

CUADERNOS DE SEGURIDAD

Núm. 306 • DICIEMBRE 2015 • 10 euros

 PUNTOSEGURIDAD.com

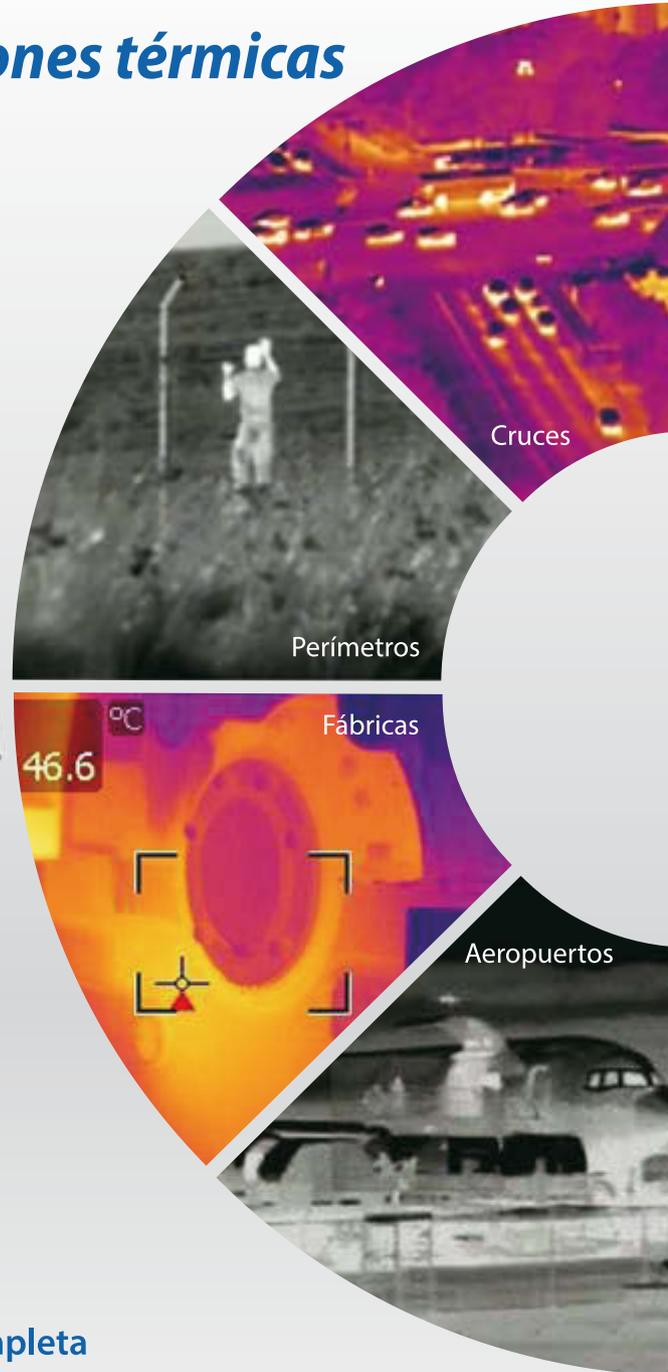
Seguridad en museos y patrimonio

Protección
contra robo e intrusión

ESPECIAL Administradores de Fincas 2015

Detección en Oscuridad Total

— Soluciones térmicas



• Análisis inteligente de vídeo



• Medición de temperatura



• Salida Tri-híbrida: IP/ HDCVI/ Analógico



• Solución & Monitorización Térmica Completa

España



IPTECNO

Portugal



CE FC CC UL ROHS 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

NUEVAS ESTRATEGIAS Y HERRAMIENTAS

El sector ante un futuro prometedor

Con este número cerramos un año en el que el sector de la Seguridad Privada había puesto todas sus esperanzas en contar con el ansiado desarrollo reglamentario de la Ley de Seguridad Privada, Ley 5/2014 de 4 de abril. Hace doce meses, estas mismas páginas se hacían eco del esfuerzo y expectativas de un sector ante un reglamento del que depende y está en juego, en gran medida, el futuro de la Seguridad Privada. Ahora con 365 días por delante ya nadie se atreve a hacer previsiones. ¿Será 2016 el final de la crisis? ¿Será 2016 el año del Reglamento de Seguridad Privada?... Lo que si es cierto es que el sector, maduro y profesional, espera con cierta inquietud un desarrollo reglamentario que, unido a nuevas estrategias y herramientas, adapte su tejido empresarial al momento actual.

Puede que las grandes soluciones no estén a nuestro alcance, pero, sin duda, sí está en nuestra mano seguir apostando por proyectos e iniciativas, que traten de acercar la situación actual y futura de una industria en continua evolución, y de atender las necesidades e intereses de un colectivo con un amplio espíritu emprendedor.

Sobre estas premisas y fiel a su compromiso con el sector, Peldaño, editora de Cuadernos de Seguridad, celebrará a comienzos de año la I Jornada Técnica de RPAS y Seguridad Privada en Madrid, con el apoyo y colaboración de la Federación Empresarial Española de Seguridad. El objetivo del encuentro es establecer un foro que reúna al sector de la Seguridad en una jornada de trabajo en la 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. Algunos de los temas que se abordarán durante la jornada son: «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».

En este final de año, también ponemos el punto de mira en Security Forum, donde el equipo de profesionales de Peldaño trabaja ya en su cuarta edición, que se celebrará los días 25 y 26 de mayo en Barcelona, y que volverá a posicionarse como excepcional plataforma de networking e innovador espacio que se adapta a las necesidades e inquietudes de los profesionales de la seguridad. Además, en el marco del encuentro se celebrará el Congreso Security Forum 2016 que se desglosará en dos sesiones diferenciadas: Global Day, dedicado a la seguridad global, donde 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; y Cyber Day, que se centrará en la ciberseguridad.

Un año más volveremos a compartir innovación y conocimiento con los profesionales de un sector que trabaja por un futuro prometedor y está preparado desde hace tiempo para su reactivación y que, como siempre, volverá a contar con nuestro apoyo. ¡Felices fiestas!

3 EDITORIAL

El sector ante un futuro prometedor.

8 SECURITY FORUM

— *Security Forum 2016, cada vez más cerca.*

10 EN PORTADA

SEGURIDAD EN MUSEOS

Los museos, centros de arte, galerías... deben contar con un adecuado y aceptable nivel de seguridad. Se trata de instalaciones que, junto a las valiosas e insustituibles piezas y obras que albergan, se encuentran expuestas a un amplio catálogo de riesgos. Y es que la conservación y, por supuesto, la seguridad de nuestro patrimonio artístico, es uno de los objetivos de los directores de los museos, y no solo de ellos, de nuevo viene a jugar un papel fundamental la figura del responsable de Seguridad del centro museístico. Para garantizar esta prevención y seguridad, la tecnología

ha jugado y juega actualmente un papel imprescindible de ayuda. Medios y sistemas de seguridad que sirven de ayuda y complemento al fundamental trabajo que realizan los responsables de Seguridad con el fin de poder contar con dos elementos importantes: protección y prevención.

ENTREVISTAS:

— **Andrés Pérez Vega.** Director de Seguridad. Museo Thyssen-Bornemisza.



— **Juan José Pintado García.** Jefe del departamento de Seguridad. Museo Nacional de Arte de Catalunya.

ARTÍCULOS:

- «Más de 15 años de itinerario en la protección del Patrimonio Cultural», por **Jesús Alcantarilla.**
- El robo de arte: ¿son seguros los museos?, por **Antonio Gómez Montolío.**
- Videovigilancia y mucho más en museos, por **Alfredo Gutiérrez.**
- La tecnología de sensores multifocal vigila la Millenium Square, por departamento Panomera Multifocal Sensor Systems. Dallmeier.
- Informe Protecturi 2015.

33 SEGURIDAD ADMINISTRADORES DE FINCAS

ENTREVISTA:

- **Manuela Julia Martínez Torres.** Presidenta del Colegio Profesional de Administradores de Fincas de Madrid.
- **Juan Manuel Rodríguez.** Director comercial de Grusegur 4 y Gruser 4.

CUADERNOS DE SEGURIDAD

www.puntoseguridad.es

Nº 306 • DICIEMBRE 2015

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
ISSN: 1698-4269
Precio: 10 €. Precio suscripción (un año, 11 núms.) 93 €, (dos años, 22 núms.) 165 € (España).

«Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra solo puede ser realizada con la autorización de sus titulares, salvo excepción prevista por la ley. Dirijase a CEDRO (Centro Español de Derechos Reprográficos) si necesita fotocopiar o escanear algún fragmento de esta obra (www.conlicencia.com; 91 702 19 70 / 93 272 04 45)».



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

De conformidad con lo dispuesto por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y el Real Decreto 1720/2007, le informamos que sus datos están incorporados a un fichero responsabilidad de Ediciones Peldaño, S. A., y que serán tratados con la finalidad de gestionar los envíos en formato papel y/o digital de la revista, de información sobre novedades y productos relacionados con el sector, así como poder trasladarle, a través nuestro o de otras entidades, publicidad y ofertas que pudieran ser de su interés. Si no está de acuerdo, o si desea ejercitar los derechos de acceso, rectificación, cancelación y oposición puede dirigirse a Ediciones Peldaño, S. A., Avda. Manzanares, 196. 28026 Madrid o al correo electrónico distribucion@epeldano.com

ARTÍCULOS:

- Securitas Direct: cuidamos a las personas, por **José Ignacio Jiménez**.
- Ahorro, seguridad y confort desde el dispositivo móvil, por **José González Osma**.
- Accesibilidad a las comunidades de vecinos, por **Porteralia**.
- La conciencia preventiva: de lo obligatorio a lo voluntario, por **Tecnifuego-Aespi**.
- La carta de invierno, por **Jon Michelena**.
- Estudio Tyco: «Hogar inteligente y conectado en España».

57 CIBERSEGURIDAD

- Confianza, seguridad y GCTI, por **María José de la Calle**.

60 SEGURIDAD**ENTREVISTAS:**

- **Ángel Galán**. Presidente del Instituto de Probática e Investigación Criminal (IPIC).

ARTÍCULOS:

- Cómo incide el análisis de imagen

- en la tecnología térmica, por **José Javier de la Rosa**.
- Educación ejecutiva para los profesionales de Seguridad, por **Juan Muñoz**. CPP, CSM, CSYP. Presidente de ASIS España.
- Acercamiento a la deontología profesional en la Seguridad Privada (I), por **José María García de Prado**.
- Seguridad en los hospitales: hacer más con menos, por **Noelia Castellón**.

90 C.S. ESTUVO ALLÍ

- Axis Solutions Conference Iberia 2015.
- V Congreso Protecturi.
- II Jornada «Guardia Civil-Empresa».
- 9ENISE, récord de convocatoria en torno a la ciberseguridad.

99 ACTUALIDAD

- ISM: Conclusiones del IV Foro de la Ciberseguridad.
- Cepreven: Plan Estratégico 2015-2020.
- SKL: ¿se puede registrar quién accede a las vitrinas de museos, tiendas de antigüedades, subastas...?

- Investigación Criminal. Principios, técnicas y aplicaciones.
- Prosegur mantiene en 2015 la tendencia positiva en su crecimiento.
- AGS afianza su presencia internacional de la mano de Bosch.

104 EQUIPOS Y SISTEMAS

- Bunker Seguridad incorpora la línea Redwall de Optex a su catálogo.
- Hommax optimiza sus productos contra incendios.
- Gunnebo: Safety PLUS.
- Samusng y Veracity: solución integrada de grabación y almacenamiento de vídeo.
- Vivotek: nuevas soluciones de vigilancia H.265.
- Synology: Surveillance Station.

114 UN CAFÉ CON...

- **Ángel Bahamontes**. Presidente de la Asociación Nacional de Tasadores y Peritos Judiciales Informáticos, ANTPJI.

Síguenos en twitter

@PuntoSeguridad 

ENERO 2016 - Nº 307

EN PORTADA

EL SECTOR ANTE 2016

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 2016 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 preguntado 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.



CIBERSEGURIDAD

En un mundo totalmente globalizado, donde la información traspasa fronteras, la ciberseguridad se ha convertido en un elemento fundamental para las empresas. Y es que el amplio volumen de pérdidas, tanto económicas como de imagen, que puede suponer para las compañías un ciberataque, hace necesario implantar políticas de prevención y protección.

La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno.

Por eso en el próximo número dedicaremos un apartado de nuestra publicación a la Ciberseguridad, donde expertos en la materia, entre ellos responsables de INCIBE, CNPIC, CCI, ISMS, así como grandes compañías explicarán los retos de la ciberseguridad.

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
Acal BFI	64	914531160	www.acabfi.es
Alai Secure	67	902095196	www.alaisecure.com
Axis	90	918034643	www.axis.com
Bosch Security Systems	71	902121497	www.boschsecurity.es
Bunker Seguridad	104	913316313	www.bunkerseguridad.es
Casesa	4ª Cub.	902010406	www.casesa.es
Dahua	2ª Cub.,103	865718768883	WWW.dahuasecurity.com
Dallmeier	2	915902287	www.dallmeier-electronic.com
Dorlet	59	945298790	www.dorlet.com
ESV	56	916702071	www.grupoesv.com
FF Videosistemas-Geutebrück	25	902998440	www.geutebruckspain.com
Freemática	89	937247220	www.freemática.com
Gruser 4	51,53	915913603	www.gruser4.com
Gunnebo	104	918375509	www.gunnebo.com
Hikvision	13,15,17	917371655	www.hikvision.com
Hommax	104	961594646	www.hommaxistemas.com
Honeywell	86	913136272	www.honeywell.es
I Jornada RPAS y Seguridad Privada	83	914768000	www.dronesyseguridad.com
Incibe	3ª Cub.	987877189	www.incibe.es
Iptecno	81	902502035	www.iptecnó.com
Kaba	79	917362474	www.kaba.es
Mobotix	26, 38	911115824	www.mobotix.com
Morse Watchmans	11	1159671567	www.morsewatchmans.com
Porteralia	44	934358426	www.porteralia.com
Prosegur	102	902202999	www.prosegur.es
Risco Group	41	914902133	www.riscogroup.es
Rivisa	37	938437834	www.rivisa.com
RMD	37	902194814	www.gruporomade.com
Saborit International	91	913831920	www.saborit.com
Samsung	105	916517507	www.samsungsecurity.co.uk
Securitas Direct	36,39	902221199	www.securitasdirect.es
Security Forum	9	914768000	www.securityforum.es
Seguridad Integral Canaria	85	902226047	www.seguridadintegralcanaria.com
Setelsa	61	942544354	www.setelsa.net
Sicur	87	902221515	www.sicur.ifema.es
SKL	101	943711952	www.skl.es
Synology	105	886225521814	www.synology
Talleres Aga	103	943790922	www.aga.es
TDI	103	967616116	www.cctvtdi.com
Tecnoalarm	30-31	936622417	www.tecnoalarm.es
Tecosa	65	915147500	www.tecosa.es
Tyco Integrated Fire & Security	42, 50	916313999	www.tyco.es
Vanderbilt	19	911799770	www.vanderbiltindustries.com
Visiotech	75	911883611	www.visiotech.es
Vivotek	105	886282455282	www.vivotek.com
WD	63	33170744627	www.wdc.com

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



ÍNDICE DE ANUNCIANTES

Alai Secure	67
Bosch Security Systems	71
Casesa	4ª Cubierta
Dahua	2ª Cubierta
Dorlet	59
ESV	56
FF Videosistemas-Geutebrück	25
Freemática	89
Gruser 4	51
Hikvision	13,15,17
I Jornada RPAS y Seguridad Privada	83
Iptecno	81
Incibe	3ª Cubierta
Kaba	79
Morse Watchmans	11
Risco Group	41
Rivisa	37
RMD	37
Saborit International	91
Securitas Direct	39
Security Forum	9
Seguridad Integral Canaria	85
Setelsa	61
Sicur	87
Tecnoalarm	30-31
Tecosa	65
Vanderbilt	19
Visiotech	75
WD	63

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

Security Forum 2016, cada vez más cerca

A cinco meses de la celebración, las empresas empiezan a reservar sus espacios en el área expositiva

A cinco meses de su celebración, Security Forum 2016 empieza a tomar forma. Por un lado, las empresas del sector de la Seguridad comienzan a reservar sus espacios en el área expositiva, lo que augura los mejores resultados en lo que a número de expositores y visitantes se refiere. Además, el Congreso Security Forum 2016, se desglosará en dos sesiones diferenciadas: Global Day y Cyber Day.

BAJO el lema «Ver para Crear», Security Forum volverá a convertirse en un evento ágil, flexible y orientado a la creatividad, que responderá una edición más al espíritu emprendedor y audaz que caracteriza a las empresas y profesionales del sector de la Seguridad. Esa es la prioridad de la organización que ya prepara contenidos renovados que se adapten a las inquietudes y demandas de los profesionales de la seguridad.

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 convertirá en plataforma de conocimiento para analizar los cambios y gestionar ideas para convertirlas en oportunidades.

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

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

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. ●





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

 **Peldaño**

ANDRÉS PÉREZ VEGA. DIRECTOR DE SEGURIDAD. MUSEO THYSSEN-BORNEMISZA.



MIENTRAS no se conciba la seguridad como una inversión y se considere siempre como “un gasto” los recursos serán siempre insuficientes», son palabras de Andrés Pérez Vega, director de Seguridad del Museo Thyssen-Bornemisza, quien en esta entrevista explica el día a día, entre otros aspectos, de un responsable de Seguridad de una instalación museística.

—¿Cuáles cree que son los pilares sobre los que tiene que asentarse la colaboración entre Seguridad Pública y Privada en la Protección del Patrimonio Histórico?

—En general y sin perjuicio de seguir fielmente la normativa vigente en materia de Seguridad Privada, «la Seguridad Privada tiene la consideración de complementaria y subordinada respecto de la Seguridad Pública», creo que los pilares básicos, primero, han de cimentarse, en esa legalidad; siendo éstos, una fluida y buena comunicación bidireccional en general con herramientas apropiadas (planes de colaboración con Seguridad Privada, comunicación operativa, protocolo de cooperación del Programa COOPERA, RED AZUL, etc.), y una amplia colaboración entre los actores principales, la Administración del Estado y la Seguri-

«En el museo desarrollamos una labor eminentemente preventiva y disuasoria»

dad Privada, a lo que hay que sumar el sentido común y la buena voluntad, teniendo en cuenta el devenir de los acontecimientos.

Por una parte, la responsabilidad de todo lo referente a bienes del Patrimonio Histórico es del Ministerio de Cultura y de las CCAA, así lo establece su Ley 16/1985 (PHE), que emana del art. 46 de la CE. Por otra, la CE atribuye al Estado (Art. 149.1.29) la competencia en materia de Seguridad Pública, sin perjuicio de las competencias de las CCAA, que la ejerce a través de las FCSE (Art.104.1); la competencia de la Seguridad Privada, según la Ley 2/86 de FCSE y la nueva Ley de Seguridad Privada, corresponde al CNP-UCSP.

En nuestro caso la colaboración con Seguridad Privada y Ministerio de Cultura es muy buena, en general, la operativa cotidiana nos lleva a estar en contacto permanente (transportes de obras, contratos y de seguridad, (V.S. y sistemas) y CRA de Uso Propio.

En el museo, siempre se da mucha importancia a la información que nos llega de las FCS, y a la que proporcionamos a éstas.

—¿Qué aspectos debería contemplar un sistema de gestión de seguridad implantado en un centro museístico como es el caso del Museo Thyssen-Bornemisza?

—En el Museo Thyssen-Bornemisza, conseguir un positivo equilibrio entre la seguridad de las obras de arte e instalaciones y la libertad de los visitantes para que puedan contemplar tranquilamente las obras en él expuestas; es a primera vista un espacio abierto sin obstáculos, que impacten en el visitante, todo ello, sin perjuicio del conjunto de sistemas de seguridad, poco visibles, pero muy eficaces. La ubicación de la colección, en el «Palacio de Villahermosa» es también de gran importancia, desde el punto de vista de la seguridad; en una de las mejores zonas de



Madrid, eje Prado-Recoletos y próximo a las otras dos grandes pinacotecas (El Prado y Reina Sofía), la seguridad del entorno próximo es inmejorable.

Siempre se ha optado por las mejores condiciones de conservación y seguridad, en su conjunto, ya que los bienes a custodiar son obras de arte, de ahí que la seguridad integral (seguridad propiamente dicha, PCI y autoprotección), se base en los últimos adelantos de la técnica, intentando ir por delante de la delincuencia organizada.

Todo enmarcado en el mantenimiento continuo (preventivo y corrector), bajo dos premisas fundamentales e ineludibles, que se hagan en las formas, plazos y por empresas debidamente autorizadas.

—**A grandes rasgos, ¿cuál es el día a día de un responsable de Seguridad de una instalación museística?**



—Aunque cada día puede ser muy diferente, a grosso modo, en un museo de estas características la dedicación es

absoluta, 24 horas todos los días del año, con una labor eminentemente preventiva y disuasoria, lo que nos da



La puerta del producto no se muestra en la imagen
Lector de huellas digitales opcional

Tenemos el **toque**

Guarde, administre y controle llaves, tarjetas y pequeños activos con mayor seguridad y eficiencia usando KeyWatcher® Touch. El acceso está limitado a los usuarios autorizados, y todas las transacciones se registran con disponibilidad de reportes detallados. El sistema incluso enviará automáticamente la información sobre transacciones a cualquier usuario, en cualquier momento. Y la práctica pantalla táctil de KeyWatcher hace más fácil que nunca retirar y devolver las llaves. Con nuestro diseño modular y escalabilidad completa, es fácil ver cómo seguimos mejorando la gestión de llaves. Así es como Morse Watchman se sale del marco —justo dentro de la caja.

piense dentro de la caja.

**MORSE
WATCHMANS**

resultados satisfactorios en nuestras instalaciones; no haberse producido nunca, ni un intento de intrusión, eso conlleva el estar pendiente minuto a minuto de:

—Los sistemas de seguridad contra actos antisociales, que como se puede imaginar el lector, son muchos: CCTV, todo tipo de sensores, de presencia, sísmicos, de apertura de puertas, controles de acceso, protección individualizada de obras, contadores de personas, IR, etc., cada uno con sus funciones específicas y las odiadas averías, a todo esto hay que sumar nuestra Central Receptora de Uso Propio (CRAUP).

—Servicio de vigilancia y protección de personas y bienes, llevado a cabo por los vigilantes.

—Los sistemas de Protección Contra Incendios (PCI), detección y extinción automática de incendios.

—La Autoprotección y la implantación de su plan.

—La formación continua tanto del personal propio como de los vigilantes de seguridad y auxiliares de sala.

Los visitantes del museo (1.000.000 de media al año), de su comportamiento en sala y de sus actitudes, de la que podemos filtrar, a veces, algunas anomalías.

Y, cómo no, el departamento de Seguridad registrado en la UCSP, tanto el director de Seguridad como sus delegados, que son en definitiva el combustible del motor de la seguridad.

—El patrimonio de nuestro país es uno de los grandes atractivos turísticos, ¿cree que se destinan suficientes recursos por parte del Estado para garantizar su protección y salvaguarda?

—Rotundamente, no.

Permítanme antes un comentario de un gran amigo, que sabe algo de esto, «la seguridad es cara, incómoda e incor-



dia», si falta algo, ya no es seguridad, es otra cosa.

Pues bien, mientras no se conciba la seguridad como una inversión y se considere siempre como «un gasto» los recursos serán siempre insuficientes. Sinceramente creo que no hay la suficiente concienciación ni se tiene en cuenta por las Administraciones del Estado el tema de la seguridad y protección del Patrimonio Histórico, ello origina que estos «gastos» sean relegados a los últimos lugares.

Tampoco se tienen en cuenta los ingresos que se generan por el turismo, en nuestro caso de Madrid y los empleos activos relacionados.

—¿Ha llevado a cabo en los últimos años una mejora o ampliación de los medios y servicios de seguridad con que cuenta el Museo Thyssen-Bornemisza?

—Como apunté, siempre se ha optado por los mejores y más modernos medios, tanto en seguridad contra actos antisociales como en seguridad contra incendios.

Concretamente se ha hecho un esfuerzo enorme, en estos últimos años de crisis, donde destaco el amaestramiento electrónico, protección individualizada de obras de arte, la propia CRAUP; pero la joya de estas amplia-

ciones y mejoras se lo lleva la Protección Contra Incendios, en la que se han actualizado y modernizado los sistemas de detección y extinción automática y centrales de incendio que teníamos desde hace 20 años, incluidas todas las compuertas cortafuegos del sistema de climatización, se han sustituido los antiguos paneles y central de incendios, ahora, todo está supervisado y controlado mediante un ordenador central (programa MM8000) y monitor con pantallas activas, que nos hace observar a vista de pájaro todo en conjunto que, dicho sea de paso, permite un segundo control remoto por un ingeniero.

—¿Qué papel ha jugado la tecnología a la hora de implantar los sistemas de seguridad en el museo?

—Bastante; pero téngase en cuenta que ésta también llega a la delincuencia organizada, por ello debemos tomar conciencia los que estamos en este mundillo, de que tenemos que caminar siempre por delante a los que pretenden extorsionar el Patrimonio Histórico, ya que éste es irreparable e irremplazable si se produce un daño. ●

TEXTO: Gemma G. Juanes.

FOTOS: Museo Thyssen-Bornemisza

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!**



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

España



www.es-eshop.adiglobal.com

Distribuidores Oficiales



www.casmar.es



www.hommaxistemas.com

Portugal



Bernardo da Costa

www.bernardodacosta.pt

JUAN JOSÉ PINTADO GARCÍA. JEFE DEL DEPARTAMENTO DE SEGURIDAD. MUSEO NACIONAL DE ARTE DE CATALUNYA

«La tecnología juega un papel esencial a la hora de implantar sistemas de seguridad en el museo»



LOS pilares sobre los que se debe asentar la colaboración entre Seguridad Pública y Privada son la información puntual y rápida, la eficacia, la confianza y, no cabe duda, la implicación en la protección de un bien universal como lo es el Patrimonio Histórico», explica Juan José Pintado García, jefe del departamento de Seguridad del Museo Nacional de Arte de Catalunya, quien además analiza en esta entrevista el papel que la tecnología juega a la hora de implantar sistemas de seguridad en la instalación museística.

—**¿Cuáles cree que son los pilares sobre los que tiene que asentarse la colaboración entre Seguridad Pública y Privada en la Protección del Patrimonio Histórico?**

—Los pilares sobre los que se debe asentar esta colaboración son la información puntual y rápida, la eficacia, la confianza y, no cabe duda, que la implicación en la protección de un bien universal como lo es el Patrimonio Histórico. Posiblemente es en este país donde más sensibilización, bajo mi punto de vista, existe sobre este punto. Ejemplo de ello es el intercambio de información, protección y custodia en los traslados y, cómo no, la continua consulta a través de Protecturi sobre las necesidades para dotar de más calidad en la seguridad del patrimonio por parte de los Ministerios de Cultura e Interior. De hecho ya se han trasladado varias sugerencias sobre la seguridad en el Patrimonio Histórico de cara a la formación policial en las

academias de las Fuerzas y Cuerpos de Seguridad.

—**¿Qué aspectos debería contemplar un sistema de gestión de seguridad implantado en un centro museístico como es el caso del Museo Nacional de Arte de Catalunya?**

—Dirección, organización y administración de la seguridad en el ámbito de la protección de personas, bienes y de la información.

-Estudio y valoración de las necesidades de los diferentes departamentos del museo y establecimiento de prioridades.

-Seguimiento y control de cualquier actividad museística, ya sea educativa y de ocio, para dotarla de la seguridad necesaria.

-Organización y coordinación de los equipos de vigilancia y control de salas.

-Formación del personal que trabaja en referencia a la seguridad del museo.

-Prevención, protección e investigación.

-Seguimiento de la gestión de las empresas de seguridad contratadas (vigilancia e instalaciones).

-Coordinación de las medidas de seguridad y salud laboral.

Todos estos aspectos se definen adoptando los criterios y la información facilitada por la Dirección del museo, dentro del marco de actuación del departamento y según los objetivos encargados, teniendo siempre muy

HIKVISION



Smart

COVERT

C A M E R A

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

España

Distribuidores Oficiales

Portugal



GLOBAL DISTRIBUTION
www.es-eshop.adiglobal.com



SISTEMAS DE SEGURIDAD
www.casmar.es



www.hommaxistemas.com



Bernardo da Costa

www.bernardodacosta.pt

presentes tres conceptos definidos como básicos, como son: Patrimonio, Territorio e Internacionalidad.

—A grandes rasgos, ¿cuál es el día a día de un responsable de Seguridad de una instalación museística?

—La verdad es que creo que no debe de diferir mucho del día a día de un responsable que ejerza con la misma responsabilidad en otro sector que no sea el museístico. Posiblemente hay una especialización en el tratamiento del bien que se protege (Obras de Arte), debido a factores tan importantes como la conservación preventiva, almacenamiento, transporte interno y externo, control y aplicación de diseños específicos de seguridad en las exposiciones temporales y permanentes, seguimiento de



los mantenimientos establecidos en los planes de autoprotección y su aplicación en las áreas de nueva creación, y sobre todo análisis de la viabilidad en seguridad de cualquier objeto que se expone.

La gestión en el departamento también la tenemos incrementada debido a la utilización de espacios para celebración de eventos, tanto institucionales como privados, los cuales requieren de la configuración de dispositivos de seguridad específicos, dependiendo de la complejidad del acto. Creo que cada responsable de seguridad de una instalación, sea o no museística, deja siempre plasmada su personalidad a la hora de dotarla de un criterio de seguridad. Para mí, siempre que éste sea ético y eficaz, dentro de las normas estipuladas, me parecerá acertado.

«Cada responsable de Seguridad de una instalación deja plasmada su personalidad a la hora de dotarla de un criterio de seguridad»



—El patrimonio de nuestro país es uno de los grandes atractivos turísticos, ¿cree que se destinan suficientes recursos por parte del Estado para garantizar su protección y salvaguarda?

—Como instituciones activas, implicadas en la sociedad, que aspiran a la excelencia, los museos cumplen un papel central en la cultura y son espacios para la reflexión y el conocimiento, necesitan reconocimiento y un apoyo decidido de las administraciones. No cabe duda que, debido a la crisis económica en la cual seguimos aún inmersos y que parece ser, según los economistas más optimistas, se está

HIKVISION

 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

España

Distribuidores Oficiales

Portugal



www.es-eshop.adiglobal.com



www.casmar.es



www.hommaxistemas.com



Bernardo da Costa

www.bernardodacosta.pt

saliendo, las partidas destinadas a los museos y espacios culturales a través de las Consejerías de Cultura han sido reducidas, y actualmente estamos muy por debajo de los presupuestos que se destinaban hace 5 o 6 años atrás. En cambio sube de manera progresiva cada año el turismo, siendo una de las principales atracciones culturales los museos y espacios culturales, aparte de nuestro clima y playas. Posiblemente, sí debieran tener en cuenta este factor las autoridades del Estado a la hora de incrementar recursos para garantizar su protección y salvaguardia, sobre todo, si queremos mantener en condiciones el patrimonio.

—¿Ha llevado a cabo en los últimos años una mejora o ampliación de los medios y servicios de seguridad con que cuenta el Museo?

—En línea con la respuesta dada anteriormente sobre los recortes presupuestarios por parte de las administraciones públicas, se hace difícil emplear partidas destinadas a la inversión, éstas normalmente se emplean para el pago de servicios ordinarios y extraordinarios de vigilancia, mantenimientos de instalaciones, etc. No obstante, en nuestro departamento, no hemos dejado de lado la investigación (I+D), y en algún



caso ha habido por parte de la dirección del museo un esfuerzo importante para los tiempos que corren, aprovechando alguna partida económica y las ofertas de mejoras que se ofrecen en los concursos públicos de licitación, de esta manera mejoramos aspectos tan importantes como el control de aforo general, de salas y la renovación del subsistema de CCTV. También está en curso la adaptación e integración del sistema de detección de incendios a las necesidades actuales. El hecho de no disponer de recursos para inversión, no significa que el departamento deje apartado el estudio de nuevas ideas tecnológicas que se están implantando para la mejora de la calidad técnica en los sistemas electrónicos de vigilancia. La formación es otro de nuestros pun-

tos en los que incidimos mucho sobre todo en la operativa diaria de vigilancia humana.

—¿Qué papel ha jugado la tecnología a la hora de implantar los sistemas de seguridad en el museo?

—Un papel básico, no cabe la menor duda, e incluso diría que esencial para determinadas incidencias que se dan diariamente. El museo se basa en un modelo integral de seguridad para el control de cualquier incidencia. La seguridad electrónica (activa y pasiva) a través de los sistemas de intrusión, control de accesos, CCTV, aforo, etc. nos dan la señal de alarma centralizada a través de un gestor en el centro de control de vigilancia, donde operan vigilantes de seguridad, para su análisis y posterior comunicación al resto del personal de vigilancia del edificio. No tendría razón de ser un sistema de seguridad electrónico si no hubiera una respuesta humana a la alarma, se trata de dar el equilibrio al sistema con un equipo de vigilancia formado en todos los aspectos necesarios para la protección. Estos elementos, que conforman el modelo integral de seguridad, hacen posible que bajen las incidencias y se logre en todo el espacio a proteger un clima de seguridad preventiva, que de momento nos está dando sus frutos. ●

TEXTO: Gemma G. Juanes.

FOTOS: MNAC



Acuda al mejor equipo de seguridad

VANDERBILT

Un nuevo nivel de protección

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

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

INTRUSIÓN | CONTROL DE ACCESOS | CCTV



www.vanderbiltindustries.com

JESÚS ALCANTARILLA DÍAZ. PRESIDENTE DE PROTECTURI



Más de 15 años de itinerario en la protección del Patrimonio Cultural

La idea de este artículo es mostrar, a través de mi experiencia profesional, una visión transparente a todos los profesionales que se dedican o quieren dedicarse a la protección del Patrimonio Cultural desde el ámbito de la seguridad.

El Patrimonio Cultural interesa y enriquece a innumerables personas de cualquier parte del mundo. El arte y la cultura son palancas que mueven las identidades de los pueblos y el ritmo cardíaco de la sociedad; realizando un papel esencial en la labor de «liderazgo», en la convivencia, en el pensamiento, en la investigación, en la comunicación de ideas, etc.

Para hacerlo de una manera ágil y sencilla, he optado por articular la idea a través de una metáfora que nos conducirá a un somero análisis de lo que he vivido en más de 15 años de dedicación a la protección/seguridad del Patrimonio Cultural.

Antes de entrar en la metáfora permitidme recoger dos voces del diccionario que, bajo mi criterio, son conceptos esenciales: Protección y Seguridad.

Protección: Del lat. *protectio*, -onis. Acción y efecto de proteger.

Seguridad: Del lat. *securitas*, *atis*. Cualidad de seguro. Certeza. Conocimiento seguro y claro de algo.

La metáfora que he elegido, y que creo que mejor representa mi deambular profesional, es «Un Puente».

Según el Diccionario de la Real Academia Española, un puente es, entre otras acepciones, «una construcción de piedra, ladrillo, madera, hormigón, etc., que se construye y forma sobre los ríos, los fosos y otros sitios, para poder pasarlos».

De esto escribiré a continuación. De cómo «diferentes materiales», léase procedencias, enfoques, formación, criterios, pueden confluír en un objetivo común: la construcción de un espacio de entendimiento, el puente. O dicho en jerga profesional: Cómo generar un espacio que haga viable la labor de la prevención, la protección y la salvaguarda del Patrimonio Cultural.

Dos orillas, la museológica y la de la seguridad. En medio, el cauce de la cultura.

En ese escenario, hace más de 15 años, se me abrió un reto del que desconocía la mayoría de las coyunturas a las que me debería enfrentar. Desde la orilla de la seguridad pública, el horizonte estaba plagado de interrogantes.

Aprendí que las orillas sólo tienen sentidos si existe un «cauce con caudal».

Sin el caudal –el Patrimonio Cultural– las orillas se confunden y no dejan de ser un páramo. Viendo de cerca la riqueza del «caudal», supe que no podía obviar la otra orilla, la de los profesionales de los





equipamientos culturales que desconocían el papel de los profesionales que nos dedicamos a la protección/seguridad. En ese contexto, era del todo necesario establecer un puente de comunicación para consolidar nuestra complementariedad en pos del Patrimonio Cultural.

Ese sería mi principal propósito. Conseguir la complicidad de todos aquellos que trabajábamos con el mismo fin, desde diferentes ámbitos.

Mi principal objetivo, que en aquel momento desconocía, ha sido fundamentar dos enfoques claves en nuestro sector:

- La cultura de la seguridad, entendida como una mirada o perspectiva articulada en procesos específicos que den respuestas viables a las necesidades reales de la cultura.



- La seguridad en la cultura, entendida como especialidad que sea partícipe y desarrolle los recursos idóneos para intervenir adecuadamente en cada caso, en función de los indicadores de relevancia de los entornos culturales.

Estos más de 15 años me han servido para entender la necesidad de:

- Conocer las singularidades y necesidades de las organizaciones culturales.
- Reflexionar antes de actuar.
- Aprender el valor de la contextualización. No existe el café para todos.
- Escuchar las voces de los diferentes actores de un equipamiento museístico.
- Asumir la misión, mandato, metas y objetivos organizativos y declaración de propósitos.
- Ampliar la mirada para contribuir positivamente en un entorno de alta complejidad.

medidas. Teniendo en cuenta que los componentes básicos de la protección/seguridad del Patrimonio Cultural son: el valor, el protector, la amenaza.

- Analizar la criticalidad de la interrelación entre personas, espacios y bienes.
- Elaborar códigos de comunicación en los que prevalezca la serenidad, la fluidez y el respeto.
- Promover la formación especializada como un factor clave de desarrollo profesional, permanentemente actualizable.
- Desplegar el mapa de riesgos, amenazas y vulnerabilidades ad hoc de cada organización.

Y por último, y no el menos importante, destacar el valor primordial del «factor humano». Ésta es la clave de un buen desarrollo profesional y organizativo. Al menos hasta que no seamos

«El arte y la cultura son palancas que mueven las identidades de los pueblos y el ritmo cardiaco de la sociedad»

- Descubrir esa complejidad que nos guía a generar una especialización profesional que tenga en cuenta factores que en otros entornos no se plantean.

- Ayudar al cumplimiento de lo exigido por la ley en los principios de actuación, y en lo referido a tipos de medidas de seguridad y a sus contra-

sustituídos por la ingeniería robótica. Mientras, disfrutemos de cada una de las oportunidades de aprendizaje y colaboración que nos ofrece nuestro trabajo en la protección/seguridad del Patrimonio Cultural.●

Fotos: Archivo

ANTONIO GÓMEZ MONTOLÍO. SOCIO FUNDADOR DE ADSI



El robo de arte

¿Son seguros los museos?

Sobre la pila bautismal no estaba una talla en madera, representando a San Juan Bautista. El sacerdote y algunos vecinos me informaron que la talla había sido sustraída hacía tiempo. Experimenté un sentimiento instantáneo de tristeza por haber perdido algo que sin serlo lo consideraba mío, nuestro, de todos, e indignación por la usurpación del patrimonio de un pequeño pueblo.

Se activó mi ADN de director de Seguridad y pensé qué medidas de seguridad podían haberse previsto antes del robo, quizás una combinación de seguridad física y electrónica, pero la talla estaba tan cerca de la puerta, que difícilmente se pudiera proteger bien. Esa pieza solo podía haberse salvado del expolio si se hubiese situado en un museo a tiempo.

Miles de obras de arte han sido sustraídas de iglesias en España y otros países de nuestro entorno, por ejemplo, en

Italia se estima que unas 500.000 obras de arte se han sustraído de su patrimonio en los últimos 40 años.

¿Estamos seguros que las piezas de los museos están seguras?

Tengo experiencia en la seguridad de museos y tengo buenos amigos al frente de la seguridad de muchos de ellos, y no estoy muy seguro de la respuesta que podrían darnos.

Como aficionado al arte y como profesional de la seguridad, he visitado muchos museos en múltiples países, conozco las intimidades de muchos de ellos y puedo asegurar que todos tienen un denominador común, las limitaciones económicas en las inversiones de seguridad.

Los responsables de la seguridad de los principales museos de París se quejaban hace unos años en varias reuniones de las mismas limitaciones económicas que mis amigos de los museos españoles, estoy hablando de antes de la crisis. Las inversiones en los museos se orientan al marketing, a los eventos, a comerciar con la marca y el prestigio de los museos para capturar fondos, subvenciones, y más visitantes.

Qué ocurrirá, cuando por las limitaciones impuestas en la actualización y modernización de los sistemas de seguridad faciliten la acción delictiva; cuál será el papel que adoptarán los directores generales de los museos, cuando se produzca un robo importante.

HAY un pueblo llamado Bonastre (Tarragona) con el que mantengo lazos afectivos desde mi adolescencia. Visitando su iglesia, me interesé por las obras del arquitecto Josep Maria Jujol, mano derecha de Gaudí, que durante sus estancias veraniegas en ese pueblo, del que era natural su madre, se dedicó de forma altruista a diseñar y crear cosas tan simples como unas lámparas y cosas tan importantes como la pila bautismal y el sagrario. Para este último utilizó una máquina de sulfatar en desuso, demostrando que se puede hacer arte, con cualquier cosa y con mucho talento.



Dónde irá a parar el prestigio, la imagen, los eventos, etc., cuando un museo sea robado.

Evidentemente los mayores robos de arte se producen como botín de guerra, siendo los más famosos de la

historia reciente, los capitaneados por Napoleón o Hitler. Se estima que los nazis robaron más de 750.000 obras de arte. Hay que matizar que gran parte de las obras fueron compradas bajo amenazas a precios irrisorios.



Los robos en museos, son algo que dispara la imaginación, estoy convencido que si hacemos una encuesta, el ladrón de arte es el mejor valorado por la sociedad, supongo que el cine le ha dotado de un cierto glamour. Podríamos decir que está bien visto, ser un ladrón de arte.

La historia nos ilustra con robos audaces como el de la Mona Lisa en el museo del Louvre realizado por un empleado llamado Vincenzo Peruggia el 21 de agosto de 1911. La policía francesa tardó casi dos años y medio en recuperar la obra, con diversos sospechosos detenidos como el propio Pablo Picasso (que tenía antecedentes por compra de obras de arte robadas), entre otros.

El móvil fue patriótico, Vincenzo creía que la obra más famosa de Leonardo había sido robada de Italia por Napoleón. En realidad, la Gioconda acompañó siempre a Leonardo, hasta

SI NO TIENES MÁS ESPACIO

Toda la actualidad del sector en la palma de tu mano

Síguenos también en  



App oficial

**CUADERNOS DE
SEGURIDAD**

¡Descárgatela ya
en tu móvil!

Disponible para:





su muerte, acogido en Francia por el rey Francisco I, como su pintor de corte; podemos decir que Leonardo regaló la obra al rey que le acogió en sus últimos días. Se calcula que Leonardo invirtió unos 16 años en pintar la Gioconda.

Quizás uno de los más grandes robos se produjo en el museo Isabella Stewart Gardner de Boston, Estados Unidos, en 1990. Fue el día de San Patricio y la celebración fue utilizada como «distracción». La operativa fue extremadamente sencilla, a las 1:24 h de la noche dos ladrones vestidos de policías solicitan ayuda a uno de los vigilantes del museo (el otro vigilante está haciendo la ronda), abre la puerta lateral del museo, lo inmovilizan y esperan el regreso del segundo vigilante, que también es inmovilizado. La estimación del valor del robo es variada, hay fuentes que la cifran en 5.000 millones de euros y otras fuentes en 300 millones de dólares.

La tragedia fue enorme, se perdieron obras irremplazables, entre ellas 3 Rembrandt, 5 Degás, 1 Vermeer, 1 Manet, un total de 13 obras. Uno de los Rembrandt «Tormenta en el mar de Galilea» incluye su autorretrato en el único paisaje marino que pintó.

Pero sin duda el máximo valor económico y la mayor pérdida pictórica fue «el concierto» de Vermeer.

Otro robo relevante se produjo en el museo Ashmolean en Oxford, el 1 de enero de 2000, descolgándose desde una claraboya del tejado, el lanzó un bote de humo para activar los sistemas de detección de incendios, lo que accionó el bloqueo de todas las puertas de la sala, impidiendo a los vigilantes acceder a la sala afectada. El botín fue un Paul Cezanne en concreto «Auvers sur Oise» valorado en 4,8 millones de euros.

No me resisto a comentar uno de los mayores robos por su sencillez de ejecución, se produjo el 10 de febrero de 2008 en Zúrich, en la Fundación E.G. Bührle. Poco antes del cierre un hombre armado se hizo con 4 pinturas con un valor de 162.5 millones de dólares. El famoso cuadro del niño con chaleco rojo de Paul Cézanne, sigue perdido.

Diez piezas de arte famosas que fueron robadas por los nazis

Podríamos citar múltiples robos, pero los expertos creen que realmente el robo de obras tan conocidas tiene un

mercado muy limitado y todos nos inclinamos por el robo por encargo. Pero no faltan expertos que creen que realmente el robo por encargo es algo muy puntual, y que el motivo real de las obras es su uso como garantía entre delincuentes.

Al parecer una obra robada se puede utilizar como garantía inicial para adquirir una cantidad suficiente de drogas, que una vez colocadas en el mercado generan el suficiente metálico para retirar la obra como garantía. En términos empresariales podemos decir que la obra robada es en realidad el capital inicial, sin el cual no podría accederse al crédito suficiente para el inicio de la actividad.

Sobre los directores de Seguridad de museos

Los cambios normativos que de forma cíclica se producen en España no acaban de afrontar la figura del director de Seguridad. A mi juicio, cuando una determinada actividad tiene la suficiente relevancia o nivel de riesgo, la normativa debería obligar a disponer de un director de Seguridad.

Por ejemplo si un hospital tiene más de x camas, si un museo tiene más de 500 m cuadrados o obras por valor de x, si una empresa tiene más de 50 empleados. En algunos casos no es necesario que la contratación del director de Seguridad sea a jornada completa, puede ser parcial. En otros países la presión sobre la seguridad no la ejerce el Estado, la ejercen las compañías de seguros, que son las que deberán asumir las pérdidas si se produce un acto delictivo.

Quizás los directores de Seguridad europeos nos falta la visión y el conocimiento que en los países anglosajones se tiene del Risk Management. ●

LO ÚLTIMO EN TECNOLOGÍA DE SEGURIDAD



G-Scope 1500 Series
Servidor Compacto



G-Scope 3000 Series
Servidor Profesional



G-Scope 6000 Series
Servidor Avanzado

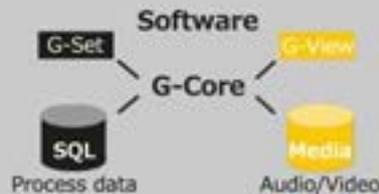


G-Scope 8000 Series
Servidor Experto

NUEVA GENERACIÓN DE SERVIDORES



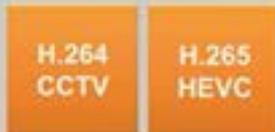
Motor G-CORE 64bit
Máxima potencia
Máximo rendimiento



Arquitectura dual de base de datos
Accesibilidad instantánea
a imágenes y metadatos



Asistente de configuración
Parametrización sencilla e intuitiva



**Compatibilidad con nuevos formatos
de compresión**
Preparado para el futuro



HTML5: acceso remoto flexible
a través de navegadores web y dispositivos móviles



Aceleración GPU
Gran potencia de procesamiento
de imágenes

ALFREDO GUTIÉRREZ. BUSINESS DEVELOPMENT MANAGER IBERIA. MOBOTIX AG



Videovigilancia y mucho más en museos

Ventaja de las cámaras de red por su calidad

Un sistema de seguridad se puede implementar a la perfección con cámaras de red. En cuanto a calidad de imagen, hardware y software, esta tecnología de vídeo digital es muy superior a la de CCTV de videovigilancia analógica.

Una imagen en vivo obtenida con la antigua tecnología analógica no tiene más de 0,4 megapíxeles, y una imagen grabada tiene generalmente 0,1 megapíxeles. Una cámara de red de por ejemplo 6 megapíxeles guarda 60 veces más detalles, lo cual permite captar imágenes con mayor campo de visión (incluso vistas panorámicas de 360°), reduciéndose así el número de cámaras y, con ello, los costes.

LOS museos son lugares que siempre han necesitado especial atención en cuanto al tema de la seguridad. Todos hemos visto como incluso en cada sala, aunque dependiendo del museo, había personal de vigilancia que no perdía ojo mientras disfrutábamos de las obras a cierta distancia para no ser regañados.

Ha pasado tiempo desde entonces, no es que ahora no haya personal de seguridad, que lo sigue habiendo, pero es cierto que la revolución de las cámaras IP caló muy pronto en este sector.

Una sola cámara por sala

Y es que la evolución de la tecnología se ha ido notando poco a poco en los museos, ya que con ciertas cámaras se podía registrar poco espacio, no todo lo que había en una sala, ni tampoco se podían reconocer las caras.

Y ahora, gracias a la tecnología alemana con su altísima resolución de imagen, que puede llegar hasta 6 megapíxeles, se puede reconocer todo, con y sin luz. Y además no se necesita más que una cámara por sala para cubrir absolutamente todo. Esto es debido a la tecnología panorámica 360° que consiguen sólo algunos modelos de cámaras.

Grabación por eventos

Esto ya se empezó a hacer hace un tiempo, para registrar solo los cambios que se percibieran y no desperdiciar espacio ni banda ancha. Pero ahora bien, la grabación por eventos saltaba en la mayoría de las ocasiones cuando no debía hacerlo, por ejemplo, si había viento. Hasta que no ha llegado la tecnología que hace posible distinguir entre falsas alertas. Esto fue una auténtica revolución para la videovigilancia para todos los sectores.

Más funciones

Antes un teléfono era un teléfono, hoy en día es una agenda, un calendario, periódico, alarma, una cámara de





fotos, de vídeos, y un largo etc., que todos conocemos. Pues con las cámaras IP de videovigilancia pasa un poco lo mismo: es mucho más que una cámara.

Ya desde hace mucho se han ido utilizando para otro tipo de activida-

des además de la videovigilancia, pero es que con el tiempo, cada vez más, las propias funcionalidades que te da la cámara son muchas y variadas. En museos tenemos casos de éxito en los que las cámaras están siendo utilizadas para

«La evolución tecnológica se ha ido notando poco a poco en los museos»



el conteo de personas, al igual que en el sector retail, e incluso para hacer estudios del comportamiento de las personas ante una exposición itinerante, o ante las diferentes salas, e incluso, el comportamiento en cada obra.

Esto es así gracias a un software integrado en la cámara que va haciendo mapas de calor según el tiempo en cada lugar de una sala, e incluso marca el recorrido de cada persona. Así en ese museo se puede utilizar una misma cámara para videovigilar y para todo esto, que es una información super útil para los museos, solo con una cámara.

Aparte, por supuesto están los usos domésticos como puede ser el caso de otro museo, situado en Salamanca, que utiliza la cámara para avisar al personal de la hora de cierre.

Eficacia total

El motivo principal de esta tendencia hacia la videovigilancia IP es que está demostrando una eficacia total, siempre y cuando el sistema implantado esté realmente bien planteado. Con esto quiero decir que no vale con instalar una cámara y listo, hay un planteamiento previo, un estudio de la situación y del lugar, que es fundamental a la hora de tener cubiertas todas las necesidades de protección requeridas.

Desde el punto de vista jurídico, no hay ningún problema siempre que se indique a los visitantes la existencia de cámaras de vídeo. Esto tiene a su vez un efecto intimidatorio, ya que nadie puede estimar el nivel de efectividad, el ángulo de visión y la calidad de imagen de las cámaras instaladas. Se trata de un instrumento eficaz de prevención que también resulta útil para investigar posibles delitos. ●

Fotos: Stockvault/Mobotix

DEPARTAMENTO PANOMERA® MULTIFOCAL SENSOR SYSTEMS. DALLMEIER

Tecnología de sensores multifocal vigila la Millenium Square

La plaza, situada en el centro de Bristol (Inglaterra), acoge magníficas esculturas e instalaciones de agua

LA Millennium Square es una popular plaza en el centro de Bristol, inmediata al At-Bristol Science Centre, un centro de ciencia interactivo. Para los visitantes del centro, la plaza, con sus fantásticas instalaciones de agua y esculturas, es un punto habitual de encuentro; una pantalla LED gigante, así como numerosos restaurantes y bares en las cercanías atraen a muchos visitantes cada año a la Millennium Square. Su ubicación junto al barrio portuario y una multitud de festivales que se celebran una y otra vez convierten la gran Millennium Square en un animado lugar en Bristol.

Por esa razón, el gobierno municipal de Bristol ha decidido aumentar la seguridad de la plaza pública e instalar un sistema de vídeo a la altura. Hasta ahora, sólo una única cámara PTZ, que formaba parte del sistema de CCTV del At-Bristol Science Centre, vigilaba la

plaza. «La sala de seguridad de @Bristol no tiene ventanas y el personal de seguridad utiliza el sistema de sensores multifocal a diario para disponer de una ventana virtual en vivo a la Millennium Square. Antes, la plaza era captada por una única cámara PTZ que, por lo general, trabajaba con un ajuste de gran angular para proporcionarnos una vista global de toda el área. El problema con esto fue que las imágenes grabadas tenían que manejarse con zoom digital cuando necesitábamos encontrar algún indicio, y llegaban a ser demasiado pixeladas como para servir como prueba», cuenta John Whittaker, Security Team Manager de At-Bristol.

Todo a la vista

De modo que, el mayor desafío consistió en encontrar una solución que suministrara una vista general

permanente de toda la plaza con la máxima resolución de detalle, pero siendo al mismo tiempo rentable y fácil de manejar. «La experiencia con la cámara PTZ ha mostrado que las grabaciones, en principio, pierden su valor para investigaciones posteriores debido a la falta de resolución. La alternativa sería varias cámaras HD distribuidas por la plaza, sin embargo, el manejo para el personal de seguridad sería muy complicado y los costes de infraestructura muy altos», señala John Whittaker explicando las consideraciones iniciales.

La solución la encontró finalmente el concejo municipal de Bristol en una conferencia del CCTV User Group, donde oyeron hablar de la tecnología de sensores multifocal del fabricante germano con sede en Ratisbona. Gracias al patentado concepto de sensores de esta nueva tecnología de cámara





ra era posible vigilar incluso grandes superficies desde un único punto de instalación, con máxima resolución y profundidad de campo continua. Y además se grababa toda la escena de manera permanente, al contrario que las cámaras PTZ que captaban sólo el área que se estaba contemplando en vivo. «La tecnología MFS nos ofrece lo mejor de ambos mundos, la perspectiva gran angular y la alta resolución de detalle, incluso en el punto más alejado», dice John Whittaker.

En colaboración con Select Electric, proveedor de CCTV, se eligió una ubicación adecuada para el sistema. Una única cámara de sensores multifocal con un ángulo de visión de 90° basta para vigilar toda la Millenium Square con máxima resolución.

Las imágenes de la cámara IP son grabadas con 12,5 ips en una appliance de vídeo del mismo fabricante. Una estación de trabajo en la sala de seguridad de At-Bristol permite tanto la vigilancia en vivo como investigaciones posteriores sobre las grabaciones. Una segunda estación de trabajo fue establecida en el centro de coordinación de emergencia de la ciudad y es usada ahí a diario por las fuerzas de seguridad para vigilar el área.

«Sabemos que ya no se nos escapa nada, porque podemos buscar incidencias en las grabaciones también a posteriori», señala entusiasmado John Whittaker. «El hecho de que toda la plaza sea grabada en todo momen-

«La tecnología MFS soporta el funcionamiento multiusuario, varios usuarios pueden ver simultáneamente las imágenes»

to con la máxima resolución de detalle, nos permite también perseguir a delincuentes que quizás en otras áreas ya hayan sido denunciados. La plaza es un cruce importante y de este modo podemos reconstruir de forma continuada el camino de los delincuentes, tanto adónde van, como de dónde vienen».

Manejo independiente del sistema

«Las imágenes del sistema MFS son visionadas y evaluadas tanto por los operadores de seguridad del centro de ciencia At-Bristol como por las fuer-

zas de seguridad del gobierno municipal; y completamente independientes los unos de los otros», explica Ray Murphy, Managing Director de Select Electric.

Al contrario de las cámaras PTZ, la tecnología MFS soporta el funcionamiento multiusuario, es decir, varios usuarios pueden simultáneamente ver las imágenes de la cámara y moverla o hacer zoom a voluntad, y esto tanto en las imágenes en vivo como, al mismo tiempo, en las grabaciones sin afectar a los otros usuarios.

Resultados excelentes

«En la Millenium Square se celebran muchos eventos durante todo el año que atraen a miles de visitantes. Hemos utilizado el sistema MFS para obtener pruebas en una serie de incidentes. Ya en las primeras semanas

tras su instalación se produjo un robo de un bolso y la policía dijo que era la mejor calidad de imagen que habían visto jamás en un sistema CCTV», dice John Whittaker.

«La tecnología de sensores multifocal es una solución única para cubrir la Millenium Square entera, lo que otro sistema no hubiera logrado nunca desde un solo punto de instalación», concluye John Whittaker de una forma positiva. «Estamos muy satisfechos e impresionados con la capacidad de rendimiento y el fácil manejo del sistema y ya no queremos renunciar a él.» ●

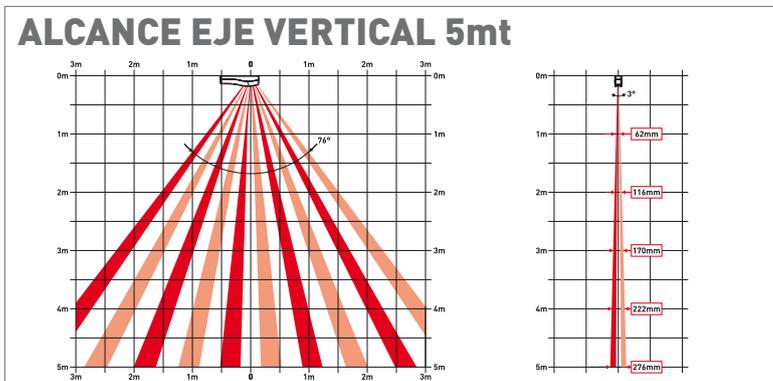
Fotos: Dallmeier

DUALRED BUS



Doble infrarrojo pasivo para la protección de puertas y ventanas

- Dos unidades de detección compuestas por un doble elemento infrarrojo pasivo y un contacto magnético
- Funcionamiento conjunto con lógica de detección AND/OR programable o como dos unidades independientes, identificadas por el sistema como dos zonas
- Auto-exclusión del contacto magnético en caso de apertura durante la fase de conexión con adaptación de la lógica de detección
- Funciones de compensación de la temperatura y autotest así como programación, gestión y control remotos de todos los parámetros de funcionamiento, como sensibilidad, alcance, contador de impulsos y antienmascaramiento, gracias a la tecnología RSC®
- También está disponible una versión convencional con salidas de relé



GLOBAL SPACE BUS



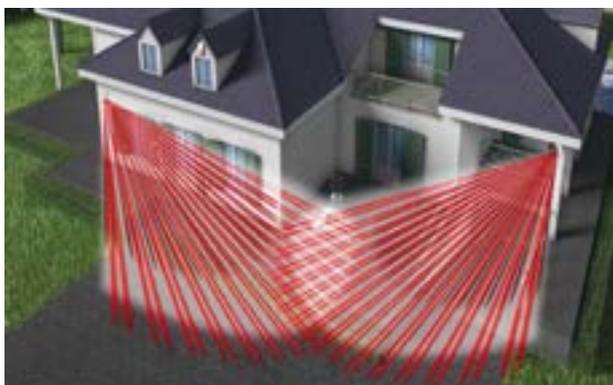
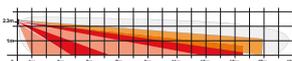
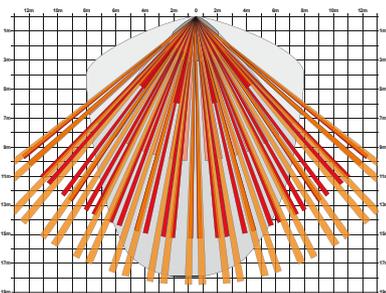
Detector volumétrico doble tecnología con triple infrarrojo y microondas para exterior



- Cuatro unidades de detección independientes, infrarrojos y microondas, que funcionan conjuntamente para individualizar y discriminar las alarmas
- Excelente cobertura del área protegida gracias a la alta densidad de zonas sensibles y a la particular protección multinivel
- Lógica de detección AND con dinámica programable, excepcional discriminación de las falsas alarmas, altísima inmunidad a las interferencias típicas de las áreas exteriores
- Funciones de compensación de la temperatura y autotest así como programación, gestión y control remotos de todos los parámetros de funcionamiento gracias a la tecnología RSC®
- También está disponible una versión convencional con salidas de relé



ALCANCE 15mt



Tecnoalarm

Via Ciriè, 38 - 10099
San Mauro T.se Torino (Italy)
tel. +390112235410
fax +390112735590
tecnoalarm@tecnoalarm.com
www.tecnoalarm.com

Tecnoalarm FRANCE

495, Rue Antoine Pinay
69740 Genas - Lyon (France)
tél. +33478406525 - fax +33478406746
tecnoalarm.france@tecnoalarm.com
www.tecnoalarm.com
Agence de Paris: 125, Rue Louis Roche
92230 Gennevilliers

Tecnoalarm ESPAÑA

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

INFORME PROTECTURI 2015

Los ingresos por el patrimonio cultural crecen un 13,4% durante la crisis

LOS ingresos económicos generados por el patrimonio cultural español aumentaron en un 13,4% entre 2009-13, hasta alcanzar los 39.254 millones de euros. Los datos figuran en el Informe Protecturi 2015 presentado en Madrid por los directivos de la Asociación Protecturi para la conservación y protección del patrimonio histórico y cultural español. Los responsables de Protecturi reivindicaron hoy el «carácter estratégico» del sector en España.

A pesar de que la inversión pública de las CC.AA. en conservación de patrimonio cultural se redujo en un

43%, durante la crisis económica creció en un 33% la declaración de nuevos Bienes de Interés Cultural (BIC).

Los resultados medidos en cifras de negocio fueron calificados de «espectaculares» por el presidente de Protecturi, Jesús Alcantarilla.

El gerente de la asociación sin ánimo de lucro, Fernando Prieto, explicó que los ingresos entre 2009-13 crecieron un 13,4%, hasta los 39.254 millones de euros. El empleo aumentó un 184%, con casi medio millón de personas contratadas, y el número de empresas se incrementó hasta un 241%.

Petróleo cultural

Andrés Martín, vicepresidente de Protecturi, destacó que España es el tercer país del mundo en bienes culturales catalogados (sólo por detrás de China y de Italia), con un total de 19.000 unidades. «Es nuestro petróleo cultural», señaló tras solicitar un esfuerzo de inversión y coordinación por parte de las instituciones culturales «a la altura de los resultados del sector».

Prevención, protección y salvaguarda

Por cada euro invertido en los cuatro años del periodo de estudio, el patrimonio histórico genera hasta 22 euros de retorno en ingresos, y la producción cultural española aportó en total un 5% del PIB nacional en el ejercicio de 2013.

Jesús Alcantarilla destacó la «incidencia del aumento de la protección de bienes en los ingresos, el empleo y la actividad empresarial» y afirmó que la gestión del patrimonio cultural «es un sector en sí mismo, muy rentable para invertir y estratégico para el país».

El presidente resumió los objetivos de Protecturi en la prevención, protección y salvaguarda del patrimonio histórico, y afirmó que se trata de «la única asociación europea transversal e inclusiva que se dedica a estos fines». ●

Jesús Alcantarilla, presidente; Andrés Martín Ludeña, vicepresidente; y Fernando Prieto, gerente, de Protecturi, durante la presentación del informe.



CUADERNOS DE SEGURIDAD

ESPECIAL Administradores de Fincas 2015

Soluciones y sistemas

**Nuevas tecnologías
para la seguridad
residencial**

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

MANUELA JULIA MARTÍNEZ TORRES.
PRESIDENTA DEL COLEGIO PROFESIONAL
DE ADMINISTRADORES DE FINCAS DE MADRID

«La seguridad, en la situación social actual, es un tema de interés en las Comunidades de Propietarios»



—El pasado mes de febrero tomó posesión como presidenta del Colegio Profesional de Administradores de Fincas de Madrid (CAFMadrid), ¿cuáles son sus objetivos prioritarios al frente de esta institución? ¿Cómo han sido estos primeros meses de su mandato?

— El objetivo principal es poner en valor nuestra profesión, así como posicionarla ante las Instituciones, trabajando de forma conjunta como los únicos profesionales capacitados para el ejercicio de nuestra actividad.

Estos primeros meses han sido intensos, centrados en la organización de la estructura interna y la proyección exterior de la profesión a través de los medios de comunicación.

—¿Cuáles son los principales retos del Colegio Profesional de Administradores de Fincas de Madrid (CAFMadrid) en la actualidad?

—La implantación de la nueva imagen profesional nacional y la recuperación de las relaciones con instituciones públicas y privadas.

—¿Qué iniciativas se han tomado para lograr estos objetivos?

—Trabajar en equipo con el resto de Colegios a través del Consejo General para identificar al colectivo con una imagen, imagen que representa la cualificación profesional de los administradores de fincas colegiados.

—¿Cuáles son las principales funciones de un administrador de fincas?

—Desarrolla sus funciones como gestor, gerente, asesor, mediador, secretario, contable y representante inmobiliario, sin descuidar la convivencia entre los vecinos e inquilinos, velando por una mejor calidad de vida.

En la Ley de Propiedad Horizontal, el artº20, define las funciones del administrador:

- Velar por el buen régimen de la casa, sus instalaciones y servicios, y hacer a estos efectos las oportunas advertencias y apercibimientos a los titulares.
- Preparar con la debida antelación y someter a la Junta el plan de gastos previsible, proponiendo los medios necesarios para hacer frente a los mismos.
- Atender a la conservación y entretenimiento de la casa, disponiendo las reparaciones y medidas que resulten urgentes, dando inmediata cuenta de ellas al presidente o, en su caso, a los propietarios.
- Ejecutar los acuerdos adoptados en materia de obras y efectuar los pagos y realizar los cobros que sean procedentes.
- Actuar, en su caso, como secretario de la Junta y custodiar a disposición de los titulares la documentación de la comunidad.
- Todas las demás atribuciones que se confieran por la Junta.



—¿Qué papel juegan los administradores de fincas en los temas relacionados con la seguridad de los inmuebles que administran?

—La seguridad, en la situación social actual, es un tema de interés en las Comunidades de Propietarios

La oferta del mercado en cuanto a soluciones para seguridad domiciliaria es adecuada aunque hay que mejorar los costes para agilizar su implantación

y, como tal, actuamos de forma directa proponiendo la implementación de dispositivos que faciliten el control de accesos y, de forma indirecta, protegiendo los bienes más preciados de la sociedad.

—El administrador de fincas debe estar cualificado para dar solución a todos los problemas que se generan en los inmuebles. ¿Cuáles suelen ser los más frecuentes?

La convivencia y el cumplimiento de la Legislación que repercute en el ámbito económico de la Comunidad. Las subvencio-

nes no son suficientes y la financiación inalcanzable por los requisitos a cumplir.

—¿Cuáles son las medidas que se utilizan con más frecuencia para prevenir las situaciones de riesgo en las residencias o en las comunidades de vecinos?

—Medidas preventivas que pocas veces se atienden hasta que no suceden los hechos, pasando en este caso a una actuación «curativa» para evitar que vuelva a suceder.

—¿Cree que es adecuada actualmente la oferta del mercado en cuanto a soluciones para la seguridad domiciliaria?

Es adecuada aunque todavía hay que mejorar los costes para agilizar la implantación.

—¿Cree que está implantada una conciencia de prevención en cuanto a medidas de seguridad en los inmuebles o en las comunidades de vecinos?

—No, porque el ser humano piensa que a él nunca le va a suceder.

Fotos: Colegio Profesional de Administradores de Fincas de Madrid (CAFMadrid)



Innovación



Securitas Direct: cuidamos a las personas

**José Ignacio Jiménez. Director de Relaciones Institucionales.
Securitas Direct**

En Securitas Direct llevamos 22 años protegiendo viviendas y negocios en España. Son más de dos décadas al servicio de las personas, nuestra vocación es cuidarlas, ofrecerles seguridad, poner a salvo a las familias y sus pertenencias. Y siempre estableciendo la máxima colaboración con las Fuerzas y Cuerpos de Seguridad, nos honra facilitar su labor, aportar nuestro conocimiento, nuestro saber hacer y nuestra tecnología, y contribuir a que España sea un país cada vez más seguro.

YA tenemos más de 770.000 clientes, somos líderes absolutos del mercado de alarmas; 770.000 razones para dar lo mejor de nosotros cada día, para buscar la manera de que los ladrones no logren su objetivo: entrar en casas ajenas y llevarse todo lo que pillen a su paso. Porque no sólo roban objetos materiales, que también -y de mucho valor, si pueden-, también se llevan por delante la tranquilidad y la confianza de las personas; hay pocas sensaciones de ultraje más grandes que la que se produce cuando sabemos que alguien ha entrado en nuestra propia casa.

TRABAJO DURO PARA INNOVAR

Los ladrones cada vez son más listos y cuentan con nuevas herramientas para perpetrar sus golpes. Nosotros no nos quedamos atrás. En estos más de 20 años, hemos trabajado duro por innovar, nuestro departamento de I+D ha buscado soluciones a las nuevas modalidades de robo que van apareciendo: a las primeras alarmas les siguieron las bidireccionales y las inalámbricas, con notables mejoras en el conocimiento de la alarma y la transmisión de las señales; hemos perfeccionado los procedimientos de verificación de los saltos de alarma -señales, imagen, sonido...-; he-





Nuestro departamento de I+D busca soluciones a las nuevas modalidades de robo que van apareciendo

mos mejorado los protocolos de aviso a la policía; incorporamos el servicio de acuda; las cámaras de alta definición...

Y cuando nos hemos enfrentado a los inhibidores de frecuencia, el último gran reto -hasta ahora- para los equipos

de seguridad, hemos dado una vuelta de tuerca a nuestra capacidad innovadora: hemos desplegado una red propia de 1.500 antenas, con cobertura nacional, que permite a nuestras alarmas transmitir señales por una vía dis-

tinta a la red GSM convencional. Esta tecnología, absolutamente exclusiva de Securitas Direct, permite detectar la inhibición de la frecuencia, y aun en esas circunstancias, seguir enviando información a nuestra central receptora de alarmas.

No fue una decisión fácil, desplegar una red nacional de antenas no es algo que esté al alcance de cualquiera, pero decidimos ir a por ello porque estábamos convencidos de que era la única manera fiable de proteger a nuestros clientes contra la cada vez más habitual utilización de inhibidores de frecuencia.

La red está lista y hemos empezado a utilizarla con resultados muy satisfactorios. Poco a poco iremos incorporando nuevas funcionalidades a través de esta infraestructura, que está diseñada para la seguridad de nuestros clientes, que son nuestra razón de ser.

Fotos: Securitas Direct

Contactos de empresas, p. 7.



// Ofreciendo a nuestros clientes servicios de seguridad personalizados a sus necesidades.
// Apostando por la innovación, la excelencia y la diversificación de servicios en Andalucía.



Prevención:
Seguridad física

Grupo RMD Seguridad es la división del Grupo Romade dedicada a la gestión de equipos humanos especializados en velar de forma activa por la seguridad de su empresa.



Ponemos a su disposición servicios pensados para la supervisión directa:

- Control de entrada y salida de mercancías
- Chequeo, control de acceso y conteo de personas
- Supervisión de vehículos en obras o almacenes
- Gestión de paquetería y correspondencia



DISPONGA DE LA MÁS ALTA TECNOLOGÍA EN SUS INSTALACIONES



*Homologados por la Dirección General del Estado, con el número 729.
* Con el Certificado de Calidad por Bureau Veritas, ISO 9001.



PREVENCIÓN:
Seguridad Física



ACCESO:
Servicios generales.



CONTROL:
Sistemas y equipos Tecnológicos



PERSONALIZACIÓN:
Servicios Especiales



FORMACIÓN:
Innovación y excelencia profesional

OFICINAS CENTRALES

Avda. Olivares, 17 Pol. Industrial PIBO 41110 - Bollullos de la Mitación (Sevilla)
Tel. 902 194 814 • Fax. 954 002 319

Domótica



Usos del videoportero IP en entorno residencial

Alfredo Gutiérrez. Business Development Manager para Mobotix AG Iberia

La palabra domótica (Del lat. domus, casa, e informática) se define en el Diccionario de la Real Academia como el conjunto de sistemas que automatizan las diferentes instalaciones de una vivienda. Para completar un poco más podemos decir que sistemas están implicados y los servicios que deben aportarnos: servicios de gestión energética, seguridad, bienestar y comunicación, principalmente. El objetivo de la domótica es hacernos la vida más fácil y cómoda, ahorrar energía y mejorar la seguridad.

CUANDO hablamos de la automatización y control, tenemos que tener en cuenta que este control puede ser centralizado y/o remoto, y que se refiere a los aparatos y sistemas de instalaciones eléctricas y de electrodomésticos que pueden estar integrados por medio de redes interiores y exteriores de comunicación, cableadas o inalámbricas.

Los avances tecnológicos que surgen día a día están permitiendo que se introduzcan nuevas posibilidades y funcionalidades en este sector de manera vertiginosa, ya que es un área que se basa al 100% en la tecnología. De hecho, son las nuevas tecnologías las que han permitido el nacimiento de la domótica y la aplicación del VoIP (Voz sobre el proto-

colo de IP de Internet), gracias a lo cual se ha podido transformar una cámara en mucho más que una cámara, en un siste-

ma de vídeo en red con un gran abanico de aplicaciones de las cuales muchas de ellas son de carácter domótico. La VoIP, convergencia de voz y datos, sobre una misma red permite transmitir el canal de audio recogido en sincronización con el streaming de vídeo. Esto dota a las cámaras de funciones de interfono para interactuar con los individuos que se encuentran delante de la cámara. Así es como funciona nuestro videoportero IP. Pero para entender su utilidad y funcionamiento mejor veamos algunos ejemplos de cómo un videoportero IP nos puede ayudar tanto en nuestro hogar como en nuestro entorno empresarial.

Todas las personas quieren sentirse seguras en sus casas, por ello los clien-



La central de Alarmas más grande de Europa

+ N°1 en Alarmas con verificación por imagen

Presencia en 14 países de Europa y Latinoamérica con más de 1,6 millones de clientes satisfechos.

+ Central de Alarmas Líder en España

Más de 750.000 clientes en España. Más de 700 vigilantes de Acuda para garantizar una intervención inmediata.

+ 4.000 profesionales pendientes de Usted

Le protegen 24 horas al día los 365 días del año. Tiempo medio de respuesta 27 segundos (2012).

Líderes en Seguridad. Referencia en tecnología y usabilidad en Alarmas.

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



902 33 44 50
www.securitasdirect.es

DGP: 2737

N°1 en Alarmas





tes ven muy importante poder controlar la zona de acceso de su edificio de pared a pared y de techo a suelo. Nosotros, en nuestro videoportero, apostamos por la tecnología Hemispheric para poder ver toda el área situada delante de la puerta, lo que hace que el área vi-

mos con tecnología RFID, que además de llamar al timbre, permite acceder sin llave mediante el transpondedor RFID o introduciendo un número PIN. Se guardan todos los números PIN, datos de transpondedor y horas de acceso necesarias para abrir la puerta. Así se en-

El objetivo de la domótica es hacernos la vida más fácil y cómoda, ahorrar energía y mejorar la seguridad

sualizada puede centrarse siempre en las zonas de mayor interés. También es importante que cuenten con gran resolución del sensor de imagen para que se puedan ampliar los detalles sin ningún problema.

Aunque no se encuentren en el edificio es importante saber qué ha pasado mientras se ha estado ausente, por ello el videoportero IP debe grabar de forma automática si llaman al timbre o algo se mueve delante de la puerta. Además, algo a tener en cuenta es que al volver al edificio se permita ver, a posteriori, cuando alguien ha tocado el timbre, ha habido alguien cerca de la puerta o una luz del exterior se ha encendido.

Cada vez son más las comunidades de vecinos que están sustituyendo sus llaves por incorporar la tecnología. ¿Cómo se hace esto? Nosotros lo hace-

mos protegidos contra robos y manipulaciones, y no hay problemas de pérdidas de llaves.

VENTAJAS

Las ventajas son muy claras: con un único sistema telefónico, que puede gestionar varias líneas telefónicas de entrada a la vivienda, el sistema permite telefonía clásica, telefonía SIP con audio y vídeo (con el consiguiente ahorro de costes) y control no solo de los videoporteros, sino también del resto de cámaras que eventualmente puede tener instaladas en la vivienda, así como otros dispositivos domóticos.

Con la visión panorámica de 180° permite ofrecer imágenes en las que se vea al visitante perfectamente, aunque el videoportero no se encuentre instala-

do directamente junto a la puerta (como en algunos casos ocurre), y que si se tuviese un portero convencional de 90° sólo permite ver a la persona cuando ésta se encuentra enfrente de la lente. Por lo tanto da más seguridad, ya que desde tu casa puedes observar todo lo que ocurre enfrente de tu puerta. Además tener una elevada resolución del sensor de imagen permite ampliar los detalles sin perder calidad.

Otra de las ventajas es poder ver todo lo que ha ocurrido en tu ausencia: cuántas veces han llamado al timbre, ver la gente que se ha acercado a tu puerta, cuándo ha sucedido algo, etc. Esto da mayor seguridad a la hora de abandonar el edificio, ya que se sabe que de todo se va a poder tener constancia.

En conclusión, poner un videoportero IP en el entorno residencial hace que las personas vivan más seguras y tranquilas, ya que saben que van a tener todo bajo control estén o no estén en su domicilio.



**Ilimitadas Posibilidades,
Una Solución de Seguridad
Novedad - Con Video-verificación en tiempo real**



Novedad - Soporta
hasta 50 zonas



LightSYS™2 es un sistema de seguridad híbrido y versátil que puede ser instalado en negocios y hogares

LightSYS™2 ofrece:

- Video en vivo bajo demanda y video verificación
- Atractiva App para Smartphone que ofrece un sistema de control fácil de usar en cualquier lugar
- Fácil instalación y servicios remotos a través del Bus de RISCO
- Flexibilidad de comunicaciones con IP, GSM/GPRS, RTC – todo dentro de la misma central
- Completa gama de accesorios inalámbricos bidireccionales y en el Bus de RISCO



Hogar digital



Ahorro, seguridad y confort desde el dispositivo móvil

José González Osma. Director de Servicios y Residencial de Tyco

Vivimos en un mundo de constantes cambios en el que, en unos pocos años, todo se ha digitalizado. ¿Quién no tiene un teléfono móvil, una tablet o un ordenador portátil? Este escenario ha sentado las bases para que hoy en día sea una realidad la automatización y el control a distancia de nuestra vivienda, consiguiendo así una utilización idónea de los recursos energéticos y un importante ahorro económico.

SEGÚN los datos del estudio «Hogar Inteligente y Conectado en España» realizado por Tyco, que analiza la percepción del hogar digital entre la población española, más de un tercio de los españoles valora poder disfrutar de las ventajas del «hogar digital», principalmente del ahorro, la seguridad y la comodidad que pueden proporcionar la automatización y control remoto del hogar. Sin embargo, el 57% de los encuestados reconoce que su implantación generalizada se encuentra condicionada por el importante desembolso económico que supone su implementación.

Sin embargo, hoy ya existen en el mercado soluciones como Tyco Interactive Security, que ponen el hogar digital al alcance de todos los bolsillos. Actualmente, cada vez más viviendas y negocios están incorporando estos servicios,

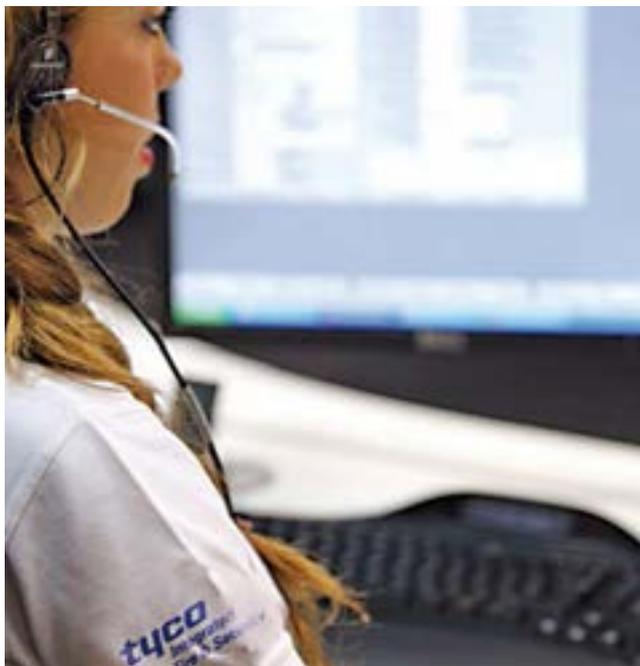
que integran la tecnología más avanzada y garantizan un mayor ahorro, seguridad y comodidad para todos los miembros de la familia. Con el hogar digital, es posible el control completo del hogar o el negocio desde una sencilla aplicación que se puede utilizar en cualquier dispositivo móvil. Permitiendo visualizar en vivo la vivienda o negocio a través de cámaras IP, grabar clips de vídeo, controlar remotamente la calefacción, encender y

apagar todos los dispositivos conectados a la red y controlar entradas y salidas.

SISTEMAS DE ALARMAS

Tyco Interactive Security es un sistema de alarma de alta seguridad con detección de imagen y audio conectada a una central receptora de alarmas. La central proporciona respuesta inmediata durante las 24 horas del día con aviso a las Fuerzas de Seguridad del Estado. Al sistema de alarma se le han incorporado funcionalidades de control y gestión de los recursos energéticos y de confort, aprovechando el desarrollo de los teléfonos inteligentes.





Hoy en día es una realidad la automatización y el control a distancia de nuestra vivienda

Entre las principales ventajas que incluye el hogar digital, destacan:

- Visualización en vivo de la vivienda o del negocio a través de cámaras IP: Esta función permite ver en cualquier mo-

mento y desde cualquier lugar, lo que está sucediendo en la vivienda o el negocio. El usuario puede acceder a las cámaras desde su teléfono móvil, tablet o PC y gestionar o almacenar los vídeos en la nube.



- Automatización de dispositivos: El sistema permite controlar de forma remota todos los dispositivos conectados a la red eléctrica. De esta forma es posible encender o apagar luces, electrodomésticos, etc., desde los dispositivos móviles. Como medida de seguridad también se puede simular la presencia en el domicilio gracias a la creación de patrones de iluminación.

- Gestión remota del sistema de alarma: el usuario puede conectar y desconectar total o parcialmente el sistema y los distintos elementos de nuestra vivienda desde su móvil.

- Control de la calefacción y ahorro energético: permite encender y apagar dispositivos eléctricos y programar el termostato de la calefacción a distancia, permitiendo así gestionar mejor el consumo y aprovechar al máximo los recursos energéticos.

El desarrollo de los dispositivos móviles y el acceso a internet ha favorecido que empresas como Tyco se conviertan en grandes aliados a la hora de proteger y optimizar los gastos del hogar o negocio.

Accesibilidad a las comunidades de vecinos

Lo más relevante de esta Ley es que coloca la accesibilidad universal como uno de los ejes de los procesos de rehabilitación de edificios y de regeneración y renovación del tejido urbano. Explica el preámbulo de la Ley, la Obligación Exigida en la Ley 26/2011 de la realización de los ajustes razonables en accesibilidad universal antes de 2015 y sus obras correspondientes. A partir de ese momento son exigibles en todos los espacios públicos urbanizados y todos aquellos vinculados de alguna forma a la Administración Pública.

A disposición final primera modifica el artículo 10 de la Ley de la Propiedad Horizontal buscando incrementar las condiciones de accesibilidad en las comunidades de propietarios, destacando:

Las obras de accesibilidad deberán realizarse obligatoriamente, aun cuando no exista acuerdo de la Junta de Propietarios. La iniciativa de las obras puede realizarla cualquier vecino independientemente de que en la vivienda viva una persona con discapacidad, o sea mayor de 70 años.

Desde hace años los principales fabricantes de porteros y videoporteros, Fermax, Golmar y Tegui ya incorporan en sus catálogos artículos específicos para ayudar a las personas con alguna discapacidad. Las placas de la calle incluyen los sintetizadores de voz y los pictogramas luminosos que indican el estado de la instalación. Las unidades interiores disponen de Bucle Inductivo y pantallas táctiles. Todo ello pensado para eliminar barreras y hacer las comunidades accesibles para todos.

Desde Porteralia, el distribuidor especialista en porteros, videoporteros y controles de acceso, estamos trabajando para difundir la ley a todos los actores implicados: Administradores de Fincas, Instaladores de Telecomunicaciones, Arquitectos, Ingenieros y al usuario final sobre todo y conseguir una verdadera Smart City accesible para todos.

Toda la información la podrá encontrar en: www.accesibilidad.eu.





LÍDER EN FABRICACIÓN E INSTALACIÓN DE VALLAS, VERJAS Y PUERTAS RESIDENCIALES E INDUSTRIALES

En RIVISA trabajamos para satisfacer las necesidades de nuestros clientes, ofreciendo una extensa gama de cercados metálicos, verjas, puertas batientes y deslizantes para delimitar, proteger, privatizar y decorar todo tipo de espacios.

 **RIVISA**[®]
SISTEMAS DE PROTECCIÓN PERIMETRAL



902 197 626

rvs@rivisa.com

www.rivisa.com

Protección contra incendios en las viviendas

La conciencia preventiva: de lo obligatorio a lo voluntario

Tecnifuego-Aespi

El nivel de protección contra incendios en los edificios está ligado directamente a la cultura de la sociedad, al consumo energético y a los avances tecnológicos de los propios sistemas instalados. Cuanto más elevado es el nivel cultural y económico de una sociedad, mayor es la demanda de sus ciudadanos hacia una protección contra incendios adecuada. Las enseñanzas sobre prevención en caso de incendio forman parte de una asignatura en las escuelas de numerosos países europeos, donde incluso se dan clases prácticas a los alumnos sobre evacuación de emergencia, utilización de un extintor de incendios, etc.

EN España aún estamos muy lejos de que entre los ciudadanos haya calado esta cultura de la prevención, aunque es cierto que cada vez más personas reclaman a la hora de adquirir una vivienda, ya sea individual, en un edificio de pequeña altura o en un bloque de más de 9 plantas o 28 metros de altura (considerados de alto riesgo, por lo que es obligatorio instalar mayor número de medidas para la protección en caso de incendio), que se incluyan determinados aparatos y sistemas que les proteja en caso de declararse un incendio.

El consumo energético es un parámetro que se utiliza como dato de referencia para valorar las necesidades de protección contra incendios de una so-

ciudad. Cuanta más energía se utiliza, existe más actividad, más equipos y, en consecuencia, mayor es el número de riesgos a proteger.

Los avances tecnológicos en los equipos y sistemas de protección contra incendios permiten hoy detectar un incendio en cualquier tipo de ambiente y en una fase muy temprana, casi incipiente y sin falsas alarmas, con sistemas algorítmicos de análisis, identificación puntual, etc. Así mismo los sistemas de rociadores automáticos ofrecen gran variedad de opciones para controlar riesgos y apagar fuegos bajo cualquier condición constructiva. Lo mismo sucede en el caso de los sistemas de control y evacuación de humos y calor, sistemas de extinción por agentes gaseosos limpios,

nuevas eficacias en extintores, elementos y sistemas de protección pasiva, etc.

LO OBLIGATORIO

En el Código Técnico de la Edificación (CTE) se establecen las condiciones que deben reunir los edificios y los sistemas y equipos que hay que instalar obligatoriamente para proteger a sus ocupantes frente a los riesgos de incendio, para prevenir daños en los edificios próximos a aquél en el que se declare un incendio y para facilitar la intervención de los bomberos. Es de aplicación obligatoria en los proyectos y las obras de nueva construcción y de reforma de edificios de vivienda.

Por un lado, en esta norma se indica la denominada Protección Pasiva contra Incendios que debe reunir un edificio dependiendo del uso que se le dé: vivienda, residencial (hoteles), hospitalario, garaje, comercial, administrativo (administración pública, y bancos), docente (escuelas, universidad, e institutos). El promotor, constructora y equipo técnico que realice el edificio debe satisfacer en cuanto al diseño general una serie de condiciones de compartimentación, evacuación y señalización para «garantizar el confinamiento y control de incendios y facilitar la evacuación». Estos parámetros se calculan según el tamaño de la superficie a proteger y la densidad de ocupación, se definen el número y disposición y dimen-

sión de las salidas, pasillos y escaleras, características de puertas, pasillos y escaleras, señalización e iluminación en casos de evacuación, etc.

Además, se realiza una definición de los requisitos de comportamiento ante el fuego de los elementos constructivos y materiales, para garantizar la estabilidad y resistencia térmica del edificio. Se determina la estabilidad ante el fuego exigible a la estructura portante del edificio, la resistencia exigible a los elementos constructivos como medianerías, fachadas y cubiertas, puertas de paso, materiales incluidos en paredes y cerramientos, etc.

Por otro lado, se indican los elementos de Protección Activa que se deben instalar también en relación al uso que tenga el edificio (vivienda, comercial, hospitalario, etc.). Estas instalaciones además están reguladas por el Reglamento de Instalaciones de Protección contra Incendios. Este Reglamento establece y define las condiciones que deben cumplir los aparatos, equipos y sistemas, así como su instalación y mantenimiento, y regula los requisitos que deben cumplir instaladores y mantenedores en protección contra incendios. Es obligatorio que la instalación y el mantenimiento de aparatos, equipos y sistemas lo realicen empresas autorizadas por la comunidad correspondiente.

LA PRINCIPAL CAUSA DE INCENDIO EN LA VIVIENDA ES...

Es un conjunto de factores que básicamente confluyen en la falta de prevención. Si un incendio fortuito se produce y se han tomado las medidas de seguridad adecuadas es muy probable que se controle a tiempo y que no haya que lamentar graves incidentes. Cuando una persona se sensibiliza sobre el riesgo de incendio, toma las medidas de prevención que están en sus manos para evitarlo, tanto de

comportamiento como de equipamiento, lo que implica una reducción importante del riesgo de incendio.

RECOMENDACIONES DE LOS PROFESIONALES

Independientemente de lo exigido por la legislación vigente en la materia, según el denominado «Uso Vivienda», la Asociación Española de Sociedades de Protección contra Incendios, TECNIFUEGO-AESPI, que agrupa empresas de todas las especialidades en la materia, recomienda instalar los equipos y sistemas que se mencionan a continuación. Además es importante integrar desde el principio, en el diseño del edificio, la protección contra incendios: tanto los elementos de Protección Activa como los de Protección Pasiva.

La Protección Pasiva comprende el conjunto de aplicaciones de productos resistentes al fuego que mejoran la resistencia térmica del edificio. La protección estructural es una parte relevan-

placas rígidas de fibrosilicato. Hay otros elementos en Protección Pasiva que atienden a la compartimentación de las zonas de fuego del edificio (puertas cortafuegos, sellado de penetraciones, etc.).

Por su parte, la Protección Activa tiene un papel esencial en la detección y extinción de incendios. Esta protección se realiza mediante una combinación de extintores portátiles, bocas de incendio equipadas, rociadores automáticos, sistemas de evacuación de humos, sistemas de inundación mediante gases inertes, sistemas de detección y alarma, etcétera.

El usuario final dispone de una manera de verificar y garantizar la calidad de los elementos constructivos a través de las marcas de conformidad a Norma para dichos elementos (Marcado CE)

MANTENIMIENTO DE LOS EQUIPOS

Una vez se consigue proteger un edificio debidamente, el siguiente paso es mantenerlo. La importancia del mantenimiento en las instalaciones supone que el equipamiento garantiza su vigencia permanente en condiciones de operación, teniendo en cuenta que la utilización de estos equipos y sistemas quizá no tenga que hacerse nunca, pero si fuera necesario lo sería en las condiciones de emergencia propias de un incendio. Para realizar un correcto mantenimiento es necesario disponer de planos de los sistemas y equipos que se vayan a revisar. El manual de instrucciones y la memoria descriptiva para conocer las características de este equipamiento son igualmente imprescindibles.

Control de calidad de los productos de Protección contra Incendios: cumpliendo las normas UNE/EN que exige la Reglamentación. Realizando los ensayos correspondientes en los laboratorios de Ensayo de productos contra incendios. Instalando y manteniendo los productos y equipos.



© freepik.com

te de la Protección Pasiva. El efecto que produce esta protección, equivale técnicamente a mejorar la masividad de la estructura para retrasar la aparición de tensiones estructurales y dilataciones. Las protecciones estructurales más usadas son las pinturas intumescentes, los proyectados de yeso con perlitas y las

Prevención y Protección



La carta de invierno

Jon Michelena.
Director General de CEPREVEN

Todos los años, al iniciarse el estío, todos los vecinos de nuestra urbanización recibimos una carta de nuestro administrador, que dicho sea de paso, es uno de los que se puede presumir. Tras un doloroso proceso de prueba y error, hemos dado con un profesional serio y capaz que ha puesto en evidencia a sus predecesores. No aludiré a su filiación, ni tampoco pretendo redactar un panegírico de los administradores de fincas, no es éste el objeto de este artículo...

VOLVIENDO al escrito estival, en él se nos indica con amplio grado de detalle las conductas idóneas y diversos consejos para evitar ser víctimas de los malhechores durante nuestras merecidas vacaciones. No podremos demostrarlo, es muy probable que, gracias a estas indicaciones que nos hacen llegar nuestros administradores, muchos de nosotros nos hayamos encontrado nuestras viviendas en el mismo estado en el que las dejamos días atrás, cuando partimos ilusionados hacia el merecido periodo vacacional, evitándonos el inesperado disgusto de encontrarnos nuestro hogar patas arriba y con el desconsuelo de haber perdido para siempre la cubertería de plata de nuestra abuela, el televisor de 55 pulgadas y el portátil que con tanta ilusión compramos para nuestro hijo.

Quiero agradecer a todos los administradores de fincas, en mi nombre y en el de todos aquellos que no necesitan ir a la comisaría nada más llegar de

© freepik.com





vacaciones, el pequeño detalle de enviarnos unas sencillas consignas a finales de junio. Gracias, señor administrador.

Pero después del verano llega el otoño, y más tarde el invierno. Casi sin darnos cuenta ya estamos a sus puertas y el frío ya se hace notar. No importa, tenemos a nuestro alcance ropa de abrigo para continuar con nuestra vida sin grandes inconvenientes, y en nuestros hogares disponemos de confortables sistemas para generar calor en la cantidad que cada uno de nosotros considere oportuno, bien por decisión propia o por consenso familiar. Estufas, braseros, radiadores, chimeneas... todo vale para luchar contra el crudo invierno.

EL INVIERNO NO PARECE PELIGROSO

Todos los años por estas fechas espero otro escrito de mi administrador, pero éste nunca llega. El invierno no parece peligroso. Los amigos de lo ajeno reducen su actividad, por lo visto con el frío la gente sale menos a la calle y no es necesario alertar sobre los peligros de

Como propietario de una finca espero recibir pronto un escrito sobre la prevención de incendios en el hogar

los robos en viviendas. Pero el invierno también tiene sus amenazas. Son otras desgracias, quizá menos probables, pero pueden ser devastadoras. Entre todos destaca el riesgo de incendio. Durante el invierno se producen gran número de incidentes de este tipo y la mitad de los muertos en viviendas por esta causa suceden en los tres meses que lo componen. Si todo sigue en la línea de ejercicios anteriores, todo hace prever que este invierno morirán más de 60 personas en sus hogares a causa de incendios, y un número indeterminado lo harán en los días posteriores por no superar las lesiones producidas en los mismos. Muchos más serán los que podrán abandonar sus viviendas a tiempo y sufrirán daños corporales. Se sentirán afortunados en un primer momento por haber salvado su vida y la de sus seres queridos, pero rápidamente se darán cuenta de que el fuego es el peor de los

ladrones. Se lleva todo y nos deja con lo puesto. Todos los años mueren varias personas en las escaleras de su edificio, intentado abandonarlo a través de una vía de evacuación inundada por el humo, porque nadie les ha contado que en ese caso, y siempre que el incendio no se haya producido en su vivienda, es mucho más seguro permanecer en ella y esperar a que los rescaten los cuerpos de bomberos.

MEDIDAS DE PREVENCIÓN

Por eso todos los años espero la carta de mi administrador por estas fechas. Una carta sencilla, un pequeño folleto de los que cualquier asociación como la nuestra edita y pone a disposición de quien lo desee¹, en la que nos recuerde los peligros que conlleva la generación

de calor, en la que nos haga saber dónde están los extintores de la finca, en la que nos indique cómo hay que usarlos, en la que se señalen las consignas básicas de prevención, en la que se nos informe de la existencia de detectores domésticos de humo...

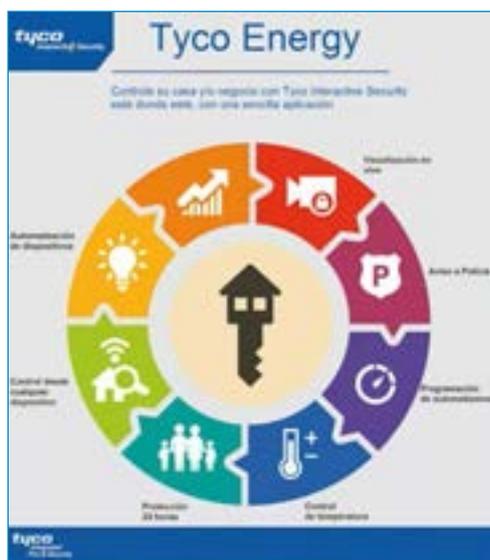
Como propietario de una finca espero recibir pronto un escrito sobre la prevención de incendios en el hogar, como prevencionista me pongo a disposición de todos los administradores de fincas para ayudarles a transmitir las necesarias consignas de prevención a todos los propietarios que, como yo, confían a diario en su gestión.

¹ En nuestra web www.cepreven.com pueden disponer de un folleto titulado «Haga su hogar más seguro, prevenga los incendios» y un vídeo de animación sobre el uso de extintores, ambos de forma gratuita.

Estudio Tyco: «Hogar Inteligente y Conectado en España»

Seguridad, una de las razones principales para apostar por el hogar digital

Según los datos del estudio «Hogar Inteligente y Conectado en España» realizado por Tyco, empresa especializada en soluciones de seguridad y protección contra incendios, más de un tercio de los españoles valora poder disfrutar de las ventajas del «hogar digital y conectado», principalmente el ahorro, seguridad y comodidad que pueden proporcionar la automatización y control remotos del hogar. El 38% piensa que una casa inteligente es más económica de mantener que una casa tradicional. Sin embargo, su implantación generalizada se encuentra condicionada por la idea que comparte el 57% de los españoles, de que su puesta en marcha supone un desembolso económico que todavía no se encuentra al alcance de la mayoría.



La seguridad del hogar y de sus ocupantes sigue siendo una de las preocupaciones más importantes para la mayoría de los españoles (36%). El 37% de los encuestados considera que poder controlar y ver desde el móvil lo que sucede en el hogar cuando está fuera de casa es una de las principales ventajas del Hogar Inteligente y Conectado.

La seguridad es la preocupación más importante. Mejor si puede controlarse desde el móvil

Tyco Interactive Security, la solución presentada por la com-

pañía, incorpora funcionalidades de control y gestión de recursos energéticos y de confort al sistema de seguridad y alarma en el hogar o negocio, aprovechando el desarrollo de los teléfonos inteligentes. El nuevo producto permite, entre otras funciones, visualizar en cualquier momento y en tiempo real lo que sucede en el hogar a través de cámaras IP, y video on-demand, controlar desde el móvil la temperatura del hogar y encender o apagar a distancia diferentes dispositivos conectados a la red.

En este sentido, Tyco Interactive permite la visualización en vivo de la vivienda o del negocio a través de cámaras IP. Esta función permite ver en cualquier momento y desde cualquier lugar, lo que está sucediendo en la vivienda o el negocio. El usuario puede acceder a las cámaras desde su teléfono móvil, tablet o PC y gestionar o almacenar los vídeos en la nube (video on-demand). El sistema garantiza además la total privacidad del hogar, ya que sólo el usuario tiene acceso a estas cámaras, los operadores de la CRA sólo reciben las imágenes de los vídeo-detectores al producirse un salto de alarma. Además, Tyco Interactive Security integra las probadas capacidades de seguridad de Tyco, que incluyen un sistema de alarma de alta seguridad con detección de imagen y audio, conexión a la Central de Recepción de Alarmas de Tyco, que se encuentra entre las más reconocidas del mercado, y garantiza el control y la

SEGURIDAD

Autorizada D.S.E. N° 3288



"...porque además de una imagen somos un gran equipo de profesionales..."

**"SOMOS MAS...
... QUE UNA IMAGEN"**

"...porque nuestra mejor imagen, es la satisfacción del cliente..."



SERVICIOS



C/ Garcia de Paredes, 68 1º 28010 - Madrid

Tif. 91 5913603

www.gruser4.com - www.grusegur4.com



La seguridad del hogar y de sus ocupantes sigue siendo una de las preocupaciones más importantes para la mayoría de los españoles (36%)

atención por parte de un equipo altamente profesional y conectado 24h con los cuerpos de seguridad del Estado.

En el estudio realizado por Tyco, un 40% de los españoles deja encendida la calefacción al salir de casa y tan sólo cuatro de cada diez españoles la apaga, aunque la casa esté fría al volver. Además el 57% realiza un uso ineficiente de la calefacción, situando el termostato por encima o por debajo de la temperatura recomendada -entre 22 y 24 grados-. El 71% piensa que podría ahorrar mucho en calefacción sin mermar su comodidad, si pudiera encenderla solo cuando va a estar en casa. No en vano el ahorro energético es, para el 37% de los encuestados, la principal ventaja del Hogar Inteligente. El uso ineficiente de la calefacción supone un despilfarro inútil de energía y dinero además de tener un impacto negativo en el medioambiente. Actualmente, la factura media de calefacción se sitúa entre 100 y 200 euros/mes para el 46% de los encuestados.

La nueva solución Tyco Interactive Security permite, por ejemplo, controlar a distancia los distintos elementos de nuestra vivienda, como el termostato de la calefacción, a través de tablets y teléfonos inteligentes, de manera que podamos aprovechar al máximo los recursos energéticos. En cuanto a la iluminación también hablamos de ahorro: gracias al control remoto podemos apagar alguna luz que nos hayamos dejado encendida, activar el encendido

de luces exteriores sólo durante la noche, o si nos hemos ido de vacaciones y pensamos que hemos dejado algo en-

cendido, podemos comprobar y dejarlo tal y como lo necesitemos.

El control remoto del confort, una de las funcionalidades más valoradas

Nuestro estilo de vida no tiene horarios fijos y no nos permite parar ni un momento. Por eso los españoles (28%) valoran especialmente poder controlar a distancia el estado de confort de la casa (calefacción, iluminación, aire acondicionado, electrodomésticos) y gestionar en remoto los sistemas electrónicos del hogar. Además, el 27% de los españoles considera que la comodidad es una de las principales ventajas que ofrece la automatización del hogar.

En este sentido, Tyco Interactive Security, con una sencilla instalación, permite la automatización del hogar a través de módulos inalámbricos y controlar el estado de los dispositivos conectados al sistema con un simple click en el teléfono. Gracias a ello, proporciona mayor comodidad y se adapta a las necesidades y estilo de vida de sus usuarios.

«El desarrollo de la telefonía móvil, la conectividad y el internet de las cosas han dado lugar a la aparición del hogar inteligente y conectado. Atentos a esta tendencia imparable, Tyco ha revolucionado los sistemas tradicionales de seguridad para adaptarlos a las necesidades de los usuarios de hoy en día, que no sólo reclaman seguridad para su hogar, sino también capacidades de control y confort. Tyco Interactive Security combina la seguridad con el ahorro energético y el control de los diferentes elementos del hogar para adaptarse al estilo de vida de sus habitantes y proporcionar mayor confort y comodidad, junto a un nivel de seguridad sin precedentes», José González Osma, Director de servicios y residencial de Tyco IF&S.



JUAN MANUEL RODRÍGUEZ. DIRECTOR
COMERCIAL DE GRUSEGUR 4 Y GRUSER 4

«El objetivo principal es intentar que nuestros clientes estén dotados de los medios y medidas de protección más adecuados»



—¿Cuál es la actividad y principales líneas de negocio del Grupo?

—Nuestro Grupo se crea hace más de 15 años, con el objetivo de ser un referente de calidad, tanto en el sector de la Seguridad Privada (Vigilantes de Seguridad), como en el amplio sector de los servicios demandados por comunidades y empresas (Conserjes, Controladores, Auxiliares de Servicios, Limpieza...). Por ello, desde los inicios, ponemos al mando de nuestras empresas a directores y jefes de departamento con una demostrada profesionalidad, que en la actualidad cuentan ya con una experiencia de más de 28 años.

Nuestros primeros clientes fueron Comunidades de Propietarios (grandes urbanizaciones, complejos residenciales, edificios, garajes, etc.), y es un tipo de cliente fundamental hoy en día para nuestras empresas, ya que en la actualidad representan más del 75% del total de nuestros clientes, siendo por tanto la principal línea de negocio del Grupo.

En la actualidad, estamos en disposición de ofrecer a este tipo de clientes, un servicio de máxima calidad, ya que nuestro Grupo cuenta con una vasta experiencia y profesionalización, tanto en el estudio y

análisis de factores de riesgo, como en la posterior determinación y ejecución de soluciones integrales eficaces, que cumplan fielmente los objetivos que demandan este tipo de clientes.

—La demanda de seguridad en comunidades de vecinos ha crecido en los últimos años, ¿qué objetivos se ha planteado su compañía respecto a esta demanda?

—El objetivo principal es intentar que nuestros clientes estén dotados de los medios y medidas de protección más adecuados, en relación a los riesgos a los que se encuentran expuestos. Para ello, desde el primer contacto que establecemos con el cliente, intentamos que tome conciencia de su situación concreta, en primer lugar de cuáles son los riesgos que afectan a su comunidad, de que los mismos pueden materializarse en cualquier momento, por tanto son tangibles, e incluso cuantificables económicamente, y de cuáles son los medios y medidas que pueden llegar a controlarlos o minimizarlos al máximo.

Es cierto que en los últimos años existe una mayor sensación de inseguridad, generalizada en todos los sectores que, evidentemente, apoya nuestros planteamientos y argumentos, tendentes a un proceso de concienciación, de forma que el cliente sea capaz de admitir su propia necesidad en materia de seguridad, pero esa demanda de seguridad, no siempre se concreta en la contratación de la empresa, o del sistema de seguridad más adecuado, lejos de ello, a menudo se circunscribe únicamente a la posición económica más ventajosa, y no a los criterios de seguridad más idóneos para la comunidad.

Es un esfuerzo inicial, a veces arduo y complejo, pero solamente a partir de ese momento de concienciación, el cliente está en disposición de valorar, en su justa medida, la importancia de contar con una

empresa, que realice un trabajo metódico y exhaustivo, en el estudio de sus necesidades. Es entonces, cuando admite el análisis y el consejo profesional, y es desde nuestra forma de entender la seguridad, el único camino para conseguir un grado de protección satisfactorio en sus instalaciones.

—En su opinión, ¿cuáles son las necesidades actuales en el mercado residencial en materia de seguridad ?

—Para establecer la necesidad en materia de seguridad, hay que partir inicialmente por definir el valor a proteger. El mercado residencial, en cualquiera de sus formas (complejos residenciales, de viviendas...), tiene un diferenciador por otro lado, de otro tipo de clientes (empresas, industrias, comercios, organismos oficiales...); es cierto que una comunidad de propietarios, incluye instalaciones, bienes y equipos (como en cualquier entidad o empresa), pero además es una vivienda, representa un hogar, construido con un esfuerzo individual, con una significativa valoración personal, que incluye además un elemento de valor incalculable, la protección a la familia.

Una vez que se han analizado los distintos valores a proteger, es fácil definir la necesidad que cada cliente tiene en materia de seguridad. Esencial es, para cada propietario, conseguir la sensación de tranquilidad que da el saber que su hogar está protegido las 24 horas. La forma de llegar a este idílico estado, pasa por obtener una eficacia real en materia de seguridad, y ello se consigue gracias a la adecuada combinación de medios, que integran el factor humano



con protocolos de seguridad correctamente adaptados, medidas operativas y de actuación que contemplen todos los casos (procedimientos habituales y de emergencias), dotación de sistemas tecnológicos de vanguardia, controles de acceso que permitan el libre tránsito de personas autorizadas, anulando cualquier intento de intrusión no autorizada, instalaciones de videovigilancia con monitorización remota, tecnología IP, sistemas de alarma perimetral y/o de interior, con conexión y verificación visual por C.R.A., controles de paso mediante llaves electrónicas con chip integrado, lectores de proximidad o de huella, y tantos otros medios y sistemas que, combinados adecuadamente, conseguirán dar a cada cliente la mejor relación inversión / grado de protección.

Es en los Administradores de Fincas, en quienes en muchos casos, recae la responsabilidad de la selección y presentación de empresas de seguridad a

las Juntas de Gobierno, así como el planteamiento de medios y medidas, para mejorar la seguridad de las comunidades administradas. Es fundamental por tanto que, atendiendo a la relevancia de los valores representados, los Administradores, además de ser, conocedores de las normativas y reglamentos en materia de seguridad, dediquen su máximo esfuerzo en la selección y propuesta de empresas que tengan una sólida experiencia en el sector, y que planteen con rigor y seriedad profesional, medios y medidas adecuadas y eficaces, para garantizar la seguridad y protección de sus representados.





—¿Qué aspectos diferenciales caracterizan a su compañía en relación con otras que operan en el mismo ámbito?

—Nuestro slogan dice: «Somos más que una imagen», y creemos y apostamos por su significado. Cada empresa establece su imagen corporativa, sin embargo es evidente que esto debe quedar en segundo plano, debiendo ir más allá.

Las comunidades de propietarios deberían buscar empresas que puedan afrontar con garantías el reto de la protección de sus propietarios e instalaciones, y ello sólo tendrá plenas garantías de éxito, si se analizan prioritariamente empresas consolidadas en el sector, con amplia experiencia en servicios similares, que operen con seriedad y rigor profesional en sus fórmulas de trabajo, que ofrezcan una dedicación plena a cada cliente, de forma individual y personalizada, que se encuentren a la vanguardia de las técnicas y tecnologías más eficaces, y sobre todo, que sean capaces de ofrecer estos servicios, con una excelente relación calidad /precio.

Pues bien, nuestras empresas, creadas hace más de 15 años, cuentan con profesionales que vienen

desarrollando, desde hace más de 28 años, su labor en cargos directivos, técnicos y de mandos intermedios dentro del sector, lo que garantiza un alto nivel de formación y experiencia en el mismo.

Por otro lado, la prestación de servicios de seguridad y de servicios auxiliares con controladores y conserjes representa un porcentaje importante, con respecto al volumen total de clientes en nuestras empresas, por lo que un alto grado de los esfuerzos y dedicación de nuestras compañías, se invierten en formación y cualificación profesional de todo nuestro personal, relacionado siempre con la tipología de estos clientes.

La composición de nuestras empresas, su organigrama, distribución e infraestructuras, se han desarrollado teniendo muy en cuenta este tipo de clientes, por lo que podemos garantizar una dedicación, totalmente individual y personalizada a cada uno de ellos. Un ejemplo es la labor que desarrollan los distintos departamentos al inicio de cada nuevo servicio, o el control y supervisión posterior que se realiza de los mismos. (Ej. todos nuestros servicios son visitados, por nuestros inspectores, varias veces por semana).

Nuestro personal se mantiene siempre al día, formándose en las nuevas tecnologías y su aplicación práctica en los servicios, buscando constantemente las soluciones más eficaces para proponer a nuestros clientes, de forma que cualquier inversión que realicen, tenga un resultado rentable a corto o medio plazo.

Nuestro personal se mantiene siempre al día, formándose en nuevas tecnologías y buscando las soluciones más eficaces para nuestros clientes

Por último, y en consecuencia lógica a los tiempos que corren, hemos minimizado todo lo posible la incidencia y repercusión de nuestros costes, por supuesto sin sacrificar la dotación de medios (humanos y técnicos), necesarios para mantener un correcto servicio a nuestros clientes. De esa forma, hemos ajustado al máximo nuestros precios, con el fin de poder ofrecer una excelente relación calidad / precio.

SEGURIDAD PARA COMUNIDADES DE PROPIETARIOS



REVISIÓN TÉCNICA, DIARIA Y REMOTA DEL SISTEMA SEGURIDAD SIN COSTES AÑADIDOS NI DERRAMAS

ALTA DEL FICHERO DE CÁMARAS Y DATOS EN LA AEPD | TELÉFONO PERMANENTE 24 HORAS ANTE INCIDENCIAS
VIGILANCIA VIRTUAL EN TIEMPO REAL | RONDAS DIARIAS ALEATORIAS DE VIDEOVIGILANCIA



El sistema integrado de videovigilancia y control de accesos de **Grupo ESV** está particularmente pensado y diseñado para mejorar la seguridad y la convivencia de los vecinos de la comunidad y especialmente para agilizar y facilitar al administrador la gestión de las comunidades ya que no exige derramas ni costes añadidos.

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

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

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

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

Grupo **ESV**



gruposv.com

SEDE CENTRAL:

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



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

Confianza, seguridad y GCTI

Del DRAE: Confiar: depositar en alguien, sin más seguridad que la buena fe y la opinión que de él se tiene, la hacienda, el secreto o cualquier otra cosa¹.
Confianza: Esperanza firme que se tiene de alguien o algo²

«Privacy and security are important brand differentiators and companies need to move from a mindset of meeting compliance requirements to becoming a steward of consumer data». Del correo enviado por Craig Spiegle, director y fundador de la «Online Trust Alliance» a la NIST el 1 de agosto de 2011³. Aunque esta cita ya tiene más de 4 años, el contenido del correo no ha perdido vigencia en absoluto.

LAS brechas de seguridad en todo tipo de organismos, tanto públicos como privados, compañías tecnológicas o de cualquier otro sector, y hasta en empresas dedicadas a desarrollar y vender herramientas de intrusión en los sistemas -como la empresa italiana Hacking Team,⁴ que en julio de este año sufrió un ataque divulgándose una gran cantidad de información de clientes-, están pasando a ser consideradas sucesos cotidianos.

En el individuo esta cotidianidad podría tener, entre otros, dos efectos a cual más nocivo, consecuencias ambos de considerarlos irremediables, y como tales, rendirnos a su inevitabilidad. Uno de ellos sería dejar de tomar medidas adecuadas para evitar la intrusión,

otro sería dejar de utilizar los servicios proporcionados a través de la red, como consecuencia de la pérdida de confianza en los sistemas y, por extensión, en las empresas que los proporcionan.

El primer efecto causaría a nivel de dispositivo individual -de hecho está

causando por negligencia o ignorancia- daños por virus con efectos de secuestro del contenido del ordenador, cifrándolo y solicitando dinero como rescate (ransomware); o uso por terceros de dispositivos sin permiso del propietario, creando redes de ordenadores esclavos (botnets) utilizados posteriormente para actuaciones ilícitas, como por ejemplo ataques distribuidos de denegación de servicios (DDoS, Distributed Denial of Service); o para entrar en una red de una empresa a través de un dispositivo móvil autenticado; o simplemente robo de información contenida en los dispositivos, importante para el individuo,

para la empresa en la que este trabaje o para terceros relacionados con él.

El segundo efecto daría al traste con la digitalización del mercado y los servicios en particular, y de la sociedad de la información en general.

La Global Commission on Internet Governance (GCIG) publicó este pasado mes de abril «Toward a Social Compact for Digital Privacy and Security», de lo que se hizo eco iTTi⁵, un importan-



te documento de 29 páginas que, al considerar necesario restaurar la confianza en el uso de internet, proponía que todas las partes interesadas colaboraran en la adopción de normas para un comportamiento responsable de dicho uso.

Sin embargo, no es sólo cuestión de datos en línea. Hoy día, todas las organizaciones utilizan para su gestión tecnologías de la información aunque no sea en-línea, manejando datos sobre sus trabajadores, asociados, clientes, socios, proveedores, etc., así como los datos producto de la relación establecida con ellos. Y sus sistemas son susceptibles de ser atacados y que estos ataques tengan éxito.

Por tanto, aunque no se utilicen directamente servicios en-línea, los datos que es necesario proporcionar a una entidad con la que se está estableciendo alguna relación o los datos producto de dicha relación -por ejemplo, los de una prueba médica- se van a almacenar probablemente en un sis-

tema informático. Y este sistema informático es probablemente accesible desde la red. Como se indica en la cita que abre este artículo, «las empresas han de transformarse en administradores de datos» de los terceros con los que se relacionan.

Los negocios y las instituciones dependen en gran medida de un bien intangible que se llama «marca». La marca de una empresa es como la reputación de las personas. Esta marca está ligada a la confianza -hipótesis que los demás hacen sobre la conducta futura de la empresa- que sepan transmitir.

Según un estudio, realizado por el instituto Ponemon⁶ y publicado el 26/08/2015, para responder a la pregunta: what erodes trust in digital brands?⁷

-el 63% de los consumidores no confían en las webs de compañías que han tenido brechas de seguridad;

-el 55% de los consumidores no confían en webs que no tienen salvaguardas para proteger la información personal;

-el 50% de los consumidores aún después de un año de una brecha de seguridad perciben negativamente una marca;

-el 69% de los consumidores han dejado webs de compañías por problemas de seguridad.

Aunque este estudio se centra en las páginas web y la marca digital, casi todas las empresas han sufrido o están sufriendo una transformación digital, y tienen página web, a través de la cual ofrecen más o menos servicios y se comunican con sus clientes, siendo, en muchos casos, la página web la generadora -y mantenedora, junto con las redes sociales- de su marca, ya digital.

Como consecuencia de todo lo anterior, un aspecto que ha entrado de lleno en la imagen de marca de una institución o empresa ha sido la seguridad de sus sistemas informáticos, ya que en ellos residen datos de terceros y, por tanto, contractualmente o no, deben ser garantes de la seguridad de dichos datos, al haber sido cedidos en la confianza de una relación.

Enlazando con las definiciones con las que se iniciaba este artículo, los datos se depositan y son confiados sin más que con la buena opinión que se tiene de la empresa -imagen de marca- y en la esperanza firme de que sean tratados adecuadamente para el fin para el que se ceden.

La seguridad de la información ha pasado de ser un tema «de los informáticos» a ser un tema «de negocio». La posible pérdida o robo de información generados por la aplicación y uso de las tecnologías de la información, especialmente, del «siempre conectados» es un riesgo que ha de gestionarse adecuadamente dentro de la política de gestión de riesgos de la compañía en cuestión, y estar sobre la mesa de su órgano de gobierno.

Entender la [ciber]estrategia es esencial, pero salvo honrosas excepciones, los temas de [ciber]seguridad -y los temas de TI en general- se tratan



principalmente desde un punto de vista técnico, ignorando que sólo un enfoque estratégico puede preparar a las empresas para conseguir ventaja sobre los ciber-atacantes. El órgano de gobierno necesita preguntarse porqué es necesaria la [ciber]seguridad, qué caracteriza las distintas amenazas, cuál es el riesgo derivado del uso de las TI, qué nivel de [ciber]seguridad se necesita para disponer de un sistema que funcione y con capacidad para recuperarse de un ataque -resiliencia-⁸. En resumen, la estrategia para defender el valor y anticipar nuevos escenarios de amenazas.

En realidad, la decisión de cómo se utilizan las tecnologías de la información y los riesgos asociados, o lo que se ha llamado «Gobierno Corporativo de las TI», debería formar parte de la agenda de dicho órgano de gobierno. En palabras de la Organización Internacional de Normalización (ISO, International Organization for Standardization), el Gobierno Corporativo es «el sistema mediante el cual se dirige y controla el uso actual y futuro de las TI. [...] ... y es un subconjunto del gobierno de la organización o del gobierno corporativo.»⁹

En iTTi, prestamos atención preferente al gobierno corporativo de las tecnologías de la información por quien tiene, en las empresas y organismos, la obligación y potestad para ejercerlo; esto es, por quien tiene la responsabilidad última de decidir sobre la aplicación y uso de dichas tecnologías en el ámbito de la organización: el Órgano de Gobierno (Consejo de Ministros, Consistorio, Consejo de Administración, Patronato, Rectorado, ..., según el caso).

Ese Órgano de Gobierno ha de ocuparse, además, de identificar a todos los «interesados» (incluidos sus intereses y demandas).

No nos vamos a quejar si las TI se sientan en el consejo aunque sea de la mano de la seguridad ...

¹ url [a 2015.10.18]: <http://dle.rae.es/?w=confiar&m=form&o=h>

² url [a 2015.10.18]: <http://dle.rae.es/?w=confianza&o=h>

³ url [a 2015.10.04]: http://www.nist.gov/itl/upload/OTA_DOC_Cyber-securityGreenPaper-2.pdf

⁴ url [a 2015.10.04] http://politica.elpais.com/politica/2015/07/07/actualidad/1436284983_731864.html

⁵ Palao, Manolo. «Hacia un nuevo contrato social sobre la privacidad y seguridad digitales», abril, 2015. url [a 2015.10.04]: <http://www.ittrendsinstitute.org/perspectives/item/nuevo-contrato-seguridad-digital>.

⁶ url [a 2015.10.18]: <http://www.ponemon.org/blog/what-erodes-trust-in-digital-brands>

⁷ url [a 2015.10.18]: https://ns-cdn.neustar.biz/creative_services/biz/neustar/www/resources/whitepapers/it-security/ponemon-report-2015.pdf

⁸ url [a 2015.10.18]: <https://blogs.mcafee.com/executive-perspectives/fighting-fire-fire-will-lead-us-dangerous-future/>

⁹ "ISO/IEC 38500:2015 applies to the governance of the organization's current and future use of IT including management processes and decisions related to the current and future use of IT. [...] ... defines the governance of IT as a subset or domain of organizational governance, or in the case of a corporation, corporate governance." url [a 2015.10.23].

NUEVA CPU AS/3 IP-X
CERTIFICADA EN NORMAS
UNE-EN 60731 (GRADO 3)
UNE-EN 60732

ACCESOS/INTERFONIA IP
INTRUSION
ALARMAS TECNICAS
CCTV
INCENDIOS

CONTROL DE ACCESOS E INTEGRACION DE SISTEMAS DE SEGURIDAD
www.dorlet.com

DORLET
SEGURIDAD INTELIGENTE

Parque Tecnológico de Alava - C/ Albert Einstein, 34
01510 Miñano Mayor - ALAVA - SPAIN
Tel. 945 29 87 90 Fax. 945 29 81 33 dorlet@dorlet.com

DELEGACION MADRID
C/ Segovia, 65
28005 MADRID - SPAIN
Tel. 91 354 07 47
Fax. 91 354 07 48
madrid@dorlet.com

DELEGACION SEVILLA
C/ San Blas, 11-19, Dpto 111
41006 BARCELONA - SPAIN
Tel. 93 201 10 88
Fax. 93 201 13 78
barcelona@dorlet.com

DELEGACION BARCELONA
C/ San Blas, 11-19, Dpto 111
41006 BARCELONA - SPAIN
Tel. 93 201 10 88
Fax. 93 201 13 78
barcelona@dorlet.com

SAP

ÁNGEL L. GALÁN. PRESIDENTE DEL INSTITUTO DE PROBÁTICA E INVESTIGACIÓN CRIMINAL (IPIC)

«Las técnicas de investigación pueden ayudar a mejorar el trabajo de los profesionales de la seguridad privada»



Fomentar el acceso al conocimiento práctico de la probática e investigación a los profesionales de la seguridad, abogacía, periodismo, criminología, detectives privados, psicología..., así como desarrollar y promover la formación en materia de investigación, son, entre otros, los objetivos que persigue el Instituto de Probática e Investigación Criminal (IPIC). Así lo asegura Ángel Galán -Comisario Principal Honorario del Cuerpo Nacional de Policía-, presidente del IPIC, quien en esta entrevista explica el origen, temáticas, y perfil del profesorado con que cuenta el centro, así como todo aquello que pueden aportar las técnicas y conocimiento de la investigación a los profesionales de la seguridad privada.

CUÁL es el origen del Instituto de Probática e Investigación Criminal (IPIC)?

—Es la idea de una serie de personas, fundamentalmente investigadores, pero también magistrados, periodistas, peritos judiciales, abogados, psiquiatras, detectives privados y directores de seguridad sobre la necesidad de transmitir la experiencia de expertos en investigación de campo, con el fin de que los profesionales que trabajan de una u otra forma en ese área, tengan una mejor formación. Yo recogí ese guante y decidí, junto a otras personas, fundar el Instituto de Probática e Investigación Criminal (IPIC).

—**Como presidente del IPIC, ¿qué le llevó poner en marcha una institución de estas características?**

—Según pasaban los años, iba comprobando la desaparición de buenos investigadores y la falta de formación y de perfil de las personas que iban asumiendo su labor. Era desalentador. En diferentes campos de la investigación, veía huecos de investigación, que las Fuerzas y Cuerpos de Seguridad tenían que ir dejando, por falta de tiempo, como las desapariciones, las sustracciones de obras artísticas o arqueológicas, las sustracciones de material sensible de las empresas, etc., a la vez que comprobaba la formación, a mi juicio, excesivamente teórica, de las instituciones públicas y privadas dedicadas a ese fin.

Por todo ello decidí que era un buen momento de, al menos, transmitir mis experiencias y conocimientos para que

no desaparecieran conmigo, tanto en la investigación propia, como en el diseño de los cursos que había desarrollado para el CNP y para otros cuerpos policiales de diferentes países.

—¿Podría señalarnos cuáles son los objetivos generales que persigue el IPIC?

—Desarrollar y promover la formación en materia de investigación, que sea de interés para profesionales e instituciones públicas y privadas, en el ámbito de los procesos judiciales, desde el momento en que se conoce el suceso que será instruido posteriormente por un juzgado, hasta el momento de la sentencia, con especial profundidad en la investigación de la realidad del hecho y de los diferentes tipos de prue-

ba que pueden realizarse, así como las herramientas que es posible utilizar en este último caso.

Fomentar el acceso al conocimiento práctico de la probática e investigación a los profesionales de la abogacía, periodismo, criminología, psicología, detectives privados, seguridad y cualquier otro profesional interesado.

Impulsar y promover la difusión de obras científicas en el campo de la Probática e Investigación.

—¿Qué tipo de cursos, máster,... ofrece el IPIC y a quiénes van dirigidos?

—Diferentes cursos sobre la amplia materia que el Instituto trata, fundamentalmente en investigación, nego-



«Desde el IPIC se fomenta el acceso al conocimiento práctico de la probática e investigación de los profesionales de la criminología, abogacía, seguridad...»

ciación protección e inteligencia. Buscando siempre la extensión, horarios, materia y ponentes más solicitada por los asistentes a los cursos, las asociaciones profesionales o incluso que la propia sociedad demanda.

Con extensión que va desde un máster, a jornadas y seminarios.

Estos cursos van dirigidos a todos los profesionales, que de una u otra manera están implicados en el área socio jurídica de la investigación. Esto es des-

de investigadores hasta juristas, pasando por peritos de todo tipo, seguridad privada, periodistas, guionistas, empresarios, etc.

—¿Qué temáticas se abordan en los planes de formación del Instituto?

—Todas las que deben investigarse. La desaparición, el homicidio, la negociación, el terrorismo, los delitos contra el patrimonio histórico, los contrarios a la propiedad industrial o intelectual, la protección, la seguridad, la inteligen-



SOLUCIONES AVANZADAS PARA LA GESTION TECNICA DEL EDIFICIO

Sistemas de Control de Accesos y Presencia
 Sistemas de Supervisión (Intrusión, Incendio)
 Video y Audio en entornos TCP/IP (LAN, WAN, INTERNET)
 Control de instalaciones técnicas en edificios

DIVISION DE CONTROL DE EDIFICIOS



www.setelsa.net



cia, los incendios, los delitos dentro de establecimiento turístico, la extorsión, el secuestro, la inteligencia, el compliance, etc.

—¿Cuál es el perfil del profesorado que imparte la formación en el Instituto?

—Los ponentes son todos profesionales en ejercicio activo del tema que tratan o retirados que se han dedicado, en su mayor parte de vida profesional, al tema que exponen. Esto quiere decir, que los ponentes sobre investigación son o han sido durante tiempo investigadores de campo. Los periodistas son redactores de sucesos de medios de carácter nacional o periodistas de investigación con probada experiencia. Los letrados son penalistas de prestigio contrastado. Los que exponen la instrucción son magistrados de instrucción en activo, etc.

—¿Qué nivel, en cuanto a investigación criminal, tienen las Fuerzas y Cuerpos de Seguridad en España, con el resto del mundo?

—El Cuerpo Nacional de Policía fue en sus orígenes un cuerpo exclusivamente de investigación, desde la segunda mitad del siglo XIX, hasta la creación del Cuerpo Nacional de Policía, con la fusión del CGP con la Policía Armada. Actualmente la investigación ha perdido peso en la organización, ganando peso la seguridad en general y sobre todo la de grandes eventos.

La Guardia Civil fue en su inicio más un cuerpo de seguridad rural, aunque en la actualidad ha incrementado el peso en la investigación de todo tipo de delitos y en cualquier zona.

Los otros dos cuerpos autonómicos, se inician con profesionales de los anteriores y con preparación de escuelas de otros países y otras formas.

En síntesis podríamos decir que la investigación sigue existiendo en España. Personalmente creo que la preparación de los investigadores es excesivamente teórica y sin la más mínima información de los profesionales con experiencia, lo que está bajando el nivel.

No hay que remontarse muchos años atrás, para comprobar que los profesores en la Escuela General de Policía de Miguel Ángel eran los responsables

—¿Qué puede aportar el Instituto de Probática e Investigación Criminal en el ámbito formativo a los profesionales de la Seguridad Privada?

—Puede aportar mucho. Como digo existen infinidad de casos que las Fuerzas de Seguridad no pueden hacer frente, por razones muy variadas, y que puede y debe de involucrarse la seguridad privada. Para ello tienen un problema, su preparación.

La preparación tanto de los detectives privados, como los graduados en criminalística es absolutamente teórica, y en esas condiciones es muy difícil hacer

frente a una desaparición, a una desaparición de documentación de una empresa, etc.

Deben de tener una mayor formación, tanto de técnicas, como de conocimiento de cómo funciona el sistema en España y quiénes son los actores.

—¿Cree que las técnicas y conocimiento de la investigación puede ayudar a mejorar el trabajo y cualificación de los diferentes profesionales de la seguridad privada?

—Sin género de duda. Se les enseñará a reconocer los datos que inicialmente son necesarios, a reconocer los datos que las escenas nos muestran, a preparar una hipótesis lógica e ir contrastando sus probabilidades, así como cambiando la hipótesis si los datos que van surgiendo en la investigación así lo entienden.

De cualquier modo creo que los que mejor lo pueden decir, son aquellos profesionales que ya han realizado algún curso con nosotros y valorarán positiva o negativamente nuestro proyecto. ●



IPIC
¿QUIERES APRENDER A INVESTIGAR?
En el IPIC te reunimos, de la mano de los mejores profesionales

El Instituto de Probática e Investigación Criminal ofrece cursos monográficos, genéricos y mixtos que ayudan a los profesionales de todos los ámbitos involucrados en la investigación criminal (criminalólogos, fuerzas y cuerpos de seguridad del Estado, periodistas, jueces, investigadores privados, etc.) a comprender la investigación criminal desde una visión integral que abarca todos los ámbitos. Los contenidos surgen en experiencia real y aplicada que han trabajado en los casos más mediáticos y de mayor impacto social, y brindamos una oportunidad única para adquirir una formación práctica y aplicada de la mano de los mejores profesionales.

Listado de Cursos

- I Curso sobre Investigación de Desapariciones
- II Curso sobre Investigación criminal y probática
- III Curso sobre la Escena del Delito
- Curso de Inteligencia Económica
- Investigación de delitos contra el Patrimonio Histórico
- Curso general sobre investigación delictiva
- Investigación de Incendios
- Situación en Establecimientos Turísticos

IPIC
Tel: 914 52 10 26 info@instituto.org www.instituto.org



PURPLE para videovigilancia

Discos duros para videovigilancia

Cada disco tiene su función.

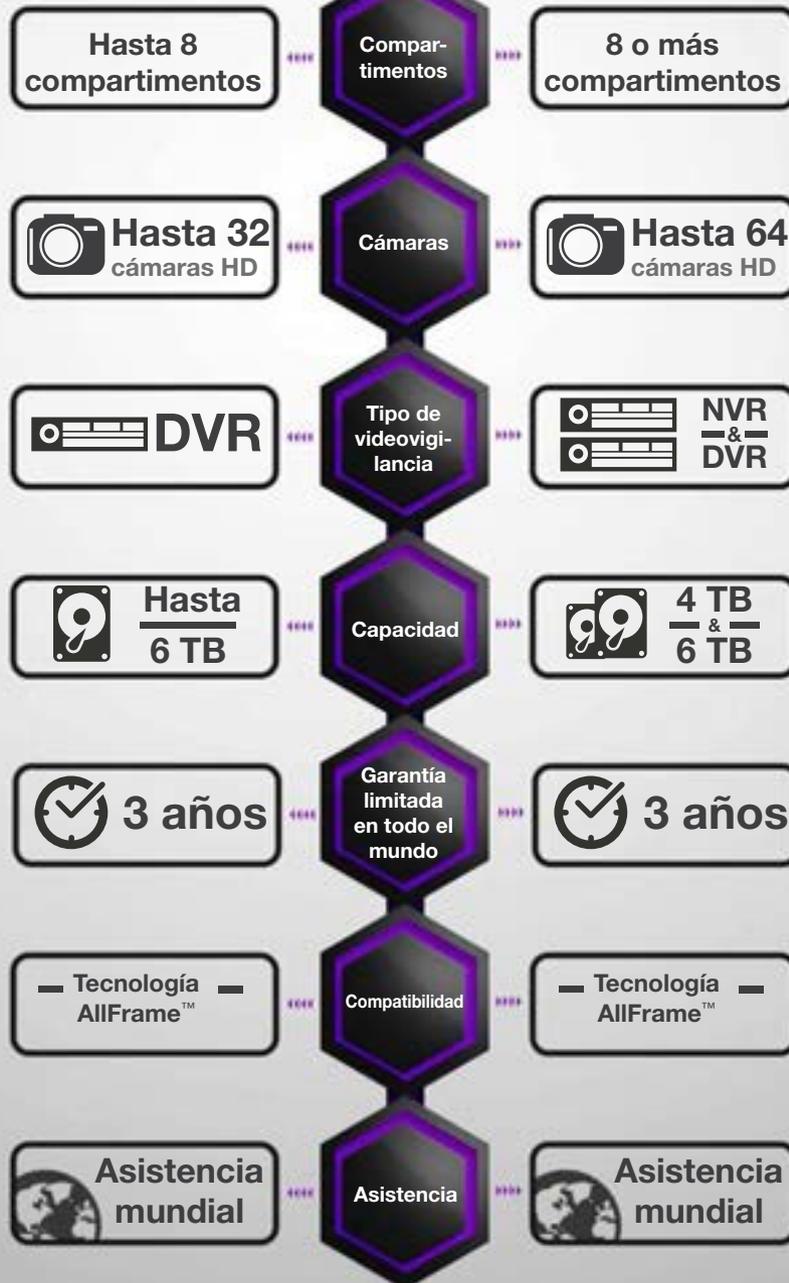
WD Purple™

Sistemas de videovigilancia con grabación de vídeo digital (DVR) para medianas empresas



WD Purple™ NV

Sistemas de videovigilancia con grabación de vídeo en red (NVR) para grandes empresas



JOSÉ JAVIER DE LA ROSA. KEY ACCOUNT MANAGER. ACAL BFI IBERIA

Cómo incide el análisis de imagen en la tecnología térmica



La primera gran duda que nos asalta es qué tecnología utilizar. Hay una regla no escrita que determinará si inclinamos nuestra instalación hacia térmico o visible, las distancias a cubrir. Hoy por hoy, el parámetro que delimita este primer factor podemos asegurar que es la distancia de los 150 metros. Por debajo de esta distancia, las cámaras visibles nos aportan una mejor respuesta a nuestras necesidades. Evidentemente «ve-

Cuando tenemos que diseñar nuestro perímetro de seguridad, siempre surgen varias dudas. ¿Qué topología de red utilizo? ¿Qué software de gestión y edición? ¿Qué hardware para el centro de control? ¿Visible o térmico? ¿Análisis de imagen? Intentaremos dar respuesta a estas dudas, haciendo un especial hincapié en la Analítica de Imágenes.

mos». Además, el reconocimiento e identificación de un objetivo en escena, gracias a la analítica, es inmejorable y la relación solución/presupuesto es importante.

Por lo tanto, si una mayoría de nuestras distancias son superiores a 150 metros, nuestra decisión es fácil, cámaras térmicas.

Una vez dado el primer paso, tenemos que decidir con qué modelos de cámara realizaremos nuestro perímetro. Para ello es importante tener varios conceptos claros. Para explicarlo voy a utilizar la fórmula para hallar las distancias con análisis de imagen:

$$D_{dca} = 1000 / [(C_{imr}) \times \left[\frac{\text{Tamaño del píxel}}{\text{Longitud focal}} \right]]$$

Ddca = Distancia de detección

Cimr = Cantidad de información mínima requerida (en el análisis)

La cantidad de información que mi sistema de análisis de imagen necesita para procesar la identificación de mi objetivo, es el primer factor que determinará, y mucho, la distancia de trabajo. Cuanto menor sea el requerimiento, mayor distancia cubriremos. Hay fabricantes en el mercado cuya información requerida es muy pequeña, 7 ó 5 píxeles en la resolución vertical.

He de decir que 5 píxeles se consigue, por regla general, si la analítica de imágenes está embebida en la cámara.

Otro de los factores determinantes es el tamaño del píxel en el sensor. La mayoría de los fabricantes aportan soluciones basadas en un sensor de 25 micras; podemos considerar que en muchas instalaciones esto será suficiente. Pero si tengo distancias importantes que cubrir, mi recomendación es trabajar con sensores de 17 micras. Tengamos en cuenta que con sensores de 17 micras cubriremos un 32% más de distancia que con uno de 25 micras.

Por último, decidiremos la longitud focal con la que trabajar. Cuanta





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



Ddca 25micras= $1000/(7 \times (25/50))$ → Ddca 25micras= 285,7 metros

Ddca 17micras= $1000/(5 \times (17/50))$ → Ddca 17micras= 588 metros

Esta misma cámara sin analítica de imágenes y siguiendo el criterio Johnson a la hora del cálculo de las distancias nos cubriría 1.267 metros. Por lo tanto debemos pensar que la analítica de vídeo es tan necesaria para cubrir con garantías nuestro perímetro como restrictiva a la hora de atender nuestras necesidades.

Otra de las preguntas que nos hacíamos al principio era qué solución hardware/software busco para mi centro de control. El mercado

más longitud focal, más distancia cubriremos. Esta afirmación tan de «perogrullo» es cierta. Pero pensemos que el vídeo es geometría: si utilizamos una longitud focal de 50 mm, por ejemplo, nuestro perímetro se penalizará en dos ángulos muy a tener en cuenta. Nuestra zona muerta aumentará y nuestro campo de visión en horizontal decrecerá.

Por lo tanto debemos siempre ajustar las distancias de detección con la longitud focal y los ángulos que queremos cubrir. Para ello una recomendación: cuanta menos necesidad de información requiera mi analítica, menos longitud focal necesitaré para cubrir la misma distancia.

«Debemos siempre ajustar las distancias de detección con la longitud focal y los ángulos que queremos cubrir»

Como ejemplo de lo anteriormente desarrollado, realizaremos la fórmula que estamos utilizando con un tamaño de pixel en sensor de 25 micras, 50 mm de longitud focal y 7 pixeles de información; y otro con 17 micras, 50 mm de longitud focal y 5 pixeles de información:

nos proporciona multitud de soluciones. Ante ello, una reflexión, desde mi perspectiva buscaré una solución completa, que en un único producto pueda tener un NVR, un VMS y un panel de alarmas potente. Todo ello me permitirá una integración perfecta de mis necesidades y una solución a todos los problemas de un perímetro bien controlado.

Como resumen, busquemos conjuntar todos los parámetros. Una longitud focal adecuada, un tamaño de pixel de 17 micras, una cantidad de información para mi analítica de imagen de 5 pixeles y un software en mi centro de control potente y que cubra todas mis necesidades. Si todo ello nos lo proporciona un único fabricante, ideal. ●



SIM M2M Alto Rendimiento

Alai Secure



Especialmente diseñada
**para comunicaciones
M2M.**

5 veces más duradera y
resistente frente a condiciones
de uso adversas:

- HUMEDAD - VIBRACIONES
- GOLPES - CORROSIÓN

Soporta temperaturas
de hasta
+105°C y -45°C.

Alai Secure

Operador M2M en Seguridad

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

Educación ejecutiva para los profesionales de Seguridad



Un reto histórico para los profesionales de seguridad ha sido siempre cómo demostrar el valor que supuestamente proporcionan a sus respectivas organizaciones. Pero lo que no es sencillo de por sí, en tiempos de contracción o stress financiero se convierte en excepcionalmente difícil. Además, estos argumentos o casos de negocio se defienden normalmente en el entorno del comité de dirección, el cual es en la mayoría de los casos poco frecuentado por los responsables de seguridad y por definición muy escéptico para los asuntos que no tengan diáfanos y/o que no tengan un impacto directo sobre la cuenta de resultados, y por supuesto preferiblemente en sentido positivo.

ESTE reto, cuyo desafío tiene su origen en los 90s, es convencer a sus organizaciones que son una inversión y no un gasto o centro de costes, los que se imputan directamente al producto, que es lo que son en realidad en la mayoría de las organizaciones, salvo en aquellas en las que exista un fuerte componente de prevención de pérdidas, que no son los casos más habituales. Pero no son los únicos. En realidad no importa mucho otra cosa sobre el papel de las personas o las funciones dentro de una organización: ¿producen dinero para la empresa? o todo lo contrario, ¿son un destructor de ingresos?

Este planteamiento, que algunos opinan que se deriva de un complejo de inferioridad, tiene su origen en la magnificación de los centros de beneficios o profit centers, aquellos que tienen ingresos y costes, y también gastos directos e indirectos, cuya combinación

debería resultar en beneficios. Sin estos no hay negocio, ni por lo tanto empresa. Y esta magnificación tiene su razón de ser en la estigmatización de los centros de costes introducida, entre otros, por el gurú de la empresa Tom Peters hace más de veinte años. Cualquiera que esté incluido en uno o en otro tipo de centro (de beneficios o de costes) podrá establecer con facilidad las grandes diferencias existentes entre ambos. Por un lado, en términos de financiación y asignación de recursos, en el apoyo de la dirección, en la visibilidad, y desde luego en el potencial de carrera individual. Y como consecuencia, en las posibilidades de acceder al comité de dirección, aún ocasionalmente. No muchos se atreven a definir y defender qué centros de costes, o mejor dicho qué centros de costes necesarios, son imprescindibles para que existan centros de beneficios, que por cierto no son autónomos, y asumir la

existencia de otros elementos esenciales para el negocio, por ejemplo, los que lo protegen y facilitan.

Por este motivo los profesionales de seguridad hablan con frecuencia de ROIs (Retorno sobre la Inversión) y otros conceptos relacionados, aunque en ocasiones puedan hacerlo en exceso y fuera de contexto. Tanto como para que algunos confundan que una cosa como un activo se amortice, es decir que su impacto sobre la cuenta de resultados se periodifique a lo largo de varios años, con que sea una inversión por esta razón. Trampa peligrosa especialmente en algunos foros, como por ejemplo el comité de dirección, que es un tribunal de examen extremadamente duro. Por lo tanto, defender de forma general que la seguridad es una inversión corresponde más a un lenguaje coloquial con un recorrido limitado que a la realidad de los hechos y los números.

Tanto es así, que un creciente colectivo de profesionales consideran que la seguridad no es una inversión, aunque obviamente si lo pueda ser alguna de sus consecuencias o acciones. Lo que por otro lado, no debería afectar a su necesidad y existencia. Por ejemplo, durante la última edición del curso *Effective Management for Security Professionals*, organizado por la IE Business School en Madrid, con la colaboración de ASIS International y ASIS España, se estudió el interesante caso del relevo tecnológico en el modelo de control de accesos electrónico integrado en una de las terminales de un aeropuerto. Pero se trataba de justificar una inversión a través del ROI comparando un gasto corriente real y actual con uno inferior en el futuro, lo que obviamente justificaba plenamente la inversión. ¿Cómo se hubiera planteado entonces la adquisición de un control de accesos electrónico integrado cuando se construyó la terminal? ¿Dónde estaba el ROI en ese momento?

Siguiendo esta hipótesis se puede determinar que la seguridad no es una inversión, si no un coste o gasto necesario, dependiendo en qué parte del proceso productivo se impute, como hay otros casos dentro de una organización y algunos son simplemente imprescindibles. Un término, el de coste o gasto necesario, que ahora aceptan los gurús después de largos años de castigar a los centros de costes. Por ejemplo, el departamento legal, con el cual existen muchas similitudes. Por un lado, previniendo riesgos desde una primera línea de defensa exterior y, por otro, si alguno de estos se ha materializado, controlando y minimizando el impacto negativo de un evento ocurrido con la respuesta adecuada. A propósito, que ahora también el compliance o el cumplimiento regulatorio debería unir todavía más a los departamentos de seguridad con los



de asuntos legales en un enfoque claramente convergente.

En segundo lugar y más recientemente, la opinión incide de forma creciente en determinar como un objetivo estratégico para los responsables de seguridad el de acceder al comité de dirección, ese grupo selecto de ejecutivos –los más importantes e influyentes– que dirigen las organizaciones. Como es selecto, por definición, suele ser limitado en número.

Es fácil compartir su interés por formar parte del comité de dirección, que es más que lícito y que está motivado no por una ansia de protagonismo, sino por el deseo de participar en el diseño y desarrollo de la estrategia de la organización, y así poder influenciar desde la perspectiva de seguridad sobre los diferentes aspectos que forman parte de esta y de las operaciones de la empresa desde una fase temprana, incluso de diseño y planificación. Sin embargo parece que los perfiles, los conocimientos, las habilidades y la experiencia necesarios para formar parte del comité de dirección son algo divergentes con los que siempre han caracterizado a

los profesionales de seguridad. Pero como casi todo en la vida, el desajuste podría tener arreglo y este es precisamente el objetivo final de este artículo. Uno y otro, la seguridad como una inversión y el acceso e incluso la presencia de los responsables de seguridad en el comité de dirección, están estrechamente relacionados. Los conocimientos y la experiencia, no sólo los de la especialización en seguridad sino los generales compartidos con el resto de los directivos, y el respeto dentro de la organización, llevan al comité de dirección y desde este no sólo es posible participar en la definición de la estrategia, también participar incluso en su génesis.

No debe existir duda alguna de que en las circunstancias actuales del mundo empresarial, globalización, entornos complejos y hostiles, múltiples y nuevos riesgos y amenazas asimétricas, etc., el tratamiento del riesgo se ha convertido –o al menos debería haberlo hecho– en un asunto de la máxima importancia para la estrategia de las organizaciones, incluso en una parte nuclear de éstas. Pero no parece probable que en el comité de dirección haya sitio para todos los que tienen como supuesto objetivo del tratamiento de los riesgos de alguna u otra naturaleza. Lo que si lo es que la situación actual no puede perdurar mucho en el tiempo, y es necesario una única cabeza que gestione el tratamiento integral del riesgo dentro de las organizaciones. Y que lo haga precisamente desde el comité de dirección.

Retrocedamos por un momento a 1995 cuando Ira Somerson CPP, un consultor de seguridad norteamericano, publicada en la revista *Security Management* un artículo titulado «La Próxima Generación». El artículo comenzaba así, no lo olviden, hace 20 años: «la seguridad corporativa ha sido reactiva,



más preocupada en resolver crisis que en enfocar proactivamente las necesidades del negocio. Pero la seguridad está cambiando y los profesionales de esta disciplina deben hacerlo con ella. En el futuro, los profesionales de seguridad necesitan desarrollar más conocimientos y experiencia empresariales. Sus habilidades anteriores continuarán siendo importantes para la misión de seguridad, pero la mayoría de las posiciones directivas serán ocupadas por aquellos profesionales con mayores conocimientos y capacidades directivas».

Para trazar el argumento de su artículo, Ira Sommerson establecía determinadas teorías y se atrevía a realizar una previsión del futuro, cuya asertividad dejamos a juicio del lector. A los efectos de este artículo vamos a concentrarnos en cuatro. La primera era la expansión de los mercados globales donde la actividad se prolongará 24 horas al día y donde los directivos del siglo XXI, incluidos por supuesto los de seguridad, tendrían que adaptarse e integrarse en una fuerza laboral multinacional, multicultural y ahora se podría añadir, multidisciplinar. La segunda era que las empresas iban a continuar reduciendo su tamaño en términos humanos, lo que se denomina *downsizing*, y por lo tanto los empleados deberían estar preparados para integrarse dentro de su industria o migrar a otras para sobrevivir. Una importante derivada

de esta predicción será la pérdida de lealtad de los trabajadores hacia sus organizaciones incrementado los riesgos de seguridad. La tercera conclusión era, refiriéndose en concreto a los departamentos de seguridad, que en los próximos 20 años, si estos no eran capaces de absorber otras funciones, otras unidades de negocio lo harían con ellos. ¿Puede existir alguna relación entre esta predicción y la primera y la segunda convergencias?

Por último, Sommerson determinaba que la profesión de seguridad debería sufrir drásticos cambios y mejoras en los próximos años para posicionarse dentro de la comunidad empresarial. Por un lado, la gestión de seguridad debería ser incluida en los programas de formación de ejecutivos, para que los líderes de las empresas del futuro conocieran lo que significa esta función hoy y cómo puede afectar positivamente al futuro de sus empresas. Por otro, los ejecutivos de seguridad deberían transformarse en mejores gestores del riesgo y adquirir conocimientos no solo sobre su especialidad, sino también sobre marketing y la administración de empresas, y otros campos relacionados. Hoy los extenderíamos sin temor a equivocarnos a otras disciplinas como la negociación, capacidades de liderazgo y gestión de equipos, estrategia empresarial, comportamiento organizacional, etc.

Para Sommerson muchos iban a negarse a aceptar el cambio por estar muy cómodos con el *status-quo*. Ese ciclo, continuaba el autor, era cómodo pero dañino. Su aislamiento del corazón del negocio había sido la causa de la desaparición de muchos departamentos de seguridad en EEUU. Finalizaba el artículo con el siguiente párrafo. «Las empresas van a enfrentarse a nuevas amenazas que van a aparecer poco a poco. No todos estos riesgos se desarrollarán anticipadamente, pero los profesionales de la seguridad que amplíen sus conocimientos y habilidades, así como los que posean la mejor red de contactos con los que intercambiar información serán los mejor preparados para enfrentarse a los desafíos que acechan a corto y medio plazo.

Quizás fue una casualidad, pero sólo cuatro meses más tarde la misma revista publicada un artículo escrito por William Willie titulado «¿Puede la seguridad ser el camino hacia el comité de dirección?». Para el autor, los profesionales de seguridad eran extraordinariamente defensivos y conservadores en relación con su actividad y su contribución a los objetivos corporativos, y preferían el confort de lo conocido a progresar hacia delante y asumir riesgos. Quienes no tuvieran oportunidad de progresar hacia la gestión senior estaban condenados a ser arrinconados como especialistas, y este era un denominador muy extendido entre los profesionales de seguridad. ¿Ha cambiado algo desde entonces? Si lo ha hecho, pero todavía queda un largo camino por recorrer.

En 2004 ASIS International publica la directriz del Chief Security Officer, (el director de Seguridad senior) que en 2008 se convertía en un estándar ANSI/ASIS. El modelo es coherente, razonable y visionario. El cuadro que recoge los riesgos, los procesos y servicios; y las capacidades y habilidades

Stand
10D16



23-26
Feb.
2016

Nuestro objetivo es
facilitar la videovigilancia
profesional para todos



Visión de 360 grados en una sola imagen para que no pierda detalle.

La capacidad de ver todo en una sola imagen es un gran beneficio. Los puntos ciegos pueden minar seriamente la fiabilidad de su solución de videovigilancia. A partir de ahora, usted nunca tendrá que perder un solo detalle con la **vista panorámica de 360 grados** proporcionada por la cámara FLEXIDOME IP panoramic 5000 MP. Obtenga más información en www.boschsecurity.es. Visítenos en SICUR en el stand 10D16.



BOSCH

Innovación para tu vida

requeridas es una referencia pero adelanta la dificultad para encontrar perfiles profesionales capaces de asumir el rol del CSO de acuerdo con este perfil. Muchos de los criterios y terminología son nuevos y poseen una fuerte carga empresarial y ejecutiva. Por otro lado, han provocado actitudes defensivas en algún colectivo potencialmente afectado, no sólo por la vía de los riesgos si no también por la de los procesos. ¿Recuerdan? Absorber o ser absorbidos. La última versión de este documento, de 2013, depura aún más el perfil del CSO y simplifica su cuadro de mando, pero destaca aún más las habilidades del que ahora denomina líder ejecutivo. Estas incorporan nueva terminología y capacidades puramente empresariales y ejecutivas bastante alejadas de las que caracterizan tradicionalmente al sector. Por ejemplo, la agilidad estratégica; la compostura; la capacidad de escuchar; las habilidades para presentar y persuadir; el coraje directivo; las comunicaciones escritas; la motivación de terceros; y, citando textualmente, la gestión de la ambigüedad o la gestión de la visión y el objetivo.

Dejo al criterio de los lectores la vinculación entre la publicación de esta directriz y luego estándar, y la puesta en marcha, primero del curso de educación ejecutiva de ASIS/Wharton en Estados Unidos en 2008, y más tarde el de ASIS y la IE Business School en Madrid en 2010. ¿Cuáles son los objetivos comunes de estos dos programas de formación ejecutiva? Pues precisamente desarrollar programas de formación ejecutiva destinados a los profesionales de seguridad para

- Entender los retos empresariales a los que se enfrentan las empresas hoy en día.

- Desarrollar conocimientos estratégicos del papel de la gestión de la seguridad como clave para el éxito empresarial.

- Defender sus iniciativas en materia de seguridad para garantizar la financiación.

- Convertirse en líderes eficaces en un entorno no jerárquico y en diversas áreas funcionales.

Pero no sólo para tener como objetivo estratégico final acceder al comité de dirección como CSO, sino simplemente para desarrollar la profesión adecuadamente en el entorno actual y previsiblemente futuro de las empresas. La tendencia ha dibujado una línea per-



fectamente definida desde entonces. Y no faltan opiniones, documentos e informes que la soporten.

A finales de 2013 la ASIS Foundation y la Universidad de Phoenix publicaban un interesante estudio titulado «Los riesgos de seguridad de las empresas y las competencias necesarias de los profesionales de esta actividad». Este informe tenía como objetivo identificar los mayores riesgos a los que iban a enfrentarse las empresas en los próximos cinco años, y al mismo tiempo definir las competencias profesionales de los responsables de gestionar la seguridad en estas. Los primeros confirmaban

las previsiones del consenso. La ciberseguridad, con el componente de la dificultad de detección en muchos casos, y el énfasis para que los profesionales de seguridad física mejoren sus capacidades de seguridad lógica; las tecnologías móviles, cuya utilización se había multiplicado exponencialmente haciendo lo mismo con la vulnerabilidad de las organizaciones; la globalización y todas sus connotaciones, con la proyección del ámbito geográfico de la responsabilidad desde un entorno local y conocido a uno global y desconocido, la externalización de procesos críticos como el tratamiento de los datos o la cadena logística; los desastres naturales, incrementados por el cambio climático y la propia globalización; y por último, la delincuencia, desde el fraude y el robo interno hasta el crimen organizado o el terrorismo nacional e internacional.

Pero desde la perspectiva de este artículo, lo realmente interesante, eran y son las conclusiones del informe sobre las competencias que deben tener los profesionales de seguridad cara a los próximos años. De las ocho, ninguna correspondía al catálogo tradicional salvo la Gerencia de Riesgos Integral (ERM), pero la mayoría estaban incluidas en el perfil del CSO de 2008 y el resto lo han sido en la versión actualizada de 2013. Estas abarcan desde la gestión de empresa y financiera; hasta la formación y educación continua, como lo hace el negocio y los riesgos que le acechan; pasando por las habilidades de liderazgo y comunicación; la mentalidad estratégica y anticipatoria, para identificar y adelantarse a los riesgos nuevos y emergentes y formular respuestas; las competencias STEM, relacionadas con las tecnologías y mucho con la convergencia entre la

seguridad física y la lógica; y la multidisciplinariedad, con la formación asociada que les permita ampliar su rango de conocimientos y capacidades, con una consistente educación y un fundamento consolidado en el área de la empresa.

Además, los retos resaltaban la falta de educación y formación estandarizada y de certificaciones, algo común en estos últimos años. Se trata de conseguir lo que Valles-Calls denomina «un profesional de seguridad con un cerebro integrado», que combina esta especialidad (la seguridad) con un profundo conocimiento de la gestión con habilidades técnicas, y que utiliza nuevas aplicaciones y otras herramientas para alcanzar determinadas necesidades de seguridad específicas.

Los departamentos de Seguridad se enfrentan a los importantes cambios en la gestión que están sufriendo sus organizaciones. Sus miembros han volcado su centro de gravedad en los temas relacionados con su función, pero han puesto muy poco interés en desarrollar sus conocimientos como ejecutivos. Esta circunstancia está limitando su acceso a la mesa desde la que se planea la estrategia de las empresas. Afirma el CSO de una empresa de EEUU, «uno de nuestros mayores retos es que no perciben nuestro trabajo como un elemento de valor para la organización. Y nosotros como profesionales de la seguridad somos los responsables de un nuevo riesgo en nuestro portfolio no demostrando este valor».

Determinantes conclusiones con una muy importante vinculación de todo lo que hemos hablado hasta ahora: La Próxima Generación, al artículo de

Willie, el perfil del CSO, etc. Pero no hemos acabado todavía. En opinión de muchos analistas, uno de los defectos que caracteriza a este sector es la falta de autocrítica, el alojamiento en el confort y la aversión a los cambios, y una cierta visión endogámica de la profesión y su situación. Por eso debemos analizar y valorar con especial atención la opinión que, terceros con referencias contrastadas, puedan dar sobre nuestra actividad.

Hace sólo unos meses la revista Risk UK publicaba un interesante artículo titulado «La profesión de Seguridad: cuatro retos que deben ser resueltos». En él, su autor, David Thorp, consejero de



legado del Security Institute de UK, sin ninguna vinculación previa con el sector, definía los que para él eran estos cuatro retos. Para empezar, según sus propias palabras, lo primero que le había llamado la atención, y más procediendo del mundo del marketing, era el escaso diálogo existente entre la seguridad y el negocio. Seguidamente opinaba que «para desarrollar el perfil de seguridad era necesario alcanzar un estadio en el que esta función estuviera representada en el comité de dirección. La seguridad continúa siendo vista como un coste en lugar de un facilitador del negocio y un elemento de

valor añadido». Para Thorp, «esta profesión hacía muy poco para desarrollar la vertiente de la formación y la educación en el ámbito del negocio» y si se quería evolucionar hacia delante «era necesario influenciar a través de una nueva generación de profesionales que estuvieran al nivel del comité de dirección». ¿Pero como hacerlo?

Han pasado 20 años después del artículo de Ira Somerson y siete desde la introducción del estándar del CSO.

Lo comentamos al principio de este artículo. Primero una firme disposición por demostrar que la seguridad es una inversión. A lo mejor es un enfoque mejorable. Más recientemente,

el establecimiento como deseo por acceder al comité de dirección, desde donde se considera se puede hacer un mejor trabajo en la definición e influencia en la estrategia de las organizaciones. Como hemos visto, ambas cosas están estrechamente relacionadas.

En este momento podemos considerar que hay tres acciones cuya combinación podrían facilitarnos al acceso al

comité de dirección como profesionales de seguridad o incluso como directores de un área diferente después de haber sido responsables de seguridad. Pero no olvidemos que el comité de dirección está formado por una élite de profesionales que en teoría están extraordinariamente preparados desde el punto de vista técnico (todos tienen un pasado profesional como especialistas) y desde el punto de vista gerencial. Se sienten una élite, dentro de su empresa lo son, y además ejercen como tal.

La primera sería la evolución desde la seguridad convencional al modelo más avanzado. Desde la protección

física de los activos a finales de los 80s; y la protección de los activos físicos y de los intangibles en los 90s y principios de la anterior década. Hasta proporcionar valor añadido hace sólo un lustro. Lo que solo se puede conseguir a través de la protección de la cuenta de resultados y la protección del balance mediante una interpretación integral de la seguridad y la gerencia de riesgos. Y hacerlo a través de la primera y ahora de la segunda convergencia, y no precisamente incrementando los ingresos, sino mediante la reducción de los costes ciertos y potenciales. Y también de la incertidumbre que nos acecha.

Y en la actualidad, cara el futuro, mediante la integración de la seguridad y la gerencia de riesgos como un elemento nuclear de la estrategia de una organización. Y es este modelo y cómo llegar a él a través de las tres acciones anteriores, el que nos podrá llevar hasta el comité de dirección. Cuando nos vean como ejecutivos especializados en seguridad y no como puros profesionales de seguridad. Esto conlleva formación y educación técnica continuas, y certificaciones como el CPP, y una inmersión profunda en el concepto del ERM. Los responsables de seguridad que operan en el entorno ERM con solvencia continuarán siendo relevantes para sus organizaciones. Deben sincronizarse con el resto de departamentos y los objetivos del negocio. El ERM debe ser visto como una tremenda oportunidad de futuro. Como un profesional de seguridad pueda contribuir en el ERM de su organización, según Control Risk, depende de su conocimiento actual y futuro, de sus habilidades y actitudes, de su perspicacia empresarial y de su capacidad de liderazgo, y muchos de estos elementos pueden ser aprendidos si uno tiene el deseo de aprender.

La segunda se focaliza en la educación ejecutiva para profesionales de seguridad, en los cursos de ASIS Inter-

national en la IE Business School y Wharton. Lugares donde aprender, mejorar y ordenar los conocimientos ejecutivos necesarios que requieren las condiciones actuales del entorno para el desarrollo profesional. Les ayudarán además a no sentirse extraños en un ambiente ejecutivo y a que no los sientan ajenos. ¿Deberíamos formar y educar a los ejecutivos del negocio para que entiendan la seguridad o deberíamos formar y educar a los profesionales de la seguridad para que entiendan el negocio?, se pregunta Steve Chuppa, director de seguridad global de Johnson & Johnson. De cualquier forma los profesionales de seguridad deben hablar el mismo lenguaje que los ejecutivos de sus organizaciones y como estos deben contribuir en la planificación de una estrategia de gerencia de riesgos y seguridad alineada con los objetivos de la organización.

La tercera y última no está tan dentro de nuestro alcance, pero hay un magnífico trabajo por hacer. Se trata de extender a la comunidad ejecutiva (si es posible en una fase temprana) los conocimientos de seguridad que son necesarios para sus organizaciones. Se trataría de sembrar el conocimiento y

las inquietudes entre los ejecutivos del futuro para que conozcan la seguridad y sus posibilidades reales, lo que es obvio que no sucede ahora.

Los líderes de seguridad del futuro deben cambiar desde la norma a la razón; hablar el lenguaje del negocio; evolucionar desde la seguridad a los riesgos; y combinar su experiencia y conocimiento específico con la comprensión de los objetivos del negocio, las métricas y los procesos que permitan a las organizaciones preparar los casos de negocio para invertir o mejor dicho para afrontar su coste con el fin de maximizar las oportunidades, Control Risk dix-it. Lo define muy bien esta empresa en uno de sus últimos informes. Desde las armas, las garitas y los vigilantes hacia el asesoramiento estratégico del negocio. Para ello, el lugar adecuado parece el comité de dirección, a donde sólo se puede acceder siguiendo una bien planificada hoja de ruta.

Algunos incluso se atreverían a decir: menos armas, garitas y vigilantes, y menos confort; y más educación, enfoque y práctica ejecutiva. ●

Fotos: Asis España





www.safirecctv.com



Ref. TESTER7-IP-3HD



Ref. TESTER4-IP-3HD

NUEVOS TESTER UNIVERSAL 4.3" y 7"

- HDCVI
- HDTVI
- IP ONVIF
- ANALOG
- AHD

La herramienta definitiva para los Instaladores



IP Test para Cámaras IP Onvif
Conexión Ethernet
LAN / WiFi / PoE



Pantalla LCD Táctil | 4,3" Ref. TESTER4-IP-3HD
7,0" Ref. TESTER7-IP-3HD



Multímetro Digital
Test | Video / PTZ / Audio
Alimentación / Cable



Sistema Android
Aplicaciones de los principales fabricantes



TDR Cable Test (Ref. TESTER7-IP-3HD)
Localiza y ubica roturas en cable coaxial



UNIVERSAL
Compatible con las principales tecnologías
HDCVI / HDTVI / IP / ANALÓGICO / AHD

Distribuidores oficiales:



www.jmsystems.es



www.avantech.info



www.visiotech.es

JOSÉ MARÍA GARCÍA DE PRADO. DIRECTOR DE SEGURIDAD, PERITO JUDICIAL Y FORMADOR EN SEGURIDAD PRIVADA



Acercamiento a la deontología profesional en la seguridad privada (I)

Principios básicos de actuación y el deber de colaboración con la Seguridad Pública. Infracciones administrativas y penales

«Las normas en sí carecen de valor práctico, a menos que su contenido y significado, mediante la educación y capacitación, y mediante vigilancia, pasen a ser parte del credo de todo funcionario encargado de hacer cumplir la ley». Estas palabras escritas en el Código de Conducta para funcionarios encargados de hacer cumplir la ley y aprobado por Naciones Unidas en la Resolución 34/169 de 1979, son con las que quiero empezar esta aproximación sobre la Deontología Profesional en la Seguridad Privada.

CON ello quiero expresar que la formación en valores morales y, por supuesto, desde la libertad es necesaria y debe transmitirse atendiendo a lo especial de los deberes profesionales que enmarcan los trabajos policiales, e incluyo, por tanto, a todo el elenco que forma la Seguridad Privada. Puesto que, aunque subordinada a la Seguridad Pública, ésta forma parte por medio de las atribuciones que le delega el Estado como garante de los derechos y libertades de los ciudadanos, esenciales en un estado de derecho.

Tradicionalmente la Seguridad Pública era ejercida exclusivamente por el

Estado y considerado uno de los pilares de nuestra convivencia. Sin embargo, con la evolución de nuestra sociedad, se han desarrollado otras demandas de seguridad más privativas, a las que la Seguridad Pública no puede acceder. Es por esto, por lo que considero necesario para poder mantener ese pilar, anteriormente mencionado de la convivencia, que la Seguridad Privada con sus empresas, su personal, sus medios y sus instalaciones estén sujetos a un control oficial y legislativo, y con ello se pueda dar respuesta a la prevención e intervención de determinadas actividades delictivas.

Continuando con la reflexión, el simple hecho de quedar integrada la Seguridad Privada en el monopolio estatal de la Seguridad como actividad complementaria y subordinada ha hecho que aparezcan leyes como la 05/2014 de 4 de abril, de Seguridad Privada, con su respectiva reglamentación –desarrollándose en estos momentos– e instrucciones, que pretenden facultar a los servicios y personal privados para realizar parte de las atribuciones delegadas y, así, las Fuerzas y Cuerpos de Seguridad del Estado puedan desarrollar plenamente la misión constitucional de proteger los derechos fundamentales de todos los ciudadanos y garantizar su seguridad conjuntamente con el sector de la Seguridad Privada.

Y acomodando como premisa de partida todo esto, tendremos que convenir que el Código Deontológico profesional ha de ser compartido entre los miembros de las Fuerzas y Cuerpos de Seguridad y los de Seguridad Privada. Ya que estos últimos, en asunción de competencias en seguridad por las empresas, también pueden verse en la



posibilidad que sus empleados puedan limitar derechos y libertades de ciudadanos. Y en consecuencia, tal y como se expresa en el Preámbulo de la actual Ley de Seguridad Privada, se reconoce en su exposición de motivos: « (...) la seguridad privada se considera una parte indispensable del conjunto de medidas destinadas a la protección de la sociedad y a la defensa de los derechos y legítimos intereses de los ciudadanos.»

Teniendo en cuenta todo lo anteriormente expuesto, la Deontología Profesional en el ámbito de la Seguridad Privada ha de venir inspirada en los principios morales básicos y reglas éticas que se establecen en el Código de Conducta para funcionarios encargados de hacer cumplir la ley (Resolución 34/169 de la Asamblea General de Naciones Unidas), Declaración sobre la Policía (Resolución 690/1979 de la Asamblea Parlamentaria del Consejo de Europa) y Código Europeo de Ética de la Policía (Recomendación Rec. (2001) 10 del Comité de Ministros del Consejo de Europa).

–Código de conducta para funcionarios encargados de hacer cumplir la ley.

Es un texto en el que se aportan varias medidas importantes, a modo de requisitos previos, para garantizar

la protección de los derechos e intereses de la ciudadanía a quienes dichos funcionarios sirven. Para ello se estipula que: todo órgano de aplicación de la ley debe ser representativo de la comunidad en su conjunto, obedecerla y responder ante ella; que debe tener un sistema de leyes bien concebido, aceptado y humanitario; que la conducta del funcionario repercute directamente en el sistema; que la autodisciplina estará sujeta al escrutinio público; y, por último, que requiere el principio de convicción propia. El texto continúa con una serie de artículos que en resumen exige que se debe cumplir las leyes sirviendo a la comunidad, protegiéndola de ilegalidades, respetarán y protegerán la dignidad humana y los derechos humanos de éstas, usarán la fuerza cuando sea estrictamente necesaria, mantendrán secreto profesional, no podrán ni tolerarán torturas, tratos inhumanos, penas crueles, etc., protegerán la salud de los custodiados y no podrán cometer e impedirán actos de corrupción.

–Declaración sobre la Policía.

En este texto, la Asamblea en sus consideraciones estima la importancia de la Policía de los Estados miembros cuando admite que su labor se desa-

rolla en condiciones peligrosas, y sumando que sus funciones se complican porque las reglas no están definidas con suficiente precisión; que la policía se reforzará si posee un Código Deontológico que tenga en cuenta los derechos y libertades fundamentales; que la Policía debe contar con el apoyo de la comunidad a la que sirve; y que deben de disfrutar de un estatuto de derechos comparables a los que poseen otros funcionarios del Estado.

Seguidamente a las consideraciones, este texto incluye 16 artículos sobre ética profesional en el que se intenta determinar una conducta ideal en los que a modo de resumen cabe destacar el cumplimiento de los deberes que le impone la ley; actuaciones íntegras, imparciales y dignas evitando corruptelas; evitar e ignorar órdenes que impliquen torturas o tratos inhumanos; ejecutar las órdenes de sus superiores y abstenerse de cumplir las que sean ilegales; oponerse a violaciones de la ley y prevenirlas; evitar las consecuencias de las mencionadas violaciones; no participar en arrestos, búsquedas, etc., de personas sin haber cometido ilegalidades; será responsable de sus propios actos; actuar con la determinación necesaria; obtener instrucciones claras y precisas; velar por la salud de los custodiados; guardar secreto profesional; y por último, algunos otros más que competen a la protección de garantías.

Esta Declaración sobre la Policía también incluye un apartado denominado Status, en el que por medio de 11 artículos, especifica los derechos de formación y las condiciones profesionales del ejercicio de la profesión.

–Código Europeo de Ética de la Policía.

En este Código, y más concretamente en la definición del campo de aplicación, el Código Europeo de Ética de la Policía se aplica tanto a las fuerzas o

cuerpos de policía públicos tradicionales como a otros órganos autorizados y/o controlados por los poderes públicos, cuyo primer objetivo consiste en asegurar el mantenimiento del orden en la sociedad civil y que son autorizados por el Estado para ejercer la fuerza y/o poderes especiales para conseguir este objetivo. Es decir, en realidad este Código se dirige principalmente a la Policía tradicional pública (Policía del Estado), sin embargo, existen funciones de Policía que pueden ser confiadas a otros estamentos u órganos privados – como por ejemplo puede ser la Seguridad Privada–, pero recalando intrínsecamente que con independencia de saber si las funciones las realiza la Seguridad Pública o la Privada, ésta estará autorizada y/o controlada por los poderes públicos.

Se consideran, a continuación, que los principales fines de la Policía (y en extensión a la Seguridad Privada) en una sociedad democrática consisten (según los ámbitos detallados):

—**Objetivos.**

- Mantener la tranquilidad pública, la ley y el orden.
- Prevenir y combatir la delincuencia.
- Proteger y respetar los derechos y libertades fundamentales de los Derechos Humanos.
- Dar asistencia y servicio a la población.

—**Bases jurídicas.**

- Es el órgano público establecido por la ley.
- Las operaciones deben llevarse de acuerdo con la legislación nacional e internacional.
- El ciudadano debe tener acceso a la legislación policial, que debe ser clara y precisa.
- El personal de la policía debe estar sujeto a la misma legislación que el resto de los ciudadanos.

—**Relación con el sistema judicial penal.**

- Clara distinción entre funciones policiales, de la fiscalía, la adjudicación y el sistema penitenciario.
- Se respetará la independencia e imparcialidad de los jueces.
- No se ejercerá funciones judiciales. La delegación de estas funciones será prevista por ley.
- Asegurará la cooperación entre policía y Ministerio Fiscal.
- Respetará el papel de los abogados defensores y contribuirán a garantizar este derecho.
- No sustituirá al personal penitenciario, salvo urgencia.

—**Organización de las estructuras.**

- Ganarse el respeto de la población como garantes de la ley.
- Ejercer sus funciones bajo la responsabilidad de autoridades civiles.
- Podrán ser reconocidos fácilmente por su uniforme.
- Disponer de independencia operativa ante otros cuerpos del Estado.
- Deben ser responsables de sus acciones.
- La cadena de mando debe definirse claramente.
- Fomentar buenas relaciones entre policía y ciudadano y otros organismos.
- Estar preparado para dar información objetiva sobre sus actividades sin desvelar informaciones confidenciales.
- Garantizar la integridad de la plantilla y el respeto al Convenio Europeo de los Derechos Humanos.
- Prevenir y combatir la corrupción en todos los niveles de la organización policial.

- Reclutar en función de las capacidades y experiencias adaptadas a los objetivos de la policía.
- Poseer capacidad de discernimiento, actitud abierta y habilidades comunicativas.
- Incapacidad en caso de condenas por infracciones graves.
- Criterios de reclutamientos objetivos y no discriminatorios. Han de ser reflejos de la sociedad.
- La formación se basará en los valores fundamentales de democracia, Estado de Derecho y los derechos humanos.
- La formación debe estar abierta a la sociedad.
- La formación inicial se complementará con continuada y con especializada.
- La formación incluirá el correcto uso de la fuerza, teniendo en cuenta los derechos humanos.
- La formación incluirá el combate del racismo y la xenofobia.





BEYOND SECURITY

KABA[®]

Un único lenguaje: El de su seguridad

Todos sabemos que para hablar un idioma se necesita el vocabulario adecuado. Al igual que para un sistema de control de acceso se necesitan las herramientas y componentes adecuados.

En Kaba sabemos que no todas las puertas se abren y se cierran de la misma manera. Por esta razón, se desarrolló una solución capaz de integrar cualquier tipo de puerta, no importa si se trata de una puerta sencilla con una cerradura mecánica, una puerta con un control de acceso autónomo o una puerta conectada que requiere todo el potencial de un control de acceso a tiempo real.

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



- El personal policial debe tener los mismos derechos civiles y políticos que el resto de los ciudadanos.
- Se beneficiará de derechos sociales y económicos tan ampliamente como sea posible y teniendo en cuenta el carácter especial de su labor.
- Las medidas disciplinarias deben estar bajo control de un órgano independiente o tribunal.
- Las autoridades apoyarán al personal policial acusado infundadamente.

—Principios de acción/ intervención.

- Debe respetar el derecho a la vida.
- No debe tolerar ningún acto de tortura ni trato degradante.
- Sólo puede hacer uso de la fuerza cuando sea estrictamente necesario y para obtener un objetivo legítimo.
- Debe comprobar la legalidad de las acciones que quiera llevar a cabo.
- Debe ejecutar las órdenes de sus superiores, excepto aquellas que claramente sean ilegales.
- Desarrollará sus funciones de forma justa, imparcial y sin discriminar.
- Respetará los principios de protección de datos.
- Deberá tener siempre presente los derechos fundamentales de

las personas: libertad de pensamiento, de opinión, de conciencia, de religión, de expresión y de reunión.

- Actuar con integridad y respeto a la población y a los más vulnerables.
- Se identificará como miembro policial en las intervenciones.
- Se opondrá a cualquier forma de corrupción.
- Las actuaciones deben basarse en sospechas razonables.
- Debe respetar la presunción de inocencia.
- Debe ser objetivo y equitativo teniendo en cuenta las necesidades específicas de las personas (niños, minorías étnicas, personas vulnerables, etc.)
- Debe garantizar un interrogatorio justo.
- Tendrá en cuenta las necesidades específicas de los testigos, su protección y asistencia.
- Tendrá en cuenta el apoyo, la asistencia y la información de las víctimas sin discriminaciones.
- Facilitará los servicios de interpretación y traducción durante la investigación.
- Debe limitarse tanto como sea posible y consignar un registro de las detenciones bajo custodia.
- Tendrá que informar de las razones de la detención, acusaciones y procedimiento.
- Velará por la seguridad, la salud, la higiene y la alimentación del custodiado.
- Se facilitará la comunicación de una tercera persona, asistencia médica y acceso a un abogado por parte del privado de libertad.
- Se separará a las personas detenidas por infracción penal de otras, hombres de mujeres, mayores de menores, etc.

—Responsabilidad y control.

- La policía responderá delante del Estado, de los ciudadanos y sus representantes. Debe ajustarse a un control externo de eficacia.
- El control policial será repartido entre los tres poderes: ejecutivo, legislativo y judicial.
- Los poderes públicos garantizarán procedimientos efectivos e imparciales de recursos contra la policía.

Como conclusión y recapitulación de todo lo expuesto y detallado anteriormente y al amparo de la actual Ley de Seguridad Privada 5/2014, que considera a los servicios privados de seguridad como servicios complementarios y subordinados respecto a los de Seguridad Pública, hace que se pueda aseverar que estos servicios privados se sujeten al mismo Código Deontológico Profesional que las Fuerzas y Cuerpos de Seguridad, con lo que sería aplicable a todo el personal de las Empresas de Seguridad, estando estos integrados por los Vigilantes de Seguridad, Vigilantes de Explosivos, Escoltas Privados, Guardas Rurales con sus especialidades, los Jefes de Seguridad, Los Directores de Seguridad y los Detectives Privados.

Principios Básicos de Actuación y el Deber de Colaboración con la Seguridad Pública. Infracciones administrativas y penales.

La Ley 5/2014 de Seguridad Privada en el Título III sobre el personal de seguridad privada y más concretamente en su artículo 30, así como en el artículo 67 de su Reglamento R.D. 2364/1994 y en la Orden de Interior INT/318/11 (aún vigentes por no contravenir a esta ley según la Disposición derogatoria única), dispone determinados principios básicos de actuación para las categorías que vienen expresadas en los mismos textos. En el mencionado artículo de la Ley, se establece que:



MAGOS

radares para vigilancia

revolucionando los sistemas de seguridad civiles

 **SR110**


360° 60' 200m / 350m

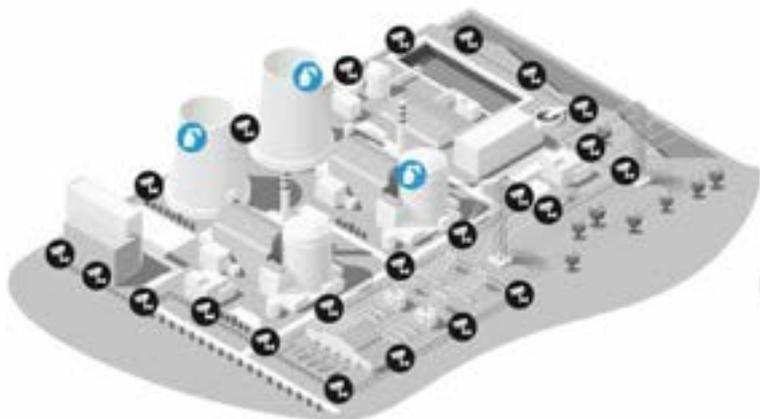


SR500 


120° 30' 400m / 600m

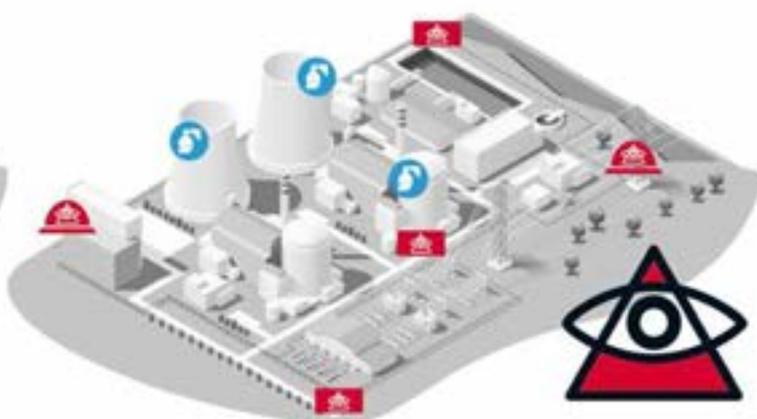
Usando radares MAGOS puedes ahorrar entre un 30 y un 60% respecto al precio de un proyecto de seguridad convencional.

PROTECCIÓN CONVENCIONAL



23 cámaras térmicas + 3 cámaras PTZ

PROTECCIÓN RADAR MAGOS



3 radares SR500 + 2 radares SR110 + 3 cámaras PTZ

Los radares MAGOS combinados con cámaras PTZ permiten disminuir la cantidad de cámaras y de sensores necesarios en una instalación de seguridad. De esta manera se reducen significativamente los costes de instalación, mantenimiento y consumo energético. Además de mejorar la seguridad del recinto, minimizando casi totalmente el número de falsas alarmas, así como la estabilidad del sistema ya que son productos 100% operativos en todas las situaciones ambientales.

C. Pla del Ramassar, 52
08402 Granollers
BARCELONA (SPAIN)

Tel. +34 902 502 035
iptecno@iptecno.com
www.iptecno.com

Productos distribuidos por:

IPTECNO

«Además de lo establecido en el artículo 8, el personal de seguridad privada se atenderá en sus actuaciones a los siguientes principios básicos:

- a) Legalidad.
- b) Integridad.
- c) Dignidad en el ejercicio de sus funciones.
- d) Corrección en el trato con los ciudadanos.
- e) Congruencia, aplicando medidas de seguridad y de investigación proporcionadas y adecuadas a los riesgos
- f) Proporcionalidad en el uso de las técnicas y medios de defensa y de investigación».

Siendo aún más clarificadora y precisa la Orden de Interior INT/318/11 (Orden anterior a la vigente ley), que de conformidad con la Ley concreta y detalla no sólo el principio de actuación sino la forma de realización. Además de incluir como básicos los principios de legalidad (contemplado el articulado de la norma), el de colaboración con las Fuerzas y Cuerpos de Seguridad (contemplado en el Título I denominado Coordinación de la Ley y en sus articulados 14, 15 y 16), la colaboración ciudadana informando de todo lo relevante a la seguridad ciudadana y en

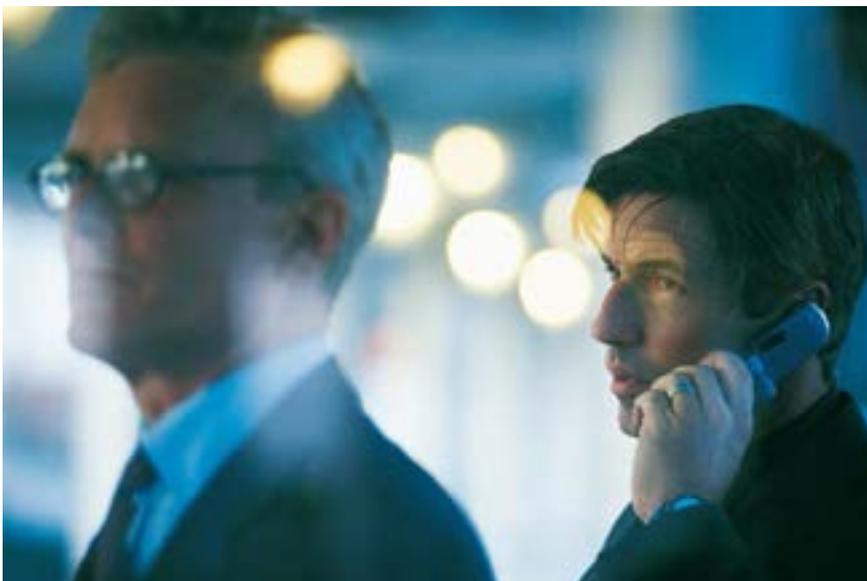
previsión de delitos, así como una rigurosa reserva profesional. Quedando dispuesto en el artículo 31 de la Orden de la siguiente manera:

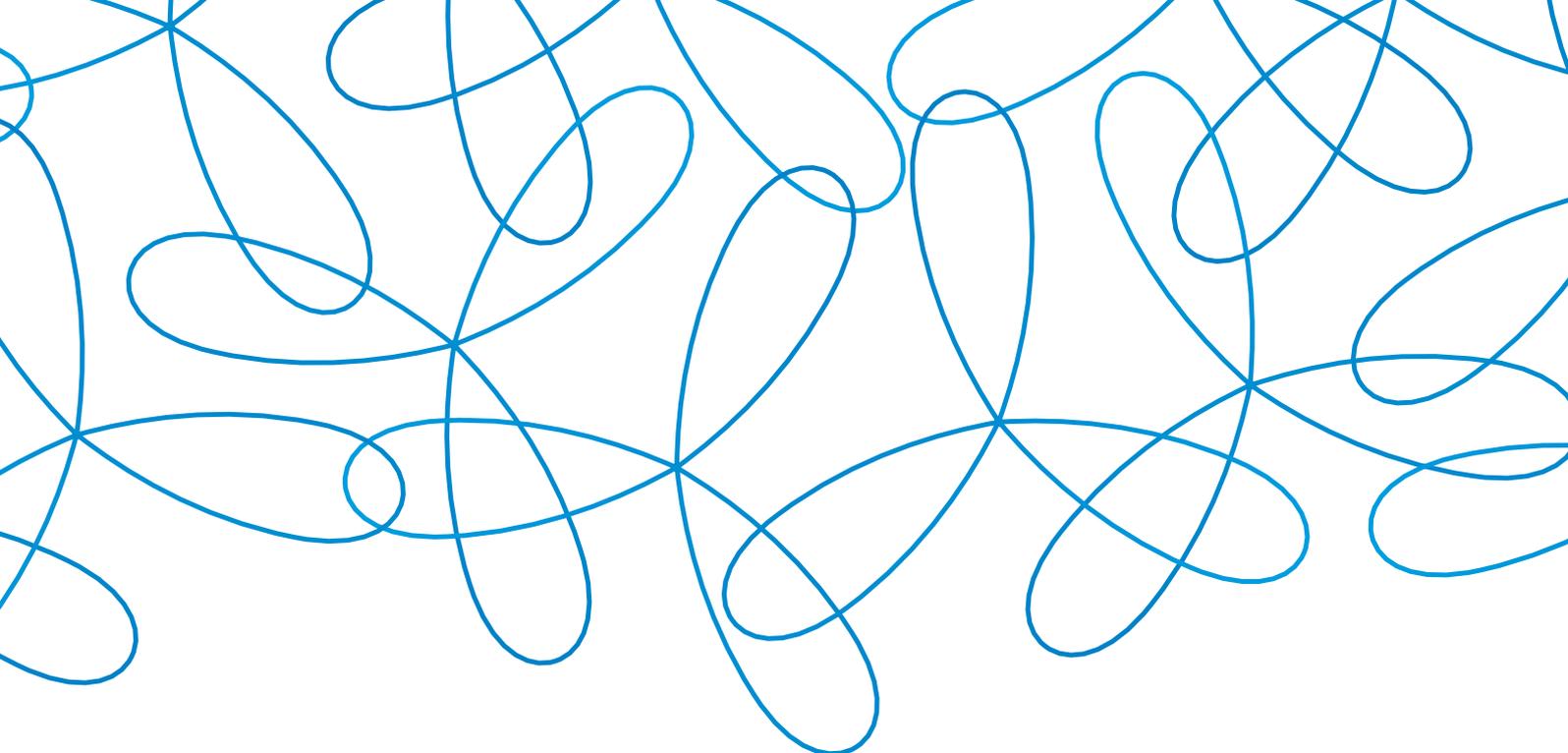
1. Legalidad y, en consecuencia, en las actividades de seguridad e investigación privada sólo se emplearán medios y acciones conforme al ordenamiento jurídico vigente.
2. Integridad, cumpliendo diligentemente los deberes profesionales oponiéndose a todo acto de corrupción.
3. Dignidad, mediante el recto ejercicio de sus atribuciones legales.
4. Protección, que implica desarrollar efectivamente sus responsabilidades para conseguir los niveles de seguridad establecidos, sin permitirse ninguna forma de inhibición en su función de evitar hechos ilícitos o peligrosos.
5. Corrección, desarrollando una conducta profesional irreprochable, especialmente en el trato con los ciudadanos, evitando todo tipo de abuso, arbitrariedad y violencia.
6. Congruencia, por cuyo principio se aplicarán medidas de seguridad proporcionadas y adecuadas a los riesgos que se trata de proteger.

7. Proporcionalidad en el uso de técnicas y medios de defensa de dotación.
8. Colaboración con las Fuerzas y Cuerpos de Seguridad, debiendo observar siempre las instrucciones policiales concretas sobre el objeto de su protección o investigación, en función de los medios de que disponga.
9. El personal de seguridad privada ejercerá la colaboración ciudadana comunicando a los cuerpos policiales competentes las informaciones relevantes para la seguridad ciudadana y la prevención del delito que conozca.
10. El personal de seguridad privada guardará rigurosa reserva profesional sobre los hechos que conozca en el ejercicio de sus funciones, especialmente de las informaciones que reciba en materia de seguridad y de los datos de carácter personal que deba tratar, investigar o custodiar, y no podrá facilitar datos sobre dichos hechos más que a las personas que le hayan contratado y a los órganos judiciales y policiales competentes para el ejercicio de sus funciones.

Por otro lado, y completando el principio de actuación número 8, en la Orden de Interior INT/318/11 incluye en los artículos 32 y 33 el deber de colaboración con las Fuerzas y Cuerpos de Seguridad, así como los requerimientos de colaboración por parte de estos. Todos ellos expresados en los artículos 66 y 76 del Reglamento RD 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada (aún vigente por no contravenir la norma actual). Y que en resumen tal y como exponen:

«El deber de colaboración con las Fuerzas y Cuerpos de Seguridad..., así como la puesta a disposición de presuntos delincuentes, instrumentos,





I Jornada Técnica **RPAS y Seguridad Privada**

MADRID
FEBRERO 2016

Más información e inscripciones:



www.dronesyseguridad.com



info@dronesyseguridad.com



+34 914 768 000

Con la colaboración de:

**CUADERNOS DE
SEGURIDAD**



Organiza: **Peldaño**

efectos y pruebas de delitos... el personal de seguridad privada facilitará... directamente y sin dilación, la información o colaboración que les resulte necesaria...»

Teniendo en cuenta los Principios Básicos de Actuación y el Deber de Colaboración con las Fuerzas y Cuerpos de Seguridad, es obvio que el incumplimiento de algún o algunos de estos principios en el desempeño de sus funciones, el personal de seguridad privada podría incurrir en infracciones administrativas y penales. A continuación, se detalla, primeramente, un resumen de las Infracciones Administrativas recogidas en la Ley 5/2014 y, seguidamente, las Infracciones Penales organizadas según vienen detalladas en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal vigente.

Infracciones Administrativas en las que puede incurrir el personal de seguridad privada relativas a la Deontología Profesional serían:

—**Infracciones muy graves:**

- Carecer de habilitación.
- Tenencia y uso de armas fuera de servicio.
- Falta de secreto profesional.
- Negativa a prestar auxilio o colaboración con FCS.
- Negativa a identificarse profesionalmente en el ejercicio de sus funciones.
- Realización de investigaciones sobre delitos perseguibles de oficio o falta de denuncia a la autoridad competente.
- Realizar actividades prohibidas en el artículo 8.4 sobre reuniones, manifestaciones, conflictos políticos...
- Ejercicio abusivo de sus funciones en relación con los ciudadanos.
- Prácticas abusivas, arbitrarias o discriminatorias, acoso moral o físico.
- Abandonos o la omisión injustificados del servicio.

—**Infracciones graves:**

- Realizar funciones que excedan la habilitación.
- Realizar funciones sin estar integrado en empresas de seguridad.
- Falta de respeto al honor y dignidad de las personas.
- La no identificación cuando sea requerida por los ciudadanos.
- La falta de diligencia en el cumplimiento de sus funciones.
- La negativa a mantenerse formado y actualizado.

—**Infracciones leves:**

- Actuación sin la debida uniformidad y medios exigibles
- Trato incorrecto o desconsiderado a los ciudadanos.
- Incumplimiento de trámites o formalidades establecidos en la ley, siempre que no sean graves o muy graves.

Infracciones penales del Código Penal en las que se puede incurrir el personal de seguridad privada (localizadas por Títulos):

—Título VI- Delitos contra la Libertad

- Podemos incluir artículos del Capítulo 1º sobre las detenciones ilegales.

—Título VII- De las torturas y otros delitos contra la integridad moral.

- Podemos incluir artículos como el 173, aunque el resto haga mención específica a funcionarios.

—Título IX- De la omisión del deber de socorro

- Podemos incluir los artículos 195 y 196.

—Título X- Delitos contra la intimidad, el derecho a la propia imagen y a la inviolabilidad del domicilio.

- Podemos incluir todo el articulado del Capítulo 1º

—Título XX- Delitos contra la Administración de Justicia

- Podemos incluir el artículo 450 del Capítulo 2º De la omisión de los deberes de impedir delitos o promover su persecución.

—Título XXI- Delitos contra la Constitución

- Podemos incluir el articulado comprendido en el Capítulo IV, secciones 1 y 2.

—Título XXII- Delitos contra el orden público

- Podemos incluir el artículo 563.

Así mismo el propio Código Penal incluye en su Libro III (Faltas y sus penas) un elenco de artículos que detallan faltas contra las personas y el orden público (artículos 619, 621, 634 y 637). ●

Fotos: Archivo





Seguridad privada en domicilios,
empresas y establecimientos
comerciales con asistencia de vigilante.

24h/365 días.



**CONTROLA TU
HOGAR/NEGOCIO
DESDE TU
SMARTPHONE**



Desde **18** €/mes
Conexión y mantenimiento



Desde **21** €/mes
Conexión, servicio acuda
y custodia de llaves.

NOELIA CASTILLÓN. SOUTHERN EUROPE CHANNEL MARKETING MANAGER.
HONEYWELL SECURITY GROUP

Seguridad en los hospitales: hacer más con menos

En un momento económico complicado en el que los presupuestos hospitalarios se han visto impactados en toda Europa, decidir cómo priorizar las inversiones, puede ser ahora un poco más complicado. Con una presión cada vez mayor por aumentar la inversión en medicamentos, equipos, formación, nuevo personal y otras variables, no es de extrañar que en algunas ocasiones la seguridad haya quedado relegada a un segundo plano. En este artículo, Noelia Castellón, Southern Europe Channel Marketing Manager de Honeywell Security Group, explica por qué es importante mantener actualizado un sistema de seguridad en un hospital, y cómo ello no tiene por qué llevar asociado un coste elevado.

AUNQUE inicialmente podríamos pensar que los hospitales no son lugares de riesgo, la realidad nos demuestra lo contrario. Por ejemplo, se produce el robo de pertenencias de pacientes o del personal, o incluso de costosos equipos como ordenadores o tablets. Otro delito habitual en el entorno hospitalario es el robo de medicamentos, así como la violencia contra pacientes y personal, que puede tomar formas muy diferentes, desde delitos menores a casos extremos.

En Inglaterra, según las cifras del NHS Protect (entidad que se encarga de proteger al personal y el material de los hospitales públicos de la delincuencia), las agresiones contra personal hospitalario aumentaron en casi un 9% de 2013 a 2014. Un reciente estudio de hospitales en Alemania, Austria y Suiza reveló que el 73% de los en-

trevistados había sufrido algún tipo de agresión, desde vandalismo hasta altercados o peleas a gran escala. En Suráfrica, los delitos violentos en hospitales públicos han experimentado un fuerte crecimiento del 50 % desde 2002.

Dichos ataques violentos al personal tienen un impacto negativo en la reputación del hospital, la contratación de personal en el sector, y en muchas ocasiones, dan lugar a interminables batallas legales.

En Europa el robo también es un problema constante en los centros sanitarios, donde cada semana se registran desapariciones de medicamentos, equipos y pertenencias de los empleados y pacientes.

Llegados a este punto, la pregunta sería entonces, ¿por qué los hospitales no invierten más en reforzar su seguridad? La respuesta más rápida podría ser: por el coste que conlleva. Afortunadamente existen una serie de soluciones de seguridad que todos los centros hospitalarios pueden poner en marcha y su implementación no supondría un gasto elevado.





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

LÍNEA 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



El control de accesos es una de las soluciones de seguridad más eficaces a disposición de los hospitales para combatir el robo. La posibilidad de establecer un perímetro de seguridad en determinadas áreas del hospital, con acceso restringido a un reducido nú-

mero de empleados de confianza, puede reducir la probabilidad de robos y la lista de sospechosos en caso de que el robo llegue a producirse. Aunque sería aconsejable que se implantase un sistema de control de accesos en todo el edificio del hospital, en una primera fase, se podría priorizar su implantación solo en áreas con equipos, medicamentos e información de elevado valor y después continuar con otras áreas.

«Las soluciones de videovigilancia IP son una inversión fundamental para cualquier hospital»

Las soluciones de videovigilancia IP son una inversión fundamental para cualquier hospital. Las mejoras que ofrece esta tecnología en la calidad de

imagen se traducen en que cuando se produzca algún incidente, los equipos de seguridad del hospital podrán identificar rápidamente al responsable y ofrecer a las autoridades grabaciones de alta resolución para su uso en los tribunales. Además, las imágenes de CCTV de alta calidad protegen al personal en caso de pleitos, con imágenes claras nítidas de los supuestos incidentes. En los casos en los que el presupuesto no permita sustituir su tecnología analógica por IP, la tecnología híbrida sería la solución adecuada. Los sistemas híbridos, que integran los sistemas existentes con la nueva tecnología IP, ofrecen una transición gradual a IP que se puede llevar a cabo a lo largo de varios años según la situación económica lo vaya permitiendo. Asimismo, los hospitales que ya cuentan actualmente con infraestructura informática,

la transición a IP se realizará con mayor facilidad aún.

Por otro lado, cabe también destacar los beneficios que la analítica de vídeo ofrece en el entorno hospitalario. Es una tecnología capaz de proporcionar alertas al personal de seguridad de los hospitales para predecir y prevenir la actividad delictiva antes de que se produzca. Por ejemplo, si un grupo de jóvenes permanece durante un periodo de tiempo sospechosamente prolongado en el aparcamiento, el responsable de seguridad recibirá una alerta de riesgo potencial. Si una persona que visita

a un familiar ingresado merodea durante mucho tiempo en torno a un armario de medicamentos, es posible investigar rápidamente el incidente. Asimismo, una de las formas en las que los responsables de los hospitales, con presupuestos limitados, pueden justificar esta inversión es centrándose en los datos empresariales que puede aportar el análisis de vídeo: el tráfico del personal, pacientes y vehículos, que contribuye a comprender y optimizar los procesos y la gestión del hospital.

Resumiendo, los hospitales disponen de distintas maneras de invertir en tecnología de seguridad y a la vez mantener su equilibrio presupuestario. Dicha tecnología puede facilitar la recuperación de la inversión de forma positiva de diferentes formas, desde reducir los robos y los costes de las primas de seguros, hasta evitar costosos litigios y ofrecer una valiosa información empresarial sobre los procesos del hospital. Pero, sobre todo, protege a las personas (pacientes, personal y visitas) en momentos de alta vulnerabilidad. ●

Fotos: Honeywell

e-Movifree®

Control integral de sus servicios y personal en movilidad, en tiempo real



e-Movifree® es la herramienta más completa para la supervisión y la gestión de los Servicios de Seguridad, que le proporciona un control total de todos sus servicios mediante aplicación móvil y plataforma web.

e-Movifree® le permite visualizar todos sus puestos activos y recibir las incidencias en tiempo real. Además, registra todos los marcajes realizados, con geoposición, y genera cuadrantes automáticos de las horas reales, ofreciéndole información vital para la gestión de su negocio.

Más información en www.emovifree.com

e-Movifree® se sustenta sobre el potente motor de negocio **e-Satellite® Business Engine** desarrollado por FREEMATICA, líder en soluciones de gestión para sectores con personal en movilidad.



EL EVENTO CONTÓ CON LA PRESENCIA DE MÁS DE 300 PROFESIONALES

Axis Solutions Conference Iberia 2015

Los asistentes pudieron conocer soluciones para los segmentos de Industria, Infraestructuras Críticas, Logística, Retail, Banca, Tráfico, Plataformas Cloud,...

Axis Communications celebró su evento anual de Partners, esta vez con un nuevo formato, mucho más dinámico y enriquecedor, que fue todo un éxito a juzgar por el record de asistencia, con más de 300 profesionales que acudieron a conocer las distintas soluciones propuestas por más de 21 empresas especialistas en soluciones para los segmentos de Industria, Infraestructuras Críticas, Logística, Retail, Banca, Tráfico, Plataformas Cloud y Grandes Plataformas de Integración para el Sector Corporativo.

La jornada comenzó con una breve introducción por parte de Edwige Maury, directora regional para el Sur de Europa, en la que trazó a grandes líneas la estrategia de Axis Communications en el medio y largo plazo. Acto seguido, Pedro Alfaro, recientemente nombrado director de

Ventas para Iberia en Axis Communications, presentó la estructura y las distintas funciones del equipo Axis Iberia que dan soporte a su canal de ventas. Las presentaciones continuaron a cargo de Paulo Silva, responsable de Formación, con un breve repaso a las últimas novedades lanzadas por Axis como el

control de accesos IP, intercomunicadores y sistemas de audio IP compatibles con el estándar de telefonía SIP, así como los nuevos domos PTZ de alto rendimiento, cámaras Multi-Lente de alta resolución y otros productos relacionados con las Infraestructuras Críticas. Y para terminar la sesión, Alberto Alonso, responsable de Desarrollo de Negocio, presentó a cada una de las 20 empresas que participaron en la zona de exposición con sus diferentes soluciones, organizadas por segmentos de mercado.

El área dedicada a exposición fue escenario de un jornada completa orientada a difundir soluciones específicas y profesionales desarrolladas por especialistas en los distintos segmentos, por ejemplo, en la zona de Retail estuvieron presentes las empresas Gunnebo, Sidma y Visual Tools, mostrando las soluciones más destacadas como el conteo de personas, las zonas calientes y gestión de efectivo, entre otras. En banca destacaron Pacom, Lanaccess y Technoaware; en la zona dedicada a tráfico estuvieron Infocom Sermar, Innoaware, S-Connect y Vaxtor Systems, mostrando las soluciones de giro indebido, semáforo rojo y control de accesos y LPR en propia cámara. En logística estuvo Seetec y Próxima Systems en Industria. En la parte de Infraestructuras Críticas los asistentes pudieron conocer las soluciones de reconocimiento facial, cámaras térmicas y muchas más de la mano de Herta, Lanaccess, Ngaro y Pacom.



En el área de las grandes plataformas de integración estaban presentes Assa Abloy, Allied Telesis, Ganetec, Milestone y App-Vision y, por último, en la zona de Plataforma Cloud, estaba la empresa R-Cable mostrando la gestión del Axis Video Hosting System de Axis Communications.

Además de la participación de estas empresas, Axis Communications también contó con una zona dedicada solamente a sus novedades en producto

donde instalaron más de sesenta soluciones, entre ellas el intercomunicador, el control de accesos, el altavoz exponencial IP, cámaras de acero inoxidable o la Q6000 entre otros productos.

«Creo que este tipo de eventos aporta un gran valor a la Industria de la Seguridad Física, en una sola jornada



es posible conocer los últimos desarrollos en hardware y software, comentar directamente con los fabricantes y especialistas sobre las tendencias de futuro, y todo ello es de gran ayuda para planificar futuras inversiones. Hay que cambiar el chip, de venta-producto a venta-soluciones/servicios, asegu-

rando el retorno de inversión para el usuario final», comenta Juan Luis Brizuela, director de Desarrollo de Negocio para el Sur de Europa.

Además contaron con la presencia de dos clientes finales, los cuales explicaron proyectos destacados en los que han colaborado conjuntamente: Miguel Ángel Gallego, director de Seguridad de la Estación Sur de Autobuses de Madrid, presentó un proyecto de reconocimiento facial

masivo en el que también ha participado la empresa Herta, y Esteban Domínguez, director de Promec, presentó el proyecto de la planta 22 del Hospital Gomez Ulla, un proyecto de alta seguridad y fiabilidad. ●

TEXTO Y FOTOS: AXIS COMMUNICATIONS

Contactos de empresas, p. 7.

La nueva generación de linternas recargables, ahora con LEDs de 3 W

no necesitan recambio de bombillas
alcance 1000m
baterías recargables NiMH
altamente resistentes



Unilux 5 LED
se recarga en la pared,
siempre lista para su uso



PowerLux 5 LED,
compacta, con función morse
e imán de sujeción



Importador oficial



SABORIT INTERNATIONAL

Importación y Distribución de Equipos para la
Seguridad, Vigilancia y Defensa

RÉCORD DE PARTICIPACIÓN CON MÁS DE 1.100 ASISTENTES

9ENISE, récord de convocatoria en torno a la ciberseguridad

Durante los días 20 y 21 de octubre más de 1.100 profesionales acudieron al Parador San Marcos de León, a la novena edición del Encuentro Internacional de Seguridad de la Información (ENISE), organizado por el Instituto Nacional de Ciberseguridad (INCIBE).



En 9ENISE más de 40 ponentes abordaron desde una perspectiva multidisciplinar diferentes retos a los que se enfrenta la Ciberseguridad en un momento en el que la sociedad y economía están transformándose profundamente.

El acto de inauguración corrió a cargo del director general de la entidad, Miguel Rego, acompañado por el director del Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), Fernando Sánchez.

Miguel Rego destacó el evento ENISE como cita ineludible para el sector, y aprovechó para repasar las iniciativas destacadas de INCIBE dentro de la pro-

gramación del Plan de Confianza en el Ámbito Digital, apuntando cuáles serán los próximos proyectos del Instituto dentro de la estrategia nacional.

El lema de las jornadas era «Ciberseguridad: motor para el desarrollo de la Economía y la Sociedad Digital», toda una declaración de intenciones de

Premio 9ENISE al mejor vídeo de concienciación en ciberseguridad

Un año más, INCIBE había convocado el premio 9ENISE, valorado en 3.000 €, que en esta edición premiaba el mejor vídeo de menos de un minuto de duración cuya temática fuera la concienciación en ciberseguridad, y cuyo ganador fue un equipo de la Universidad Carlos III de Madrid liderado por dos profesores del Computer Security Lab del Departamento de Informática de la entidad académica: José María de Fuentes y Lorena González.

En concreto, el equipo está formado por los citados profesores y ocho antiguos alumnos de la asignatura Criptografía y Seguridad de la Información de la universidad madrileña que están cursando el grado de Ingeniería en Informática. El jurado estaba compuesto por representantes de medios de comunicación, incluyendo Unidad Editorial, Grupo Prisa, Grupo Atenea, CODASIC, Borrmart y el ISMS Fórum, así como miembros de INCIBE y del ámbito de la ciberseguridad en general.



Miguel Rego, director general de INCIBE y Fernando Sánchez, director de CNPIC.



Inauguración Meridian 2015.

los asuntos que se plantearon. El congreso abordó algunos de los principales retos de esta industria, que aparte de sus desafíos técnicos ofrece grandes oportunidades para el crecimiento económico y el bienestar social. También se expusieron los principales retos del sector desde la perspectiva regulatoria y, por supuesto, tecnológica.

Las sesiones del primer día estuvieron enfocadas sobre todo al ámbito de la legislación y la economía, y las del segundo día se dirigieron al profesional técnico de la ciberseguridad. ●

FOTOS: CORTESÍA DE INCIBE.

Meridian Process 2015, reforzando las capacidades de las Infraestructuras Críticas Internacionales

El secretario de Estado de Seguridad, Francisco Martínez, fue el encargado de inaugurar la Conferencia Meridian 2015, un punto de encuentro anual que por primera vez se celebró en España en el marco de 9enise. Profesionales de más

de 30 países debatieron los asuntos más importantes relacionados con la ciberseguridad y la protección de las infraestructuras críticas.

A lo largo de su intervención, Francisco Martínez quiso poner en valor 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.

Dentro de este modelo, Francisco Martínez subrayó la figura del Operador Crítico como un componente esencial en la protección de nuestras infraestructuras que, si bien es designado por la Comisión Nacional para la Protección de las Infraestructuras Críticas, responde a los principios de colaboración público-privada y público-público que preside la nueva normativa sobre seguridad que se está aprobando en nuestro país.

Martínez aprovechó para anunciar la firma de un convenio marco con la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, «con este segundo convenio además de reforzar nuestra colaboración, pretendemos también trabajar en mecanismos y herramientas de auditoría para los operadores de infraestructuras críticas».

Finalmente, el secretario de Estado de Seguridad también anunció la puesta en marcha de la Plataforma de Información de Interés sobre Infraestructuras, restringida a los operadores críticos y específicamente diseñada para facilitar el intercambio de información con el CNPIC.

ENCUENTRO CELEBRADO EN LA REAL CASA DE LA MONEDA EN MADRID LOS DÍAS 29 Y 30 DE OCTUBRE

V Congreso Protecturi

Experiencias e itinerarios de la Protección del Patrimonio Cultural

Bajo el lema «Experiencias e itinerarios de la Protección del Patrimonio Cultural», la Asociación para la Protección del Patrimonio Histórico, Protecturi, celebró el 29 y 30 de octubre en Madrid el V Congreso Protecturi. Un encuentro, al que asistieron más de 200 expertos en arte, cultura y seguridad del patrimonio cultural, y en el que se abordaron aspectos clave del patrimonio cultural español, con interesantes ponencias de expertos españoles, así como con la aportación de especialistas internacionales. Además durante el congreso se procedió a la entrega de los Premios Protecturi 2015 a las mejores iniciativas de este año por su aportación a la cultura de la seguridad y puesta en valor del patrimonio cultural.

EL acto de inauguración contó con la presencia del secretario de Estado de Seguridad, Francisco Martínez, quien explicó que la cifra de denuncias por robos, destrucción o

daños al patrimonio cultural ha bajado de una media de 60 denuncias por año entre 2005-2014 a las 29 que se investigan en 2015. El secretario de Estado de Seguridad señaló que en los últimos

cuatro años la Guardia Civil ha realizado un total de 80 grandes operaciones de investigación y recuperación de patrimonio cultural robado. «Los últimos datos de Europol son de 2013, pero nos indican que en materia de seguridad y expolio tenemos mejores datos que países como Italia, Francia o Alemania», matizó Martínez.

Por su parte, el presidente de Protecturi, Jesús Alcantarilla, y el vicepresidente, Andrés Martín, subrayaron la importancia de la puesta en marcha de un red de alerta temprana, a través de la que Protecturi colabora con los diferentes cuerpos policiales para proteger las obras culturales españolas.

El arte de conservar

A lo largo de los dos días se sucedieron diferentes intervenciones, que comenzaron con una ponencia inaugural a cargo de Andrés Martín Ludeña, vicepresidente de Protecturi, bajo el título «Amenazas al Patrimonio Cultural Español», quien, entre otros aspectos, abordó algunos de los datos reflejados en el Informe Protecturi 2015, destacando que España es el tercer país del mundo en bienes culturales catalogados, sólo por detrás de China e Italia, con un total de 119.000 unidades.

El V Congreso Protecturi se desglosó en diversas intervenciones en las que se abordaron los siguientes temas: «El arte de conservar», a cargo de Ángela Espinar Santana, presidenta de la Asociación Profesional de Conservadores y Restauradores de España (ACRE), y Sara Martínez Garrido, vocal de Comunicación de

Vista general de los asistentes al V Congreso Protecturi.





El secretario de Estado de Seguridad Francisco Martínez en un momento de su intervención.

ACRE; «Transporte internacional de bienes culturales», por Ana Tabuenca, responsable del departamento de Arte de SIT Grupo Empresarial; «Los Museos del siglo XXI», por Manfred Sellink, director del Real Museo de Bellas Artes de Amberes, o la Mesa de Arquitectos donde participaron César Portela y Jaime Castañón.

rectora general de Administración del Museo Nacional del Prado; «De la playa a la cultura: 32 museos en Málaga», a cargo de Francisco de la Torre, alcalde de Málaga; «El Museo como punto de encuentro», por Guillermo Solana, director artístico del Museo Thyssen Bornemisza; o «Protección, respeto y

Protección y Seguridad

El día 30 se abordaron temas como «La Administración de la Protección y Seguridad del Museo Nacional del Prado», por Marina Chinchilla, di-

Francisco Martínez conversa con representantes de Protecturi y Jaime Sánchez Revenga, presidente de la Real Casa de la Moneda, primero por la dcha.



«España es el tercer país del mundo en bienes culturales catalogados, sólo por detrás de China e Italia»

seguridad en los espacios de la Abadía de Montserrat», por Ignaci M.Fossas, Padre Prior de la Abadía de Montserrat.

Además, durante el congreso se hizo entrega de los Premios Protecturi 2015, galardones anuales que premian la aportación de personas e instituciones al patrimonio cultural español.

Premio Institucional: Al Camino de Santiago, por su aportación a la cultura europea y su puesta en valor del patrimonio cultural de todos los itinerarios por los que transcurre el peregrinaje que concluye en Santiago de Compostela.

Premios individuales:

-Dr. S.C. Cheng, por sus donaciones al Museo Oriental de Valladolid, que ha incrementado con valiosas piezas de arte e historia el patrimonio cultural español.

-Sean Scully, por haber convertido la Abadía de Montserrat en un ejemplo de confluencia entre el cristianismo y el arte de vanguardia.

Menciones Honoríficas:

-Real Casa de la Moneda, por sus 400 años como referente nacional e in-

ternacional en seguridad y divulgación de la cultura.

-Revista Seguritecnia, por su contribución a la divulgación de información, análisis y reportajes sobre la protección y la seguridad del patrimonio artístico, histórico y cultural de España.

-Ubaldo Sedano, por su aportación y años de entrega profesional a la conservación y restauración de bienes culturales.

-Ayuntamiento de Málaga, por su inversión económica, su apuesta de imagen y su modelo de ciudad volcada en el atractivo del patrimonio cultural.●

TEXTO Y FOTOS: REDACCIÓN/PROTECTURI

EL ENCUENTRO TUVO LUGAR EN MADRID EL PASADO 14 DE OCTUBRE

II Jornada «Guardia Civil-Empresa»

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

Con el objetivo de analizar conjuntamente cuestiones de interés común, en la inteligencia de que las diferentes perspectivas aportadas producirán un efecto enriquecedor y generador de sinergias, se desarrolló en Madrid el pasado 14 de octubre, la II Jornada Guardia Civil-Empresa. Un encuentro que reunió a directores, directivos y responsables de Seguridad de grandes compañías españolas, en el que se abordaron temas de gran actualidad como «Situación de la seguridad de las empresas españolas en el ámbito internacional» o «Situación actual de las principales amenazas y mecanismos de colaboración».

EL acto de inauguración contó con la presencia del Teniente Coronel Cándido Cardiel, director adjunto operativo de la Guardia Civil, y del presidente de la Fundación CEOE, José María Lacasa.

El primer bloque de intervenciones se desarrolló bajo el tema «Situación de

la Seguridad de las empresas españolas en el ámbito interancional». Moderada por Juan Muñoz, CPP. Presidente de ASIS España, comenzó con la intervención de Joaquín Collado, director de Seguridad Corporativa de Acciona Infraestructuras, que abordó el «Panorama actual de amenazas y riesgos para

las empresas en el exterior con incidencia en la Seguridad Nacional», destacando al inicio de su intervención que hoy en día «las fronteras se difuminan; la seguridad está más allá de un límite fronterizo». Tras insistir en la amplia presencia de empresas españolas en el escenario económico y social internacional, Collado hizo hincapié en la necesidad de que la seguridad estuviera integrada en el propio negocio. «La dirección de Seguridad -señaló- tiene que jugar un papel muy importante dentro de las empresas. La seguridad es clave en el negocio».

A continuación tomó la palabra José María Blanco, director del Centro de Análisis y Prospectiva, que abordó «Evolución y prospectiva de las amenazas y riesgos globales». Tras explicar las tendencias e indicadores que afectan a la seguridad global en el mundo, analizó los pilares de seguridad en la internacionalización entre los que destacó inteligencia sociocultural; empatía; talento, disciplina, valentía; análisis de inteligencia...

Para finalizar, Daniel García, director de Seguridad de Desigual explicó «Organización de la seguridad corporativa ante las amenazas y riesgos globales». Abordó el concepto de Seguridad Corporativa que desarrolla la compañía, y dio paso a un análisis más detallado de las acciones de Safety y Security que desarrolla la empresa que trabaja sobre un modelo centralizado.

La segunda de las temáticas a abordar giró sobre «Situación actual de las principales amenazas y mecanismos de colaboración», intervenciones que fueron moderadas por Arturo Espejo, Co-



Vista general de la II Jornada Guardia Civil-Empresa.

*Feliz Navidad
y próspero
2016*

**NUESTRO MEJOR
REGALO ERES TÚ.
GRACIAS POR ELEGIRNOS
PARA COMUNICAR.**

COMUNICACIÓN MULTICANAL



 **Peldaño**

ronel de la Guardia Civil, jefe del Área Técnica de la Jefatura de Información.

Andrés Martín, comandante de la Guardia Civil. Jefatura de Información, abordó la «Incidencia de la amenaza terrorista yihadista», analizando el origen del islamismo radical, para acto seguido explicar el estado actual de Al Qaeda que, hoy en día está «perdiendo influencia propagadística debido al Estado Islámico». Destacó la necesidad de que las empresas se adecuen a la evolución de las nuevas amenazas y riesgos y a una mayor optimización de los sistemas de seguridad.

Óscar de la Cruz, comandante de la Guardia Civil, Jefe del Grupo de Delitos Telemáticos (UCO), explicó «Riesgos de Ciberseguridad en las empresas», realizando una anatomía de lo que es un ciberataque. Hizo especial hincapié en la necesidad de implantar una cultura de concienciación.

Finalmente, Andrés Sanz. Teniente Coronel de la Guardia Civil. Jefe Interino del SEPROSE, abordó «Visión de la Guardia Civil de la Colaboración público-privada», donde destacó la necesidad de establecer procedimientos de colaboración para ofrecer soluciones, sobre la base de un modelo flexible «donde vamos a interpretar las necesidades del sector para buscar soluciones, desde la cercanía y la proximidad, entre sector público y privado».

Acto seguido, el director general de la Guardia Civil, Arsenio Fernández de Mesa, hizo entrega de los premios Duque de Ahumada a la Seguridad Corporativa, durante el acto de clausura de la II Jornada Guardia Civil-Empresa.

El director general comenzó su intervención agradeciendo a las empresas que hayan mantenido, en tiempos difíciles, el tejido empresarial que ha



El director general de la Guardia Civil en el acto de clausura de la jornada.



Mesas de debate que se celebraron durante la II Jornada Guardia Civil-Empresa.

sido el auténtico artífice de la generación de empleo.

También se refirió a la Seguridad Corporativa, como uno más de los activos a tener en cuenta al valorar una empresa, como conjunto de acciones que las empresas llevan a cabo para proteger sus activos, tarea ardua que exige visión, información planificación, recursos y presupuesto y que, en este ámbito, «siempre tendrán en la Guardia Civil a un aliado que les apoyará en sus necesidades».

Arsenio Fernández de Mesa destacó que las principales amenazas en el momento actual tienen que ver con el ciberespacio o están vinculadas al terrorismo yihadista y que para paliar los daños es necesaria «la colaboración público-privada como eje vertebrador de un nuevo enfoque de la seguridad».

Este año han resultado galardonados:

—El BBVA con el premio a la excelencia en seguridad corporativa, por ser un referente en la gestión de la seguridad y en su colaboración con la Guardia Civil. —El Grupo Acciona, premio a la mejor acción exterior, por liderar la organización de un Foro Internacional para compartir información de seguridad entre empresas españolas en México, y desarrollarlo también en fase de proyecto en Panamá y Perú, lo cual mejora notablemente las condiciones de seguridad de las organizaciones participantes;

—El Grupo San José, premio a la mejor trayectoria de colaboración, destacando su colaboración altruista mostrada con ocasión del desastre natural de Nepal y, en concreto, por la proactiva asistencia mostrada al Equipo de Rescate en Montaña de la Guardia Civil que prestó servicio en Nepal, cuyo apoyo fue fundamental tanto a nivel informativo previamente al desplazamiento del Equipo, como por el apoyo logístico durante el despliegue y desarrollo de sus actividades operativas; y

—A la Editorial Borrmarkt, editora de la revista Securitecnia, premio a la mejor acción de difusión de la cultura de seguridad, por su historial de 35 años al servicio de la difusión de la cultura de seguridad. ●

TEXTO Y FOTOS: GEMMA G. JUANES/MIR

ISMS: Conclusiones del IV Foro de la Ciberseguridad

El IV Foro de la Ciberseguridad organizado por ISMS Forum Spain, y al que acudieron 200 asistentes, reunió en el Auditorium CaixaForum Madrid a grandes expertos del mundo de la Ciberseguridad, tanto nacionales como internacionales, para analizar, estudiar y debatir sobre el impacto que pueden llegar a tener las ciberamenazas en el ámbito empresarial, así como la necesidad de concienciar a empresas y usuarios del valor que tiene la protección de uno de sus activos más importantes: los datos.

La inauguración del foro corrió de la mano de Erka Koivunen, ex director del CERT finlandés, quien a través de su ponencia «El poder del Hacking empresarial» analizó la importancia de la Ciberseguridad en las grandes empresas. Koivunen

inició la ponencia dando su visión particular sobre qué es el hacking y añadió los tipos de hackers tradicionales existentes, a los que añadió un nuevo tipo de hacker: «el ejecutivo empresarial». Para describir este último tipo de hacker se centró en uno de los casos más actuales del panorama

internacional: «El caso Volkswagen» donde explicó el autohacking que esta empresa realizó para conseguir ahorrar en inversión. Tras la ponencia inaugural en la que Erka Koivunen explicó el papel que la Ciberseguridad tiene en las grandes empresas se dio paso a los talleres prácticos «Análisis y gestión de nuevas amenazas», donde se analizaron en detalle las últimas ciberamenazas y sus posibles soluciones. Para ello se contó con la colaboración de cuatro de los principales players del Sector como: Federico Dios, Service Line Manager, Akamai; Alberto Cita, SE Manager, Southern Europe, Blue Coat; Renaud Bidou, Senior Technical Director, Trend Micro; y Carlos Fernandez, Cybersecurity Technical Leader, Symantec.

Federico Dios, explicó la existencia de un nuevo tipo de amenaza de denegación de servicios que ha tenido una gran relevancia en el último año: el XOR DDos, un tipo de ataque que afecta a máquinas Linux, actúa a través de fuerza bruta y que es bastante complicado de eliminar. Alberto Cita centró su taller en explicar las técnicas que se utilizan en

Malvertising. El Malvertising es una técnica de distribución de malware que combina de una forma única publicidad web con los Exploit Kits.

Renaud Bidou, por su parte, analizó algunos de los malware bancarios más importantes hasta el momento y destacó el «Pkybot», un malware bancario reciente que comenzó a operar a principios de octubre y que todavía se mantiene activo. Se trata de un conjunto de herramientas en evolución dirigidas a navegadores web que aprovechan vulnerabilidades recientes que se encuentran en plugins y que, además, es capaz de detectar los antivirus, para así, no ser descubierto.



Por otro lado, el IV Foro de la Ciberseguridad contó con la presencia de Carlos Fernández para poner fin a los talleres prácticos, quien se centró en explicar una amenaza ya popular: Cryptolocker, un ataque que cita ficheros de datos residentes en máquinas infectadas y exige el pago de una suma de dinero. Tras las cuatro intervenciones prácti-

cas, tuvo lugar la tercera sesión del encuentro de la mano de Emmanuel Roeseler, Security Systems Sales Manager Spain, Israel y España de IBM Software, quien con su ponencia «La Seguridad es tan robusta como su eslabón más débil» analizó la importancia de concienciar a los usuarios de los peligros que se encuentran detrás de muchas aplicaciones de dispositivos móviles. Roeseler considera a los usuarios ese «eslabón débil» puesto que, muchas veces por falta de conocimiento o por no entendimiento, aceptan términos y condiciones que sobrepasan los límites de la Ciberseguridad. A continuación tuvo lugar la Mesa Redonda «¿Ciberseguridad sin Continuidad?» donde participaron: Alfonso Martínez, experto en Resiliencia, Intel Security; Manuel Sicilia, jefe de la Sección de Análisis del Servicio de Ciberseguridad y OCC, CNPIC; Enrique Ríos, jefe de Planificación del departamento de seguridad corporativa, Abertis; y Rodrigo Jiménez, Security advisor, Neccsia; todo ello moderado por Javier Carmona, director de Seguridad de la Información y Comunicación, Iberdrola. Todos ellos

defendieron la idea anterior de Roeseler al decir que la parte más vulnerable en la Ciberseguridad son siempre los usuarios, pero añadieron que son también las empresas las que deben invertir en este sector para garantizar a sus clientes esa seguridad. Como conclusión añadieron que la base del éxito de la Ciberseguridad se encuentra en: liderar, concienciar

y educar. Durante esta Mesa Redonda también se presentó el estudio «Top 5 amenazas» realizado por Necsia con la colaboración de ISMS Forum Spain. En este estudio se muestra también el estado de la continuidad de negocio y soluciones para mejorar la situación.

Ya por la tarde, el IV Foro de la Ciberseguridad continuó con su sesión vespertina con la segunda Mesa Redonda «Ciberseguridad sin movilidad IoT» formada por: Rafael Santos, miembro del Comité Operativo, Centro de Estudios en Movilidad y jefe de Área de Seguridad Informática en



el Ministerio de Fomento; Paloma Llana, miembro del Comité Operativo del Centro de Estudio en Movilidad y Socio-Director de Razona Legaltech; Jesús M. Domínguez, miembro del Comité Operativo del Centro de Movilidad y Enterprise Business Team Security Solutions, Samsung Electronics Iberia; y Raúl Siles, Founder & Senior Security Analyst, DinoSec; y

moderado por Fernando Picatoste, Socio de Deloitte. Durante esta Mesa se presentó el Centro de Estudios en Movilidad y se añadió la necesidad de crear conciencia no sólo en los usuarios, quienes normalmente no tienen nociones sobre seguridad, sino en las mismas empresas, que deben ser, dicen, las encargadas de invertir en Ciberseguridad y así evitar que sus usuarios corran riesgos de este tipo.

Para cerrar el IV Foro de la Ciberseguridad ISMS Forum Spain Raúl Siles ofreció una demostración de hacking en directo.

Cepreven: Plan Estratégico 2015-2020



Tras finalizar los pasos necesarios para su proceso de elaboración, el nuevo Plan Estratégico para el periodo 2015-2020 de Cepreven ha sido presentado al Consejo de Dirección celebrado el pasado 14 de octubre, a cuya sesión asistió como invitada D^a. Pilar González de Frutos, presidenta de UNESPA.

Los órganos de gobierno aprobaron dicho plan, que ha sido definido como una herramienta para impulsar el crecimiento de la Asociación mediante la adopción de diferentes líneas de actividad, siempre enmarcadas en el cumplimiento de los fines estatutarios. Para la elaboración del mismo se ha contado con la inestimable colaboración de todos los

consejeros, que han transmitido a la dirección sus impresiones sobre los temas propuestos, así como nuevas ideas que han sido incorporadas al documento.

El plan se estructura, de acuerdo con este propósito, diseñando las acciones correspondientes que permitan cumplir con la misión de la Asociación, que es «la promoción y fomento de las medidas susceptibles de adoptarse tanto por la Administración como por las entidades, empresas, particulares y la sociedad en su conjunto, para eliminar o reducir las pérdidas y daños en vidas, bienes y riqueza nacional, mediante el estudio, análisis y divulgación de las causas y fenómenos que las producen, así como paliar sus efectos y consecuencias en los aspectos humanos y económicos», siempre enfocando las actividades desde nuestra visión, basada en la colaboración con todo tipo de entidades, públicas y privadas, con el fin de adquirir y generar conocimiento para compartirlo con todos los socios y la sociedad en general. Éste se vertebra sobre cinco ejes estratégicos: Colaboración Internacional, Promoción y Difusión de Conocimiento, Calidad y Fiabilidad, Asociados y un último dedicado a los Valores que han de regir las actividades desarrolladas, dentro de los cuales se enmarcan tanto las actuales como las nuevas propuestas presentadas en el mismo.

SKL: ¿se puede registrar quién accede a las vitrinas de museos, tiendas de antigüedades, subastas...

¿Se puede registrar quién accede a las vitrinas de museos, tiendas de antigüedades, joyerías, subastas...? ¿Se puede evitar los robos o manipulaciones limpias? El Sistema IS de SKL, lanza un nuevo cierre para vitrinas.

El Sistema IS de SKL es una solución de control de accesos para los puntos más sensibles de tu negocio. Consiste en una llave inteligente (incopiable, cancelable en caso de pérdida y guarda los movimientos realizados), cierres electrónicos sin baterías, sin cables, no necesitan mantenimiento y un software de gestión muy sencillo e intuitivo donde decides quién abre (usuario), cuándo (calendario) y dónde (cierre).



Con este sistema ganarás en:

- Seguridad: restringiendo los accesos no autorizados.
- Transparencia: Siempre deja huella por donde abras.
- Ahorro: No más robos limpios, cambios de cerraduras.
- Adaptabilidad: Soluciones para distintas aplicaciones, vitrinas, puertas, vallas, armarios... y puntos de control de rondas.

Y evitarás

- Manipulaciones: En los artículos, objetos de arte...
- Robos: Robos limpios, robos que no dejan rastro.
- Descontrol: En llaves, copias no deseadas.
- Inseguridad: No saber quién accedido, cuándo y dónde.

Con el nuevo cierre para vitrinas, podremos controlar y restringir los accesos para esas zonas sensibles donde se guardan obras de arte, joyas o artículos de gran valor. Gracias a este nuevo cierre, SKL puede dar una solución más completa para museos, joye-



¿Qué más puntos puedo controlar con el Sistema IS?
Vitrinas / Armarios



Puertas / Almacén



Transporte de obras de arte



Punto de control (Control de rondas)

En SKL, queremos dar una solución integral de control de accesos para que no quede ningún punto sin gestionar. Y así, ayudarle a mejorar en los servicios de su negocio.

RESTRICCIÓN DE ACCESOS
Prohibición de gestionar la apertura de la vitrina. Cierres electrónicos en ferretería, joyería y arte.

UNA ÚNICA LLAVE. Sin necesidad de cables. Control total de las llaves activas. INCOPIALES, REPARABLES Y CANCELABLES. Una única llave para todos los cerraduras.

NO MÁS FALTA DE MATERIAL. En caso de robo limpio se garantiza gracias a los registros de accesos.

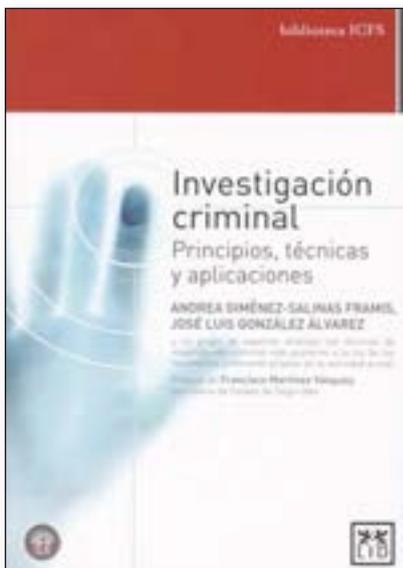
DEJA HUELLA. La cerradura y la llave guardan los eventos de apertura realizados en vitrinas.

INFORMACIÓN ACTUALIZADA. Transmisión de la base de información siempre online actualizada en el sistema (software).

Investigación Criminal. Principios, técnicas y aplicaciones

La delincuencia actual conforma un mosaico muy variado de conductas ilícitas con naturalezas y génesis diversas. Este es un libro pionero en la materia que porta una concepción internacional de las amenazas que acechan a la seguridad nacional y aporta estrategias y soluciones para hacerles frente.

Los delitos como el terrorismo, el crimen organizado, la cibercriminalidad, la delincuencia económica, la corrupción o los delitos sexuales o de género presentan niveles de complejidad dispares que demandan la especialización, actualización y tecnificación de las unidades encargadas de la investigación criminal para actuar con eficacia y eficiencia. La investigación criminal es el proceso a través del cual los especialistas reconstruyen los hechos acontecidos y aportan las pruebas de culpabilidad que permitirán al juez establecer la responsabilidad penal. En



este proceso, se utilizan diversas técnicas y procedimientos de obtención de indicios e información que permitirán reconstruir los hechos con la mayor calidad posible. En Investigación Criminal: principios, técnicas y aplicaciones, un grupo de expertos procedentes de las unidades de investigación criminal de élite y procedentes del ámbito académico describen y analiza las diferentes técnicas de investigación existentes, sus fundamentos y aplicaciones a los diversos ámbitos delincuenciales, así como sus limitaciones para los retos criminales actuales.

Esta obra será herramienta de consulta obligatoria en distintas uni-

Prosegur mantiene en 2015 la tendencia positiva en su crecimiento

Prosegur ha registrado un beneficio neto consolidado durante los nueve primeros meses de 2015 de 127 millones de euros, lo que representa un incremento del 17,1 por ciento con respecto al mismo periodo del año anterior.

En cuanto a la facturación, ésta ascendió a 2.943 millones de euros, un 6 por ciento más que en el tercer trimestre de 2014. El EBIT, resultado operativo antes de impuestos, se sitúa en 228 millones de euros, lo que también representa una mejora con respecto al mismo periodo del año anterior de un 6 por ciento.

En los resultados de los nueve primeros meses de 2015 destacan la tendencia positiva y el crecimiento sostenido de las tres líneas de negocio de la compañía: Sistemas Integrales de Seguridad, Logística de Valores y Gestión de Efectivo y Alarmas. Este periodo también ha demostrado que, a pesar de la presión ejercida por

economías como la brasileña, el modelo de negocio de Prosegur ha mantenido su resistencia y compromiso con la rentabilidad.

En cuanto a la actividad de la compañía por línea de negocio, Soluciones Integrales de Seguridad presentó en los nueve primeros meses del año un incremento de la facturación del 3,5 por ciento alcanzando los 1.479 millones de euros.

La unidad de Logística de Valores y Gestión del Efectivo logró un incremento de sus ventas del 7,7 por ciento hasta los 1.308 millones de euros en los nueve primeros meses del año. El negocio de Alarmas presentó un importante crecimiento a pesar de la estacionalidad propia del tercer trimestre en Europa. Las ventas de la unidad crecieron hasta los 156 millones de euros en los nueve primeros meses del año, lo que supone un crecimiento del 16,4 por ciento.

versidades y programas de postgrado universitarios.

Coordinadores:

Andrea Giménez-Salinas Framis es directora académica del Instituto de Ciencias Forenses y de la Seguridad. También es presidenta de la Sociedad Española de Investigación Criminológica.

José Luis González Álvarez es doctor en Psicología y máster en Psicología Clínica. Es diplomado en Ciencias Forenses y Criminología por la Universidad Autónoma de Madrid y diplomado superior en Psicología militar. Es profesor y ponente habitual en actividades de formación policial.

AGA, presencia internacional de la mano de Bosch

BOSCH Rexroth, filial de la multinacional BOSCH, ha firmado un contrato con AGA para los próximos cinco años, en los que se le suministrará un modelo de cerradura especial para un producto con unas características muy específicas, un tipo de válvula hidráulica que se instala en maquinaria para obra civil. Con este contrato, AGA refuerza su presencia en el mercado internacional, esta vez de la mano de una multinacional como BOSCH, una compañía de gran reputación y prestigio.

TDI ofrece oportunidad a socio inversor



LA marca de CCTV TDI, a punto de presentar su próximo catálogo, plantea la oportunidad a inversores interesados de incorporar a su accionariado un socio inversor.

Con una experiencia en el mercado de más de 30 años, TDI es uno de los especialistas en el campo de la videovigilancia y las telecomunicaciones.

Los interesados pueden llamar al teléfono 615 96 27 67 o bien escribir a tdi@cctvtdi.com solicitando un dossier informativo.

Dahua asegura la ciudad de Arezzo

Dahua Technology, fabricante y proveedor mundial de productos de videovigilancia con sede en Hangzhou, China, junto con Videotrend, han provisto de un sistema de monitorización de videovigilancia efectiva para asegurar la ciudad de Arezzo para cumplir con los requisitos estándar de alta seguridad de la administración de la ciudad.

Arezzo es una ciudad de Italia, capital de la provincia del mismo nombre, situada en la Toscana. Arezzo es conocida por sus iglesias, museos, su fabulosa Piazza Grande inclinada, y la producción de material de oro.

Una solución IP altamente innovadora y fiable, fue adaptada por los especialistas de Dahua para garantizar la seguridad de la ciudad. La cámara de red de

Dahua cuenta con 2 megapíxeles, escaneo progresivo sensor Exmor CMOS, proporcionando imágenes de alta calidad a 25 / 30fps @ 1080P. Es compatible con H.264 y MJPEG dual codec y detección inteligente. Con rango IR 30 metros, la cámara funciona bien en todas las condiciones de luz, día y noche.

Las cámaras de la serie ITC con un algoritmo muy eficiente proporcionan vigilancia inteligente de carreteras y calles, lugares para monitorear las condiciones del tráfico. Con su función de resolución de alta definición de imagen y la velocidad de obtura-

ción a 1/25 ~ 1 / 100.000, estos dispositivos pueden capturar imágenes ultra claras de vehículos y reconocer las matrículas, incluso cuando conducen a una velocidad muy rápida. Estos dispositivos inteligentes han integrado reconocimiento óptico de caracteres (OCR) y se pueden utilizar para control del semáforo en rojo.

Se utilizaron NVRs de la serie Dahua Súper NVR6000DR con capacidad hasta 128 canales y pantalla LCD frontal. Este modelo cuenta con módulos de alimentación redundante y también es compatible con las cámaras de red multimarca, incluyendo

Dahua, Arecont Vision, Axis, Bosch, Brickcom, Canon, CP Plus, Dynacolor, Honeywell, Panasonic, etc., con su apoyo a RAID 0/1/5 / 6/10/50/60, de

protección de datos puede llegar a la máxima seguridad y fiabilidad.

«Dahua ofrece soluciones de seguridad inteligentes que permiten un Arezzo más inteligente y seguro», dijo Elmer Zhang, director de Ventas de Europa de Dahua Technology.

«Las excelentes cualidades de las imágenes obtenidas, incluso en condiciones de luz extremas permiten la supervisión ininterrumpida de las zonas de riesgo, y por lo tanto, Dahua ha dado cuenta de su objetivo de protección para los residentes locales y turistas en Arezzo».



Bunker Seguridad incorpora la línea Redwall de Optex a su catálogo

Bunker Seguridad amplía su catálogo de soluciones perimetrales con la incorporación de la familia REDWALL de Optex, pensada especialmente para instalaciones de videovigilancia.

Al incorporar los detectores REDWALL a los sistemas perimetrales de videovigilancia se mejora la eficiencia de los mismos, porque se consigue aunar la detección efectuada por los detectores y la imagen recogida por las cámaras en el instante en que se produce dicha detección por parte del detector REDWALL,

dando una mayor capacidad de reacción al operador.

Además, Optex ha trabajado con los principales fabricantes del sector (Milestone, Genetec, Exacq Technologies) en la integración de los detectores en sus sistemas VMS (Video Management Software), lo que facilita la gestión del conjunto, al manejarse todo desde el mismo software.

La familia REDWALL cuenta con distintas líneas de producto, basadas en detección por infrarrojos y por láser: REDWALL, REDWATCH (con cámara incorporada) y REDSCAN.



Hommax optimiza sus productos contra incendios

Hommax Sistemas lanza Fireclass, una amplia gama de productos para la detección de incendios del grupo Tyco, que le permite a partir de ahora ofrecer la máxima seguridad tanto a pequeñas y medianas instalaciones como a aquellas de gran envergadura.

La incorporación de la serie Fireclass supone la plena adaptación de Hommax a la normativa de PCI que entrará en vigor el próximo año y que revisa los criterios de diseño, puesta en marcha y mantenimiento de los sistemas de detección de incendios.

Hommax pretende concienciar sobre la importancia de los sistemas de detección contra incendios en la protección de personas y bienes. Las principales agrupaciones de bomberos de las comunidades autónomas exigen que en España sea obligatoria la instalación de sistemas de detección en domicilios, como ocurre en Francia desde el pasado 8 de marzo. «También conviene mantener el lugar de trabajo limpio y ordenado. La suciedad, los derrames de líquidos y materiales como virutas, papeles y cartones pueden originar fácilmente incendios», apunta Enrique Giménez, Product Manager de Intrusión e Incendio de Hommax.

Gunnebo: SafePay PLUS

Gunnebo, especialista mundial en productos, soluciones y servicios de seguridad, ha presentado su línea de negocio para la gestión de efectivo SafePay PLUS, que garantiza la protección de los ingresos de los clientes, aumenta la productividad y mejora la experiencia de compra del consumidor.

Las nuevas cajas de depósitos inteligentes SafePay PLUS se pueden utilizar en pequeñas y grandes empresas, y simplifican los procesos de retirada de efectivo y la detección de billetes falsos, con lo que se reducen de manera muy significativa los robos y atracos en establecimientos.

La nueva gama SafePay PLUS de Gunnebo automatiza completamente el pago de efectivo y los procesos de cambio en el punto de venta, evitando que el personal maneje dinero

directamente, al tiempo que con su software de gestión propio los clientes pueden tener toda la visibilidad del flujo de efectivo desde la caja hasta el banco en tiempo real.

SafePay PLUS incorpora, además, las ventajas de la videovigilancia IP desarrollada por Axis Communications, fabricante mundial del mercado de vídeo en red.



Samsung y Veracity: solución integrada de grabación y almacenamiento de vídeo

Samsung Techwin Europe y Veracity acaban de presentar 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 con-

sume 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.



Vivotek: nuevas soluciones de vigilancia H.265

Vivotek ha presentado sus nuevas soluciones de vigilancia con H.265/HEVC, las cuales incluyen una serie de cámaras de red de 3-Megapíxeles y 5-Megapíxeles, NVRs (grabadores de vídeo de red) y VMS profesional (software de gestión de vídeo). Para maximizar la eficiencia del ancho de banda y almacenamiento, Vivotek ha presentado la tecnología Flujo Inteligente II (Smart Stream II) con la cual se logra una mayor rentabilidad. Mediante la adopción de Flujo inteligente II y la tecnología H.265 de Vivotek, los usuarios se beneficiarán con la reducción de ancho de banda y demandas de almacenamiento de datos en hasta en un 80% más que en los sistemas que emplean H.264. Todo esto permite a Vivotek alcanzar un nuevo escalón en la vigilan-



cia IP y compartir este avance con sus usuarios. «H.265/HEVC, la nueva tecnología de compresión de vídeo puede brindar el doble de eficiencia que H.264. Vivotek pretende alcanzar este gran logro a través de su propio desarrollo de la tecnología de Flujo Inteligente II», dice Tim Su, director del departamento de Productos y de Comunicaciones de Marketing.

Synology: Surveillance Station

Synology® Inc ha anunciado el lanzamiento oficial de Surveillance Station 7.1,



que cuenta con un diseño más cuidado y eficiente e incluye el protocolo de streaming en tiempo real (RTSP), ofrece compatibilidad con la multidifusión, y proporciona alertas y notificaciones perfeccionadas. Estas prestaciones permiten una mejor experiencia en la gestión de vídeo. Algunas de las características son:

- RTSP para una experiencia de vigilancia más fluida.
- La multidifusión mejora la eficiencia del ancho de banda cuando hay numerosos escenarios de uso.
- Las alertas y notificaciones avanzadas de visionado en directo permiten perfeccionar la gestión.

ÍNDICE

MATERIALES, EQUIPOS Y SISTEMAS DE SEGURIDAD

- ALARMA Y CONTROL
- BLINDAJES, PRODUCTOS
- CALZADO DE SEGURIDAD
- CENTRALIZACION DE ALARMAS
- COMUNICACIONES
- CONTROL DE ACCESOS. ACTIVO
- CONTROL DE ACCESOS. PASIVO
- DETECCIÓN DE EXPLOSIVOS
- DETECCION DE MATERIALES Y OBJETOS
- EQUIPOS DE PROTECCIÓN INDIVIDUAL
- EVACUACIÓN Y SEÑALIZACIÓN
- EXTINCIÓN DE INCENDIOS
- ILUMINACION DE SEGURIDAD
- INFORMÁTICA DE SEGURIDAD
- MATERIAL POLICIAL
- PROTECCION CONTRA EXPLOSIONES
- PROTECCION CONTRA INCENDIOS. ACTIVA
- PROTECCION CONTRA INCENDIOS. PASIVA
- PROTECCION CONTRA INTRUSION. ACTIVA
- PROTECCION CONTRA INTRUSION. PASIVA
- PROTECCION CONTRA CONTAMINACION
- PROTECCION CONTRA ROBO Y ATRACO. ACTIVA
- PROTECCION CONTRA ROBO Y ATRACO. PASIVA
- PROTECCION CONTRA VANDALISMO
- PROTECCION DE LA INFORMACION. SEGURIDAD DOCUMENTAL
- PROTECCION PERSONAL
- SANIDAD
- SEGURIDAD LABORAL
- SEGURIDAD VIAL
- VEHICULOS BLINDADOS
- VEHICULOS CONTRA INCENDIOS
- VIGILANCIA POR TELEVISION
- VARIOS. SEGURIDAD ACTIVA
- VARIOS. SEGURIDAD PASIVA

SERVICIOS DE SEGURIDAD

- APLICACIONES INFORMATICAS
- ASOCIACIONES
- CENTRALES DE RECEPCION Y CONTROL
- CUSTODIA DE VALORES
- EVENTOS DE SEGURIDAD
- FORMACION DE SEGURIDAD
- INGENIERIA Y CONSULTORIA
- INSTALACION
- INVESTIGACION PRIVADA
- MANTENIMIENTO DE SISTEMAS
- MENSAJERIA Y TRANSPORTE
- ORGANIZACION Y GESTION
- PUBLICACIONES Y AUDIOVISUALES
- VIGILANCIA Y CONTROL
- TRANSPORTE DE FONDOS Y VALORES
- VARIOS. SERVICIOS DE SEGURIDAD

ALARMA Y CONTROL



GAROTECNIA, S.A.
SISTEMAS DE SEGURIDAD

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



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



AGUERO
Proyectos e Instalaciones, S.L.

FUNDADA EN 1966

INSTALACIONES A SU MEDIDA

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



GRUPO RMD
SEGURIDAD, S.L.

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)
Tífono. 902194814 - 954108887
Fax. 954002319
gerencia@gruporomade.com
SERVICIOS EN TODA ESPAÑA



Casmart
sistemas de seguridad

Accesos CCTV Incendio Intrusión

Oficina Central:
Maresme, 71-79 - 08019 Barcelona
Fax 933 518 554
902 202 206 www.casmart.es

COMUNICACIONES



DYNASCAN
professional radio



PIHERNZ

Doctor Ramón Solanich
i Riera 13-15
08905 L'Hospitalet-BCN
Tel. 93 334 88 00*
comercial@pihernz.es
www.pihernz.com

CONSULTORIA



MBC-IURIS
Abogados y Consultores

MBC-IURIS
Abogados y consultores
C/Pau Claris, 147, 2ª, 2ª
08009 Barcelona
Tel. 931 702 417 • Fax. 931 702 416
info@mbciuris.com
www.mbciuris.com

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



TEGA
ASSA ABLUY

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

online

SEGURPARKING

Control de mandos por Internet

Sistemas de seguridad para garajes comunitarios

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



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

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



CONTROL DE ACCESO,
HORARIO, TIEMPO Y PRESENCIA

C/Samonta 21
08970 Sant Joan Despí
Tel.: +34 934774770

info@primion-digitek.es
www.digitek.es



GRUPO SPEC

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



BIOSYS
(Sistemas de Tecnología Aplicada)

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



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



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

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



Soluciones integrales en
control de Accesos
y seguridad

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

info@accesor.com
www.accesor.com



DORLET S. A. U.

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

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



SETELSA

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



ZKTECO

Camino de lo cortao, Nº 10 Nave 1
208073 • San Sebastián de los Reyes
MADRID
Tel.: +34 91 653 28 91
sales@zktechnology.eu
www.zkteco.eu

DETECCIÓN DE
EXPLOSIVOS

SISTEMAS DE
EVACUACIÓN



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



OPTIMUS S.A.

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

info@optimus.es
www.optimusaudio.com



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



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



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

PROTECCIÓN
CONTRA
INCENDIOS.
ACTIVA



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

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

www.detnov.com
info@detnov.com

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

El directorio es la zona más
consultada de nuestra revista.

Módulo: 650€/año*

Más información:
Tel.: 91 476 80 00
e-mail: publi-seguridad@epeldano.com
* Tarifa vigente 2015



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



GRUPO AGUILERA

FABRICANTES DE SOLUCIONES PCI
DETECCIÓN Y EXTINCIÓN DE INCENDIOS

SEDE CENTRAL

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

Delegaciones en:

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

Factoría de tratamiento de gases

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

Soluciones y sistemas:

** DETECCIÓN **
Algorítmica • Analógica • Aspiración • Convencional
• Monóxido • Oxyreduct® • Autónomos
• Detección Lineal
** EXTINCIÓN **
Agua nebulizada • Fe-13™ • Hfc-227Tea • Co₂



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



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.
PASIVA**



Calle Menéndez Pidal 43

Edificio B 2ª planta
28036 Madrid

Tel. 913 685 120

info@solexin.es
www.solexin.es



DICTATOR ESPAÑOLA

Mogoda, 20-24 • P. I. Can Salvatella
08210 Barberá del Vallés (Barcelona)
Tel.: 937 191 314 • Fax: 937 182 509

www.dictator.es
dictator@dictator.es

**PROTECCIÓN
CONTRA
INTRUSIÓN.
ACTIVA**



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



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



Tyco Security Products

C/ Caléndula, 95 -
Miniparc II, Ed. M, 1ª planta
28109 Alcobendas Madrid
Tf. 91 650 24 72

www.tycosecurityproducts.com
tycoacvssalesiberia@tycoint.com
tycointrusionsalesiberia@tycoint.com



BOSCH SECURITY SYSTEMS SAU

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

es.securitysystems@bosch.com
www.boschsecurity.es



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



VANDERBILT ESPAÑA Y PORTUGAL

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

**PROTECCIÓN
CONTRA ROBO
Y ATRACO.
PASIVA**

**PUERTAS Y PERSIANAS
DE ALTA SEGURIDAD**



www.colibaisarmorsystem.com



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



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



Diid Seguridad Gestión y Logística

Pol. Ind. Mies de Molladar D3
39311 CARTES - CANTABRIA
Tlfno.: 902565733 - FAX: 902565884
administracion@diid.es
www.diid.es

TELECOMUNICACIONES



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

Condesa de Venadito 1, planta 11
28027 Madrid
T. 902.095.196 • F. 902.095.196

comercial@alai.es • www.alaisecure.com

VIGILANCIA
POR
TELEVISIÓN

HIKVISION 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

STSecurity@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 - 1ªA
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.geutebrueckspain.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



Área Seguridad

Grupo Alava Ingenieros
Área Seguridad

C/Albasanz, 16 - Edificio Antalia
28037 Madrid
Telf. 91 567 97 00 • Fax: 91 567 97 11
Email: alava@alava-ing.es
Web: www.alavaseguridad.com



Josep Estivill, 67-69
08027 Barcelona, Spain.
www.ata98.com
info@ata98.com
Tel. +34 931 721 763

ASOCIACIONES



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



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



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.



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



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



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



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

info@uaseguridad.es
www.uaseguridad.es



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



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



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



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



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

¿No cree...
... que debería estar aquí?
El directorio es la zona más consultada de nuestra revista.
Módulo: 650€/año*
Más información:
Tel.: 91 476 80 00
e-mail: publi-seguridad@epeldano.com
* Tarifa vigente 2015



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



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



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



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



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



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



ASOCIACIÓN DE JEFES DE SEGURIDAD DE ESPAÑA
Avd. 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.alarmaspitz.com

INTEGRACIÓN DE SISTEMAS



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



Innovative Business Software
C/ Alcoi 106bis, 12A
08225 Terrassa (Barcelona)
Tel.: 93 789 52 05
info@innovative.es
www.innovative.es



Sant Joan de la Salle, 42. 08022. Barcelona.
Tel.: +34 93 667 40 17
Fax: +34 93 539 47 37
www.emovilia.com
E-mail: comercial@emovilia.com

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



SOCIO TECNOLÓGICO EN SEGURIDAD Y PROTECCIÓN CONTRA INCENDIOS
Stanley Security España, S. L. U.
C/ Barbadillo, 7 - 28042 Madrid
Centralita: 91 312 7777 • Fax: 91 329 25 74
scs@niscayah.es
www.stanleysecuritysolutions.es
REDGP. nº 2979 fecha 22-05-01



TELFÓNICA INGENIERÍA DE SEGURIDAD
 Don Ramón de la Cruz 82-84 4º
 28006 Madrid
 Tel.: 917 244 022 • Fax: 917 244 052
 tis.clientes@telefonica.es
 www.telefonica.es/ingenieriadeseguridad

PUBLICACIONES
 WEB



SABORIT INTERNATIONAL
 Ingeniería y consultoría de sistemas para la
 Seguridad, Vigilancia y Defensa
SABORIT INTERNATIONAL
 Avda. Somosierra, 22 Nave 4D
 28709 S. Sebastián de los Reyes (Madrid)
 Tel.: 913 831 920
 Fax: 916 638 205
 www.saborit.com



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 n° 1.833



AGUERO
 Proyectos e Instalaciones, S.L.
 FUNDADA EN 1966
INSTALACIONES A SU MEDIDA
 Antoñita Jiménez, 25
 28019 Madrid **ISO 9001**
 Tel.: 91 565 54 20 - Fax: 91 565 53 23
 seguridad@grupoaguero.com
 www.grupoaguero.com



PUNTOSEGURIDAD.COM
 TF: 91 476 80 00
 info@puntoseguridad.com
 www.puntoseguridad.com

VIGILANCIA
 Y CONTROL



Grupo RMD
 Autorizada por la D.G.P. con el n°. 729
 Avda de Olivares 17 - Plg. Industrial PIBO
 41110 Bollullas de la Mitación (Sevilla)
 Tfno. 902194814 - 954108887
 Fax. 954002319
 gerencia@gruporomade.com
 SERVICIOS EN TODA ESPAÑA



ambar
 SEGURIDAD Y ENERGÍA
SEGURIDAD
 Control accesos / Intrusión / CCTV / Detección
 incendios / Megafonía / Interfonía / Consultoría
ENERGÍA
 Eficiencia energética / Gestión inteligente de
 infraestructuras / Electricidad / Climatización
 / Consultoría energética
 www.ambarisy.e
 ambarisy@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



casesa
 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

¿No cree...
 ... que debería estar aquí?
 El directorio es la zona más
 consultada de nuestra revista.
Módulo: 650€/año*
 Más información:
 Tel.: 91 476 80 00
 e-mail: publi-seguridad@epeldano.com
 * Tarifa vigente 2015

MATERIAL
 POLICIAL



SECURITAS SEGURIDAD ESPAÑA
 C/ Entrepeñas, 27
 28051 Madrid
 Tel.: 912 776 000
 www.securitas.es



LOOMIS SPAIN S. A.
 C/ Ahumados, 35-37
 Polígono Industrial La Dehesa de Vicálvaro
 28052 Madrid
 Tf: 917438900
 Fax: 914 685 241
 www.loomis.com

Síguenos en twitter

@PuntoSeguridad





Suscríbete

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 2015)

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)

INFORMACIÓN SOBRE PROTECCIÓN Y TRATAMIENTO DE DATOS PERSONALES. De acuerdo con lo dispuesto en la vigente normativa le informamos de que los datos que vd. pueda facilitarnos quedarán incluidos en un fichero del que es responsable Ediciones Peldaño, S. A. Avenida del Manzanares, 196. 28026 Madrid, donde puede dirigirse para ejercitar sus derechos de acceso, rectificación, oposición o cancelación de la información obrante en el mismo. La finalidad del mencionado fichero es la de poderle remitir información sobre novedades y productos relacionados con el sector, así como poder trasladarle, a través nuestro o de otras entidades, publicidad y ofertas que pudieran ser de su interés. Le rogamos que en el supuesto de que no deseara recibir tales ofertas nos lo comuniquen por escrito a la dirección anteriormente indicada.



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



Ángel Bahamontes

Presidente de la Asociación Nacional de Tasadores y Peritos Judiciales Informáticos. ANTPJI

Gemma G. Juanes

CUANDO Ángel Bahamontes, presidente de la Asociación Nacional de Tasadores y Peritos Judiciales Informáticos, ANTPJI, accedió a sentarse ante «Un café con...» no sospechó que, al menos durante un rato, intentaríamos que estuviera «desconectado». Lo cierto es que, aún «acorralado» por siete ordenadores en marcha y con el teléfono móvil «pegado» a la mano, supo aunar con la destreza de un hábil conversador un académico discurso tecnológico con momentos de desenfadada charla.

Esta entrevista arranca en la azotea de un edificio de 17 plantas donde las panorámicas vistas de un Madrid de una singularidad vital son el refugio secreto de nuestro interlocutor donde recuperar la calma y tranquilidad en jornadas de extenuante trabajo. De mente y habla inquieta a partes iguales, Bahamontes se enfrenta a diario a las incógnitas de un nuevo escenario, el ciberespacio, en el que, según explica, es necesario conocer, entender, investigar y planificar medidas concretas.

«España puede presumir de contar con grandes expertos en la informática forense»

El incremento de la criminalidad en los medios informáticos junto a la implantación de las nuevas tecnologías en la sociedad, propició la aparición de una nueva actividad profesional, desarrollada en la figura del Perito Judicial Informático, un profesional con conocimientos especializados en nuevas tecnologías que «proporciona información u opinión fundada a profesionales, empresas y a los tribunales de justicia –explica– sobre los puntos litigiosos que son materia de su dictamen».

Bahamontes asumió entonces el desafío de «dignificar la profesión» y para ello no dudó en recorrer España de punta a punta en busca de los más cualificados profesionales de cada especialidad tecnológica, para que se sumaran a un apasionante proyecto, la puesta en marcha de la ANTPJI. «Un punto de encuentro de investigadores, analistas, informáticos, abogados, criminólogos, directores de seguridad,... que comparten conocimientos y experiencias –añade–, apostando por la capacitación universitaria».

Con una gran capacidad de trabajo, Ángel Bahamontes compagina la presidencia de la ANTPJI con el voluntariado en hospitales y ONGs donde desarrolla proyectos de alfabetización digital o formación para colectivos marginados. Emprendedor proactivo, visionario y creativo –además es todo un manitas en el arte del bricolaje– se muestra orgulloso al señalar que «España puede presumir de contar con grandes expertos de la informática forense que asumen los retos de la cibercriminalidad».

Lector voraz de libros en papel y formato digital sobre investigación y ciencia ficción, y apasionado de los deportes de riesgo y la música clásica, parece no querer despedirse sin insistir en que apuntemos una de sus grandes máximas en la vida: «Si se puede imaginar, se puede crear». Aquí queda escrito ●



LA CIBERSEGURIDAD A UN CLIC DE TU EMPRESA



「PROTEGE」
TU EMPRESA



 **incibe**
INSTITUTO NACIONAL DE CIBERSEGURIDAD

www.incibe.es





Compromiso



Soluciones



Calidad

Nuestras señas de identidad quedan latentes en la nueva imagen de la Compañía. Compromiso, soluciones y calidad. Una imagen renovada con un compromiso hacia nuestros clientes:

Crecemos para estar más cerca