seguras, descargan aplicaciones arriesgadas, los niños y no tan niños las descargan sin dar importancia al acto de acceder a información y contenidos que nos hacen aún más vulnerables.

Las empresas deben integrarse con otras organizaciones con las que comparten información a través de aplicaciones, canales que abren paso a nuevas vulnerabilidades, y la realidad es que, a pesar de las advertencias, siempre hay «alguien» capaz de saltarse las medidas de seguridad y barrer con la información o acceder indebidamente. Y vuelta a empezar… ¿Qué ocurre entonces? Esto no sólo no acaba nunca, sino que además, lejos de parecer tener control, cada vez empresas y particulares son más vulnerables.

Las empresas precisan mayor conocimiento de lo que acontece sobre ellas en el exterior, puertas afuera de sus organizaciones. En ocasiones, lo que ocurre en términos maliciosos, ocurre desde dentro:

«Cuando hablamos de Ciberseguridad para todos, realmente deberíamos decir Ciberseguridad en todo»

• Acciones y comportamientos de empleados y directivos, en este último caso, incluso de sus familias.

• Evolución de su modelo de negocio. La evolución de la forma de dar un servicio implica la utilización de nuevas tecnologías y la integración con terceros. Esto exige el acceso «de forma segura» a información que está en otros lugares y asimismo, dar acceso a terceros a nuestros sistemas.

Todos los modelos de negocio basados en internet, todos los servicios que se prestan desde la Red, deberán incorporar en un futuro, no muy lejano, un análisis de impacto en términos de seguridad de la información.

Sectores como la banca, con miles de millones de transacciones electrónicas, el sector salud con cada vez más pacientes conectados, dispositivos de telemedicina enviando información para la atención remota de pacientes, son dos de los escenarios más delicados, donde la información no está tan protegida como sus organizaciones se pueden permitir. Ya hay agencias de calificación que apuntan a bajar el rating de los bancos que no estén bien protegidos frente a ciberataques.

Las compañías aseguradoras comienzan a abordar la cobertura de sus seguros desde este prisma, y se encuen-

tran en la tesitura de tener que ofrecer pólizas mucho más costosas porque la cobertura ante estas situaciones así lo exige. Los servicios asociados al análisis y la valoración de las vulnerabilidades existentes para su corrección o mejora es un coste añadido que no todas las organizaciones ven accesible.

Por lo tanto cuando hablamos de «Ciberseguridad para todos», realmente deberíamos decir «Ciberseguridad en todo». Es el mundo en que vivimos, quien nos lo exige.

Y así, se hace imprescindible, visualizar un marco de acción más complejo, completo y flexible para que individuos y organizaciones estén a la altura de las necesidades.

La mayoría de las empresas cuentan con manuales que contemplan las políticas de seguridad de las compañías. Cuanto mayores y dependiendo del sector más complejas, pero es cierto que, son muchas las que adolecen de este tipo de herramienta. La definición de las políticas de seguridad permitirá a la organización estar en una mejor posición ante circunstancias y eventos que amenacen a la organización desde fuera o incluso dentro. Este es un ejercicio sencillo que no debería quedarse solamente en dar cumplimiento a las exigencias de una certificación o acto similar. Hay que conseguir que se convierta en algo vivo, flexible y una herramienta eficiente para la organización.

Estamos más vigilantes con nuestras redes y sistemas informáticos, pero precisamos hacer revisiones de forma periódica. Esto nos va a exigir contar con herramientas que faciliten la monitorización y seguimiento de contingencias, este hecho pone de manifiesto un elemento adicional y esto es que estar permanentemente actualizado en herramientas y servicios exige un presupuesto del que disponer y no de forma puntual. Y en este sentido cabe destacar que hablamos de herramientas específicas y costosas, por no mencionar la escasez de profesionales cualificados para proporcionar este tipo de servicios.

> «Las empresas precisan mayor conocimiento de lo que acontece sobre ellas en el exterior, puertas afuera de sus organizaciones»

Según se incrementa el nivel de seguridad y las exigencias legales para las compañías aparecen elementos más complejos que requieren servicios específicos. Estos servicios no son exclusivos de grandes corporaciones o de infraestructuras críticas que deben atender al beneficio de los ciudadanos.

Esas organizaciones han de tener en cuenta, de forma específica, la legislación vigente y las buenas prácticas de un sector de actividad. Contar con información e intercambiar información con Equipos de Respuesta a Emergencias de Ciberseguridad es un servicio asequible y revelador para cualquier organización. «Compartir» información con otras empresas de actividad similar o con corporaciones que, por su actividad, están próximas a delitos cibernéticos o no, resulta fundamental en este mundo globalizado.

Allá por el siglo XVII Baltasar Gracián, jesuita y escritor español del siglo de Oro, escribía en una de sus obras lo siguiente: «Trabajar siempre como si nos estuvieran observando». Un mensaje totalmente vigente en nuestro siglo XXI. En lo que se refiere a Ciberseguridad: «Trabajar siempre como si realmente la organización estuviera amenazada, en peligro». Esto no nos debe hacer caer en el alarmismo, sencillamente es una forma de actuar que todos debemos interiorizar.

Fotos: Mnemo/Freepik

Contactos de empresas, p. 7.

UNA VISIÓN ÚNICA EN CIBERSEGURIDAD PARA UN FUTURO MÁS SEGURO

Pieza clave en la ciberdefensa global, Trend Micro trabaja en estrecha colaboración con las Fuerzas y Cuerpos de Seguridad del Estado y organismos gubernamentales en todo el mundo (Policía, Europol, Interpol...) en la lucha contra la ciberdelincuencia y la protección de los datos confidenciales de las empresas.

Con Trend Micro, la seguridad se convierte en realidad.

EUROPEAN CYBERCRIME CENTRE EC3 EUROPOL

www.trendmicro.es

RICARDO CAÑIZARES SALES. DIRECTOR DE CONSULTORIA. EULEN SEGURIDAD

La **ciberseguridad** y las empresas de Seguridad Privada

No voy a intentar definir qué entendemos hoy en día por Ciberseguridad, tampoco voy a intentar explicar el motivo por el cual se ha extendido su utilización, solo voy a destacar un cambio que ha introducido la actual legislación de Protección de Infraestructuras Críticas por medio de la Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos, en las que todas las menciones a la «seguridad lógica» que figuraban en los anteriores contenidos mínimos han sido sustituidos por «ciberseguridad».

COMO ejemplo de lo anterior podemos citar el siguiente párrafo: «El operador deberá reflejar sobre qué partes de su Organización es aplicable la Política de Seguridad de protección de infraestructuras críticas, sin perder de vista que la misma ha de tener un carácter integral, considerando tanto la seguridad física como la ciberseguridad.»

Como se puede ver, se está hablando de «Seguridad Integral» en la que se engloba tanto a la seguridad física como la ciberseguridad; está hablando del paradigma de «la convergencia de la seguridad» o «Seguridad Integral».

Hace ya más de siete años, en mayo de 2008, Eulen Seguridad tomó la decisión de empezar a avanzar hacia la prestación de servicios bajo lo que entonces era un nuevo modelo de seguridad, «la convergencia de la seguridad», que había empezado a tomar forma años antes con la creación por parte de ISACA y ASIS de la Alliance for Enterprise Security Risk Management (AESRM).

En el año 2008 este modelo ya no era nuevo en España, empresas como MAPFRE lo habían adoptado y lo estaban aplicando de forma decidida, el mejor ejemplo de ello fue la creación de su Centro de Control General, órgano que agrupa la estrategia de seguridad del Grupo MAPFRE de manera integral. Supervisa tanto la seguridad relacionada con los sistemas informáticos y redes como la seguridad física.

En ese momento, nuestra compañía se convirtió en la primera empresa

de Seguridad Privada que comenzaba a prestar servicios de seguridad física y de seguridad lógica bajo el paradigma de la convergencia de la seguridad, hoy en día hablamos de Ciberseguridad y Seguridad Integral, ejemplo que ha sido seguido por otras empresas del sector de la Seguridad Privada.

Las empresas de Seguridad Privada que apostaron por el modelo de Seguridad Integral, en el que se encuentra incluida la Ciberseguridad, se encontraron con que algunos actores del mercado no entendían que la Ciberseguridad sea un campo apropiado para las empresas de Seguridad Privada, y no las veían como un proveedor de servicios de Ciberseguridad (seguridad lógica, seguridad de la información, ...), y fue necesario rebatir sus argumentos con razonamientos como el siguiente:

Una de las actividades de la Seguridad Privada es la «vigilancia y protección de bienes» y el Diccionario de la Lengua Española de la Real Academia Española, define «bienes» (sexta acepción), como «Cosas materiales o inmateriales en cuanto objetos de derecho».

Por ello, y como dentro de los bienes inmateriales se encuentra comprendida la información, uno de los activos más valiosos, hoy en día, de las empresas y organizaciones, y dentro de los bienes materiales, los sistemas informáticos que procesan, almacenan y transmiten la información, la prestación de servicios relativos a la seguridad de la información (Ciberseguridad) está comprendida dentro de la actividad «protección de los bienes» que realizan las empresas de Seguridad Privada.

Pero la Ley 5/2014, de 4 de abril, de Seguridad Privada, ha dejado perfectamente claro cuál es el escenario, cuando en varios artículos se menciona a la «seguridad informática» y expresamente se establece que las empresas de Seguridad Privada pueden prestar servicios de seguridad informática, incluso

«La Ley 5/2014 ha supuesto un antes y un después, y cuando se hable de Ciberseguridad habrá que contar con las empresas de Seguridad Privada»

define qué se entiende por seguridad informática en el campo de aplicación de la citada Ley.

No creo que quede ninguna duda de que la Ley 5/2014 ha supuesto un antes y un después, y de que a partir de este momento cuando se hable de Ciberseguridad habrá que contar con las empresas de Seguridad Privada.

El sector de la Seguridad Privada en España cuenta con grandes empresas que llevan decenas de años prestando servicios a sus clientes, como aliados estratégicos, colaborando en la consecución de sus objetivos, ayudándoles a garantizar la continuidad de sus operaciones, dando protección a todos sus activos, tanto materiales como inmateriales, todo ello aportando generación de valor.

Nadie puede poner en duda que las empresas de Seguridad Privada que han decidido prestar servicios de Ciberseguridad a sus clientes, los prestarán con la misma calidad y vocación de servicio con la que han prestado y prestan el resto de los servicios incluidos en su porfolio.

Por otra parte no hay que olvidar la gran experiencia de las empresas de Seguridad Privada en la colaboración con las Fuerzas y Cuerpos de Seguridad, y en el uso de los canales que las FCS han establecido como son Red Azul y Coopera.

Como conclusión, solo hacer constar que las grandes empresas de Seguridad Privada han comenzado a prestar servicios de Ciberseguridad, solo tienen que comprobar sus porfolios de servicios, y que estoy convencido de que cada vez más empresas del sector van a seguir este camino.

Fotos: Eulen/Flickr

Contactos de empresas, p. 7.

EMMANUEL ROESELER. DIRECTOR DE LA DIVISIÓN DE SEGURIDAD DE IBM ESPAÑA, PORTUGAL, GRECIA E ISRAEL

Claves para evitar convertirse en rehén de **Ransomware**

Encender el ordenador y encontrarte con un mensaje que te informa de que todos tus archivos han sido encriptados no es una situación tan extraña hoy día. Los datos se han convertido en información inútil a no ser que puedas descifrarlos y para ello necesitarás utilizar una clave especial por la que tendrás que pagar un buen montante de euros. Esto es un chantaje en toda regla, en una palabra: ransomware.

UN usuario puede caer en las redes de ransomware por abrir el archivo adjunto de un email con remitente desconocido. En los últimos meses, el Servicio de Respuesta ante Emergencias (ERS, por sus siglas en inglés) de IBM ha detectado un preocupante aumento de incidentes de ransomware reportados por sus clientes. En Estados Unidos, entre abril de 2014 y junio de 2015, el Centro de Lucha contra el Cibercrimen del FBI alertó de 992 reclamaciones y más de 18 millones de dólares en pérdidas relacionadas con la variante denominada CryptoWall.

Ransomware no es nuevo. Nació a finales de los 80, pero continúa aumentando su grado de sofisticación. Los métodos de encriptación actuales hacen prácticamente imposible recuperar los datos secuestrados, y solo se aceptan pagos para el rescate en bitcoins, lo que dificulta en gran medida el seguimiento de los cibercriminales que están detrás. Además, se ha ganado a pulso el sobrenombre de «scareware» porque a las víctimas se les dice que han sido contagiadas por visitar páginas web «inapropiadas», de modo que a menudo prefieren pagar el rescate antes de pasar por el trance de avisar a un experto de seguridad.

Las organizaciones que quedan a merced de este chantaje se ven abocadas a pagar la suma solicitada si quieren recuperar documentos importantes cuando no pueden hacerlo por otra vía. Por ejemplo, en caso de que falle el backup o se haya finalizado sobre archivos encriptados. No hay una respuesta sencilla, pero habría que evitar la opción de pagar a no ser que se agoten todas las vías posibles.

Está claro que el conocimiento y la prevención es la mejor defensa. Desafortunadamente, una vez se detecta ransomware suele ser demasiado tarde para recuperar los documentos. A continuación, desgranamos cinco pasos de

la Guía de Respuesta de Ransomware elaborada por IBM ERS, que permitirá a su compañía prevenir en la medida de lo posible un incidente de este tipo:

1. Educar y formar al usuario. Es necesario proporcionar formación periódica sobre amenazas que puedan encontrarse en el día a día y sobre lo que debe hacerse y lo que no en el entorno de trabajo. Una buena medida puede ser enviar un falso phishing para evaluar si los empleados han respondido correctamente ante esta amenaza.

2. Bloquear ficheros adjuntos ejecutables en emails. Siempre que sea posible, configurar el servidor de correo electrónico para impedir el envío de ejecutables, incluyendo los archivos comprimidos ZIP que incluyan extensiones como .exe, .vbs, .com o .scr, entre otras.

3. Restringir la ejecución de programas desde aplicaciones de archivos temporales. La mayoría de los ransomware comienzan intentando copiar las partes útiles de la carpeta de archivos temporales para continuar la cadena de ejecución y ataque. Si se logra bloquear esto, la infección de malware también podrá ser bloqueada.

4. Mantener actualizados antivirus complementándolos con soluciones de análisis de comportamiento. Las soluciones de seguridad endpoint como los antivirus actúan como el principal mecanismo de detección y siempre tiene que contar con la última actualización. En este sentido, también son recomendables soluciones adicionales que se basen en patrones de conducta y aplicaciones fiables, no en firmas. Asimismo, las empresas deberían adoptar políticas serias para la gestión de parches, especialmente en aquellos programas que generan mayor volumen de vulnerabilidades como Adobe Flash y Java. En concreto, Flash ha sido catalogado como una de las principales vías de entrada para ransomware, una

circunstancia que ha llevado a organizaciones a deshabilitarlo por defecto.

5. Testear con regularidad el sistema de backup, almacenar la información crítica fuera del endpoint y tener copia en ubicaciones no accesibles desde el puesto de trabajo. Para reducir la posibilidad de ser víctimas de ransomware y evitar los costes de un rescate, es vital cerciorarse de que el sistema corporativo de backup funciona correctamente a la hora de recuperar copias no cifradas de los datos perdidos. A menudo las empresas afectadas tienen que pagar el rescate porque sus backup no responden correctamente. Además, es vital concienciar a los empleados de que no almacenen información crítica en sus terminales, sino en ubicaciones seguras en la red corporativa sujetas a un backup regular.

Más del 80 por ciento de los responsables de seguridad cree que el desafío de las amenazas externas va a continuar aumentando, mientras que el 60 por ciento reconoce que su organización no cuenta con armas en caso de ciberguerra, según el estudio con CISOs más reciente de IBM. El dinero que pueden obtener los cibercriminales con información valiosa favorece la existencia y propagación de ransomware, pero estos cinco pasos van a contribuir a la defensa de su organización frente al chantaje del cibercrimen.

Un mundo con mayores posibilidades, más abierto y más innovador como el que posibilita la tecnología es, inevitablemente, un mundo más expuesto al riesgo. Existe una gran variedad de tipos de peligros en la Red que las empresas no conocen y que les suponen cada año pérdidas millonarias, llegando a superar la cifra de 100 millones en la mayoría de los casos. Lo que buscan los ataques fundamentalmente es o bien buscar información o buscar dinero, directa o indirectamente. Y hay una tercera intención que es la de dañar la imagen de la empresa.

La clave no es, evidentemente, quedarse quieto para evitar el peligro. La clave es avanzar más deprisa y con más inteligencia para ser capaces de responder a los riesgos, asegurándonos de que todo el enorme potencial de innovación y progreso que contiene la sociedad digital pueda desarrollarse plenamente de forma segura. ●

Fotos: IBM

Contactos de empresas, p. 7.

JAVIER OSUNA. JEFE DE DIVISIÓN DE SEGURIDAD Y PROCESOS DE CONSULTORÍA TECNOLÓGICA. GMV

Cibervigilancia avanzada

Desde la antigüedad hasta no hace demasiado tiempo, leer y escribir estaba al alcance de grupos reducidos. Transmitir mensajes desde una ubicación hasta otra acarreaba esfuerzos importantes, dependiendo de la cantidad y distancia entre los destinatarios, y sin demasiada garantía de éxito. Las nuevas tecnologías han supuesto una revolución y un cambio radical en la forma en que la sociedad se informa, comunica e interactúa.

AUNQUE parezca lejano, hasta finales del siglo XX para publicar información se seguía un proceso tedioso, selectivo y en muchas ocasiones infructuoso. Para ello, lo primero implicaba la generación y firma de algún contenido; obviamente, cuanto mayor fuese la reputación del originador mayor era la receptividad de los editores, mayor la probabilidad de aprobación y mayor la difusión de la publicación. Para ello, el contenido debía llegar a la persona adecuada, que ésta se tomase la molestia de revisarlo, ocasionalmente era modificado y/o censurado, aprobado o rechazado, respaldado por el editor y finalmente publicado en un ámbito, medio o localización concreta.

Con la aparición de Internet, es posible acceder a la información publicada, independientemente de su origen, desde cualquier lugar del mundo, y desde la adopción de la tecnología móvil y la aceptación generalizada del uso de redes sociales, foros, chats y demás, cualquier usuario tiene a su alcance una hoja en blanco para escribir/publicar/opinar y leer lo que quiera desde cualquier ubicación, en cualquier momento. Tal es así, que en 2014 el presidente de Google, Eric Schmidt, afirmó que había 5 millones de terabytes de datos en Internet de los que tenían indexados alrededor del 0,004%.

El resultado de dicha democratización, revolución y aceleración en la creación e intercambio de contenidos ha supuesto un beneficio enorme a la sociedad y ha causado perjuicios de diversa índole. Por un lado, figura el grado de certidumbre o credibilidad de los contenidos que cualquier persona anónima puede generar sobre cualquier tema. Por otro, generar información es fácil, actualizarla es un pelín más complicado, y eliminarla, en muchos casos, es misión imposible; de hecho, se puede empezar a hablar del concepto de ciberbasura; aunque, lo dejaremos para otra ocasión.

Uno de los mayores cambios que ha supuesto la adopción del ciberespacio es la inexistencia de fronteras que, junto a la carencia de acuerdos y le-

gislación internacional, la dificultad de identificar el origen, la financiación de determinados gobiernos y la incapacidad de estar a todo, hace que traviesos, delincuentes, acosadores, ciberanarquistas, organizaciones sin escrúpulos, mafias, grupos terroristas y gobiernos, entre otros, aprovechen para ocultarse entre la masa y campen a sus anchas para llevar a cabo actividades ilegales o paralegales.

Huelga decir que la rápida adopción de la combinación Internet, móvil y redes sociales, junto a su generalizada aceptación a nivel mundial, ha generado un número de usuarios, que según distintas fuentes, fluctúa entre un tercio y la mitad de la población mundial. El perfil de éstos varía atendiendo a la edad y la naturaleza del mismo. Por un lado se encuentran niños, adolescentes, jóvenes, adultos y ancianos, y por otro, particulares, autónomos, pymes, empresas, ONGs, Corporaciones, Administraciones Públicas y Gobiernos. En ambos grupos existen grados de concienciación muy dispares en materia de seguridad y un enorme desconocimiento sobre las consecuencias del uso inadecuado de los medios sociales. Imaginemos que en un periodo inferior a 10 años, más de la mitad de la población tuviese acceso a fabricar determinado tipo de medicamentos sin licencia.

Dentro de dichas actividades ilegales o paralegales que en este nuevo contexto pueden darse cabe destacar:

- El robo y venta de credenciales e información.
- Compraventa de productos ilícitos.
- Publicación de información confidencial.
- Actividades fraudulentas con la finalidad de robar y blanquear dinero.
- Suplantación de identidades con fines delictivos.

«Uno de los mayores cambios que ha supuesto la adopción del ciberespacio es la inexistencia de fronteras»

- Falsedades y rumores para dañar la reputación de personas y organizaciones.
- Coordinación y orquestación de actividades fraudulentas.
- Extorsión y ciberacoso.
- Coordinación de ataques, movilizaciones y concentraciones.
- Espionaje industrial y nacional.
- Adoctrinamiento y reclutamiento.
- Compartición de información y experiencias no aceptadas generalmente.
- Uso indebido de servidores, ordenadores y credenciales comprometidas.

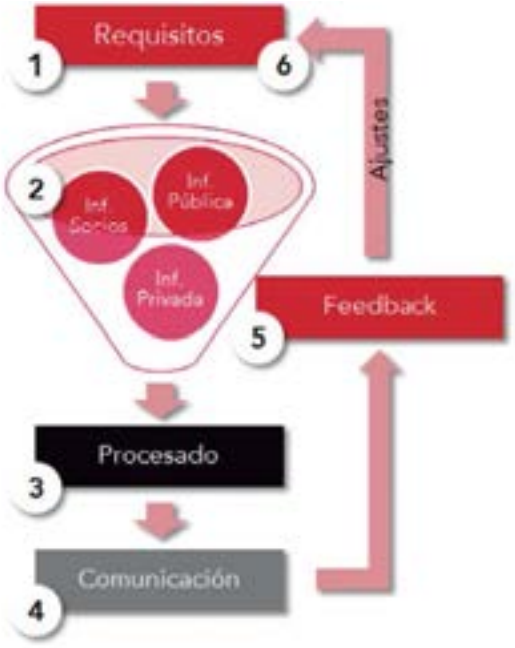
Todo ello ha generado inquietud a nivel internacional en agencias de inteligencia, Gobiernos, Fuerzas y Cuerpos de Seguridad del Estado, Corporaciones y colectivos de usuarios que se ven incapaces de defenderse frente a tales amenazas. En este sentido, encontrar información que pueda suponer una amenaza para la integridad de ciudadanos, organizaciones y países se ha convertido en algo prioritario. Dada la cantidad de usuarios e información que existe, el reto es equivalente a encontrar agujas en pajares accesibles y diseminados física y lógicamente a través del planeta.

A raíz de esta necesidad y ante la demanda por parte de clientes, grandes corporaciones, con estrictos requisitos de seguridad, GMV diseñó hace seis años un servicio a medida, de carácter artesanal, para dar apoyo a la inteligencia, basado en la Cibervigilancia complementando actividades de Ciberseguridad y Ciberfraude.

Vigilancia Digital

Las organizaciones acuden a servicios de Cibervigilancia para disponer de un mayor y mejor conocimiento sobre la información que se maneja en la red sobre ellas, así como determinar aquella que pueda suponer una amenaza e incrementar de esta manera su seguridad.

Gráfico 1



Ante esta demanda efectiva, nuestra compañía ha evolucionado el servicio que viene prestando desde hace años implementando su propia solución: Atalaya. Una respuesta de vigilancia digital que aplica tecnologías emergentes como algoritmos de inteligencia artificial y BigData. La combinación de ambas tecnologías permite procesar grandes volúmenes de datos obtenidos de fuentes de información diversas como buscadores, redes sociales, blogs, IRCs, RSS, contenedores de información, redes P2P, foros especializados, youtube, otras redes públicas o no, etc., y convertirlos en información de una forma eficiente, disminuyendo considerablemente el número de falsos positivos y negativos. **Gráfico 1**

La utilización de esta solución está diseñada para implantar o reforzar buenas prácticas como la centralización del control, adhesión a requisitos de cliente, protección de fuentes, explotación sistemática de la información, compartimentación de los casos de investigación, revisión continua y entrega en tiempo.

Alguna de estas buenas prácticas son recomendadas por el principio CROSS-CAT-V.

Para optimizar los resultados aportados por los algoritmos de «aprendizaje» o (Explicar) es posible desglosar automáticamente la información en partes más pequeñas y clasificar, también de forma automática, dichos fragmentos en base a muestras aprendidas con anterioridad. Esto facilita la localización de fugas de información confidencial, encontrar aportaciones de otros actores sobre diversos temas o predecir acciones que se están planificando contra la organización en la que trabajamos para proteger.

Adicionalmente, Atalaya facilita la adaptación de la parametrización de búsqueda para optimizar los resultados, porque evidentemente, los hábitos y habilidades de evasión van cambiando conforme las capacidades de detección mejoran.

Otra de las técnicas empleadas es la compartición de información que pueda suponer una amenaza; de hecho, regulaciones y legislaciones tienden a requerir dicho mecanismo. De este modo, organizaciones y/o agencias gubernamentales pueden compartir información que alerte a otros sobre amenazas. A fecha de hoy, existe un gran recelo en proporcionar información que muestre las «vergüenzas» internas de una organización y, por otro lado, no podemos obviar que es difícil discriminar entre aquellos de quien fiarse y de quienes no.

En conclusión, estar al tanto de lo que se dice, se vende y se orquesta contra tu organización supone una ventaja competitiva directamente proporcional al ritmo frenético marcado por las nuevas tecnologías y medios sociales en la forma de ofrecer servicios y hacer negocios en un mundo moderno y global. ●

Fotos: GMV

Contactos de empresas, p. 7.

SEGÚN UN ESTUDIO DE LA CONSULTORA QUOCIRCA, ENCARGADO POR TREND MICRO

España, entre los países de la UE más afectados por los ciberataques dirigidos

«España se ha visto fuertemente golpeada por los ataques dirigidos en el último año. Las organizaciones españolas están sufriendo algunas de las peores pérdidas de datos que se están produciendo en Europa, estando relacionadas en su mayoría con el robo de tarjetas de crédito y datos personales.
Sin embargo, en vez de preocuparse por el cibercrimen, lo están más por verse atacadas por prácticas de espionaje por parte de la competencia». Ésta es una de las principales conclusiones que se extrae de la investigación correspondiente a España y que ha sido encargada por Trend Micro a la consultora independiente Quocirca.

SEGÚN el estudio, «The trouble at your door», en el que participan 600 organizaciones europeas procedentes de Alemania, España, Francia, Italia, Países Nórdicos y Reino Unido, se pone de manifiesto que, independientemente de dónde procedan los ataques, las empresas españolas están entre las menos preparadas para defenderse ante este tipo de incidentes de seguridad que otras compañías europeas.

El objetivo de esta investigación es examinar el conocimiento y las experiencias relacionadas con los ciberataques dirigidos en las organizaciones europeas de diferentes sectores.

Entre los diferentes sectores de actividad analizados, el de TI es el que concentra el mayor número de ataques, posiblemente debido al conocimiento que los trabajadores tienen sobre el problema de las ciberamenazas. Sin embargo, éste es el sector mejor preparado para combatir tal situación. Servicios Financieros, Administración Pública y Retail, le siguen de cerca; pues en todos ellos existe un tratamiento amplio de datos personales y/o información relacionada con tarjetas de pago. Según la investigación, las empresas enmarcadas en el sector Utilities deberían estar más concienciadas e incrementar las medidas de seguridad puesto que las fugas de datos provocadas en este ámbito por los ataques dirigidos son altas.

Objetivo: España

Esta edición española de este estudio, correspondiente a 2015, analiza cómo están de preparadas las organizaciones para hacer frente a los ataques dirigidos en nuestro país en comparación con la media europea. Así, se pone de manifiesto que el 10% de las corporaciones españolas se encuentran entre los 25 primeros puestos dentro del ranking Top 40 de los peores ciberataques dirigidos. Por sectores, el de

Retail fue el más afectado, seguido por Servicios Financieros, Transporte (clasificación que incluye los servicios de distribución y logística) y Utilities.

Estos ciberataques dirigidos han sido los que peores consecuencias en términos de daños a la reputación, pérdida de datos y/o costes económicos han tenido para los negocios.

Por otro lado, de las 600 organizaciones europeas participantes en la investigación, un total de 369 compañías afirman haberse visto afectadas por ciberataques dirigidos durante los últimos 12 meses. Por su parte, 95 corporaciones confirmaron no estar completamente seguras de haber estado expuestas a un ataque dirigido. Por el contrario, las 136 restantes creen que no se han visto afectadas en ningún momento por estas amenazas.

En términos generales, de estas 369 empresas europeas que se han enfrentado a ataques de seguridad, 251 confirman que al menos un ataque se ha realizado con éxito; 133 sufrieron robo de datos o vieron cómo su información no estaba segura, mientras 64 informaron de daños significativos o serios para su reputación.

En el último año se registraron 12 incidentes con robo de datos de tarjetas de pago en España, más que en cualquier otra región de Europa; igualmente, hubo 11 denuncias de robo de datos personales y se informó de 3 incidentes contra la propiedad intelectual entre las firmas españolas encuestadas. Según la investigación, sólo el 27% de los negocios nacionales cuenta con un plan de respuesta ante brechas de datos; porcentaje que es, con mucho, el más bajo de todos los mercados que participan en la investigación.

El coste asociado a estos ciberataques en la región, en cada una de las empresas afectadas, fue de aproximadamente un millón de euros.

Los cibercriminales suelen centrarse en el robo de tarjetas de pago y datos personales más que en la propiedad intelectual. A pesar de esto, los negocios españoles se preocupan más por el espionaje industrial a escala local, ya sea dentro de España o en la UE, con un total de 4,3 puntos en comparación con los 3,8 de media europea. Contrasta esto con que España es la región que menos se preocupa por el cibercrimen (3,4 puntos) frente a los 4,3 del resto de Europa.

A pesar de este panorama, las organizaciones españolas son las menos propensas a considerar que los ataques dirigidos son inevitables; sólo el 6% opina esto frente al 24% del resto de países europeos participantes en la investigación. Según esto, sólo el 5% se mostraba confiada en sus sistemas, porcentaje similar al resto de Europa. La conclusión a la que llega Quocirca es que España está siendo fuertemente golpeada por los ataques dirigidos y las organizaciones españolas deberían estar haciendo mucho más para mitigar el problema.

«La investigación presentada en este informe tiene un mensaje claro: casi con total probabilidad su organización será víctima de un ciberataque dirigido en algún momento. Existe la posibilidad de que más de 1 de cada 10 intentos de ataque concluya en una pérdida de datos importantes y/o daños a la reputación de la compañía», afirma David Sancho, responsable de investigación de Trend Micro en Iberia. Sin embargo, poner en marcha algunas medidas «antes, durante y después de pueden minimizar tales pérdidas de datos, daños a la reputación y el coste global para el negocio de dichos ataques».

Para Tomás Lara, director general de Trend Micro Iberia: «en general, las organizaciones españolas son las menos preparadas para defenderse contra los ataques dirigidos; la consecuencia de esto es que nuestras empresas están sufriendo algunas de las peores pérdidas de datos en Europa. La amenaza de los ataques dirigidos no va a desaparecer, por lo que la única buena práctica pasa por estar preparados y contar con iniciativas, tecnologías y servicios en nuestras empresas que puedan medir y contrarrestar los efectos de forma considerable. El cibercrimen no va a desaparecer, pero sí se puede combatir».

Fotos: Trend Micro

Contactos de empresas, p. 7.

ENCUENTRO ORGANIZADO POR INCIBE

Éxito de asistencia en **Cybercamp 2015**

Más de 10.000 personas visitaron CyberCamp 2015 y otras 12.000 lo siguieron a través de video streaming

Más de 10.000 personas visitaron CyberCamp 2015 y otras 12.000 lo siguieron a través de video streaming. Son las primeras cifras que arroja el balance de Cybercamp 2015, el gran evento dedicado a la ciberseguridad, que se celebró del 26 al 29 de noviembre en Madrid. Un encuentro que contó con un amplio programa de conferencias, así como las primeras Cyberolimpiadas de seguridad para colegios en España, entre otras actividades.

EL secretario de Estado de Telecomunicaciones y de Sociedad de la Información, y el secretario de Estado de Seguridad, Víctor Calvo-Sotelo y Francisco Martínez-Vázquez, respectivamente, inauguraron CyberCamp 2015, el gran evento de ciberseguridad que se celebró del 26 al 29 de noviembre en Madrid.

Identificar, atraer, gestionar y en definitiva, ayudar a la generación de talento, son los objetivos de esta gran fiesta del mundo de la ciberseguridad, organizada por el Instituto Nacional de Ciberseguridad (INCIBE), que engloba actividades para todos los sectores y para todas las edades, además de contar con más de 120 ponentes expertos en la materia.

El secretario de Estado de Telecomunicaciones, Víctor Calvo-Sotelo, explicó que CyberCamp es «un punto de encuentro de profesionales presentes y profesionales futuros, y una forma de sensibilización y concienciación sobre la importancia de conseguir un elevado nivel de confianza en las Nuevas Tecnologías». Tras indicar que entre enero y octubre de 2015 se habían resuelto en España 42.800 incidentes de ciberseguridad, recalcó que «el riesgo es real, pero estamos preparados para hacer frente a estas amenazas».

Por su parte, el secretario de Estado de Seguridad, Francisco Martínez-Vázquez, aseguró que «somos testigos de una revolución que no tiene precedentes en la historia» y añadió que «todos somos conscientes de las vulnerabilidades que supone la ciberseguridad» pero recalcó que «el binomio tecnología-seguridad ofrece cosas muy buenas».

Por último, el director general del INCIBE, Miguel Rego, resaltó que Cybercamp se fundamenta en tres ejes principales: la generación de talento, la generación de tejido empresarial y las familias. Rego señaló que actualmente «se demandan muchos profesionales y

esa demanda no puede ser atendida, por lo que hay que trabajar desde la 'cantera', con los muchachos más jóvenes», y añadió que Cybercamp permite que las empresas de ciberseguridad tomen contacto con posibles candidatos..

CyberCamp 2015 incluyó un amplio programa de conferencias a cargo de los mejores ponentes del panorama nacional e internacional en materia de ciberseguridad, además del foro «Empleo y talento» donde más de una veintena de empresas realizaron entrevistas a posibles candidatos. Asimismo,contó con un apartado específico para familias, con talleres, charlas y actividades lúdicas. Concursos como el Hackathon o las primeras Cyberolimpiadas de seguridad para colegios en España, son otras citas importantes que han tenido lugar en este evento en el que también hubo un espacio dedicado al ocio, donde pudieron contemplarse multitud de novedades tecnológicas.

Así, cerca de mil chavales, de edades comprendidas entre los 12 y los 18, participaron en estas primeras CyberOlimpics de España. Un total de 110 centros educativos de Enseñanza Secundaria, Bachillerato y Formación Profesional participaron en esta iniciativa, demostrando sus habilidades técnicas en distintos campos de la seguridad en Internet y las nuevas tecnologías.

En el acto de clausura del evento, el secretario de Estado de Telecomunicaciones y Sociedad de la Información, Víctor Calvo-Sotelo, destacó que se habían duplicado las cifras de asistencia con respecto a la primera edición y recalcó que se ha cumplido el objetivo principal que no es otro que «promover un punto de encuentro con los profesionales de hoy y los futuros talentos del mañana y conectarlos con la necesidad real del sector».

Por su parte, el director general del INCIBE, Miguel Rego, dio las gracias a la comunidad hacker, a los emprendedores, a las empresas y a las familias que visitaron CyberCamp y destacó el excelente nivel de los jóvenes que han participado en los diferentes retos y concursos.

Finalmente, Rego aportó algunas cifras que hablan de la importancia adquirida por esta gran fiesta de la ciberseguridad, recordando que más de 1.000 chavales han participado en las CyberOlympics, se han presentado 42 proyectos de emprendimiento, 19 empresas han participado de forma presencial en el Foro «Empleo y Talento» realizando entrevistas a posibles candidatos para ocupar puestos de trabajo y otras 31 lo han hecho a través del foro virtual.

*Fotos: **INCIBE***

MANUEL LATORRE. DIRECTOR COMERCIAL DE HIGH SECURITY. TYCO IF&S IBERIA

Cuestión de seguridad en los **Data Centers**

La creación de datos está a la orden del día, en el momento en que compartimos información ya sea en Facebook, Twitter, LinkedIn o simplemente participando en un blog o una página web estamos generando datos. Si una sola persona genera una gran cantidad de datos, imagínense a nivel empresarial en todo el mundo. Estos datos tienen que ser guardados en un centro de datos.

ANTERIORMENTE, los datos de las empresas se guardaban en salas de servidores locales, pero las empresas optan cada vez más por proveedores de co-ubicación para cubrir sus necesidades de almacenamiento de datos. Los motivos son un mayor control de su infraestructura común de telecomunicaciones, mientras se benefician de la tecnología más moderna, de la escalabilidad, seguridad y disponibilidad que ofrecen los centros de datos a terceros. Externalizar la necesidad de mayor capacidad de centros de datos en un proveedor de alojamiento constituye la mejor solución para muchas empresas que no tienen interés en construir sus propios centros de datos, pudiendo así centrarse más en su negocio principal, sin perder el control de sus datos, sistemas, procesos o conocimientos.

En los últimos años, debido al gran aumento en el tamaño de datos, las empresas se han visto obligadas a innovar en los centros de datos para poder ofrecer una amplia variedad de conectividad y una disponibilidad operativa que sea segura, en la que se puedan desarrollar negocios en comunidad en un centro de co-ubicación y con el mundo exterior. Así los centros de datos se esfuerzan para estar al día con las crecientes exigencias del mercado.

La seguridad está en constante cambio, ya que es una parte fundamental para el funcionamiento de los centros de datos. Pero no sólo basta la seguridad informática. Tener una buena seguridad y protección contra incendios es algo fundamental para estas instalaciones, ya que es necesario garantizar que todos los datos se almacenen en un entorno seguro.

Protección de gran fiabilidad

Las actuales soluciones de seguridad proporcionan una protección de gran fiabilidad. Por ejemplo, las de control de acceso son muy eficientes para evitar intrusiones y mantener una vigilancia exhaustiva de las personas que tienen accesos a las diferentes zonas del CPD, evitando el robo de datos. Los sistemas de extinción de incendios por gases permiten proteger las instalacio-

nes frente a incidencias provocadas por causas eléctricas o accidentales.

Especialmente sensibles a los incendios

Los grandes centros de datos pueden ser especialmente sensibles a los incendios, debido al gran número de aparatos eléctricos y las temperaturas que generan. Esto hace necesario instalar sistemas de detección y extinción de incendios adaptados. Los sistemas de extinción por gas más innovadores permiten continuar con la actividad mientras está activada la alarma contra incendios, esto es algo fundamental ya que evita bloquear todo el centro de datos cuando se produce una alarma por incendio. Los volúmenes de aire que se bombean en una habitación de un centro de datos son muy grandes, por lo que si éstos pasaran a través de un fuego, lo que ocurriría en un minuto sería desastroso. En cambio, si el espacio está protegido con un gas para extinción de incendios, el fuego no resistirá.

Soluciones devideovigilancia

Otras de las soluciones de seguridad de Tyco para este tipo de espacios incluyen también videovigilancia, sistemas de intercomunicación, de control de acceso y de detección de intrusos con lectores de tarjetas. Actualmente, todos estos sistemas de control pueden centralizarse y gestionarse de forma remota, lo que permite una mejor gestión de la seguridad, no sólo en el centro de datos, sino en todo el conjunto de la empresa. Gracias a ello es posible organizar las autorizaciones, tramitar permisos y garantizar accesos a distancia. Este nivel de normalización ahorra costes a las empresas con centros y oficinas en diversos lugares.

> «Los grandes centros de datos pueden ser especialmente sensibles a los incendios, debido al gran número de aparatos eléctricos y las temperaturas que generan»

Empresas integradoras

Las empresas integradoras de seguridad se convierten en un aliado estratégico e imprescindible para asegurar la protección de los centros de datos. Sólo un especialista en seguridad es capaz de identificar los riesgos específicos a los que se enfrentan los centros de datos, proporcionar las herramientas técnicas imprescindibles para proteger instalaciones de todo tipo y ofrecer el consejo y orientación necesarios para diseñar una estrategia de seguridad fiable y óptima, que responda a la perfección a todas las necesidades específicas de cada CPD. ●

Fotos: Tyco IF&S/Flickr

Contactos de empresas, p. 7.

RAM OFIR. DIRECTOR GENERAL DE AMIMON

Seguridad en tiempo real con latencia cero

No hay duda, el equipamiento técnico más popular de este año son los drones o, como la FAA prefiere denominarlos, Sistemas Aéreos no Tripulados (UAS). Si bien el uso comercial de drones en gran parte aún está prohibido, hay una tendencia al desarrollo de aplicaciones que estimulará el rápido crecimiento del uso de drones tanto por parte de aficionados, como por profesionales.

GRACIAS a los avances en electrónica, baterías y tecnologías inalámbricas, los drones ahora son capaces de añadir un nuevo valor y nuevas opciones para muchas aplicaciones, desde ayudar a los agricultores a localizar sus vacas, hasta mejorar la repercusión de la difusión de los deportes al aire libre. Pero no hay ninguna aplicación que tenga más potencial para salvar vidas que la utilización de cámaras montadas en drones para resolver algunos de los desafíos de seguridad acuciantes de nuestro tiempo.

A diferencia de su uso por parte de aficionados, las aplicaciones de seguridad profesional a menudo requieren la captura y transmisión de secuencias de vídeo, más allá de las capacidades tecnológicas de los sistemas basados en drones precedentes. Este artículo abordará las aplicaciones de seguridad en vídeo basadas en drones, incluyendo inspecciones de seguridad y tareas de búsqueda y rescate, y se considerarán algunos de los factores clave para una implementación con éxito, incluido el cambiante panorama normativo.

Tecnologías de respaldo principales

Hay tres áreas de mejora tecnológica que son factores de respaldo esenciales en el uso del vídeo en el ámbito de la seguridad. La primera de ellas es la capacidad de los drones de reducido tamaño de llevar cámaras de alta calidad. En este sentido, los dos lados de la ecuación están experimentando mejoras. Los drones están aumentando su capacidad con baterías más ligeras, motores y fuselajes más robustos y cámaras de alta calidad que cada vez se hacen más pequeñas y ligeras. Hoy en día el mayor de los pequeños drones multirrotor, con 8 rotores y diseñado para maximizar la carga útil, puede fácilmente llevar cámaras de alta resolución con capacidades de filmar tanto en el espectro visible como en el de infrarrojos.

La segunda área tecnológica de respaldo es la disponibilidad de soportes de cámara orientables y ligeros, que ofrecen un eficaz aislamiento frente a las vibraciones y un posicionamiento y control de la cámara. Hoy en día hay muchos modelos disponibles que pueden montar una amplia gama de cámaras, incluyendo discretos modelos en miniatura, cámaras réflex digitales y hasta pequeñas cámaras de tipo cinematográfico. La gama de productos abarca desde soportes de aislamiento de bajo coste hasta soportes motorizados sensibles de proveedores como DJI, Storm, Tarot y otros. Representan un avance importante, porque de lo contrario la vibración de los rotores de los drones y el efecto de las condiciones ambientales afectarían negativamente a la calidad de vídeo.

La tercera tecnología de respaldo es la del enlace inalámbrico con la cámara. Las señales inalámbricas se utilizan para controlar el propio dron, lo que permite a un piloto controlar la posición del mismo y maniobrar según sea necesario. En este caso cualquier retraso de la señal podría causar problemas. El operador de la cámara debe poder ver exactamente lo que está filmando la cámara en tiempo real. Los nuevos productos como Amimon Connex, ya

en el mercado, transmiten vídeo en Full HD con latencia cero. Este nivel de visibilidad y control es necesario para que el operador de seguridad pueda controlar la cámara y capturar las imágenes deseadas.

Aplicaciones y ventajas relacionadas con la seguridad

Combinando las capacidades de estas tecnologías de respaldo, los drones equipados con cámaras de vídeo se pueden adaptar para satisfacer las necesidades de tareas de seguridad específicas, incluidas las inspecciones de seguridad de infraestructuras y las operaciones de búsqueda y rescate.

Como ejemplo, considere un posible caso de amenaza de seguridad en un puente de ferrocarril o en otra instalación de infraestructuras complejas. En el pasado, la única manera de poder tener una visión muy cercana de la parte inferior de un puente era colocar un andamio o una plataforma equivalente, o hacer que una o más personas subieran a su estructura. Ambos enfoques permitirían su inspección, pero también plantearían nuevos problemas de seguridad. Incluso es posible que estas mismas instalaciones ofrecieran un acceso a la estructura a los mismos delincuentes.

Con uno o más drones equipados adecuadamente, esta misma inspección de puentes podría llevarse a cabo de forma rápida, segura y sin ofrecer oportunidades de vandalismo. En este caso, los drones estarían equipados con cámaras de alta resolución, ofreciendo un excelente rendimiento tanto en condiciones de poca luz como si van equipados con una fuente de luz propia. El tamaño de los drones seleccionados debería ser el apropiado para posibilitar su movilidad por los espacios de la estructura con un margen adecuado para el error. El enlace de vídeo en tiempo real tendría latencia cero a resolución completa para permitir al operador controlar el dron con eficacia y seguridad en este espacio restringido. Tener este enlace con latencia cero es fundamental para esta operación, ya que cualquier latencia de vídeo mientras se pilota un dron a través de espacios estrechos aumentaría las posibilidades de dañar, destruir o perder el dron y la cámara.

Pongamos otro ejemplo y examinemos dos casos recientes: dos fugados de una cárcel de alta seguridad en una zona rural boscosa y el caso de un francotirador escondido en un terreno de similares características. En estos dos casos, se utilizaron cientos de oficiales y voluntarios para buscar en la zona en la que se pensaba que los fugitivos se escondían, lo que supuso un laborioso y costoso procedimiento. Se cree que los oficiales estuvieron en ocasiones cerca de estos sujetos sin darse cuenta y cuando se percataron de ello, no tenían a su disposición la capacidad de seguirlos cuando huyeron.

Se podría haber utilizado en esta ocasión uno o más drones con cámaras térmicas para complementar el trabajo de los agentes, ayudando a la detección de la presencia y los movimientos de los fugitivos. Debido a la naturaleza de la situación, los drones se podrían ha-

Contactos de empresas, p. 7.

ber utilizado durante las horas nocturnas, cuando los fugitivos posiblemente aumentaron sus movimientos al abrigo de la oscuridad. Como en el caso anterior, tener un enlace de vídeo en tiempo real con latencia cero sería fundamental para esta aplicación, debido a la disminución de la capacidad del operador de ver la posición y el movimiento del dron. En su lugar el operador depende de la propia secuencia de vídeo transmitida para mantener unas condiciones de vuelo seguras, evitando colisionar con árboles, tendidos de cables y otros obstáculos similares.

En cada una de estas aplicaciones, el uso de drones ofrece las ventajas adicionales de la velocidad y la flexibilidad operativa en comparación con otras alternativas. Los drones pueden estar preparados para entrar en acción en cuestión de minutos, en lugar de en horas o días, ofreciendo apoyo rápidamente en las fases más tempranas de las operaciones. Esta capacidad de poder actuar rápidamente se traduce en menos interrupciones operativas y menores costes en el caso de las inspecciones de infraestructuras, y en búsquedas más rápidas de fugitivos, ayudando a limitar la extensión de la zona de búsqueda.

Desafíos de la implementación

Recientemente se han producido grandes avances, tanto en el aumento de las capacidades de los pequeños drones como en la reducción de sus costes, pero todavía hay barreras significativas para su uso generalizado.

En primer lugar, todos los sistemas aéreos, incluyendo los drones, están bajo la supervisión de la FAA. Antes de 2012, los operadores consideraban a los drones como «aeromodelismo» y por lo tanto no estaban sujetos a los rigurosos requisitos de pruebas de fuselaje y certificaciones de pilotos que se requieren para otras aeronaves. En 2012, una nueva ley federal definió claramente a los aparatos de aeromodelismo como aeronaves, añadiendo específicamente la competencia de la FAA, pero permitiendo ciertas aplicaciones, incluyendo agencias gubernamentales autorizadas y su uso estrictamente en el ámbito de la afición. Por el momento, todos los usos con fines comerciales están prohibidos salvo autorización expresa de la FAA, pero esa situación probablemente cambie en breve. La FAA ha otorgado aproximadamente 1000 exenciones caso por caso, y ha propuesto nuevas normas cuya ejecución se encuentra en consideración para los próximos meses.

Si se implementan las normas propuestas, muchas de las reglas de las operaciones comerciales serán similares a las normas de funcionamiento actuales respecto a las aficiones. Por ejemplo, los drones deben pesar menos de 55 libras (25 kg), solo pueden utilizarse durante el día y deben mantenerse por debajo de los 500 pies desde el nivel del suelo y dentro del rango visual del operador. Los requisitos más importantes son para los operadores: las normas propuestas requieren que los operadores tengan al menos 17 años de edad, que sean examinados por la TSA y que se certifiquen por la FAA, superando una prueba de conocimientos aeronáuticos periódica cada 24 meses. Si bien esto parece un gran paso, continúa siendo mucho menor que el requisito actual para los operadores comerciales que tienen una licencia de piloto.

También hay un considerable sentimiento público contra los drones y la preocupación por las cuestiones sobre la privacidad, que es poco probable que desaparezca, aunque las operaciones con drones comerciales se vuelvan más cotidianas. Con la intención de ayudar a solucionar esto, al menos 13 estados ya han puesto en práctica la nueva legislación relativa a los derechos de privacidad y a otras cuestiones relacionadas que no están reguladas por la FAA y que se centran principalmente en la seguridad. Algunos expertos también han señalado que las leyes de allanamiento y privacidad sí prohíben algunos de los comportamientos que preocupan a la gente, y permanecerán en vigor.

Avanzando

Aún estamos en una fase muy temprana de la comprensión de todas las posibilidades que ofrecen los drones al sector de la Seguridad, pero está claro que se convertirán en una herramienta de gran valor. Seguiremos trabajando para un mundo más seguro para todos. ●

*Fotos: **Amimon***

Contactos de empresas, p. 7.

sicur

Salón Internacional de la Seguridad
International Security, Safety and Fire Exhibition

23-26 FEBRERO
February
2016

ORGANIZA / *ORGANISED BY*
IFEMA Feria de Madrid

Seguridad contra incendios y emergencias
Fire safety and emergency

Seguridad laboral
Safety and health at work

Security

Defensa
Defense

www.sicur.ifema.es

LINEA IFEMA / *IFEMA CALL CENTRE*

LLAMADAS DESDE ESPAÑA / *CALLS FROM SPAIN*
INFOIFEMA 902 22 15 15
LLAMADAS INTERNACIONALES (34) 91 722 30 00
INTERNATIONAL CALLS
FAX (34) 91 722 57 88
sicur@ifema.es

Mª AMOR DOMÍNGUEZ. MANAGER IT BUSINESS UNIT. TÜV NORD CUALICONTROL

La certificación en IT y la empresa segura

«A pocos kilómetros de aquí, por ejemplo, hay un edificio que maneja gran parte del tráfico transpacífico de Internet. Solo haría falta que alguien fuera al sótano de ese edificio... Es decir hay puntos vulnerables y un ataque es posible», Leonard Kleinrock, entrevista de XL Semanal, ABC, noviembre de 2015

Ya no se discute en ningún foro, empresa o conversación entre particulares la necesidad de proteger el mayor bien que hoy día parece que tenemos los humanos, esto es la información y con ella nuestra intimidad. Por eso, la protección de nuestras infraestructuras tecnológicas, nuestras redes de información, nuestros Centros de Procesos de Datos, y nuestras aplicaciones necesitan una protección mayor que la que pueden ofrecer los componentes tecnológicos.

EFECTIVAMENTE, el mercado de los productos de Seguridad, valorado según los expertos en aproximadamente 50 billones de dólares no parece suficiente para evitar que las organizaciones sean atacadas y nuestros datos personales expuestos.

En la prestigiosa Conferencia RSA de San Francisco de abril del pasado año, su nuevo presidente, el Sr. Amit Yoran, identificó cinco riesgos esenciales para que las organizaciones se puedan proteger, tales como:

1. Las barreras de protección, por avanzadas que sean, no son suficientes. Los últimos ataques no han entrado vía malware.
2. Es muy importante conseguir una visibilidad completa de la red, desde los puertos de entrada hasta la nube. Sin esta visibilidad 360º los ataques pasarán desapercibidos.
3. La gestión de identidades y autenticación son más importantes que nunca, así como el control riguroso de accesos.
4. Es imprescindible integrar todas las fuentes de información sobre los incidentes de Seguridad, tanto internos como externos.
5. Valorar en primer lugar lo que es de verdad importante para el negocio y esto protegerlo y defenderlo.

Grafico 1

Si miramos con detalle estos cinco elementos, vemos que hay una necesidad latente de proceso, de proceso claro que permita desde la identificación de los bienes tecnológicos que se deben de proteger a la atención inmediata a un incidente cuando se detecta y las medidas a seguir para resolver los daños causados.

Estos procesos tienen que ser cla-

ros, conocidos dentro de la organización y suficientemente estandarizados para permitir la colaboración de otras entidades que puedan verse igualmente involucradas, e incluso la participación de Fuerzas de Seguridad del Estado si es grave.

En esta situación la certificación, entendida como adopción de modelos probados que obligan a una serie de controles determinados, se ha convertido en un elemento clave para garantizar la seguridad de IT.

Tanto las legislaciones europeas, tales como la ley eiDAS, orientada a la identificación digital y de obligado cumplimiento para los prestadores de servicios de confianza a partir del 1 de julio de 2016, como normativas y leyes nacionales, tales como el Esquema Nacional de Seguridad, la Ley de Protección de Infraestructuras Críticas, que identifica aquellos sectores esenciales para el funcionamiento del Estado o de la sociedad, como la Estrategia de Ciberseguridad Nacional, reconoce la necesidad de que los elementos y procesos que intervienen en un Sistema de Información estén validados y certificados conforme a un estándar ampliamente aceptado.

Hay que tener en cuenta, además, que el sector IT es un sector reciente, donde esta tendencia a la regulación se ha ido creando a medida que ha habido incidentes que han arriesgado la economía, los negocios o la vida diaria.

¿Qué beneficios puede ofrecer la certificación de los procesos y componentes tecnológicos? A mi modo de ver hay varios beneficios evidentes más allá del cumplimiento más o menos obligatorio:

1. La identificación y validación de procesos esenciales para la operativa de IT y por lo tanto para la operativa del negocio, desde la forma de desarrollar software, a cómo proteger los activos tecnológicos.

Grafico 2

2. El juicio de un tercero imparcial, especializado en el tema a certificar, lo que aporta la visión del experto auditor no solo en el propio entorno del cliente sino en relación con organizaciones parecidas.
3. La capacidad de comparar, dentro del mismo sector, con otros sectores pero con características más o menos comunes de tamaño, número de clientes, etc.

Sin embargo, y a pesar de lo importantes que son, los beneficios de la Certificación no terminan en el proceso seguro, de tal manera que ante un incidente se puede reaccionar de manera rápida y eficaz e involucrando a todas las partes necesarias.

A este hecho, se une la necesidad de las organizaciones de crear infraestructuras que además de ser seguras sean rentables y eficientes, es decir que utilicen los recursos adecuadamente.

No se puede hablar de empresa segura desde el punto de vista de las Tecnologías de la Información si se ignora sobre lo que están sustentadas, es decir, si se ignora el papel de los Centros de Procesos de Datos.

Estas infraestructuras, están en estos momentos inmersas en la ola de la certificación, ya que se hace imprescindible la necesidad de revisión de un tercero de confianza sobre su construcción y operativa.

Tal como muestra el **gráfico 2** anterior solo se puede garantizar la fiabilidad y disponibilidad de una instalación si se verifican al menos lo siguientes elementos:

1. Dónde se ha construido el Centro de Proceso de Datos.
2. Cómo se ha construido y aislado.
3. Qué medidas de prevención de incendios se han instalado.
4. Cuál es el plan de seguridad física de la instalación.
5. Cómo se hace el suministro eléctrico.
6. Cómo se resuelven los temas de ventilación y aire acondicionado para crear una infraestructura segura y eficiente.
7. Cómo es la organización del Centro de Proceso de Datos y que conocimiento hay en la empresa sobre el mismo.
8. Control de los documentos relativos al funcionamiento del Centro de Proceso de Datos.

Volviendo a citar a uno de los fundadores de Internet, el Sr. Leonard Kleinrock, la tecnología se encuentra en plena pubertad, siendo en estos momentos un adolescente alocado, misterioso y rebelde. La pregunta es si será un adulto responsable…Agradezco la confianza del Sr. Kleinrock en la humanidad… La respuesta es si… todos los adolescentes lo hacen…. ●

Fotos: TUV Nord

Contactos de empresas, p. 7.

TECNIFUEGO-AESPI: DÍA DEL FUEGO EN ANDALUCÍA

Anteponer la **calidad a ningún otro criterio**

FuegoSur contó con un aforo completo

Aforo completo y gran interés en el encuentro de FuegoSur, un nuevo Día del Fuego que se desarrolló en el Colegio Oficial de Peritos e Ingenieros Técnicos Industriales de Cádiz. El acto, organizado por la Asociación TECNIFUEGO-AESPI, en colaboración con el Consejo Andaluz de Ingenieros Técnicos Industriales y la Junta de Andalucía, contó con la presencia de Gema Pérez Lozano, delegada Territorial de Economía de la Junta de Andalucía, que dio la bienvenida a los asistentes y alertó del riesgo de incendio en las actividades diarias, como son los centros de trabajo, la vivienda, etc.

POR su parte, Domingo Villero, decano del COPITI y presidente del Consejo Andaluz de Colegios de Ingenieros Técnicos Industriales, dio la bienvenida a los asistentes y animó a cumplir eficazmente los trabajos realizados anteponiendo la calidad a ningún otro criterio. Asimismo, Xavier Grau, secretario general de la Asociación, presentó los datos económicos del sector «que factura alrededor de 2.500 millones de euros al año», y un pequeño vídeo donde se resumen los medios de seguridad contra incendios que se deben instalar en una vivienda.

La primera parte de la jornada, moderada por Vicente Puentes, jefe del Servicio de Industria, comenzó con la ponencia «La Protección contra Incendios (PCI) desde el punto de vista del Técnico Titulado», en la que Juan C. Pinto de COPITI se refirió a los requisitos que se deben cumplir y al trabajo de calidad a la hora de presentar los proyectos, visados, etc. «La calidad es primordial en un sector de tanta importancia como el de seguridad contra incendios».

Acto de inauguración de FuegoSur.

La siguiente intervención sobre «Actuaciones de un Organismo Notificado e Inspecciones Reglamentarias», fue introducida por Francisco Martín, de Bureau Veritas, que informó de la normativa y los trámites a seguir para evaluar y verificar las condiciones de los productos contra incendios, según la modalidad de la evaluación. «Certificar da la posibilidad de comercializar y destacar un producto sobre otros», resaltó.

A continuación se informó a los asistentes de las cuestiones básicas de la «Norma UNE 192005: Inspecciones en las instalaciones contra incendios industriales». Damaris Ruiz, representante de una empresa instaladora asociada a TECNIFUEGO-AESPI, recalcó qué aspectos se deben tener en cuenta a la hora de una inspección en un establecimiento industrial, el control de documentos exigidos, si ha habido un cambio de actividad, comprobar qué instalaciones hay, si funcionan correctamente, el mantenimiento, etc.

El segundo bloque de ponencias comenzó con «Aplicación de la Normativa de PCI por el Consorcio de Bomberos de Cádiz», y fue desarrollada por José Enrique Vargas, jefe de Bomberos en la Bahía de Algeciras, que puso varios ejemplos de actuaciones, donde las construcciones ignífugas habían reteni-

do durante el tiempo suficiente el incendio, pudiéndose así evacuar y trabajar en la extinción. Además, el ponente detalló los aspectos más importantes en los que hay que fijarse cuando se realizan las inspecciones a instalaciones de PCI.

En el siguiente tema, «Los productos y servicios. Normas AENOR», Pablo A. Corróns, de AENOR, informó de los servicios de la entidad de normalización, y las ventajas que tiene suscribirse para disponer de las actualizaciones y las normas de PCI, además de consultas, guías y publicaciones. «Las consultas vía web son muy sencillas y útiles», aseguró.

Finalmente, Francisco Ruiz, vicepresidente de TECNIFUEGO-AESPI, adelantó algunos de los aspectos más novedosos del «Borrador del nuevo Reglamento de Instalaciones de Protección contra Incendios, RIPCI». Por ejemplo, el nuevo contrato de mantenimiento, la exigencia de inspecciones a edificaciones no industriales, la actualización de todas las normas UNE, la inclusión de sistemas, como agua nebulizada, control de humos, señalización; la conexión de los sistemas de detección a una central de alarmas de una empresa de PCI; la posibilidad de telemantenimiento; y la reducción de los plazos para realizar el mantenimiento de los sistemas.

Vista general de los asistentes.

«En un animado debate los asistentes plantearon dudas y preguntas, incidiendo las consultas en el contenido del nuevo RIPCI

Al finalizar las ponencias se abrió un animado debate en el que los asistentes plantearon sus dudas y preguntas a los ponentes sobre diversos aspectos, incidiendo las consultas en el contenido del nuevo RIPCI, un reglamento fundamental que se espera se publique cuanto antes dada la repercusión en la seguridad.

FuegoSur es una nueva iniciativa, patrocinada por Rockwool, Cottes, Viking, Colt, Ebara, Ruca, Firelanz, Fireoca, Sicur y Aenor, que se suma así a los días del fuego, organizados por TECNIFUEGO-AESPI, en toda España, con el afán de tomar el pulso a la situación profesional y administrativa de la seguridad contra incendios, informar de las novedades en tecnología y normativa, y en definitiva mejorar la protección frente a los incendios. ●

Fotos: Tecnifuego-Aespi

DR. JOSÉ JULIÁN ISTURITZ. DOCTOR EN DERECHO PÚBLICO. PROFESOR DE LA ESCUELA DE PREVENCIÓN Y SEGURIDAD INTEGRAL DE LA UNIVERSIDAD AUTÓNOMA DE BARCELONA

Responsabilidades en eventos de pública concurrencia

A propósito de un caso, el siniestro del Madrid-Arena

La noche del 31 de octubre al 1 de noviembre 2012 (noche de Halloween), se había organizado en el pabellón multiusos, propiedad del Ayuntamiento de Madrid, denominado como «Madrid Arena» y ubicado en la Casa de Campo, un evento consistente en un espectáculo musical. Simultáneamente y coincidiendo con este evento, también estaba convocado en los alrededores, un macro-botellón que fue declarado ilegal.

SEGÚN consta en las diligencias previas del Juzgado[1], al parecer el aforo autorizado era de 10.620 entradas, mientras que se vendieron aproximadamente 23.000, entrando posteriormente unas 3.000 personas más, a través de un portón previsto como salida de emergencia.

De las 8 vías de evacuación existentes, 3 eran practicables, pero 5 estaban obstruidas tanto por barras, escenario y demás artilugios relacionados con el evento. Además, el denominado «portón cota cero» (una puerta para entrada de mercancías y salida de emergencias) se abrió para que entraran más personas.

Debido a un cúmulo de circunstancias, se produce una avalancha en el interior del establecimiento que causó cinco fallecimientos y más de treinta heridos, principalmente por aplastamiento.

En principio, grosso modo se imputan indiciariamente 8 delitos de homicidio por imprudencia grave y 10 delitos de lesiones. Además, las correspondientes responsabilidades civiles directas de las aseguradoras y subsidiarias de las empresas que de una u otra manera intervinieron o tuvieron relación con el evento.

A modo de resumen, el Juzgado considera que lo sucedido fue un proceso de integración y concurrencia de codicias, negligencias, dejación de funciones y actuaciones irracionales y temerarias que dieron como resultado el fallecimiento de 5 niñas, que pudo y

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

debió haberse evitado y que hubo inactividad criminal por parte de todas aquellas personas que tenían que haber velado por la seguridad.

Sobre el Procedimiento Judicial

Se abrieron diligencias previas por parte del Juzgado de Instrucción número 51, de Madrid, el cual ha dictado varios Autos. El que más nos ocupa es un Auto de transformación, en el cual se analizan los hechos y establece imputaciones.

Recientemente, se ha abierto fase de juicio oral, conociendo y enjuiciando la causa la Audiencia Provincial de Madrid, que se estima comience el juicio a comienzos de 2016.

Destinatarios y propósito

3.1 Destinatarios

Este artículo está especialmente destinado a responsables, técnicos e interesados, fundamentalmente en la planificación de la autoprotección en emergencias y protección civil y de manera singular, a los técnicos competentes para formular planes de autoprotección. A estos últimos puede servirles para poner «acentos» y especial cuidado en determinadas partes de los planes.

También es útil para empresas de seguridad, de control de accesos, videovigilancia y similares.

3.2 Propósito

El propósito de este artículo es reflexionar, desde un punto de vista profesional, sobre la prevencion y organización del dispositivo de atención de emergencias del evento, las personas y empresas afectadas y su grado de participación, todo ello en base a lo recogido, hasta ahora, en los Autos del mencionado Juzgado.

Este trabajo, por tanto pretende poner en valor aquellos aspectos que sobre todo deberemos tener en cuenta a la hora de organizar la seguridad de un evento, así como ser conscientes de los aspectos que la judicatura tiene más en consideración.

3.3 Consideraciones

Es preciso tener en cuenta las siguientes consideraciones previas:

a) En la fecha del siniestro, estaba en vigor la Norma Básica de Autoprotección[2] ya que se promulgó en 2007.

b) Las reflexiones y comentarios de este trabajo, son como consecuencia de los Autos de diligencias previas existentes hasta la fecha, de forma que en ningún caso presupone culpabilidad alguna, puesto que se carece todavía de sentencia de algún tipo, por lo que el propósito del mismo es únicamente reflexivo y docente.

Organizaciones afectadas

Especial singularidad cabe al analizar a qué organizaciones tiene en cuenta este procedimiento y qué responsabilidades se les imputa y en calidad de qué. En definitiva, quien tiene responsabilidad.

Teniendo en cuenta que este trabajo es de carácter científico y en caso alguno recriminatorio ni de petición de responsabilidad alguna, se han obviado los nombres concretos de las organizaciones afectadas habiéndose conceptualizado su función.

Principalmente, son las siguientes **(Cuadro 1):**

ORGANIZACION	FUNCION (en calidad de...)
Administración pública local (Municipio > 100.000 habitantes)	Propietario del espacio (edificio) donde se realiza el evento
Sociedad pública municipal	Sociedad pública (100% del Ayuntamiento) encargada de la gestión del espacio
Organizador directo del evento	Sociedad mercantil encargada de: Venta de entradas. Funcionamiento interior.
	Intendencia del evento
Empresa de seguridad privada	Sociedad mercantil encargada de: Seguridad exterior. Accesos. Controles y requisas. Control "portón cota cero"
Empresa de provisión de personal	Sociedad mercantil: No queda clara su función, ya que por una parte provee de personal y por otra parece que efectúan también el control de accesos y entradas, así como la seguridad interior.

Merece especial mención que se establece como responsables civiles directos a las dos compañías aseguradoras y como responsables civiles subsidiarios, a todas las empresas citadas anteriormente.

Funciones especialmente afectadas

En esta fase, el Juzgado de Instrucción tiene especialmente en cuenta a personas con funciones en las siguientes líneas:

a) Participantes en la organización del evento. Tanto el organizador directo, como los responsables de la empresa pública de la gestión del espacio, como del Ayuntamiento, titular de la instalación. Así por ejemplo, reprocha desde los propietarios, accionistas, como a los directores generales que han tenido relación directa con el evento, bien por acción o por omisión.

b) Relación directa con la seguridad

y emergencias: Tanto al director de Seguridad y Emergencias, como al Jefe de emergencias y al Jefe de Operaciones, todos de la sociedad pública gestora del espacio, así como, a los jefes operativos de la empresa de seguridad.

c) Otros. El maître del evento por haber permitido que las barras y demás elementos, estuvieren ubicados, obstaculizando las salidas de emergencia.

Estamos por tanto ante un reproche penal a todo un cúmulo de actores que se relacionan con la organización del evento y/o con sus medidas de seguridad. Esto hace necesario reflexionar a la hora de efectuar un plan de autoprotección, sobre la importancia de definir claramente las funciones de cada actor, tanto sea persona jurídica (empresa) o física (personal).

Además, como se verá, son muy significativos los testimonios de otros actores; en principio ajenos al evento pero que acuden al siniestro; una vez detectado este. Son principalmente, los policías locales y los miembros de los equipos de emergencias médicas. Como consecuencia de esto, resulta muy significativa la necesidad de encontrar una adecuada «complicidad profesional» con estos actores del sistema público de atención de emergencias para tenerles en cuenta en la planificación de la seguridad de un evento de este tipo.

Relación de causalidad de hechos

A tenor de lo recogido en los autos, para el Juez es más que evidente la relación de causalidad entre la apertura del portón, la entrada de la multitud bebida y descontrolada y el trágico resultado.

Se dieron las siguientes circunstancias concurrentes, principales:

a) Organización y ejecución de un macro-botellón ilegal en el exterior.

b) La existencia de un sobre aforo en el interior del establecimiento que hacía imposible la permanencia en el, con lo que se produjo una evacuación espontánea de gran número de los asistentes.

c) La apertura de una entrada (portón cota cero) con la entrada masiva de unas 3.000 personas.

d) Coincidencia de la evacuación espontánea, con la entrada masiva.

Para el Juez, existe por tanto una relación causal entre el botellón y la tragedia.

Análisis de actuaciones y posiciones

De la lectura del Auto mencionado, hay que destacar algunos aspectos que, desde un punto de vista organizativo, nos identifican algunos puntos importantes a tener en cuenta.

Este apartado es especialmente significativo ya que nos da una idea de aquellos aspectos en los que más se focaliza algún hecho reprochable, tanto desde un punto de vista organizativo, como penal.

7.1 Sobre el desconocimiento de deficiencias:

En referencia al Coordinador Jefe de Seguridad, cuando este manifiesta «que no tenía conocimiento de las deficiencias de seguridad del interior del Madrid-Arena, dando por hecho que su empresa estaba al corriente de todo», el Juez lo califica de paroxismo de descoordinación y de negligencia.

De esta manera se pone de manifiesto que, ante un proceso penal, no parece aceptable que teniendo una determinada responsabilidad, se alegue desconocimiento, cuando el hecho entra en el ámbito de sus atribuciones.

7.2 Sobre la falta de acción por supuesta falta de competencia

En referencia al director general de la empresa organizadora del evento, que estuvo en todo momento en el mismo, manifiesta el Juez que tuvo que ser plenamente consciente de que se habían puesto a la venta un número de entradas inmensamente superior al autorizado. Además, reconoce haber oído en un momento determinado la expresión «abrir el portón» (referido al portón de cota cero, que permitió la entrada masiva de unas 3.000 personas).

El Juez considera que Refugiarse, como hace varias veces el imputado, en que «no tenía competencias», en nada excusa su negligencia, pues siendo consciente como necesariamente

lo era, de que existía un amplísimo sobreaforo, que se había sobrepasado escandalosamente el número de entradas autorizadas y de que el portón de cota cero, al abrirse lo único que podía hacer era agravar la situación, como así fue, con competencias o sin ellas, como director general de la empresa organizadora se tenía que haber opuesto a la medida adoptada, lo que evidentemente no hizo, no manifestando ni siquiera su disconformidad con lo que estaba ocurriendo.

Este apartado resulta muy significativo dado que deja clara la necesaria intervención de un directivo de la compañía organizadora del evento, ante una situación crítica, de forma que al menos, tenía que haber manifestado su disconformidad o haber hecho todo lo que estuviera a su alcance para evitar la tragedia.

7.3 Sobre la obediencia debida

La empresa de seguridad encargada del control de accesos y requisas, en varias ocasiones refiere que «hizo más livianas las requisas» por orden del titular del establecimiento. El Juez, reprocha esta actitud ya que considera que al haber sido contratada para ello, es responsabilidad de la propia empresa de seguridad esa función, por lo que no procede un refugio en la «obediencia debida» y la considera inaceptable, pues sería tanto como dar por bueno que cualquier acción, omisión, descuido o negligencia por parte de la empresa encargada de la seguridad está bajo el escudo protector y ninguna responsabilidad puede alcanzarles.

Cuando el Juez se refiere al Jefe de equipo de la empresa de seguridad que argumenta «obediencia debida», manifiesta que ante una grave imprudencia, no existe ningún tipo de obediencia debida. Además, da orden temeraria, de todo punto improcedente y que el mismo califica de sorprendente.

7.4 Las cámaras de seguridad

Especial relevancia tiene las cámaras de seguridad a las que el Juzgado da una importancia significativa, considerándolas como de vital importancia para el desarrollo del evento, multitudinario, complejo en su gestión, formado en su práctica totalidad por personas muy jóvenes y muy bebidas, de altísimo peligro potencial y de consecuencias inevitables cuando se producen avalanchas, como desgraciadamente ocurrió.

Sobre la persona que debía controlar las cámaras y abandona su puesto, el Juez lo califica como, una desastrosa actuación por abandono reiterada y temerariamente en diversas ocasiones un servicio de control y vigilancia esencial para la seguridad del desarrollo del concierto. De hecho, insiste en varios apartados sobre la persona encargada del citado control de las cámaras, al haber abandonado durante una hora su puesto de trabajo, de forma que esta actitud la califica de patética.

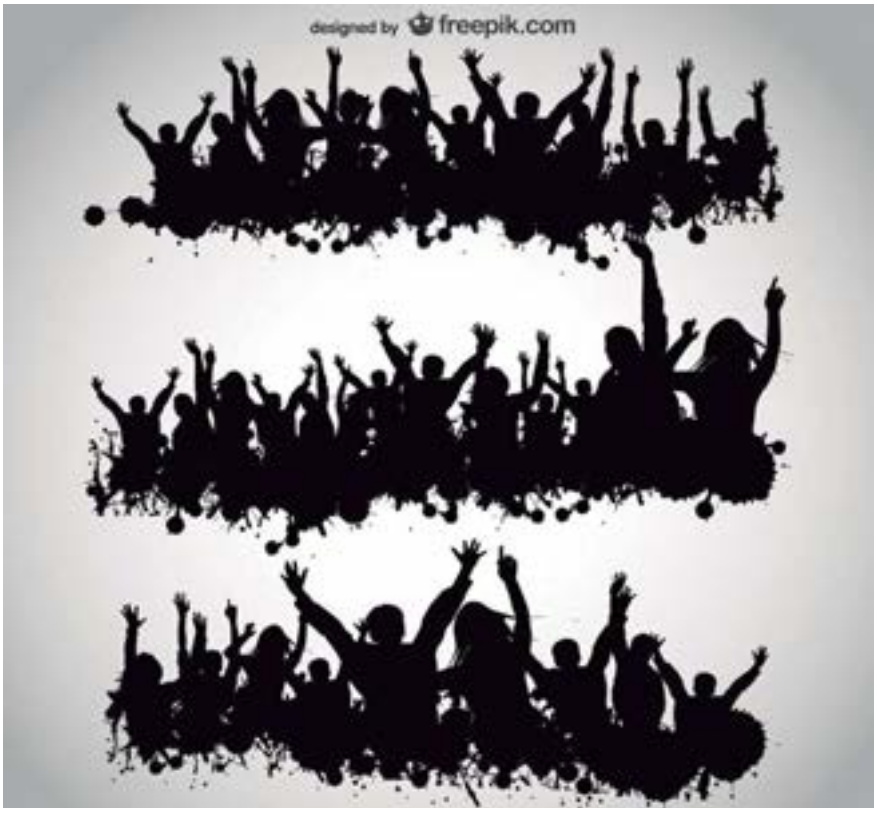
Pero además, no solo reprocha a esta figura sino también a su supervisor, el cual debía haber controlado esta situación por no «controlar al controlador» y lo califica como un comportamiento muy negligente.

7.5 Sobre la apertura de una salida de emergencia utilizada como entrada

Se insiste en varias ocasiones sobre que las imágenes son inequívocas e incuestionables de que entraron unas 3.000 personas por el portón (se refiere al portón de cota cero) en evidente estado de embriaguez y lo hacen desde una rampa prevista para mercancías y salida de emergencia, nunca como entrada. Todas estas personas acabarán siendo determinantes de la tragedia.

De hecho, insiste qué persona accionó el mando de apertura de la puerta y quién dio la orden de apertura reprochando penalmente esta decisión, ya que se la considera como causante de la tragedia al producirse la avalancha por el sobreaforo exagerado.

El Juez averigua, según el Auto,



«De las 8 vías de evacuación existentes, 3 eran practicables, pero 5 estaban obstruidas por barras, escenario y demás artilugios relacionados con el evento»

quién es la persona que decide la apertura del portón, quedando acreditado que fue el coordinador de proyectos y operaciones de la sociedad pública que gestiona el establecimiento.

Llama la atención que esta decisión no hubiera sido, o al menos no consta así en Autos, consultada con el director de Seguridad y Emergencias, ni con el Jefe de Emergencia, ambos pertenecientes a su misma organización pública, lo cual parece ser habitual a tenor de lo declarado por el director de Seguridad y emergencias que manifestó «que el departamento de Operaciones no consulta con el de seguridad».

7.6 Sobre la enfermería (o botiquín)

El habitáculo utilizado como enfermería, el Juez califica como simulacro de enfermería, debido a su falta de equipamiento ya que carecía hasta de agua corriente.

Sobre este hecho, abunda sobre el director médico, al haber asumido esta instalación como tal, sin contar con las mínimas medidas, a tenor de las declaraciones de varios miembros forenses, así como otros del SAMUR[3] de Madrid.

Hasta tal punto reprocha el Juez esta instalación que la califica como cuarto trastero, sin ventilación, ni luz suficiente y aspecto realmente sorprendente y sin agua corriente.

En tal habitáculo, eufemísticamente llamado enfermería, no existía medio material o instrumental alguno que hiciera suponer que se podía atender a cualquier emergencia médica (…). En otra parte, se refiere a él como trastero, garaje o habitáculo multiuso que se había improvisado como enfermería sin contar con los mínimos medios exigibles. Lo que viene a concluir identificándolo como auténtico lujo de despropósitos.

7.7 Servicios médicos

Al respecto del director médico comienza señalando que no es irrelevante que el director médico tenía alrededor de 80 años en la fecha del evento, lo cual y por razones más que evidentes, cuestiona que una persona de tal edad, esté en condiciones de ponerse al frente de los servicios médicos de este acontecimiento (…).

Reprocha el hecho de que aceptara el desempeño de esta función con pleno y cabal conocimiento de que se trata de un habitáculo no concebido para enfermería. Además, manifiesta que aceptó hacerse cargo de las responsabilidades derivadas de la asistencia médica en un evento multitudinario, en unas paupérrimas condiciones materiales y de dotación instrumental, que aceptó voluntariamente y por dinero, ponerse al frente de los servicios médicos sin contar con los mínimos medios materiales e instrumentales necesarios para la función que asumía.

Todo ello, al margen de las imputaciones que le recrimina en el ejercicio de su profesión que considera que, ni pudo ni supo hacer frente a la situación gravísima que se le planteaba. Su supervisión en la preparación y dotación del habitáculo, mal llamado enfermería, fue negligente y temeraria y su actuación fue insuficiente, incompetente y en opinión de este juzgado, carente de toda profesionalidad.

Por otra parte, considera al médico encargado junto a su padre, de la asistencia sanitaria del evento, que ni diagnóstico correctamente, dando por fallecidas a unas niñas que no lo estaban, ni actuó con diligencia y solvencia profesional, ni asesoró o instruyó a los técnicos de ambulancias. Considera su comportamiento profesional como incuestionablemente errático, equivocado en el diagnóstico, insuficiente en la praxis y totalmente impropio de un profesional.

7.8 Sobre la actuación de la Policía Municipal

Merece la pena destacar las referen-

cias al servicio de Policía Municipal, al que califica que estuvo en el lugar de los hechos de forma manifiestamente insuficiente, esporádica y con una pasividad totalmente inadecuada para la gravedad de los hechos que estaban aconteciendo.

Esto lo fundamenta en determinadas declaraciones de varios miembros de la policía municipal, así como, diversos testigos.

Considera que la Policía Municipal ni evitó, ni palió, ni aminoró, sino que tuvo una actitud que benevolentemente puede ser calificada de contemplativa y en todo caso, muy alejada de sus estrictas obligaciones. Además, considera que no hubo previsión, ni medios suficientes, ni reuniones de coordinación previas.

7.9 Sobre los responsables de la seguridad:

a) El director de Seguridad y Emergencias del titular de la gestión del establecimiento:

El Juez le reprocha, entre otras actuaciones que no procediera a precintar el recinto, pese al requerimiento de los agentes de la autoridad.

Llama la atención que el titular de esta función, declara entre otros aspectos, que:

- –No tiene potestad alguna para parar un evento, aunque detecte fallos de seguridad.
- –El departamento de Operaciones no consulta con el de Seguridad.
- –Desconoce que tenga que haber un espacio para enfermería.
- –Ignora que había salidas de emergencia no practicables.
- –No conoce la normativa de incendios.

b) El coordinador jefe de Seguridad del titular de la gestión del establecimiento:

El Coordinador jefe de seguridad declaró que el escenario estaba montado entrando por el portón de cota cero a la izquierda y que estaba tapando una de las salidas de emergencia, añade el Juez, sin que conste que tomara iniciativa alguna al respecto.

Manifestó que, pese a que en otras ocasiones se celebraban reuniones previas de coordinación, en este caso, no se celebró. Además, reconoce que el escenario tapaba una de las salidas de emergencia. Se le imputa en calidad de coautor.

c) El Jefe de Emergencias del titular de la gestión del establecimiento

Realiza las funciones de dar la «voz de alarma». El Juez manifiesta que hubo una nula actuación del jefe de Emergencias en un evento en el que por negligencia de unos y otros, fallo todo lo que podía fallar.

El jefe de Emergencias, según figura en el Auto, ni superviso, ni como jefe de Emergencias dio voz de alarma alguna, ni ordenó modificar estructura alguna, incluyendo las barras que tapaban los vomitorios, ni evitó que la totalidad de las puertas de evacuación estuvieran cerradas, salvo tres.

El Juez considera que: A la vista de lo anterior resulta difícil de imaginar que hizo el jefe de Emergencias en un evento que a simple vista, superaba el aforo permitido, tenía cerradas o tapiadas las salidas de emergencias de la pista central, dio lugar a que se abriera un portón por el que accedieron a la pista central, absolutamente sobresaturada, no menos de 2.000 personas, según está perfectamente grabado por las cámaras de seguridad, en avanzado estado de embriaguez, circunstancia que tuvo una relevancia capital en la tragedia que posteriormente se desencadenaría y que el propio jefe de Emergencias, refiriéndose expresamente a la apertura del portón, califica como ha quedado dicho, de barbaridad».

7.10 Empleados sin relación directa con la seguridad

a) Maître: Destaca la figura del maître, persona que se encarga, entre otras funciones, de la ubicación de las mesas y barras. El Juez, le imputa en calidad de coautor al no haber tenido en cuenta que estas obstaculizaban las vías de evacuación.

b) Coordinador de operaciones del titular del establecimiento: Al ser el que da la orden de abrir el portón de cota cero (supuestamente desencadenante del incidente), el Juez le recrimina que desconociera el aforo real. Además,según se desprende de sus declaraciones y a criterio del Juez, es imposible inferir de forma mínimamente racional qué operaciones coordinaba y qué entiende por coordinar.

Además, considera que es una imprudencia y le imputa en calidad de autor.

c) Inspector de servicios de la empresa de seguridad: Le considera un lamentabilísimo papel protagonista. Da una orden que el mismo reconoce como una barbaridad y, además, no supervisa al operador del control de cámaras. Le imputa en calidad de coautor.

7.11 La función directiva

El Juez critica la actitud del director general de una de las empresas de control de accesos por inacción y a otro por notoria actuación de mala fe con intención premeditada y malintencionada. Les imputa en calidad de coautor. También reprocha la actuación de uno de los socios mayoritarios de una de las empresas de seguridad, que estuvo en el evento, por no cumplir con sus funciones ya que ni se ocupa, ni se preocupa de que sus trabajadores realicen correctamente su función…

CONCLUSIONES

Podemos destacar las siguientes conclusiones ejecutivas:

a) La figura del director de seguridad cada vez es más relevante.

b) En este incidente se ha puesto de manifiesto la necesidad de:

–Identificar claramente las funciones de cada empresa.

–Identificar claramente las funciones de cada puesto de responsabilidad.

–La importancia de la visualización y control de las cámaras.

–El respeto por el aforo.

–La coordinación entre el responsable de operaciones y de seguridad y emergencias es crucial.

c) Ante un incidente con víctimas y resultado de muerte y con gran impacto social, ninguno de los actores que intervienen en la organización del evento está libre de toda sospecha.

d) Las personas con mando directo o responsabilidad sobre otras personas, tienen una responsabilidad profesional crítica.

e) Es imprescindible disponer de un centro de control único, donde recibir toda la información del evento, donde se ubiquen personas con capacidad de decisión y ,en base a ella, tomar las decisiones adecuadas.

Por último, destacar que este tipo de actuaciones judiciales -que como se ha dicho con anterioridad, no supone presunción alguna de culpabilidad, en tanto haya, que no la hay, sentencia firme-, debe servirnos para reflexionar, dar carácter y entidad a este tipo de eventos y sobre todo, dar la importancia que tienen los planes de autoprotección, su contenido y responsabilidades, porque «cuando todo va bien no pasa nada», pero cuando las circunstancias «reman en contra», afloran las incompetencias, descoordinaciones y disfunciones que a veces resultan fatales.

Fotos: Archivo/Freepik

[1]Principalmente Auto de fecha 29 de agosto de 2014, diligencias previas procedimiento abreviado 7279/2012. Número identificador único 28079 2 0464332 /2012. Disponible en: http://www.poderjudicial.es/stfls/SALA%20DE%20PRENSA/NOTAS%20DE%20PRENSA/JI%2051%20Madrid%2015.04.15%20(7279-12).pdf

[2]Real Decreto 393/2007, de 23 de marzo, por el que se aprueba la Norma Básica de autoprotección de los centros, establecimientos y dependencias dedicados a actividades que puedan dar origen a situaciones de emergencia.

[3]Servicio de Asistencia Municipal de Urgencia y Rescate perteneciente al Ayuntamiento de Madrid. Curiosamente, el director médico de la instalación y también imputado es precisamente el que fuera Concejal creador de este servicio, a finales de la década de los 80.

BIBLIOGRAFIA

ANITUA, P., Manual de protección civil, Gobierno Vasco-Eusko Jaurlaritza, Vitoria-Gasteiz,2006.

BALLBE, M., Seguridad integral. Un nuevo concepto, Instituto Superior de Estudios de Seguridad, Barcelona, 2003.

BALLBE, M., MARTINEZ, R., Soberanía dual y constitución integradora: la reciente doctrina federal de la Corte Suprema norteamericana, Ariel Derecho, Barcelona, 2003.

ISTURITZ, J.J. Tesis doctoral «Regulación y organización de sistemas de emergencias y protección civil: diseño de un sistema asimétrico, multifuncional y multifactorial».

Universidad Autónoma de Barcelona. 2013. Disponible en:

http://ddd.uab.catrecord/116340?ln=es

IZU, M., «De la Protección Civil a la gestión de emergencias: la evolución del marco normativo», en: Revista Aragonesa de Administración Pública, nº 35, Zaragoza, 2009.

OCHOA, J., «El modelo público de seguridad civil o protección civil español», en: Revista jurídica del Perú, nº 53, Trujillo (Perú), 2003.

ENCUENTRO ORGANIZADO POR LA FUNDACIÓN ESYS

El reto de la convergencia entre Seguridad Física y Ciberseguridad

La Fundación Empresa, Seguridad y Sociedad (ESYS) celebró el pasado 24 de noviembre una jornada de trabajo bajo el título: «Las Empresas ante el Reto de la Convergencia entre la Seguridad Física y la Ciberseguridad», que estuvo moderada por Alfonso Bilbao, presidente de la Comisión Técnica de ESYS.

LA jornada contó con la intervención de Javier Gómez-Navarro, presidente de la Fundación ESYS, quien destacó que, aunque la Seguridad Física no ha perdido su papel, la Ciberseguridad se ha convertido en primordial para el mundo de los negocios. «Los bancos no tienen miedo a los atracos, pero sí a las amenazas cibernéticas». Cada activo de la empresa está sometido a diferentes amenazas, tanto físicas como lógicas. La Fundación ESYS apuesta por una convergencia de ambos modelos, es decir, un nuevo modelo que integre Seguridad Física y Lógica en un concepto global de Seguridad Integral.

Manuel Carpio, director de Seguridad de la Información y Prevención del Fraude de Telefónica, realizó un planteamiento sobre los diferentes modelos de convergencia que existen en las organizaciones. La convergencia de las diferentes «Seguridades» que coexisten en una gran empresa es camino obligado para una organización de seguridad eficaz y eficiente del siglo XXI.»

José Luis Moya, responsable de Gobierno Security de Gas Natural Fenosa, hizo hincapié en que, en un entorno de riesgos globales, las empresas «debemos aprovechar el viento a favor del actual impulso de la Ley de Protección de las Infraestructuras Críticas, promoviendo un posicionamiento en la organización que dé un enfoque integral a la estrategia y táctica dentro de una Dirección de Security única dedicada a la protección de las personas, los activos (incluido la información) y los procesos de la compañía…».

Otro de los modelos de convergencia en Seguridad presentados fue el de Endesa. Su director de Seguridad, Florencio Retortillo, expuso los principales pilares en los que se sustenta y la necesidad de evaluar correctamente los riesgos dentro de la empresa. En su intervención, el director de Soluciones Integrales de Seguridad de Prosegur, José María Pena, trazó un paralelismo: «La Seguridad es a la sociedad como la salud es al individuo». Es decir, «al igual que cada persona tiene unos objetivos personales y profesionales, que solo pueden alcanzarse sobre la base de una buena salud, una empresa cuenta con unas metas de negocio que solo puede hacer realidad si posee una adecuada seguridad». En definitiva, se trata de un análisis integral de riesgos, que encarna lo que Fernando Sánchez Gómez, director del Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC), proponía al hablar de la necesaria «convergencia de todos los tipos de Seguridad que existen».

De hecho, comentó el director del CNPIC, «la Ley de Infraestructuras Críticas recoge la existencia de un interlocutor único en cada empresa para temas de Seguridad». Para llevar a cabo esta tarea, insistió Sánchez, es necesario superar recelos y empezar a compartir información. ●

CONGRESO AECOC DE PREVENCIÓN DE PÉRDIDA

Juntos para proteger el **patrimonio comercial**

Contar con una economía sana, segura y estable es clave para combatir los hurtos comerciales

AECOC, la Asociación de Empresas de Gran Consumo, reunió el pasado 19 de noviembre en Madrid a más de 180 profesionales de las áreas de seguridad y prevención de la pérdida de las principales compañías del país, para analizar, entre otros, las novedades que la reforma del código penal aprobada el pasado año introduce en materia de protección del patrimonio.

RAFAEL Catalá, Ministro de Justicia, encargado de inaugurar el encuentro, aseguró que España está creciendo de media un 3.3%, lo que supone el triple que los demás países de la Unión Europea, que lo hacen en torno al 1%. Catalá quiso reconocer el esfuerzo de la ciudadanía en los últimos años para volver a generar crecimiento económico y empleo en España, donde actualmente se crean uno de cada dos puestos que se generan en la Europa del euro, según sus palabras. En su discurso, el titular de justicia destacó la importancia de contar con una economía sana, segura y estable, para reducir la delincuencia relacionada con el hurto comercial. El Ministro también quiso agradecer a AECOC su participación y esfuerzo en la reforma del Código Penal, que ha adoptado gran parte de las reivindicaciones demandadas desde hace años por la Asociación en la lucha contra el hurto comercial. Entre las reivindicaciones que se han modificado en el nuevo Código Penal, Catalá ha destacado la eliminación de la falta para recategorizarla como delito leve con una pena de multa de 1 a 3 meses de prisión y los agravantes sobre la multi reincidencia, la inutilización de dispositivos de seguridad y la pertenencia a banda organizada.

Rafael Catalá, ministro de Justicia, en el acto de inauguración del encuentro AECOC.

El presidente de AECOC, Javier Campo, participó también en el bloque inaugural destacando la importancia de resolver un problema que hace años que resta eficiencia y competitividad a la cadena de valor. Durante 2014, las empresas de la gran distribución perdieron 1.675 millones de euros, lo que supone un 0.8% de sus ventas. El problema que han tenido las compañías para frenar el hurto ha sido tradicionalmente la impunidad con la que actuaban bandas organizadas, un aspecto reformulado en el nuevo código penal, con agravantes específicos que ayudan a luchar contra este problema.

La colaboración público-privada es, sin duda, un reto imprescindible para luchar contra la pérdida. Las Fuerzas de Seguridad del Estado tienen un papel determinante en este escenario, por ello, Carlos A. Vázquez, comisario principal y vocal asesor del Gabinete del Secretario General del Estado de Seguridad, analizó la importancia de co-

laborar entre administración pública y sector privado a fin de cumplir con la nueva normativa.

A lo largo de la jornada participaron en el Punto de Encuentro destacados profesionales de las áreas de seguridad y prevención de la pérdida. En este sentido, Álvaro Martín, director de Seguridad de DIA; Carles Oliveras, director de Seguridad de Media Markt; y Eloi Solé, director de Ventas de Wrigley, analizaron las soluciones que pueden llevar a cabo los diferentes departamentos para evolucionar hacia una compañía competitiva y segura. Coordinar las áreas de Seguridad con las de Ventas y conseguir alinear sus objetivos es un reto para el sector.

Las empresas Tesco y Wrigley realizaron un proyecto conjunto con el objetivo de reducir la pérdida desconocida, donde analizaron todos los procesos desde la recepción en el centro de distribución hasta el momento de la venta en las tiendas de formato convenience. Eloi Solé, director de Ventas de Wrigley, abordó los retos a los que se enfrentaron las compañías y cómo el proyecto influyó en la ventas.

Por su parte, Ignacio Gil, responsable de Seguridad de Decathlon, analizó su sistema de protección a través de la tecnología RFID, que utiliza en un 85% de sus referencias, y en la que ha encontrado un aliado para mejorar la visibilidad del stock de tienda y la disponibilidad de producto.

Mesa de Debate «La difícil tarea de garantizar la seguridad y promover las ventas».

Por su parte, Olga García, responsable de los departamentos de Procesos, Sistemas y Pérdidas de Perfumerías IF, abordó las mejoras obtenidas por su compañía en los años que llevan implantando un plan específico para la lucha contra la pérdida que implica a todos los departamentos de la compañía.

Además en el encuentro se presentaron dos estudios. En efecto, a lo largo de 2014, las empresas del sector de la gran distribución han perdido 1.675 millones de euros a causa del hurto comercial, lo que según el estudio «La Pérdida en la Gran Distribución en España 2015», elaborado por AECOC y EY, supone un 0.82% de sus ventas. El porcentaje de pérdida se mantiene prácticamente estable con respecto a 2013, aunque las pérdidas económicas aumentan debido al incremento de las ventas en el sector. Se trata de productos que claramente no tienen como objetivo el auto consumo sino la reventa en mercados paralelos, en este sentido, según el estudio de 2014, un 88% de las compañías considera que el principal motivo por el que se hurta es para revender los productos en mercados paralelos.

Asimismo, las compañías afirmaron que en un 81% de los casos, los robos son ejecutados por bandas organizadas o ladrones profesionales.

Por otro lado, la plataforma de estudios del comprador AECOC Shopper View, ha elaborado un estudio en colaboración con Tyco, para analizar el grado de conocimiento que tienen los consumidores de los distintos dispositivos anti hurto, y especialmente, cómo afectan a su decisión de compra.

Los consumidores españoles consideran positivo que la tienda cuente con sistemas de seguridad, siendo los spiders y soportes, los dispositivos que se conciben como más necesarios por su efectividad disuasoria. Más de un 83% de los encuestados también afirmó que los vigilantes son el sistema que mejor imagen da a la tienda. ●

Un momento del encuentro profesional.

Texto y Fotos: AECOC/ Redacción.

TECNIFUEGO-AESPI: DÍA DEL FUEGO EN MADRID

La necesidad de **instalar y mantener** por empresas autorizadas

Conocimiento, ética profesional e inspección, pilares para la confianza en la Seguridad contra Incendios

Bajo el epígrafe «La necesidad de instalar y mantener por empresas autorizadas», TECNIFUEGO-AESPI reunió a más de un centenar de profesionales que acudieron a un debate abierto con un completo tándem de expertos en las diversas áreas de la Seguridad contra Incendios. Un debate donde surgió la necesidad de incrementar el conocimiento, la ética profesional y la inspección como pilares para mejorar y profesionalizar la Seguridad contra Incendios (SCI). En este sentido, el director general de Industria de la CAM, Carlos López Jimeno, lanzó una propuesta para aunar a todos los implicados en una gran Campaña de Inspección.

En esta segunda edición del Día del Fuego en Madrid, que ha contado con la colaboración de la Fábrica Nacional de Moneda y Timbre (FNMT), Jaime Sánchez Revenga, presidente y director general de esta entidad, inauguro la jornada y recordó la importancia que se da en la FNMT a la Seguridad contra Incendios: «Mantenemos un cuidado especial en esta área, tanto a nivel de equipamiento y material de protección y extinción, como de personal propio, ya que disponemos de bomberos, personal de mantenimiento, etc.». Por su parte, Vicente Mans, presidente de TECNIFUEGO-AESPI, hizo un breve análisis de la situación y el reto común a todos los asistentes y ponentes de «profesionalizar el sector, ya que si no se trabaja con alta calidad, las vidas y los bienes pueden correr riesgo, en caso de incendio».

Vicente Mans, presidente de Tecnifuego-Aespi, Jaime Sánchez Revenga, presidente y director general de la FNMT, y Antonio Tortosa, vicepresidente de Tecnifuego-Aespi, en el acto de inauguración.

Vicente Mans y Antonio Tortosa, presidente y vicepresidente respectivamente de la Asociación, hicieron entrega de una placa conmemorativa del 400 aniversario de la Fábrica Nacional de Moneda y Timbre a su presidente Jaime Sánchez Revenga.

Tras la presentación, comenzó la mesa de debate, moderada por Antonio Tortosa, con un solo punto a tratar desde diferentes ángulos: «La necesidad de instalar y mantener por empresas de SCI autorizadas».

La primera ponente, Amparo de la Puerta, jefa de Área de Instalaciones Industriales y Capacitación Reglamentaria de la Comunidad de Madrid (CAM), recordó que la Administración exige a las empresas una Declaración Responsable que debe estar documentada para cuando las autoridades lo soliciten. Realizamos inspecciones periódicas documentales y de 210 expedientes, hemos inhabilitado y sancionado a 26 empresas», aseguró.

Marta Ríos, ingeniera de instalaciones de SCI de Bureau Veritas, hizo hincapié en la obligatoriedad (Reglamento

Instalaciones de Protección contra Incendios, RIPCI) e importancia del mantenimiento de las instalaciones de SCI, incluyendo las de protección pasiva. Jon Michelena, director de Cepretec-Cepreven, destacó los beneficios del control por parte de terceros: «El control voluntario debe ser una iniciativa cada vez más usual entre las empresas, ya que en la reglamentación actual existen muchas lagunas y no por ello se va a realizar una instalación defectuosa o no basada en reglamentos existentes».

Ángel Meca, director de Seguridad del Hospital Gregorio Marañón, informó de las peculiaridades de un centro hospitalario, donde hay enfermos que no pueden moverse, y por tanto la sectorización es prioritaria, y en el que es imposible el cese de actividad para realizar obras «en este contexto, tenemos que trabajar con mucho cuidado y esmero, difundiendo y promoviendo una cultura de la seguridad».

Por su parte Andrés Pérez, director de Seguridad del Museo Thyssen-Bornemisza, destacó en su intervención los tres pilares en los que se basa su servicio: plan integral de seguridad, eficaz mantenimiento de los equipos de protección contra incendios e implantación del plan de autoprotección. «De todo ello, la prevención es la pieza angular –argumentó-, de nada sirve instalar los mejores equipos si luego no se mantienen».

Siguió la intervención de Andrés Martín, vicepresidente de Protecturi y director de Seguridad de EVO Banco, que aseguró que la Ley de Seguridad Privada ordena que el director de Seguridad sea el responsable de todos los riesgos. Por ello es muy importante participar desde el principio en el proyecto, en la planificación y en el diseño del plan integral de seguridad, incluida la Seguridad contra Incendios. El último interviniente fue Manuel Martinez, coordinador del Comité Sectorial de Instalación, Mantenimiento e Ingeniería de Sistemas y Equipos de TECNIFUEGO-AESPI. A través de un vídeo muy didáctico y diversos ejemplos de malas instalaciones alertó, por un lado, de la falta de conciencia social del riesgo de incendio, y por otro, de la falta de profesionalidad de determinadas empresas y usuarios que, a costa de la crisis, las primeras realizan trabajos nefastos, y los otros, solo se fijan en el precio final, sin importarles la calidad y la eficacia de la instalación y su mantenimiento.

Vicente Mans hace entrega a Jaime Sánchez Revenga de una placa conmemorativa del 400 aniversario de la FNMT.

La segunda parte de la jornada tuvo como protagonistas a los profesionales asistentes que realizaron reflexiones, preguntas e intervenciones tratando diversos temas, como la necesidad de aumentar la inspección por parte de las autoridades, «porque las empresas registradas se pueden controlar, pero y las que no se registran», se preguntó un participante. Igualmente se trató la necesidad de formación reglada y lo esencial que resultan los conocimientos actualizados para los profesionales de un sector que trabaja para la protección de vidas y bienes. Asimismo salió a relucir la falta de una autoridad central de control en Seguridad contra Incendios, la cantidad de normativa y legislación existente «menos normas y más sentido práctico y el buen hacer profesional», recordó un asistente. En otro momento, se mencionó al enemigo común: economizar en un tema tan delicado y especializado. Se animó a que desde el Ministerio de Educación se integre en el plan de estudios de los colegios de Primaria una asignatura de autoprotección, como sucede en casi toda Europa.

Carlos López, director general de Industria, Energía y Minas (CAM), clausuró la jornada, proponiendo a los presentes: autoridades, empresas, usuarios, asociaciones y profesionales en general, una gran campaña de inspección para resolver las deficiencias detectadas por el sector. ●

Texto y Fotos: Tecnifuego-Aespi/Redacción

II CONGRESO ADESYD

«Compartiendo (visiones de) Seguridad»

La Asociación de Diplomados Españoles en Seguridad y Defensa (ADESyD), celebró en Madrid, el pasado 24 de noviembre, el "II Congreso ADESyD" bajo el lema "Compartiendo (visiones de) Seguridad". El objetivo era fortalecer la conciencia de corresponsabilidad entre los distintos actores del sector de la seguridad, pública y privada, aportando un enfoque integral.

LAS ponencias trataron de abordar las diferentes facetas de la seguridad, desde las más clásicas, vinculadas a las necesidades de la defensa nacional, hasta las más modernas.

Tras la presentación del Congreso, que corrió a cargo de Jesús Alonso Martín, María Angustias Caracuel Raya y José Díaz Toribio, procedió a inaugurar el mismo la Defensora del Pueblo Soledad Becerril y Bustamante. A continuación, Manuel Zafra impartió la conferencia "La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional". Al igual que la edición anterior, el II Congreso ADESyD se dividió en cuatro paneles:

Seguridad Nacional

Esta primera parte contó con Juan Carlos Iravedra, que habló de la Inteligencia para la Seguridad Nacional; Luis Enrique Martín Otero, con la ponencia "Amenazas Biológicas como consecuencia de las migraciones, cambio climático y guerras"; Ángel Liberal Fernández, que abordó los problemas de seguridad provocados por la Colonia de Gibraltar; Enrique Silvela Díaz-Criado, que habló de Comunicación Operacional; y Miguel Peco Yeste, que cerró el panel con la ponencia "Más allá de la intervención militar: Ideas para un futuro marco de la Defensa en España".

Seguridad Internacional

Inauguró el panel Ángeles Cano Linares, que habló de la Seguridad en el Sahel; a continuación Javier Gil Pérez analizó el rol de la inmigración afgana y pakistaní en la actual crisis de refugiados siria; Francesco Saverio Angió, explicó un tema de máxima actualidad como es la expansión territorial y la capacidad bélica de DAESH en el escenario mesopotámico; Iván Bravo Boris, abordó la modernización de la defensa en América Latina; y finalmente Xavier Boltaina Bosch, habló en su ponencia de "Corea del Norte: El arma nuclear y la sociología del sistema y sus fuerzas armadas".

Seguridad Pública

Comenzó esta parte del Congreso con la ponencia de Félix Brezo Fernández y Yaiza Rubio Viñuela sobre el uso de BOTS por parte de DAESH en las redes sociales; Selva María Orejón Lozano habló de la protección de la identidad digital de los miembros de los Cuerpos de Seguridad y sus instituciones; María Teresa Sánchez González realizó un análisis de la Seguridad y la Defensa desde la perspectiva de la Información Internacional; y Jaime del Olmo Morillo-Velarde habló de la Seguridad Alimentaria, el Medio Ambiente y el Cambio Climático.

Seguridad Privada

Comenzó Ignacio Olmos Casado explicando el marco jurídico de la Seguridad Privada y la colaboración con la Seguridad Pública; David Corrales del Pecho analizó la figura del Director de Seguridad; Francisco Lebrero Rodríguez impartió la conferencia "Seguridad informática en el contexto de las empresas privadas: las nuevas amenazas"; y Diego Miranda Giménez de Azcárate habló de la necesidad de innovar en los Departamentos de Recursos Humanos y Seguridad en el sector turístico.

Finalmente, para clausurar el Congreso, Diego López Garrido, vicepresidente de la Asamblea Parlamentaria de la OTAN y miembro del Consejo de Honor de ADESyD, impartió la ponencia "La respuesta de la comunidad Internacional ante el terrorismo de DAESH". ●

ORGANIZADO POR IFEMA SE CELEBRARÁ DEL 23 AL 26 DE FEBRERO

SICUR 2016: mayor oferta y representación internacional

La Galería de Nuevos Productos de SICUR 2016 destaca 41 propuestas de vanguardia en seguridad

SICUR 2016 celebrará una nueva edición entre los días 23 al 26 de febrero, en Feria de Madrid. Una convocatoria, organizada por IFEMA, que volverá a reunir a empresas, asociaciones, profesionales y usuarios de seguridad en torno a un escenario de alta representación sectorial, tanto desde el punto de vista de oferta como de demanda. Al cierre de esta edición la Galería de Nuevos Productos de SICUR 2016 había destacado 41 propuestas de vanguardia en seguridad.

ASÍ lo confirman los datos registrados en la pasada edición que congregó a 1.300 empresas participantes y 38.963 visitantes de 74 países, convirtiendo a SICUR en la plataforma por excelencia de esta industria, así como en el espacio donde tomar el pulso al mercado y conocer las novedades de vanguardia en materia de protección y prevención.

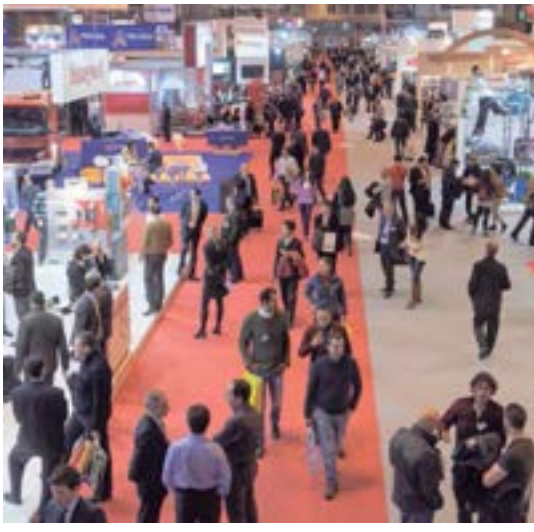
Además, todo apunta a que SICUR 16 crecerá en todos sus parámetros. El buen ritmo de contratación registrado hasta la fecha, y la labor que viene desarrollando la organización del Salón para potenciar la presencia de profesionales y usuarios de seguridad, nacionales e internacionales, abren expectativas muy positivas para la próxima convocatoria. En este sentido, y al margen del gran atractivo que despierta la oferta del Salón, se está trabajando en un ambicioso programa de jornadas técnicas que, en el marco de FORO SICUR, abordará temas transversales de interés para los usuarios de la seguridad de todos los sectores de la actividad, con un formato muy dinámico y orientado al debate.

La oferta de SICUR se presentará en distintas áreas monográficas representativas de la Seguridad Contra Incendios y Emergencias, en la que se enmarcan las empresas especializadas en la protección activa y pasiva contra el fuego, así como en las soluciones para mejorar la respuesta en situaciones de emergencia; la Seguridad Privada y Pública, en el sector Security y un contenido fuertemente marcado por el avance tecnológico al servicio de la protección de bienes y vidas; la Seguridad Laboral, en SICUR Prolabor, con lo último en Equipos de Protección Individual –EPIs–, así como en medidas de prevención y salud laboral, y el sector de Defensa, que acogerá a las empresas suministradoras de productos para el ámbito naval, aeronáutico, espacial, armamento, soluciones electrónicas e informáticas, vehículos terrestres, industria auxiliar, así como otros desarrollos realizados para el mercado civil adaptados al ámbito de Defensa.

SICUR se completará con el desarrollo de múltiples actividades con contenidos divulgativos, exposiciones, exhibiciones, demostraciones operativas, etc., que ofrecerán un contexto de gran dinamismo e interacción profesional.

Al cierre de esta edición la Galería de Nuevos Productos había galardonadado 41 propuestas de vanguardia en seguridad. Un jurado de expertos profesionales de los diferentes sectores ha seleccionado 21 productos de aplicación al ámbito de la Seguridad Laboral; 6 a Seguridad contra Incendios y Emergencias; y 14 en Security.

Fotos: Sicur



Resolución del Parlamento europeo sobre SCI en el sector turístico

EL Parlamento Europeo ha aprobado una resolución sobre «nuevos retos y conceptos para la promoción del turismo en Europa», en la que se incluye un artículo (56) que afecta a la protección contra incendios en hoteles y apartamentos turísticos. Con ello se ha dado un importante paso adelante para reforzar y armonizar la seguridad contra incendios en los países de la Unión Europea (UE).

El artículo 56 de la nueva Resolución europea dice así: «Se considera que el mantenimiento de las normas de seguridad contra incendios en los servicios de turismo en la UE es un ingrediente esencial de buena calidad; por tanto se acoge con satisfacción, el Libro Verde de la Comisión titulado Seguridad en hoteles y alojamientos turísticos». Además, se tiene en cuenta las alegaciones presentadas por las asociaciones de consumidores, las organizaciones de seguridad contra incendios y del sector turístico que apoyan la acción a nivel de la UE sobre la seguridad en el sector. Por todo ello, se pide a la Comisión que presente propuestas de normas mínimas para la seguridad del turismo en la UE, en particular en el ámbito de la seguridad contra incendios y de seguridad de monóxido de carbono (CO); y se subraya la necesidad de una recopilación sistemática de datos sobre la seguridad en este tipo de alojamientos.

Euralarm (de la que TECNIFUEGO-AESPI es miembro activo) acoge con gran interés la resolución y se pone a disposición de la Comisión Europea para iniciar una nueva etapa en estrecha colaboración para materializar así las propuestas en favor de la seguridad contra incendios en establecimientos turísticos.

El Libro Verde elaborado por Euralarm

AES celebra su Asamblea General Ordinaria

La Asociación Española de Empresas de Seguridad (AES) celebró su Asamblea General Ordinaria con la asistencia de más de 50 personas, encuentro en el que también se desarrolló una jornada informativa. Los miembros de la Junta Directiva explicaron a los asistentes el informe de gestión de 2015, los objetivos de la Asociación para 2016, se aprobó el informe económico de 2015 y el presupuesto de 2016 y se eligieron los vocales de la Junta Directiva.

En las ponencias que siguieron a la Asamblea, los coordinadores de las áreas de trabajo de la Asociación informaron a los asociados sobre la actividad de las mismas. Así, en el área de CRA, Paco Ramos detalló el análisis y propuesta de las señales de atraco. En el área de seguridad electrónica, ingeniería, instalación y mantenimiento, Julio Pérez habló sobre propuestas para el diseño, operación, instalación y mantenimiento de las medidas y elementos de seguridad física y electrónica a incluir en los planes de protección específica. En el área de seguridad física, Antonio Pérez explicó la diferenciación entre sistemas de depósito y cajeros automáticos. Y en el área de certificación, Antonio Escamilla invitó a los asociados a enviar los certificados de producto sobre los que tuvieran dudas para su estudio por parte de los miembros de esta área de trabajo.

Además siguieron unas interesantes ponencias sobre temas de candente interés para las empresas de nuestra industria, como fueron las demandas contra las empresas de seguridad por su Responsabilidad Civil. Las CRA e instaladoras en el punto de mira. Cómo reducir el riesgo de ser demandados cuando el cliente ha sufrido un robo y/o cómo ganar la demanda por parte de Rubén Salgado, Abogado de LEXCAM; las nuevas infraestructuras en el transporte, tema del que habló Manuel Sánchez Gómez-Merelo, vocal de la Junta Directiva de AES. La situación de la morosidad en España. Prevención de la misma por parte de las empresas, por parte de Pilar Ferrer, directora ejecutiva de la Plataforma Multisectorial contra la Morosidad; y la tecnología BIM, contexto nacional e internacional, por parte de Sergio Muñoz Gómez, presidente de Building Smart Capítulo español.

se basó en un informe y unas conclusiones tras una encuesta sobre el tema. En el mismo se señala que existen lagunas reguladoras y falta de armonización en Europa, lo que socava la seguridad contra incendios del usuario. Además, existen diferencias sustantivas de un Estado miembro a otro en términos de definiciones básicas y los umbrales que determinan el nivel de protección contra incendios, medidas de seguridad requeridas por la ley o cumplimiento de las normas existentes.

Acuerdo Tesa & Vodafone

A partir de ahora un smartphone, con tecnología NFC, puede sustituir a las llaves o tarjetas de empleado tanto en grandes corporaciones como en pymes. Se trata de una innovadora solución desarrollada por Tesa Assa Abloy para clientes de empresa Vodafone.

Con sólo descargar la app Vodafone Wallet se podrá gestionar el acceso del personal fijo u ocasional a aquellos recintos corporativos (oficinas, salas de reuniones, despachos...) que dispongan de un sistema de control de accesos electrónico.

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

Con esta innovación el sistema de control de accesos SMARTair que permite el control y la seguridad de todas las puertas de un edificio de oficinas con una credencial electrónica inteligente sin contacto se amplía y convierte la experiencia de apertura en una opera-

Fallece David Álvarez presidente y fundador del Grupo Eulen

El presidente y fundador del Grupo Eulen, David Álvarez Díez, falleció el pasado 26 de noviembre en Madrid a los 88 años de edad.

David Álvarez Díez, uno de los grandes empresarios de este país, recientemente había recibido la Gran Cruz del Mérito Civil, otorgado por el Gobierno de España, y el Marquesado de Crémenes, por S.M. El Rey Juan Carlos I, además de ostentar desde 1999 la Medalla de Oro al Trabajo.

Nació en Crémenes (León) hace 88 años, aunque siendo muy niño su familia se traslada a Bilbao, ciudad en la que inicia sus actividades empresariales, fundando, hace más de 60 años, una academia de preparación para escuelas técnicas por la que pasan más de 1.000 alumnos y en la que ejercen la docencia, con él, 20 profesores.

En 1962 constituye la empresa Central de Limpiezas El Sol, a través de la cual aborda la actividad de la limpieza desde una perspectiva empresarial seria, rescatando dichos servicios de la marginación en que se encontraban inmersos en la economía sumergida y dignificando una actividad que se consideraba menor o secundaria.

Central de Limpiezas El Sol es el punto de partida de lo que hoy es el Grupo EULEN de Servicios, en el que se integran, junto con las actividades de Limpieza, otras muy importantes como el Mantenimiento de Instalaciones, Seguridad, Facility Services & Management, Trabajo Temporal, Medio Ambiente, Servicios Sociosanitarios y Servicios Auxiliares, que componen a día de hoy una macroempresa de más de 84.000 empleados en España Portugal, EE.UU. Colombia, Costa Rica, Chile, Jamaica, México, Panamá, Perú, República Dominicana, Libia, Omán y Qatar.

ción cómoda (cualquier modificación puede hacerse de modo remoto y no es necesario reprogramar la cerradura), adaptable (conviven las dos opciones: tarjeta y smarphone NFC) y segura.

Diode, nuevo distribuidor de Mobotix en España

MOBOTIX, el mayor fabricante mundial de sistemas en red de videovigilancia de cámaras megapíxel, ha firmado un acuerdo de colaboración con DIODE, a partir del cual se convierte en distribuidor oficial de sus soluciones en España y Portugal.

Diode desarrolla su actividad en el mercado informático y electrónico de alta tecnología como mayorista. Es especialista en distribución de soluciones de identificación automática y movilidad, comunicaciones, IoT y M2M, desde hace 40 años.

Ambas compañías buscan la excelencia de los productos, así como la aportación de soluciones de valor añadido, por lo que el acuerdo genera grandes expectativas en cuanto a las posibilidades del tándem Mobotix-Diode.

«Tenemos mucha ilusión puesta en Diode, ya que encaja con nuestra filosofía de apuesta por IoT, integración con otras tecnologías y creación de soluciones de valor añadido enfocadas a cada mercado vertical», comenta Alfredo Gutiérrez, Business Development Manager de Mobotix AG para Iberia. «Por lo tanto, creo que va a ser una relación muy fructífera para ambas partes».

David Tajuelo, Business Development Manager de Comunicaciones de Diode, señala que «asociarnos con Mobotix supone un nuevo paso en nuestra estrategia de contar con fabricantes que aporten soluciones tecnológicas avanzadas y diferenciales. Así, podemos aportar nuestro valor añadido al canal, con formación, preventa y soporte técnico, para poder añadir ventaja competitiva a nuestros partners».

Secure&IT: Secure&View, el centro de vigilancia y seguridad gestionada

Secure&View©, el centro de vigilancia y seguridad gestionada de Secure&IT (www.secureit.es) permite a las empresas disponer de un servicio de gestión, administración y alerta temprana de eventos de seguridad, que facilita a las organizaciones tener el control total del estado de seguridad y salud de los activos de información corporativos.

Secure&View© está controlado por expertos en ciberseguridad y sistemas de información, aplica procesos ITIL y cuenta con la certificación ISO 27001, estándar internacional que acredita la eficiencia y efectividad de un Sistema de Gestión de Seguridad de la Información.

El objetivo del centro de Seguridad Gestionada de Secure&IT es garantizar la Confidencialidad, Integridad, Disponibilidad y Legalidad de la información y servicios TIC de las empresas, minimizando riesgos en las mismas debido a ciberataques y otras amenazas, al tiempo que optimiza los ajustados presupuestos en Seguridad de las Tecnologías de la Información.

La monitorización continua de los sistemas es uno de los factores primordiales que garantizan un adecuado nivel de seguridad en el servicio IT. Ése es el aspecto más importante de la actividad desarrollada en SOC (Security Operations Center) Secure&View© una continua y precisa monitorización de los sistemas bajo control, realizando funciones tanto de polling periódico como de alert por evento, de modo que se establece una comunicación bidireccional entre los sistemas gestionados y los sistemas de monitorización.

El SOC de Secure&IT gestiona en la actualidad más de 25 millones de eventos diarios, entre los que se encuentran amenazas de cryptolocker y ransomware, accesos a sitios web maliciosos, infecciones malware, detección de intentos de intrusión a infraestructuras y sistemas críticos, y otros tráficos no deseados en la red. Toda esta información es intercambiada con los sistemas gestionados mediante la combinación de diversos protocolos de red y son transmitidos de forma cifrada y segura entre las empresas y el Centro de Seguridad.

El servicio tiene grandes beneficios para los clientes: mejora de la disponibilidad, estado de salud y seguridad de su infraestructura tecnológica; conocimiento puntual y exacto del estado la red y sistemas de la empresa; notificación (vía email, SMS o teléfono) de las incidencias en los sistemas y las actuaciones a llevar a cabo para su resolución; sistemas bajo control durante las 24 horas del día, los 365 días del año.

Hochiki presenta un informe de sistemas de seguridad

UN estudio realizado por Hochiki Europe indica que más de la mitad (56 %) de las empresas europeas ponen en riesgo la seguridad de los ocupantes del edificio por no ajustar sus sistemas de seguridad de acuerdo con los cambios en la utilización del espacio.

En muchas grandes ciudades, la demanda de espacio de oficina de grado A supera la oferta disponible, por lo que las empresas están invirtiendo en equipamiento y acondicionamiento para adaptarse a las necesidades cambiantes, pero pasando por alto la modificación acorde de los sistemas antiincendios y de seguridad y de la iluminación. Los cinco mayores problemas de los sistemas antiincendios:

1. Registros inadecuados (60 %).
2. Cambio del uso de la sala sin una correcta adaptación de los sistemas (56 %).
3. Los detectores necesitan una limpieza (51 %).
4. El instalador original no implantó el sistema más adecuado para el entorno (48 %).
5. Es necesario sustituir los detectores (34 %).

Realizado por el principal diseñador y fabricante de sistemas de seguridad vital, el estudio de los instaladores también reveló que el 55 % consideraba que a sus clientes les preocupaba más el gasto inicial que el coste total de propiedad, lo que podía poner en riesgo el rendimiento a largo plazo. Así lo explica Simon Massey, jefe de sección de asistencia técnica y formación de Hochiki Europe: «Aunque el sector de la construcción trabaja para dar respuesta al incremento de la demanda de espacio de grado A en ciudades europeas como Londres y Milán, las empresas recurren, como es comprensible, a los recursos que tienen a su disposición para adaptarse a su crecimiento».

En el estudio también se pone de relieve un aspecto importante como es el gasto en mantenimiento. Una quinta parte (22 %) de los encuestados cree que los encargados de los edificios consideran que el mantenimiento es un gasto innecesario. Por otro lado, casi

Grupo Eulen desembarca en Abu Dhabi

El Grupo EULEN, especialista en prestación de servicios a empresas, ha constituido una nueva empresa en Abu Dhabi, EULEN Management & Facilities Services L.L.C., con el socio local Ahmed Almazrouei Group (AAG).

El objetivo de la compañía creada es poder operar en toda la zona de UAE (Emiratos Árabes Unidos), así como dar un paso más en el plan de internacionalización del Grupo EULEN.

Así, EULEN FM&FS proveerá de servicios de Facility Services (limpieza, mantenimiento, jardinería y medio ambiente, servicios auxiliares...) en un mercado con grandes oportunidades para la externalización y que ha tenido un importante crecimiento durante los últimos años.

De esta manera, la compañía amplía su presencia en Medio Oriente donde el pasado año desembarcó en Qatar y cuya expansión internacional se vio reforzada también en 2014 con la creación de la empresa IdeaFM GmbH, junto con el Grupo alemán Dussmann, que permite al Grupo EULEN prestar servicios de facility management en más de 30 países.

Durante la firma del acuerdo, estuvieron presentes Ahmed Mohamed Marzouq Almazrouei -presidente de AAG y de EULEN FM&FS-; Mohamed Ahmed Mohamed Almazrouei –consejero de AAG y EULEN FM&FS– y Mohamed Mazen Al Jabi –Consejero Delegado de AAG y de EULEN FM&FS–. Por parte del Grupo EULEN, acudió Emilio García Perulles, subdirector General de FS y consejero de la nueva empresa; y Fernando Artiach, socio y consejero de EULEN FM&FS.

tres cuartas partes (74 %) creen que lo consideran un mero trámite.

Cuando se les pregunta acerca de los problemas que observan más a menudo, los instaladores afirman que muchos se debían a malas decisiones de instalación y a prácticas de mantenimiento inadecuadas. Por ejemplo, en lo que respecta a los sistemas antiincendios, casi la mitad (48 %) de los instaladores consideraba que las empresas tenían instalado un sistema inapropiado para el entorno, mientras que el 51 % creía que a los detectores les hacía falta una limpieza. En el caso de los sistemas de iluminación de emergencia, se daba una situación similar: el 57 % indicaba que las baterías de los equipos no estaban cargadas, mientras que más de dos quintas partes (44 %) presentaban niveles de lux inadecuados.

Massey realizó estas observaciones acerca de los resultados: «La previsión de crecimiento del PIB europeo para este año es del 1,7 %, por lo que es probable que muchas empresas se vean obligadas a seguir adaptándose a lo que tienen, pero esto no debería ir en detrimento de la seguridad general».

«Informar sobre la importancia de este aspecto, y del mantenimiento en general, se está convirtiendo en una cuestión ineludible y los integrantes de este sector tienen la responsabilidad de apoyar a las empresas para que revisen periódicamente el estado de sus sistemas de seguridad a fin de proteger sus edificios, independientemente de la tipología que estos presenten».

AGA: renovación del certificado VDS

AGA ha acudido a la asamblea organizada en Sevilla por AES (Asociación Española de Seguridad) como miembro de la asociación y como vocal del comité técnico (CTN 108).

Con su presencia y trabajo en dicha asociación la compañía constató su interés y preocupación por adaptar y normalizar las certificaciones europeas al mercado nacional, mejorando aquellos procesos y mecanismos que garanticen a nuestros clientes la mayor calidad de los productos. Esta apuesta de futuro se ve de nuevo recompensada con la renovación del certificado emitido por VDS. Este organismo es un ente certificador alemán que audita artículos de nuestro catálogo y, en este caso, las cerraduras de alta seguridad con las referencias 236, 237, 246, 247 y 248 han conseguido superar el examen con éxito.

Nombramientos en Tyco Integrated Fire & Security

José González Osma.

Tyco Integrated Fire & Security, empresa especializada en soluciones de seguridad y protección contra incendios, ha nombrado a José González Osma nuevo director de Servicios y Residencial, área enfocada a dar servicios de seguridad y vigilancia a hogares y pequeñas empresas, así como servicios de monitorización a grandes empresas y corporaciones.

Las principales responsabilidades de González en su nuevo puesto serán las de gestionar y reforzar el liderazgo de la compañía en el mercado de la seguridad, optimizando todos los recursos para conseguir un fuerte crecimiento y soportar así mayores retos, debido a la evolución del sector durante los últimos tiempos. Entre sus funciones se encuentra la tarea de asegurar la sostenibilidad del crecimiento, manteniendo una alta especialización y diferenciación, apostando por una oferta innovadora y de valor para sus clientes de residencial y pymes.

Además, Tyco IF & S, ha nombrado a Alfonso Crespo como nuevo director de ventas de Retail en España y Portugal para Tyco.

Las principales funciones de Crespo en su nuevo puesto serán las de potenciar el modelo de venta de soluciones integradas para el retail en áreas tan estratégicas como la gestión de los inventarios en tienda, la optimización de la cadena de suministro, la trazabilidad y control de caducidad de los productos perecederos, la pérdida desconocida, la gestión del tráfico en tienda y el control de fraude en tienda entre otras.

Crespo se unirá a la consecución de los principios estratégicos de la compañía, caracterizados por la integración, la innovación y la diferenciación.

Alfonso Crespo

Contactos de empresas, p. 7.

Dahua: serie de cámaras en red 4K Ultra-HD

Dahua Technology, fabricante especializado en el mundo en productos de videovigilancia con sede en Hangzhou, lanza su serie de cámaras en red 4k Ultra-HD- DH-IPC-81200. Esta nueva serie es la de gama más alta que ofrece Dahua, cuenta con una resolución de 12-Megapixel (4k UHD) y un código 4K ultra-HD con detección inteligente.

Todos los modelos de la serie de cámaras en red DH-IPC-81200 proporcionan una total resolución de 3840 x 2160 a una velocidad de imágenes máxima para generar imágenes espectaculares. Esta serie emplea el alto estándar Sony Exmor R 1/1.17" de sensor de color con 12-Megapixel de resolución efectiva, y el Ambarella Cortex-A9 1GHz dual core que genera imágenes más claras y una más alta sensibilidad con inferior ruido. Con una sensacional calidad de vídeo y resolución 4K Ultra-HD, la nueva serie de cámaras de red 4K Ultra-HD está adaptada para instalaciones interiores y exteriores con la que proporcionar imágenes nítidas y fidelidad a pantalla completa.

Dahua HFW81200E-Z y HDBW81200E-Z permite un zoom óptimo de 4 tiempos con focalización sincronizada y puede hacer zoom rápido y enfocar en cinco segundos. La poderosa lente ofrece un amplio ángulo de visión (106° ~32°). La serie 4K ultra-HD adopta la nueva función E-PTZ que ofrece auto-tracking para objetos que disparan la alarma. El hardware de alta gama se complementa con un igualmente poderoso firmware y software que permite una variedad

de funciones inteligentes, incluyendo IVS, detección facial, conteo de personas y mapa de calor. La serie de cámaras en red 4k Ultra-HD brinda una nueva experiencia visual para los usuarios fácil de utilizar, al tiempo que proporciona máxima seguridad y eficiencia en las operaciones.

Modelos:

- 12 Megapixel Ultra HD Network Bullet Camera (HFW81200E-Z.)
- 12 Megapixel Ultra HD Network IR Dome Camera (HDBW81200E-Z).

Bosch: visualización de alarmas con central de incendios

El sistema de seguridad de Bosch introduce un sistema de gestión de seguridad para un máximo de 31 centrales de incendio en red con un máximo de 5.000 puntos de detección. El software de monitorización y visualización es compatible con los sistemas de Bosch de alarma contra incendios, series 1200 y 5000, y soporta hasta diez operadores simultáneamente. El sistema puede tener licencia para 2.500 (FSM-2500) o hasta un máximo de 5.000 puntos de detección (FSM- 5000).

FSM-2500 y FSM-5000 son soluciones sofisticadas para aplicaciones de incendios en las que la visualización es obligatoria mientras que no se requiere la integración en un sistema integral de gestión de edificios. Se conectan a cualquiera de los paneles independientes o a una red de paneles, por Ethernet sobre cobre o cables de fibra óptica. Ambos, Ethernet y las redes de panel basadas en CAN son compatibles. La instalación del nuevo sistema de monitorización de incendios se realiza fácilmente mediante asistentes, que guían al usuario a través de todos los pasos necesarios para la configuración del servidor y del cliente. Se detecta y se asume automáticamente la configuración del panel, evitando así entrada de datos manual complicada y que puede generar errores.

Synology: sistema de videovigilancia Network Video Recorder NVR216

Synology® Inc. ha lanzado Network Video Recorder NVR216, un sistema de videovigilancia con almacenamiento ampliable y compatible con apps como la DS cam de Synology, con las que se puede acceder a las imágenes desde cualquier lugar. El NVR216 ha sido pensado para oficinas y tiendas donde cada rincón es indispensable. Cuenta con una conexión HDMI a 1080p y es compatible con hasta 4 o 9 cámaras IP, dependiendo del modelo. De esta manera, facilita la monitorización y gestión de las grabaciones de videovigilancia y de las cámaras IP.

El NVR216 está equipado con un puerto HDMI a 1080p que facilita la conexión con un monitor y permite visualizar hasta 9 canales de videovigilancia a 720p/30FPS sin la necesidad de tener un ordenador costoso. Gracias a un amplio abanico de puertos, incluyendo el USB 3.0 y el USB 2.0, el NVR216 puede conectarse a un ratón y un teclado para navegar entre las diferentes secuencias de vídeo y acceder a las herramientas de gestión. El NVR216 ha sido diseñado para un bajo consumo energético: sólo gasta 14W, y aun así, ofrece 9 canales de transmisión de vídeo en streaming y grabación continua. En el caso que las grabaciones de videovigilancia necesiten más espacio, el NVR216 se puede ampliar hasta 4 discos al conectarse a una unidad de expansión DX213.

El NVR216 funciona con el sistema de grabación de vídeo en red Synology Surveillance Station, que ofrece una interfaz intuitiva y un gran número de funciones de vigilancia. Al utilizar ambos dispositivos, los usuarios pueden sacar el máximo del panel de Live View, al realizar operaciones en pantalla que les permitirán monitorizar las transmisiones de vídeo desde varias cámaras IP, utilizar el panel Timeline para seleccionar una fecha y hora y reproducir grabaciones desde múltiples canales a la vez. Asimismo, también pueden instalar herramientas de análisis inteligentes, como la detección de movimiento, que se usa para captar comportamientos sospechosos.

Scati: plataforma de grabación IP para localizaciones remotas

SCATI, empresa especializada en soluciones integrales de vídeo IP, ha presentado su nueva gama de plataformas de grabación IP Scati Vision Serie A.

De reducidas dimensiones (35 x 145 x 84 mm (HxWxD); son capaces de gestionar 2 cámaras a resolución megapíxel con total estabilidad y máximo rendimiento. Además, se pueden equipar con hasta 256 GB de almacenamiento al incorporar algoritmos de procesado avanzado de imagen.

Su formato altamente compacto y el módulo 3G integrado hacen de estas plataformas de grabación IP la solución ideal para localizaciones remotas y desatendidas.


Nota de prensa

SCATI presenta su plataforma de grabación IP para localizaciones remotas

Conectividad asegurada

El módulo 3G no sólo actúa como back-up en caso de fallo de la red, sino que también asegura la conectividad incluso en las instalaciones más remotas bajo cualquier circunstancia.

Fácilmente instalable en ATM's, su uso conjunto con la aplicación Scati Cash permite relacionar las imágenes con la información de las transacciones, posibilitando la detección de operaciones fraudulentas.

Scati Vision permite la gestión, monitorización, búsqueda y exportación de vídeo localmente, a través de Scati Vision WEB o desde aplicaciones de Centro de Control SCATI, constituyendo un sistema escalable ideal para instalaciones distribuidas.

Vivotek: herramienta de diseño de proyectos 3D para diseñadores de Sistemas de Vigilancia

Vivotek ha lanzado una Herramienta de Diseño de Sistemas de Vídeo IP, que permite a los diseñadores de sistemas simular la cobertura de cualquier sistema de cámaras de red de Vivotek en 2D y 3D. Esta herramienta gratuita ayuda a los diseñadores de sistemas a ahorrar tiempo cuando necesitan determinar la posición ideal para cualquier cámara de red. También hace que el diseño de sistemas de videovigilancia profesional no sólo sea más rentable sino también más inteligente.

La Herramienta de Diseño de Sistemas de Vídeo IP de Vivotek ofrece cuatro beneficios principales:

• **Plan de Información Precisa:** La Herramienta de Diseño de Sistemas de Vídeo IP de Vivotek incluye las especificaciones detalladas de todas las cámaras de red de Vivotek. Los diseñadores de sistemas por lo tanto son capaces de diseñar con mayor precisión una estrategia de seguridad mediante la herramienta de cálculo de longitud focal de lente y ángulo de visión.

• **Funciones Fáciles de Usar:** La Herramienta de Diseño también puede estimar los requerimientos de ancho de banda y almacenamiento de información con el fin de ayudar a diseñar los sistemas de vídeo en red para cualquier número de cámaras de red, servidores de vídeo y ofrecer una visión general de la implementación del sistema para muchos escenarios de vigilancia diferentes.

• **Visualiza las Comunicaciones:** Cuenta con una interfaz completamente intuitiva y utiliza modelado 2D y 3D, por lo cual los diseñadores de sistemas pueden comprobar con precisión el campo de visión de cada cámara.

• **Escenarios Realistas:** Para desarrollar un plan más realista del sistema, la Herramienta de Diseño de Sistemas de Vídeo IP de Vivotek permite a los diseñadores de sistemas subir imágenes de planos en formatos JPEG, JPG, BMP e imágenes de fondo en PDF. La Herramienta de Diseño de Sistemas de Vídeo IP de Vivotek está disponible en el sitio web de Vivotek y soporta los siguientes sistemas operativos: Windows 10, 8, 7, Vista, XP SP2. Para usuarios de Mac, por favor, instale Parallels Desktop con antelación.

Trinity, solución integrada de grabación y almacenamiento de vídeo de Samsung y Veracity

Samsung Techwin Europe y Veracity han presentado TRINITY™, una solución conjunta de videovigilancia en red que no requiere de NVR. TRINITY, que se beneficia de la capacidad de procesamiento de las cámaras con plataforma abierta (Open Platform) WiseNet III de Samsung, permite ejecutar simultáneamente múltiples aplicaciones vanguardistas entre las que se encuentra COLDSTORE, la solución de almacenamiento directo más galardonada de Veracity. Los usuarios se benefician de un sistema robusto y escalable que no requiere un servidor o un dispositivo de grabación de red (NVR). Soporta audio, metadatos y vídeo, y ofrece prestaciones innovadoras: conmutación a nivel de cámara en caso de fallo y capacidad de recuperación ante interrupciones de la red. Como resultado, se consiguen grandes ahorros en licencias de software y en costes de hardware (NVR) en los que se incurre normalmente cuando es preciso contar con un sistema de grabación basado en redes IP. Además, con un conjunto COLDSTORE de hasta 120 TB, que consume solo 60 vatios, es posible ahorrar hasta un 90 % de energía en comparación con las soluciones convencionales de almacenamiento en servidor. Esto permite al usuario acogerse a las subvenciones medioambientales de la Unión Europea.

Contactos de empresas, p. 7.

ÍNDICE

MATERIALES, EQUIPOS Y SISTEMAS DE SEGURIDAD

SERVICIOS DE SEGURIDAD

ALARMA Y CONTROL

GAROTECNIA
Valdelaguna, 4 local 3
28909 Getafe (Madrid)
Tel.: 916 847 767 - Fax: 916 847 769
garotecnia@garotecnia.com
www.garotecnia.com
Autorizada por la D.G.P. con el nº 2.276

Tyco Integrated Fire & Security

Edificio Ecu-I
Ctra. de La Coruña, km 23,500
28290 Las Rozas (Madrid)
Tel.: 902 444 440 - Fax: 91 631 39 78
www.tyco.es

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

FUNDADA EN 1966
INSTALACIONES A SU MEDIDA
ISO 9001

Antoñita Jiménez, 25
28019 Madrid
Tel.: 91 565 54 20 - Fax: 91 565 53 23
seguridad@grupoaguero.com
www.grupoaguero.com

Central Receptora de Alarmas/Videovigilancia
Autorizada por la D.G.P. con el nº. 729
Avda de Olivares 17 – Plg. Industrial PIBO
41110 Bollullos de la Mitación (Sevilla)
Tlfno. 902194814 – 954108887
Fax. 954002319
gerencia@gruporomade.com
SERVICIOS EN TODA ESPAÑA

Accesos · CCTV · Incendio · Intrusión
Oficina Central:
Maresme, 71-79 · 08019 Barcelona
Fax 933 518 554
902 202 206 *www.casmar.es*

COMUNICACIONES

Sistemas de seguridad para garajes comunitarios

C Aragón 355 - 08009 Barcelona
T 902 154 105
info@segurparking.com
www.segurparking-online.com

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

El directorio es la zona más consultada de nuestra revista.

Módulo: 660€/año*

Más información:
Tel.: 91 476 80 00
e-mail: publi-seguridad@epeldano.com
*** Tarifa vigente 2016**

CONTROL DE ACCESOS ACTIVO

3M España S. L.
C/Juan Ignacio Luca de Tena, 19-25
28027. Madrid.
Tel. 913 216 416
Fax. 913 216 748
mgonzalez3@mmm.com
www.3m.com/es/seguridad

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

SKL Smart Key & Lock
Ferrerías 2,
20500 MONDRAGÓN -SPAIN-

+34 943 71 19 52
info@skl.es
www.skl.es

DIGITEK
a member of primion group

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

GRUPO SPEC

C/ Caballero, 81
08014 Barcelona
Tel. 93 247 88 00 • Fax 93 247 88 11
spec@specsa.com
www.grupospec.com

---

biosys

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

---

by demes
avanzando juntos hacia el futuro

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

RISTER
PRESENTCO®

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

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

---

accesor
Soluciones integrales en control de Accesos y seguridad
DDS

Carrer Esperança, 5
08500 Vic (Barcelona)
Tel.: 902 447 442
Fax.: 938 864 500

info@accesor.com
www.accesor.com

DORLET

DORLET S. A. U.

Parque Tecnológico de Álava
C/Albert Einstein, 34
01510 Miñano Mayor - ALAVA - Spain
Tel. 945 29 87 90 • Fax. 945 29 81 33

e-mail: comercial@dorlet.com
web: http://www.dorlet.com

---

setelsa link
Sistemas Electrónicos y Telecomunicación S.A.

SETELSA
Polígono Industrial de Guarnizo - Parcela 48-C Naves "La Canaluca" 2 y 4
39611 GUARNIZO-CANTABRIA. ESPAÑA
Tel.: 942 54 43 54
www.setelsa.net

DETECCIÓN DE EXPLOSIVOS

COTELSA

COTELSA
Basauri, 10-12, Urb. La Florida
Ctra. de La Coruña, Aravaca
28023 Madrid
Tel.: 915 662 200 - Fax: 915 662 205
cotelsa@cotelsa.es
www.cotelsa.es

TECOSA

TELECOMUNICACIÓN, ELECTRÓNICA Y CONMUTACIÓN

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

TARGET TECNOLOGIA

TARGET TECNOLOGIA, S.A.
Ctra. Fuencarral, 24
Edif. Europa I - Portal 1 Planta 3ª
28108 Alcobendas (Madrid)
Tel.: 91 554 14 36 • Fax: 91 554 45 89
info@target-tecnologia.es
www.target-tecnologia.es

SISTEMAS DE EVACUACIÓN

OPTIMUS
SOUND & COMMUNICATION

OPTIMUS S.A.

C/ Barcelona 101
17003 Girona
T (+34) 972 203 300

info@optimus.es
www.optimusaudio.com

BOSCH

BOSCH SECURITY SYSTEMS SAU
C/ Hermanos García Noblejas, 19
Edificio Robert Bosch
28037 - Madrid • Tel.: 902 121 497
Delegación Este:
Plaça Francesc Macià, 14-19
08902 L'Hospitalet de Llobregat (Barcelona)
Tel.: 93 508 26 52 • Fax: 93 508 26 21
Delegación Norte: Tel.: 676 600 612
es.securitysystems@bosch.com
www.boschsecurity.es

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

---

by demes
avanzando juntos hacia el futuro

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

---

aguilera

GRUPO AGUILERA

FABRICANTES DE SOLUCIONES PCI DETECCIÓN Y EXTINCIÓN DE INCENDIOS

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

Delegaciones en:

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

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

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

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

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

PROTECCIÓN CONTRA INTRUSIÓN. ACTIVA

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

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

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

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

TELECOMUNICACIONES

PROTECCIÓN CONTRA INCENDIOS. PASIVA

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

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

Calle Menéndez Pidal 43
Edificio B 2ª planta
28036 Madrid

Tel. 913 685 120

info@solexin.es
www.solexin.es

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

PROTECCIÓN CONTRA ROBO Y ATRACO. PASIVA

VIGILANCIA POR TELEVISIÓN

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

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

CERRADURAS ALTA SEGURIDAD
Talleres AGA, S. A.
C/ Notario Etxagibel, 6
20500 Arrasate-Mondragón
GUIPÚZCOA (Spain)
Tel.: (+34) 943 790 922 • Fax: (+34) 943 799 366
talleresaga@aga.es • www.aga.es

HIKVISION SPAIN
C/ Almazara 9
28760- Tres Cantos (Madrid)
Tel. 917 371 655
Fax. 918 058 717
info.es@hikvision.com
www.hikvision.com

Samsung Techwin Europe Ltd

P. E. Omega - Edificio Gamma
Avenida de Barajas, 24 Planta 5 Oficina 5
28108 Alcobendas (Madrid)
Tel.: 916 517 507

STEsecurity@samsung.com
www.samsungcctv.com

IPTECNO Videovigilancia
C/ Pla de Ramassar, 52
08402 Granollers.
Tlf.: 902 502 035 • Fax: 902 502 036
iptecno@iptecno.com
www.iptecno.com

Dahua Technology Co, Ltd.

No.1199, Bin'an Road, Binjiang
District, Hangzhou
310053 China
+86-571-87688883 • +86-571-87688815

overseas@dahuatech.com
www.dahuasecurity.com

Visiotech
Avenida del Sol, 22
28850, Torrejón de Ardoz (Madrid)
Tel.: 911 836 285 • Fax: 917 273 341
info@visiotech.es
www.visiotech.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.: 00 331 70 74 46 27
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

N2V
C/ Torrent Tortuguer, 7 - nave 4
Pol. Ind. Els Pinetons
08291 RIPOLLET (Barcelona)
Tel.: 93 580 50 16 - Fax: 93 580 36 58
n2v@n2v.es
www.n2v.es

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

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

El directorio es la zona más consultada de nuestra revista.

Módulo: 660€/año*

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

* Tarifa vigente 2016

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.

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

EVENTOS DE SEGURIDAD

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

CERTIFICACIONES

INSPECCIÓN Y CERTIFICACIÓN

C/ Caleruega, 67, Planta 1
28033 Madrid
Tel. 917663133
http://www.tuv-nord.es/

ASOCIACIONES

ASOCIACIÓN DE EMPRESAS DE SEGURIDAD Y SERVICIOS DE ANDALUCIA
C/ DOCTOR DUARTE ACOSTA Nº 7
11500 PUERTO DE SANTA MARIA · CADIZ
Tel. 677.401.811
Fax: 954.002.319
gerencia@adessan.es

C/ Alcalá 99
28009 Madrid
Tel. 915765255
Fax. 915766094
info@uaseguridad.es
www.uaseguridad.es

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

ASOCIACIÓN ESPAÑOLA DE INGENIEROS DE SEGURIDAD
C/ San Delfín 4 (local 4 calle)
28019 MADRID
aeinse@aeinse.org
www.aeinse.org

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

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
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 - 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

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

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

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

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

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

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

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

ASOCIACIÓN DE INVESTIGACIÓN PARA LA SEGURIDAD DE VIDAS Y BIENES CENTRO NACIONAL DE PREVENCIÓN DE DAÑOS Y PÉRDIDAS
Av. del General Perón, 27
28020 Madrid
Tel.: 914 457 566 - Fax: 914 457 136

FEDERACIÓN ESPAÑOLA DE SEGURIDAD
Embajadores, 81
28012 Madrid
Tel.: 915 542 115 - Fax: 915 538 929
fes@fes.es
C/C: comunicacion@fes.es

ASOCIACIÓN DE JEFES DE SEGURIDAD DE ESPAÑA

Avd. 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

FORMACIÓN DE SEGURIDAD

TECNOSYSTEMS
Formación especializada en video IP
Avenida de Brasil 29, 28020 Madrid

Telf.: 916 323 168
www.videoipformacion.es

Homologado por el Ministerio del Interior y la Junta de Andalucía.

Avda de Olivares 17 • Plg. Industrial PIBO.
41110 Bollullos de la Mitación (Sevilla).
Tlfno. 902194814 – 954108887
Fax. 954002319
gerencia@gruporomade.com

CENTRALES DE RECEPCIÓN Y CONTROL

ALARMAS SPITZ S. A.
Gran Vía, 493 - 08015 Barcelona
Tel.: 934 517 500 - Fax: 934 511 443
Central Receptora de alarmas
Tel.: 902 117 100 - Fax: 934 536 946
www.alarmasspitz.com

INTEGRACIÓN DE SISTEMAS

ARQUERO SISTEMA CORPORATIVO

Avda. de la Feria 1
Edificio Incube - sala 8
35012 Las Palmas de Gran Canaria
Tel.: **928 09 21 81**
www.sci-spain.com

TELECOMUNICACIÓN, ELECTRÓNICA Y CONMUTACIÓN

Grupo Siemens
Industry Sector
División Building Technologies
Ronda de Europa, 5
28760 Tres Cantos - Madrid
Tel.: +34 91 514 75 00 - Fax: +34 91 514 70 30

APLICACIONES INFORMÁTICAS

SOFTWARE DE GESTIÓN DE ALARMAS

Gestión de Incidentes – Plataforma de Vídeo
Mapas Interactivos – Dispositivos Móviles
Innovative Business Software
Tel.: 691 540 499
info@innovative.es
www.innovative.es

SERVICIOS AUXILIARES

SEDE CENTRAL

Parque Empresarial La Finca
Paseo del Club Deportivo, 1 - Bloque 13
28223 Pozuelo de Alarcón (Madrid)
Tel.: 902 01 04 06
Web: www.servicass.es
E-mail: servicass@servicass.es

INSTALACIÓN Y MANTENIMIENTO

Homologación de registro D.G.S.E. nº 432

INSTALACIÓN Y MANTENIMIENTO
INTRUSIÓN – CCTV – INCENDIO – ACCESOS
SUBCONTRATACIÓN
ALICANTE, VALENCIA, MURCIA, ALBACETE

www.seguridadlevante.com
902 400 022
info@seguridadlevante.com

TELEFÓNICA INGENIERÍA DE SEGURIDAD
Don Ramón de la Cruz 82-84 4ª
28006 Madrid
Tel.: 917 244 022 • Fax: 917 244 052
tis.clientes@telefonica.es
www.telefonica.es/ingenieriadeseguridad

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

FUNDADA EN 1966

INSTALACIONES A SU MEDIDA

ISO 9001

Antoñita Jiménez, 25
28019 Madrid
Tel.: 91 565 54 20 - Fax: 91 565 53 23
seguridad@grupoaguero.com
www.grupoaguero.com

VIGILANCIA Y CONTROL

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

SEGURIDAD
Control accesos / Intrusión / CCTV / Detección incendios / Megafonía / Interfonía / Consultoría

ENERGÍA
Eficiencia energética / Gestión inteligente de infraestructuras / Electricidad / Climatización / Consultoría energética

www.ambarsye.es
ambarsye@ambar.es
902 55 08 01

Avda. Manzanares, 196
28026 Madrid
Tel.: 914 768 000 - Fax: 914 766 057
publi-seguridad@epeldano.com
www.instalsec.com

SEDE CENTRAL

Parque Empresarial La Finca
Paseo del Club Deportivo, 1 - Bloque 13
28223 Pozuelo de Alarcón (Madrid)
Tel.: 902 01 04 06
Web: www.casesa.es
E-mail: casesa@casesa.es

TRANSPORTE Y GESTIÓN DE EFECTIVO

SECURITAS SEGURIDAD ESPAÑA
C/ Entrepeñas, 27
28051 Madrid
Tel.: 912 776 000
www.securitas.es

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

PUBLICACIONES WEB

MATERIAL POLICIAL

PUNTOSEGURIDAD.COM
TF: 91 476 80 00

info@puntoseguridad.com
www.puntoseguridad.com

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

SEGURSERVI, S. A.
Empresa de Seguridad
Moreno Nieto, 9
28005 Madrid
Tel.: 902 191 200 - Fax: 913 658 179
segurservi@segurservi.es
Web: www.segurservi.es
Autorizada por la D.G.P. con el nº 1.833

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

El directorio es la zona más consultada de nuestra revista.

Módulo: 660€/año*

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

* Tarifa vigente 2016

Suscríbase

CUADERNOS DE SEGURIDAD

RELLENE SUS DATOS CON LETRAS MAYÚSCULAS (fotocopie este boletín y remítanoslo)

Entidad: _____ N.I.F.: _____
D. _____ Cargo: _____
Domicilio: _____
Código Postal: _____ Población: _____
Provincia: _____ País: _____
Teléfono: _____ Fax: _____
Actividad: _____
E-mail: _____ Web: _____

Forma de pago:

❑ Domiciliación bancaria c.c.c. nº _____
❑ Cheque nominativo a favor de EDICIONES PELDAÑO, S. A.
❑ Ingreso en Banco Popular c.c.c. 0075 0898 41 0600233543
❑ Cargo contra tarjeta VISA nº _____ Caducidad _____

Firma

TARIFAS (válidas durante 2016)

ESPAÑA
❑ 1 año: 93€ ❑ 2 años: 165€ (IVA y Gastos de envío incluido)

EUROPA
❑ 1 año: 124€ ❑ 2 años: 222€ (Gastos de envío incluido)

RESTO
❑ 1 año: 133€ ❑ 2 años: 239€ (Gastos de envío incluido)

Peldaño

Departamento de Suscripciones: 902 35 40 45
Avda. del Manzanares, 196 • 28026 Madrid • Tel.: +34 91 476 80 00 • Fax: +34 91 476 60 57
suscripciones@epeldano.com • www.puntoseguridad.com

Ignacio Gisbert

Jefe de Personal, Seguridad y Servicios de Cecabank

«En la vida se aprende del ayer pero siempre se mira hacia el futuro»

Gemma G. Juanes

NADA más cruzar las primeras palabras ya supimos que esta entrevista acabaría reflejando una historia cargada de sentido común. Sobran los minutos para descubrir a un hombre que evoca los momentos de su biografía de forma extraordinaria, porque hoy, inmersos en un mundo convulso, ha sabido buscar y encontrar lo bueno de cada instante. Esta es la crónica de un encuentro plagado de franqueza y sinceridad, donde nuestro protagonista ofrece, casi sin darse cuenta, pequeñas pistas de cómo afrontar las pruebas y retos de toda una vida.

No erraríamos al decir que Ignacio Gisbert, jefe de Personal, Seguridad y Servicios de Cecabank, es de aquellos que creen en el compromiso, el esfuerzo y la generosidad. El que hoy habla para «Un café con…» ha desarrollado gran parte de su trayectoria profesional en el ámbito jurídico –es licenciado en Derecho, diplomado en Derecho Laboral, director de Seguridad…– en distintos organismos y sectores –CEOE, patronal de las Cajas de Ahorros, sector pesquero…–, antes de asumir su actual puesto, que le sumergió de lleno en el mundo de la Seguridad Privada.

Escucha con una inquebrantable tranquilidad una ráfaga de preguntas profesionales mientras se intercala una curiosidad de obligado interés, ¿y qué tal el cambio hacia este sector? Gisbert, de pausada y clara conversación, responde veloz: «Esta es una profesión tremendamente interesante y adictiva. Un sector honesto, donde he encontrado unos profesionales con una ilimitada solidaridad y generosidad para compartir sus conocimientos y experiencia». Su discurso continúa con un sincero y amable reconocimiento hacia todos aquellos «padres» de la Seguridad Privada, sin los cuales hubiera sido imposible alcanzar «un sector cada vez más profesional y competitivo en el ámbito empresarial e intelectual», matiza.

Inteligente, educado, ingenioso y con un sorprendente sentido del humor, solo ha hecho falta virar la temática de la conversación hacia temas más personales para conocer a un ser humano de gran talante, con una visión global del mundo… y, además, oceanógrafo. Describe una infancia feliz, que le enseñó a extraer lo positivo de la vida, con recuerdos de horas de estudio y tardes de juego. Sincero, emotivo, carismático e inquieto –«soy nervioso y activo por naturaleza ... ¡pero nunca me estreso!. Disfruto por igual tanto de mi trabajo como del ocio». Tiempo libre que dedica en exclusiva a su mujer y sus hijas, a quienes ha inculcado la afición a la lectura, acompañándolas una vez al mes a coger libros en la biblioteca.

De vestir clásico y elegante, y «nada coqueto», asegura cuidar su alimentación y practicar deportes náuticos. Disciplinado, curioso, hombre de claros y rotundos principios –«en la vida se aprende del ayer –afirma– pero siempre se mira hacia el futuro», parece tener la fórmula mágica para sobrevivir hoy en día: unas gotas de generosidad, humildad, tolerancia... Tomaremos nota. ●

Plataforma de seguridad CORPORATIVA

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

Plataforma abierta de seguridad con amplio catálogo de productos integrados.

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

Integración natural dentro del ecosistema de tecnologías de información.

ARQUERO SISTEMA CORPORATIVO

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

HIKVISION

TURBO HD TRIBRID SYSTEM

La tecnología Turbo HD de Hikvision marca un hito en la evolución de la era analógica. Los usuarios de CCTV analógico van a poder disfrutar de una resolución Full HD sin necesidad de cambiar el cableado de las instalaciones analógicas ya existentes. Permite la transmisión de vídeo sin retardo en 1080P a través de cable coaxial y es compatible con cámaras analógicas tradicionales, cámaras IP de Hikvision y dispositivos con el estándar HDTVI.

¡ABRÓCHENSE LOS CINTURONES, EL HÍBRIDO ANALÓGICO HD HA PUESTO EL TURBO!

sicur
Visítanos en el pabellón: 10
stand D-11

First Choice for Security Professionals

HIKVISION SPAIN - C/ Almazara, 9 - 28760 Tres Cantos (Madrid). Tel. +34 91 7371655 - Fax +34 91 8058717
info.es@hikvision.com - www.hikvision.com