# CUADERNOS DE SEGURIDAD

www.puntoseguridad.com

Núm. 283 ● NOVIEMBRE 2013 ● 10 euros

## Seguridad en Infraestructuras Críticas

## Sistemas de videograbación digital

Security FORUM

Las empresas reservan sus espacios en el área de exposición


CENTRAL RECEPTORA


VIGILANTES DE SEGURIDAD

# CYRASA

*grupo fragaservi*

Web: www.cyrasa.com
email: cyrasa@cyrasa.com

902194749

SISTEMAS DE SEGURIDAD

PROTECCIÓN CONTRA INCENDIOS

## CAMBIOS NORMATIVOS, CONGRESOS...

# 2013, un año para recordar

A poco más de un mes para que finalice 2013, el sector de la seguridad privada marcará en su calendario este año. Pese a que la situación económica por la que atraviesa España sigue «pesando como una losa» en todas y cada una de las diferentes actividades empresariales, incluida la de la seguridad privada, este sector está de enhorabuena: 2013 se recordará como el punto de inicio del camino hacia una nueva normativa.

Un camino que comenzó a tener forma el pasado mes de junio cuando el Consejo de Ministros aprobaba el proyecto de una nueva Ley de Seguridad Privada –CUADERNOS DE SEGURIDAD fue testigo de la iniciativa–, que impulsará la coordinación y cooperación entre los sectores de la seguridad pública y privada y abrirá la posibilidad de prestar nuevos servicios demandados por la sociedad y que no estaban recogidos en la anterior normativa de 1992. Más de 20 años después, el sector demandaba a «voces» una nueva regulación que se adaptara a la realidad y necesidades actuales de una actividad que ha experimentado en los últimos tiempos un extraordinario desarrollo. Objetivo del nuevo texto normativo –actualmente en trámite parlamentario– es regular el sector de una manera integral en el que la seguridad privada pasa a ser complemento de la seguridad pública. Los principios de complementariedad, cooperación y corresponsabilidad unido a la irrenunciable preeminencia de la seguridad pública sobre la privada constituyen los ejes rectores de la nueva norma.

Pero no sólo el sector de la seguridad privada afronta cambios normativos, también el de la seguridad contra incendios. El nuevo Reglamento de Instalaciones de Protección contra Incendios (RIPCI) –el anterior data de 1993– parece que también está en marcha, después de que el Ministerio de Industria, Energía y Turismo enviase a las asociaciones del sector –para que presentasen sus alegaciones– el borrador del Real Decreto que aprobará una norma, que fomentará el desarrollo de esta actividad en nuestro país. De nuevo, es un sector, en este caso el de la protección contra incendios, el que reclama la revisión de un documento acorde con la evolución técnica, legal y normativa que ha experimentado estos años.

Y para finalizar, PELDAÑO también recordará este 2013 como un año marcado por la puesta en marcha de proyectos e iniciativas, que han tratado de acercar la situación actual y futura de un sector en continua evolución y con un amplio espíritu emprendedor. La primera edición de Security Forum –la organización ya trabaja en el evento de 2014– se consolidó como una excepcional plataforma de networking y encuentro para los profesionales de la seguridad, un nuevo espacio donde atender a las necesidades e intereses de un colectivo que reclama encuentros de estas características para revitalizar el tejido empresarial.

Encuentros como el I Congreso de Seguridad Privada de Euskadi celebrado el pasado 30 de octubre en Bilbao que, organizado por PELDAÑO y CUADERNOS DE SEGURIDAD, contó con la asistencia de 250 profesionales. Una enriquecedora jornada de trabajo donde se analizó la realidad más actual a la que se enfrenta el sector en general y, en este caso, de una forma más concreta el de la Seguridad Privada en el País Vasco. Lo dicho: 2013, un año para recordar.

CUADERNOS DE SEGURIDAD

www.puntoseguridad.es

Nº 283 • NOVIEMBRE 2013

Peldaño

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

**Director General:** Ignacio Rojas.
**Gerente:** Daniel R. Villarraso.
**Director de Publicaciones:** Antonio Rojas.
**Directora de Contenidos:** Julia Benavides.
**Directora de Marketing:** Marta Hernández.
**Director de Producción:** Daniel R. del Castillo.
**Coordinación Técnica:** José Antonio Llorente.
**Jefa de Administración:** Anabel Lobato.
**Director de Sistemas de Información:** Raúl Alonso.

**Director de Promoción:** 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, Andrea Hidalgo.

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

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




FIPP · EUROPEAN PRESS NETWORK Fire prevention division · EUROPEAN PRESS NETWORK Security division · coneqtia

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



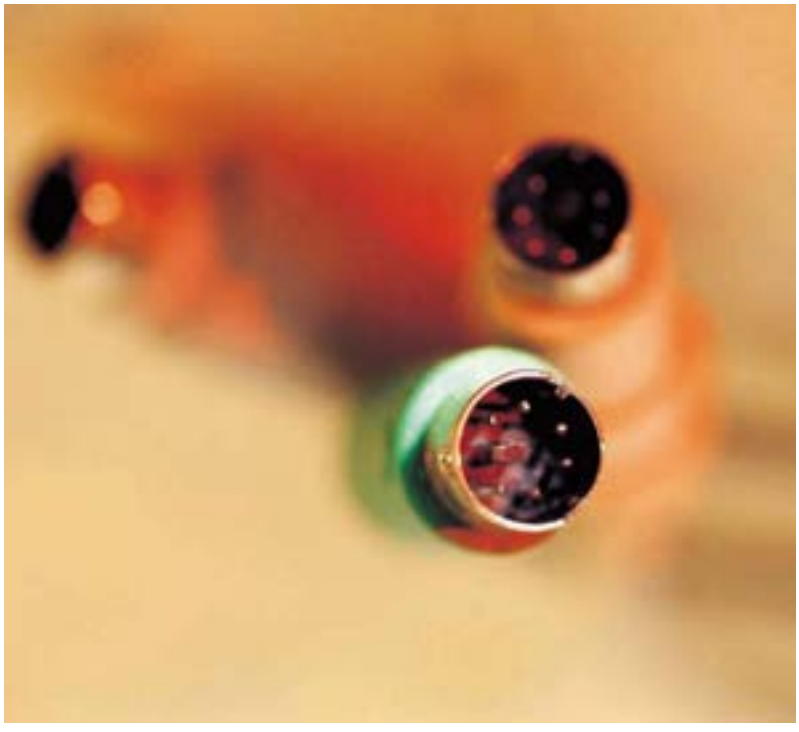


# DICIEMBRE 2013 - Nº 284

# EN PORTADA

## SEGURIDAD EN MUSEOS Y PATRIMONIO

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 sólo de ellos, de nuevo juega un papel fudamental 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. Servicios y sistemas de seguridad que sirven de ayuda y complemento al excelente trabajo que realizan los responsables de la seguridad con el fin de poder contar con dos elementos importantes: protección y prevención.



## PROTECCIÓN CONTRA ROBO E INTRUSIÓN

Una rápida y continua evolución es por lo que están pasando los sistemas de protección contra robo e intrusión, derivada, en gran medida, por la necesidad de ir adaptándose a las exigencias de una demanda que cada vez pide y exige más, así como a la normativa vigente. Elementos que han provocado que las empresas dediquen una gran parte de sus esfuerzos a desarrollar dispositivos y sistemas aún más perfeccionados.

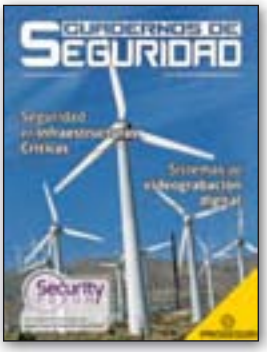
Y es que la tecnología juega un papel muy importante en el avance de este tipo de sistemas y equipos, lo que deriva en soluciones y dispositivos con una mayor fiabilidad y eficacia, acorde a las necesidades de los usuarios. Y son estos los que, día a día, demandan sistemas y equipos cada vez más innovadores.

**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 |
|---|---|---|---|
| Alai Secure | 29 | 902095195 | www.alaisecure.com |
| Alava Ingenieros | 97 | 915679700 | www.alavaseguridad.com |
| Axis | 22, 105 | 918034643 | www.axis.com |
| Bosch Security Systems | 101 | 902121497 | www.boschsecurity.com |
| By Demes | 45 | 934254960 | www.bydemes.com |
| Casesa | 4ª Cub | 902010406 | www.casesa.es |
| Casmar | 28, 71,96,100 | 933406408 | www.casmar.es |
| Checkpont Systems | 95 | 914322500 | www.checkpointsystems.es |
| Cyrasa | 2ª Cub | 902194749 | www.cyrasa.com |
| Dallmeier | 48,51, 105 | 915902287 | www.dallmeier-electronic.com |
| D-Link | 98 | 934090770 | www.dlink.com/es |
| Dorlet | 73 | 945298790 | www.dorlet.com |
| Eulen | 92 | 916 31 08 00 | www.eulen.com |
| Euroma | 99 | 915711304 | www.euroma.es |
| Eyevis | 75 | 918793806 | www.eyevis.com |
| FF Videosistemas | 41,104 | 902998440 | www.geutebruckspain.com |
| HID Global | 69 | 4401440714850 | www.hidglobal.com |
| Hikvision | 9,102 | 31235542770 | www.hikvision.com |
| Hochiki | 19,25 | 4401634260133 | www.hochikieurope.com |
| Hommax Sistemas | 47 | 961594646 | www.hommax.com |
| Honeywell | 77 | 902667800 | www.honeywell.com/security/es |
| Iptecno | 37 | 902502035 | www.iptecno.com |
| Lilin Spain | 102 | 902108533 | www.meritlilinspain.com |
| Locken | 35 | 913533942 | www.locken.es |
| LSB | 50 | 913294835 | www.lsb.es |
| Milestone | 93 | 4588300300 | www.milestonesys.com |
| Mobotix | 84, 104 | 911115824 | www.mobotix.com |
| Nice Security | 99 | 91 790 2008 | www.nice.com |
| Prosegur | 93 | 915898500 | www.prosegur.es |
| Pyronix | 3ª Cub | 1709700100 | www.pyronix.com |
| Radwin | 97 | 97237662900 | www.radwin.com |
| Risco Group | 31 | 914902133 | www.riscogroup.es |
| Riva | 17 | 4902433970370 | www.rivatech.de |
| Saborit | 63 | 913831920 | www.saborit.com |
| Samsung | 24,27, 100 | 916517507 | www.samsungsecurity.co.uk |
| Schneider Electric | 103 | 916245500 | www.schneider-electric.com |
| Security Forum | 11 | 914768000 | www.securityforum.es |
| Seguridad Integral Canaria | 61 | 902226047 | www.gruporalons.com |
| Setelsa | 59 | 942544354 | www.setelsa.net |
| Sicur | 91 | 902221515 | www.sicur.ifema.es |
| Siemens | 92 | 915148000 | www.siemens.com |
| Stanley Security Europa | 102 | 913127777 | www.stanleysecuritysolutions.eu |
| Teb Iberica | 54,55 | 918063897 | www.teb-online.com |
| Tecosa | 38 | 902 36 73 58 | www.tecosa.es |
| Telefónica | 83 | 917244022 | www.telefonica.com/ingenieriadeseguridad |
| Thales | 42,43, 97 | 985228990 | www.thalesgroup.com |
| Tyco Integrated Fire and Security | 33,94, 101, 103 | 902444440 | www.tyco.es |
| Tyco Security Products | 32, 105 | 9166502472 | www.tycosecurityproducts.com |
| UTC Fire & Security | 100 | 912191168 | www.utcfssecurityproducts.es |
| Vigilant | 85 | 965856457 | www.vigilant.es |
| Visual Tools | 79 | 917294844 | www.visual-tools.com |
| Vivotek | 53,99 | 886282455282 | www.vivotek.com |

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




## ÍNDICE DE ANUNCIANTES

# **Gemma G. Juanes**, redactora jefe de CUADERNOS DE SEGURIDAD, recibe la Medalla al Mérito Policial

## La periodista cuenta con 15 años de experiencia profesional en el sector de la Seguridad Privada

Gemma G. Juanes tras la imposición de la Medalla al Mérito Policial.

NUESTRA compañera Gemma G. Juanes, redactora jefe de la revista CUADERNOS DE SEGURIDAD, recibió el pasado 8 de octubre la medalla al Mérito Policial con Distintivo Blanco. Con motivo de la festividad de los Santos Ángeles Custodios, patronos del Cuerpo Nacional de Policía (CNP), la periodista fue condecorada en un acto en el que también se impusieron diferentes distinciones al Mérito Policial, entre otros, a funcionarios del CNP, miembros de la Guardia Civil, Fuerzas Armadas y personas ajenas al CNP.

Gemma Juanes, con 15 años de experiencia en el sector de la Seguridad Privada, es licenciada en CC. de la Información, rama Periodismo, por la Universidad Complutense de Madrid (UCM), y Máster en Periodismo Profesional del Diario ABC. Además es Diplomada Superior en Criminología y Detective Privado por la UCM.

Comenzó su trayectoria profesional en el diario «ABC», en las secciones de Sucesos y Madrid, para incorporarse posteriormente a la redacción del periódico «La Información de Madrid», donde fue redactora de las páginas de Sucesos, Madrid y Reportajes. También formó parte de la edición de Madrid del periódico «La Vanguardia», donde realizó los reportajes especiales «Fin de Semana».

Nuestra compañera junto a Esteban Gándara, Comisario Jefe de la Unidad Central de Seguridad Privada del Cuerpo Nacional de Policía.

Gemma G. Juanes se incorporó a «CUADERNOS DE SEGURIDAD» asumiendo inicialmente funciones de redacción. En 2007, tras la incorporación de la publicación a Grupo Peldaño, es nombrada redactora-jefe del Área de Seguridad de la editorial, así como posteriormente responsable también de «INSTALSEC», otra de las publicaciones que edita este grupo de comunicación.

«Es un reconocimiento que comparto con todos y cada uno de los profesionales de este sector que día a día, con su conocimiento y experiencia, hacen posible que desempeñe mi trabajo», ha explicado Gemma G. Juanes, quien admite que «esta distinción reafirma mi compromiso de colaboración y difusión de la realidad, necesidades e intereses de un sector que siempre ha respetado y valorado el papel que cumplen las publicaciones profesionales del sector de la seguridad».

Desde estas páginas queremos transmitir a nuestra compañera la cariñosa felicitación de todo el equipo de Peldaño por esta merecida distinción. ¡Enhorabuena! ●

Fotos: *MIR/Redacción*

HIKVISION

DS-2DF7286
DS-2DF7276


# Defog HD

# Tracking 30x

## MIRA LO QUE QUIERAS

## DETENIDAMENTE Y SIN DEMORA

Si quieres ver objetos con claridad, detenidamente y realizar un seguimiento sin errores, no busques más allá de los domos de alta velocidad HD 30x smart network de HIKVISION.

Caracteristicas

- 2MP(1920x1080)/ 1.3MP(1280x720)
- 30X Zoom Óptico
- IR Inteligente, 120m distancia IR
- Tracking inteligente, Desempañado inteligente.
- Codificación ROI
- 3D DNR, D WDR, HLC/BLC
- 3-Streams

Productos

DS-2DF7286
Domo de alta velocidad Network IR de 2 Megapixels
DS-2DF7276
Domo de alta velocidad Network IR de 1.3 Megapixels

www.hikvision.com

HIKVISION
Headquarters
Tel: +86-571-8807-5998
overseasbusiness@hikvision.com

Hikvision Europe
Tel: +31-23-5542770
saleseuro@hikvision.com

HOMMAX
Hikvision Distributor: Hommax Sistemas
Tel: +34-902-465-000
ventas@hommaxsistemas.com

EL ENCUENTRO SE CELEBRA EL 28 Y 29 DE MAYO DE BARCELONA

# Las empresas reservan ya su espacio en el área de exposición

## Dispondrán de un excepcional escaparate en el que mostrar los últimos productos, equipos y servicios de seguridad

La segunda edición de Security Forum sigue avanzando en su organización. A poco más de un mes de finalizar 2013, son muchas ya las empresas que han reservado su espacio para participar en Security Forum 2014, el evento que se ha consolidado como un espacio de networking y encuentro para los profesionales de la seguridad, y que en esta edición potenciará su vertiente internacional y fortalecerá su carácter innovador.

### FICHA TÉCNICA

**Fechas:** 28 y 29 de mayo de 2014.

**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 de seguridad.
- Seguridad lógica.
- Control de accesos.
- IP/redes.
- Protección contra robo e intrusión.
- Protección contra incendios.

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

SECURITY Forum se ha convertido en una auténtica plataforma de negocio donde participar y compartir experiencias. Por ello, muchas son las empresas que han comenzado a reservar su espacio en el área de exposición de esta segunda edición del salón, conocedoras de que dispondrán de un excepcional escaparate en el que mostrar sus productos, servicios y equipos.

El encuentro volverá a ser un evento ágil, flexible y orientado a la creatividad, que responderá al espíritu emprendedor y audaz que caracteriza a las empresas y profesionales del sector de la seguridad.

Security Forum 2014 mantendrá el formato novedoso que le caracterizó en su primera edición, y seguirá apostando por reforzar el tejido empresarial de un sector en continua evolución, que demanda nuevos escenarios de intercambio de conocimiento y plataformas de negocio. En un mismo espacio se congregará a los principales expertos en materia de prevención y seguridad, y la mayor oferta comercial nacional e internacional a través del área de exposición, proporcionando a los profesionales una oportunidad excepcional para conocer un completo porfolio de novedades, tendencias y avances tecnológicos en el sector de la seguridad integral. El área de exposición acogerá: CCTV, integración de sistemas de seguridad física, seguridad lógica, control de acceso, IP/redes, protección contra robo e intrusión y protección contra incendios.

> «El área de exposición acogerá: CCTV, integración de sistemas de seguridad física, seguridad lógica...»

En la web www.securityforum.es puede consultar la información actualizada sobre la próxima edición, así como el resumen de la edición de 2013. ●

**CCIB**
Centro de Convenciones
Internacional de Barcelona

Barcelona
**28 y 29 de mayo**
2014

# Security FORUM

International Security Conference & Exhibition



Un espacio donde se tomarán importantes decisiones.

¿Te lo vas a perder?

## DESCUBRE SECURITY FORUM

¿Quieres vivir una experiencia interactiva del Security Forum? Descárgate la aplicación en realidad aumentada Layar desde tu smartphone de forma gratuita, enfoca con tu móvil esta página y descubre un nuevo concepto de evento: Security Forum

layar

CUADERNOS DE SEGURIDAD

Peldaño

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

**HAN COMENZADO LOS TRABAJOS PARA EL DESARROLLO DE LOS PLANES ESTRATÉGICOS DE LOS SECTORES ENERGÍA, NUCLEAR Y FINANCIERO.**

# Seguridad en Infraestructuras Críticas, el trabajo continúa

HACE poco más de dos años que entró en vigor la Ley 8/2011, de 28 de abril, por la que se establecen las medidas para la protección de las infraestructuras críticas, y que tiene por objeto establecer las estrategias y estructuras adecuadas, que permitan dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en materia de protección de infraestructuras críticas, previa identificación y designación de las mismas, para mejorar la prevención, preparación y respuesta de nuestro Estado, frente a atentados terroristas u otras amenazas que afecten a las mismas.

Y es que, hoy en día, los Estados modernos se enfrentan a nuevas amenazas y riesgos, que confieren a la Seguridad Nacional un carácter cada vez más complejo. Todo ello unido a la mayor dependencia que la sociedad actual tiene del sistema de infraestructuras, que aseguran el mantenimiento de los servicios esenciales, hace que su protección sea una de las mayores prioridades para las diferentes naciones, entre las que se incluye nuestro país.

A modo de recordatorio, las infraestructuras críticas - un 80 por ciento de ellas están en manos del sector privada, según el Ministerio del Interior-, de acuerdo al Plan Nacional de Protección de Infraestructuras Críticas se pueden dividir en 12 sectores estratégicos:

- Centrales y redes de energía.
- Tecnologías de la información y las comunicaciones.
- Sistema Financiero y Tributario (por ejemplo, banca, valores e inversiones).
- Sector sanitario.
- Espacio.
- Instalaciones de investigación.
- Alimentación.
- Agua (embalses, almacenamiento, tratamiento y redes).
- Transportes (aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, y sistemas de control del tráfico).
- Industria Nuclear.
- Industria Química.
- Administración (servicios básicos, instalaciones, redes de información, activos, y principales lugares y monumentos nacionales).

La implantación de esta nueva normativa en el sector de las infraestructuras críticas «solamente puede ser positiva«, así lo asegura Fernando Sánchez Gómez, director del Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), quien además añade que «La promulgación de la Ley y del Real Decreto de desarrollo del Reglamento correspondiente, que obedecía a la obligación de trasponer una Directiva de la Unión Europea para mejorar la protección de las infraestructuras críticas europeas, nos ha permitido sentar las bases para establecer un sistema integral de protección de infraestructuras críticas a nivel nacional. Al llevar funcionando el CNPIC desde marzo de 2008, las relaciones con los operadores principales de los sectores estratégicos, se han llevado a cabo de una forma constante. Nunca antes había habido una cooperación entre empresas privadas y la Administración Ge-

neral del Estado tan en profundidad y de tan larga duración».

Ahora, y dentro del proceso de implantación del Sistema de Protección de Infraestructuras Críticas, en el marco de la Ley 8/2011 de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, y su desarrollo reglamentario a través del Real Decreto 704/2011, se han iniciado los trabajos para la elaboración de los Planes Estratégicos de los sectores recogidos en la citada norma, con el objeto de proteger las infraestructuras estratégicas de cada uno de ellos frente a las eventuales amenazas que puedan ponerlas en situación de riesgo.

Se han constituido 6 grupos de trabajo multidisciplinares de expertos (electricidad, gas, petróleo, nuclear, sistema financiero y sistema tributario), coordinados todos ellos por el CNPIC y con participación de los Ministerios de Economía, Hacienda, Industria, Banco de España, Comisión Nacional del Mercado de Valores, así como de empresas consultoras de primer nivel que colaboran en el proyecto.

El resultado de todo ello será el desarrollo de los trabajos tendentes a la identificación y conocimiento de los servicios esenciales que se deben garantizar y proteger, así como las consecuencias e impacto que tendría su interrupción para la sociedad. Una vez se finalicen los primeros planes se elevará su aprobación a la Comisión Nacional para la Protección de las Infraestructuras Críticas, que se convocará a dichos efectos. A partir de ese momento se empezarán a designar de forma oficial los primeros operadores críticos sectoriales, según el procedimiento designado por la Ley 8/2011 PIC. A lo largo de 2014 se tiene la intención de abordar el resto de Planes Estratégicos Sectoriales (Administración, Agua, Alimentación, Espacio, Investigación, Químico, Salud, Tecnologías de la Información y las Comunicaciones y Transporte), con el fin de implantar de forma completa la normativa vigente en materia de protección de infraestructuras críticas.

Por lo tanto el trabajo continúa, ya que los trabajos de los Planes Estratégicos se irán acometiendo de manera secuencial y progresiva. «La nuestra es una carrera de fondo, por lo que, obviamente, no podemos considerar que se haya acabado nuestra labor. Seguimos y seguiremos cooperando con los operadores críticos para garantizar la adecuada provisión de los servicios esenciales a la sociedad», explica Sánchez Gómez. ●

> «Hoy en día, los estados modernos se enfrentan a nuevas amenazas y riesgos, que confieren a la Seguridad Nacional un carácter cada vez más complejo»

Fotos: *Archivo.*

**FERNANDO SÁNCHEZ GÓMEZ.** DIRECTOR DEL CENTRO NACIONAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS (CNPIC)

# «El Equipo de Respuesta CERT-IC dotará a las empresas de los sectores estratégicos de una capa adicional de seguridad»

TRAS la entrada en vigor de la Ley 8/2011, de 28 de abril, hace ya más de dos años y medio, por la que se establecen las medidas de protección de las infraestructuras críticas, Fernando Sánchez Gómez, director del Centro Nacional para la Protección de las Infraestructuras Críticas, valora de manera positiva su implantación en el sector de las IC. Además, durante la entrevista, destaca que las relaciones con los operadores de los sectores estratégicos se han llevado de una forma constante. «Nunca antes había habido una cooperación entre empresas privadas y la Administración General del Estado tan en profundidad y de tan larga duración», subraya.

**—Más de dos años después de la entrada en vigor de la Ley 8/2011, de 28 de abril, por la que se establecían las medidas de protección de las infraestructuras críticas, ¿qué valoración haría de su implantación en el sector de las IC? ¿Cómo se está llevando a cabo?**

—La valoración solamente puede ser positiva. La promulgación de la Ley y del Real Decreto de desarrollo del Reglamento correspondiente, que obedecía a la obligación de trasponer una Directiva de la Unión Europea para mejorar la protección de las infraestructuras críticas europeas, nos ha permitido sentar las bases para establecer un sistema integral de protección de las infraestructuras críticas a nivel nacional.

Al llevar funcionando el CNPIC desde marzo de 2008, las relaciones con los operadores principales de los sectores estratégicos (energía, transporte, energía nuclear, industria química, agua, alimentación, financiero-tributario, espacio, instalaciones de investigación, salud, administración y tecnologías de la información y las comunicaciones) se han llevado a cabo de una forma constante. Nunca antes había habido una cooperación entre empresas privadas y la Administración General del Estado tan en profundidad y de tan larga duración.

La nuestra es una carrera de fondo, por lo que, obviamente, no podemos considerar que se haya acabado nuestra labor. Seguimos y seguiremos cooperando con los operadores críticos para garantizar la adecuada provisión de los servicios esenciales para la sociedad.

**—Para poner en marcha la aplicación de las medidas de protección de las IC, se diseñaron una serie de planes de actuación a nivel nacional, sectorial, de los operadores... A grandes rasgos, ¿podría indicarnos en qué consisten esos planes y su estado actual?**

—Los planes previstos son el Plan Nacional de Protección de las Infraestructuras Críticas, los Planes Estratégicos Sectoriales, Planes de Seguridad del Operador, Planes de Protección Específicos y, para redondear la actuación integral a nivel nacional, los Planes de Apoyo Operativos.

El Plan Nacional de Protección de las Infraestructuras Críticas, de 7 de mayo de 2007, tiene por objeto reducir su vulnerabilidad frente a los riesgos que para las mismas y, en último término, para la sociedad, se derivan tanto de los accidentes naturales como de los atentados terroristas o actos criminales que puedan perpetrarse contra ellas. Al

establecer una serie de niveles de seguridad, que conllevan distintas actuaciones por parte de las Fuerzas y Cuerpos de Seguridad, entre otros actores, está coordinado con el Plan de Prevención y Protección Antiterrorista, de marzo de 2005. Ambos están clasificados. El Plan Nacional ya contemplaba planes territoriales y sectoriales.

Los Planes Estratégicos Sectoriales son los planes de definición del funcionamiento de cada sector crítico o de sus subsectores.

Estos planes permitirán conocer cuáles son los servicios esenciales proporcionados a la sociedad dentro de cada sector o subsector, su funcionamiento general, las vulnerabilidades existentes a nivel estratégico y los elementos de los que se compone, las dependencias de otro sectores, las dependencias generadas en otros sectores, las interdependencias mutuas (en su caso), las consecuencias potenciales de su interrupción y las medidas estratégicas necesarias para su mantenimiento. También permitirán identificar a los operadores críticos y establecerán las bases para determinar la criticidad de las instalaciones específicas, en cada subsector.

Se está trabajando actualmente en los planes estratégicos sectoriales mediante asociaciones público-privadas entre los departamentos ministeriales competentes para cada sector o subsector crítico y los principales operadores de cada uno de los mismos, bajo los auspicios de la Secretaría de Estado de Seguridad, a través del CNPIC.

Una vez designados los operadores críticos, éstos tendrán que redactar sus respectivos Planes de Seguridad del Operador, donde se defina básicamente la política de seguridad que sigue la compañía.

Posteriormente a la aprobación de los planes de seguridad del operador, los operadores críticos tendrán que redactar Planes de Protección Específicos para cada una de las infraestructuras críticas que gestionen o sean de su propiedad.

Para completar el círculo, en cada demarcación territorial donde estén ubicadas las infraestructuras críticas concretas mencionadas en el punto anterior, se desarrollarán Planes de Apoyo Operativo para garantizar el auxilio por parte de las Fuerzas y Cuerpos de Seguridad en caso de ataque externo, en coordinación con la seguridad interior.

> «Seguimos y seguiremos cooperando con los operadores críticos para garantizar la adecuada provisión de los servicios esenciales para la sociedad»

**—El Centro Nacional para la Protección de Infraestructuras Críticas junto con el INTECO pusieron en marcha un Equipo de Respuesta ante Incidentes –CERT- ¿podría explicarnos en que consiste y cuáles son sus funciones específicas?**

—La Secretaría de Estado de Seguridad firmó hace justamente un año con la Secretaría de Estado de Telecomunicaciones y la Sociedad de la Información un convenio de colaboración, fruto del cual se aumentaron las capacidades operativas del INTECO-CERT y se incrementó su «constituency» al ámbito propio del Ministerio del Interior. El CERT-IC es el equipo de respuesta a incidentes cibernéticos dedicado a la gestión de los problemas de ciberseguridad, que afectan a las infraestructuras críticas y a aquellos incidentes cibernéticos que puedan ser competencia del Ministerio del Interior o alguna de sus unidades tecnológicas.

El CERT-IC se configura como la herramienta del Ministerio del Interior para la gestión de la ciberseguridad y la prevención y reacción ante incidentes cibernéticos. Además, cuando se produzca un incidente en una infraestructura crítica en la que intervenga el CERT-IC, se articulará la comunicación

Hace más de dos años que entró en vigor la Ley 8/2011 de 28 de abril.

de ese incidente a las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) si el mismo debiera ser perseguido por éstos. La Oficina de Coordinación Cibernética (OCC) de la Secretaría de Estado de Seguridad, que se está actualmente creando en el seno del CNPIC, será el órgano encargado de esa comunicación con las FCSE, manteniéndose siempre la confidencialidad de la información y el anonimato de las fuentes de que se trate.

Este equipo de respuesta servirá para dotar a las empresas que operan en sectores estratégicos para la sociedad de una capa adicional de seguridad, que les asegure una respuesta más amplia ante incidentes de ciberseguridad.

Además de la respuesta a un incidente ya ocurrido, desde el CERT-IC se ofrece también un servicio de prevención y de alerta temprana, destinado a la detección (y corrección) de vulnerabilidades específicas de una infraestructura crítica con anterioridad a que las mismas puedan ser explotadas por un atacante.

> «El equipo de respuesta CERT-IC se configura como la herramienta del Ministerio del Interior para la gestión de la ciberseguridad y la prevención y reacción ante incidentes cibernéticos»

**—Entre las herramientas de coordinación entre todos los agentes el CNPIC trabajaba en la creación del Sistema Hermes, ¿cómo se está llevando a cabo la implantación de este instrumento? ¿Cuáles son sus funciones concretas?**

—Hermes es un sistema de información gestionado por el CNPIC en el que, partiendo de la información operativa suministrada por las Fuerzas y Cuerpos de Seguridad, interactúan los operadores de infraestructuras estratégicas almacenando información sobre las instalaciones que gestionan, sus activos en materia de seguridad, etcétera.

Esta herramienta proporciona un canal de comunicación seguro entre todos los actores que intervienen en el escenario de la PIC (operadores, FCSE, CNPIC), haciendo más ágil el intercambio de información sobre recomendaciones de seguridad, amenazas, alarmas, etcétera.

El sistema Hermes ya está desarrollado y se espera que durante el presente año comience a utilizarse por los distintos operadores estratégicos, que se irán añadiendo de forma progresiva conforme se avance en la implantación de los distintos planes estratégicos.

El CNPIC viene trabajando desde hace años en todos y cada uno de los sectores estratégicos.

**—Recientemente han comenzado los trabajos para el desarrollo de los planes estratégicos de los sectores Energía, Nuclear, y Financiero y Tributario, en los que CNPIC es órgano coordinador de los grupos de trabajo, ¿qué aspectos comprenderán esos planes? ¿Cuáles son sus objetivos?**

—Como he dicho anteriormente, al tratar todos los planes, los Planes Estratégicos Sectoriales son los planes de definición del funcionamiento de cada sector crítico o de sus subsectores.

Se han iniciado en mayo de este año los trabajos para la elaboración de los primeros planes estratégicos de los sectores que usted menciona, a través de unos grupos de trabajo multidisciplinares formados por expertos del sector público y privado.

Los Planes Estratégicos Sectoriales comprenderán, para cada sector objeto de estudio, los servicios esenciales proporcionados a la sociedad, el funcionamiento general de éstos, las vulnerabilidades del sistema, las consecuencias potenciales de su interrupción y las medidas estratégicas necesarias para su mantenimiento. A través de un análisis general y estratégico de riesgos a nivel sectorial, se identificarán aquellas vulnerabilidades y amenazas potenciales, tanto de carácter físico como lógico, que afecten al sector en cuestión.

El objetivo es, proponer para su implantación, en función de los resultados obtenidos del estudio de cada sector:

- medidas organizativas y técnicas ne-

cesarias para prevenir, reaccionar y, en su caso, paliar, las posibles consecuencias de los diferentes escenarios que se prevean;
- medidas preventivas y de mantenimiento; y
- medidas de coordinación con el Plan Nacional de Protección de las Infraestructuras Críticas.

**—Se tiene previsto a corto plazo abordar los planes del resto de sectores estratégicos (Administración, Agua, Alimentación....)?**

—El CNPIC viene trabajando desde años atrás en todos y cada uno de los doce sectores estratégicos, identificando aquellas infraestructuras estratégicas. Sin embargo, los trabajos de los Planes Estratégicos Sectoriales se están acometiendo de forma secuencial y progresiva. Una vez se vayan finalizando los planes estratégicos de los primeros sectores anteriormente mencionados, se iniciarán inmediatamente los estudios y trabajos de los sectores restantes: transporte, industria química, agua, alimentación, espacio, instalaciones de investigación, salud, administración y tecnologías de la información y las comunicaciones.

Aunque cada uno de los sectores estratégicos tiene sus particularidades, seguiremos las mismas líneas de trabajo que se han ido siguiendo en los primeros planes, incorporando aquellas novedades y metodologías que hayan dado buenos resultados en los trabajos previos.

**—¿Cuáles considera que son las bases estratégicas a la hora de implantar una protección y seguridad adecuadas en una Infraestructura Crítica?**

—En primer lugar, hay que tener en cuenta la enorme responsabilidad que implica proporcionar un servicio que es esencial para la sociedad.

Esto por sí solo obliga a replantearse el objeto de la actividad empresarial, no haciendo un enfoque restrictivo, desde el punto de vista comercial solamente. El gasto necesario para implementar las medidas necesarias para garantizar la seguridad debe interpretarse no como una carga, sino como una inversión para garantizar la ausencia de consecuencias negativas para la población, y asegurarse de esa manera una mejor imagen, que contribuirá a aumentar la confianza de los usuarios de los servicios esenciales, aumentando de la misma manera la competitividad de la empresa de que se trate.

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

Los Planes Estratégicos Sectoriales son los planes de definición del funcionamiento de cada sector crítico o de subsectores.

**ANTONIO GARCÍA VILLACAÑAS.** JEFE DEL DEPARTAMENTO DE SEGURIDAD PATRIMONIAL. DIRECCIÓN DE SEGURIDAD CORPORATIVA. IBERDROLA

# *«Asegurar el suministro eléctrico y el normal desarrollo de las actividades son nuestro **objeto y razón de ser**»*

En todos los proyectos en los que se involucra a la Dirección de Seguridad Corporativa de Iberdrola se busca la eficacia en la gestión y la eficiencia operativa», así lo asegura Antonio García Villacañas, jefe del departamento de Seguridad Patrimonial de Iberdrola, en una entrevista en la que analiza, entre otros aspectos, la implantación de la Ley de Infraestructuras Críticas, o el papel de la tecnología en la seguridad en las grandes compañías energéticas.

**—Para comenzar, ¿podría indicarnos las líneas de negocio actuales de la compañía, número de trabajadores...?**

—Las líneas de negocio de Iberdrola son la generación, distribución y comercialización de electricidad y gas. Desarrollamos nuestra actividad industrial y comercial en decenas de países, destacando España, Reino Unido, Estados Unidos, México y Brasil. En total, el grupo cuenta con 30.500 empleados.

**—Una gran compañía, como es Iberdrola, ¿cómo tiene estructurada su Dirección de Seguridad Corporativa? ¿Cuáles son sus funciones específicas?**

—La Dirección de Seguridad Corporativa se constituyó en 2001, y en ella se encuentran integradas las funciones de protección de los activos más relevantes de Iberdrola: personas, bienes e información. Esto nos permite aportar soluciones integrales a cada uno de los ámbitos de la organización con una visibilidad de 360º.

La Dirección de Seguridad Corporativa se estructura en cuatro departamentos: seguridad internacional, seguridad operativa y normalización, seguridad de los sistemas de información y las comunicaciones, y seguridad patrimonial.

**—¿Cuáles considera que han sido los últimos avances tecnológicos que han tenido una mayor e importante aplicación en el ámbito de las grandes compañías energéticas?**

—Son varios los ámbitos en los que las tecnologías han generado un importante impacto en el modelo de ne-

**Las líneas de negocio de Iberdrola son la generación, distribución y comercialización de electricidad y gas.**


El grupo cuenta con 30.500 empleados.

gocio. Los nuevos sistemas de telecontrol de los entornos productivos (generación y distribución), los entornos de gestión (procesos de negocio), el tratamiento de la información de clientes y, sin duda, las infraestructuras con tecnologías vanguardistas aplicadas a la protección de su patrimonio. Como referencia, en el caso de Iberdrola, los centros de control de seguridad física y lógica.

En todos los proyectos en los que se involucra a la Dirección de Seguridad Corporativa de Iberdrola se busca la eficacia en la gestión y la eficiencia operativa.

**—¿Qué elementos cree que deben confluir para conseguir un grado de seguridad satisfactorio en instalaciones del tipo de las de Iberdrola?**

—Siendo objetivos en esta autoevaluación, y contrastándola con nuestro entorno, considero que nos encontramos en una situación de privilegio, que hemos conseguido, con un esfuerzo relevante, mantener en el tiempo. Es importante la dependencia directa con el primer nivel de decisión en el grupo. Eso nos permite llegar al máximo nivel jerárquico de cada organización para trasladarle la verdadera aportación de valor que la seguridad representa, generándose un binomio de protección y beneficio que ha adquirido la consideración de imprescindible.

Por este motivo, tras el asesoramiento recibido por nuestra parte en el análisis, valoración y gestión del riesgo, no hemos encontrado dificultades significativas para el desarrollo de nuestras actividades.

**—Hace poco más de dos años que entró en vigor la Ley 8/2011, de 28 de abril, por la que se establecían las medidas de protección de las infraestructuras críticas. ¿Qué valoración haría de su implantación**

**en el sector de las IC, donde se incluye el sector de Energía?**

—El impacto que debería representar esta nueva regulación en Iberdrola es mínimo. Los objetivos de asegurar la continuidad del servicio de suministro eléctrico y garantizar el normal desarrollo de las actividades de la organización son nuestros «objeto y razón de ser». La consecución de estas metas, que nos marcamos tras nuestra incorporación en 2001, nos hacen sentir especialmente orgullosos, al comprobar que hemos acertado en nuestra previsión. Al contar con esta anticipación, y tras realizar un tremendo esfuerzo inversor, hemos conseguido que nuestras infraestructuras de consideración crítica se encuentren protegidas.

**—¿Cree que la protección de las infraestructuras críticas supondrá un nuevo reto para la tecnología?**

Sin duda. La transformación de las infraestructuras críticas ya existentes y la incorporación de otras servirán de acicate para que las nuevas tecnologías sigan evolucionando.

**—Bajo su visión profesional, ¿qué ha aportado la Ley de Infraestructuras Críticas al marco general de normativa española respecto a la seguridad?**

—Considero que fundamentalmente ha aportado los conceptos de método, orden e integración.

> «Las transformación de las infraestructuras críticas ya existentes y la incorporación de otras servirán de acicate para que las nuevas tecnologías sigan evolucionado»

Por un lado, se hace necesaria la aplicación de un método riguroso basado en análisis objetivos -para ello se contempla dentro de la Ley un marco de referencia-, así como la gestión del riesgo. Ambas cuestiones deben quedar documentadas (PSO y PPE).

Por otro lado, se incluye el concepto de orden, ya que disponer del Plan Operativo de Seguridad en cada compañía conlleva la integración de todos los aspectos de la seguridad en las distintas funciones que conforman las infraestructuras críticas: personas, bienes e información.

Iberdrola está presente en España, Reino Unido, Estados Unidos...

Por último, se destaca la integración, lo que permite disponer en un único plano y al mismo tiempo de todas las infraestructuras y servicios.

**—¿Cree que en los últimos años han variado los riesgos y amenazas a los que se enfrentan los responsables de Seguridad?**

—Mi respuesta es un sí rotundo, ya que existen nuevos escenarios. En el ámbito físico, las prácticas al uso son las mismas: hurto, sabotaje, agentes antisociales, etcétera, todas ellas con pequeñas variaciones. Pero en el ámbito de las tecnologías de la información nos encontramos en un escenario asimétrico: es totalmente anónimo, el don de la ubicuidad está garantizado, los conocimientos de especialización van por delante de los nuestros y disponen de grandes capacidades y recursos.

**—¿Qué acciones lleva a cabo Iberdrola para garantizar la seguridad y salud laboral de sus trabajadores en sus diferentes plantas e instalaciones?**

—Esta es una preocupación constante y permanente para Iberdrola. Para ello existe una organización específica especializada en esa importante tarea, la de Prevención de Riesgos Laborales, con cuyos integrantes mantenemos una estrecha relación profesional.

La Dirección de Prevención de Riesgos Laborales, no solamente actúa para cumplir con lo estipulado en la legislación vigente, sino que lleva a cabo un extraordinario esfuerzo a favor de la prevención, potenciando la formación de los trabajadores, propios y ajenos. El principio de Riesgo Laboral 0 viene impuesto por nuestra presidencia. ●

*Fotos: IBERDROLA*

**EUSEBIO MORENO ORBIS.** DIRECTOR DE SEGURIDAD

# «La tecnología es un elemento dinamizador de la estrategia de seguridad»

**PARA comenzar, ¿podría explicarnos qué es el Consejo de Seguridad Nuclear y cuáles son sus funciones concretas?**

—El Consejo de Seguridad Nuclear (CSN) es un ente de Derecho Público, independiente de la Administración General del Estado, con personalidad jurídica y patrimonio propio e independiente de los del Estado, y único organismo competente en materia de seguridad nuclear y protección radiológica. Está constituido por un presidente y cuatro consejeros, conforme a lo dispuesto en el artículo 4, apartados 1 y 2 de la Ley 15/1980 de Creación del Consejo de Seguridad Nuclear, modificado por la Ley 33/2007.

**—Hace poco más de dos años que entró en vigor la Ley 8/2011, de 28 de abril, por la que se establecían las medidas de protección de las infraestructuras críticas, ¿qué valoración haría de su implantación en el sector de las IC, donde se incluye el sector Nuclear?**

—Aunque evidentemente tenga mi opinión al respecto, existen otras unidades en la estructura organizativa de este CSN, que son competentes en esta materia y que podrían dar una opinión institucional mucho más informada que la mía y a ellos les remito.

**—¿Cree que la protección de las infraestructuras críticas supondrá un nuevo reto para la tecnología?**

—Sin duda alguna es, y en el futuro más cercano será aún más, un elemento dinamizador de la estrategia de seguridad no sólo de las infraestructuras críticas, sino de instalaciones que sin ser críticas decidan tener un nivel de protección adecuado a los nuevos riesgos que ya se están afrontando desde cualquier departamento de Seguridad.

**—¿Cuáles considera que serían los elementos clave a la hora de implantar una adecuada protección y seguridad de las IC?**

—El horizonte es la seguridad.

El trayecto ineludible y urgente comenzaría:

- Adaptando la legislación vigente en materia penal a los riesgos que afrontamos.
- Adecuando la selección y formación del personal operativo (sin olvidar sus retribuciones, su estatus profesional, etc.) a los nuevos riesgos.
- Actualizando la capacidad de respuesta de las Fuerzas y Cuerpos de Seguridad del Estado en las infraestructuras críticas e instalaciones que requieran especial protección.
- Profundizando en la coordinación institucional, efectiva, real, leal y bidireccional entre el Ministerio del Interior y los departamentos de Seguridad.
- Definiendo e implantando políticas nacionales de ciberseguridad.

**—Bajo su visión profesional, ¿qué ha aportado la Ley de Infraestructuras Críticas al marco general de normativa española respecto a la seguridad?**

—Ha aportado sobre todo el impulso necesario para que todas las partes implicadas afronten el diseño e implantación de medidas de protección imprescindibles en nuestras infraestructuras críticas.

**—¿Cree que en los últimos años han variado los riesgos y amenazas a los que se enfrentan los responsables de Seguridad?**

Se incrementan los riesgos y amenazas que veníamos valorando con nuevos riesgos que hace unos años ni valorábamos: ciberterrorismo, terrorismo islamista, terrorismo biológico, nuclear, etc. ●


**OLIVIER LANDEL.** BUSINESS DEVELOPMENT MANAGER PARA EL SEGMENTO DE TRANSPORTE DE AXIS COMMUNICATIONS SOUTHERNEUROPE

# Seguridad inteligente

## Redes de tránsito y transporte

A pesar del desplome de los presupuestos, los responsables de las agencias de tránsito deben seguir creando entornos seguros para los trabajadores y los pasajeros. En los últimos 10 años, han apostado por las cámaras para la seguridad en estaciones, trenes y autobuses, pero siguen atascados en cómo monitorizar las cámaras y qué buscar. Sin embargo, una nueva era se está abriendo paso con la llegada de las cámaras IP, que reemplazan a los antiguos sistemas analógicos y cambian la forma de monitorizar y localizar los problemas. Anthony Incorvati, director de Desarrollo de Negocio en el sector de transporte dentro de Axis Communications, destaca que la clave del nuevo sistema es la sencillez: «simplemente, funciona. Lo conectas y ya puedes trabajar.»

La videovigilancia sobre los sistemas de tránsito lleva vigente más de una década y ha requerido una significativa inversión en tecnología analógica, lo que puede frenar a muchas organizaciones a la hora de migrar a la nueva tecnología. «Un problema para nosotros es que el coste de un sistema analógico es menor al de un sistema IP, por lo que, cuando ofrecemos una solución IP tenemos que ajustarnos al rango de precios esperado», señala Danny Peleg, director de Marketing para el área de tránsito de Genetec. «Y las soluciones sin servidores nos permiten cumplir las expectativas e incluso rebajar el coste total». Esta compañía proporciona una solución que permite a los operadores de tráfico librarse de los servidores en sus sistemas de cámaras, a favor de suministrar los datos de forma inalámbrica. «El servidor es la pieza más débil del puzle. Cuando hay problemas, normalmente es por el servidor», destaca Peleg.


**La videovigilancia sobre los sistemas de tránsito lleva vigente más de una década.**

## Las cámaras analógicas, en extinción

Frente a sus predecesoras analógicas, las redes de cámaras IP no son sistemas cerrados. Pueden abrirse y ser vistos por múltiples agencias si fuese necesario, y los costes de actualización se reducen al no ser necesario reemplazar el sistema físico. Las actualizaciones de software pueden realizarse en los sistemas y, frente a los viejos sistemas de cámara, no necesitan ajustarse manualmente. Las cámaras IP pueden durar hasta siete años, reduciendo aún más los costes de reemplazo y actualización. «Los proveedores de sistemas analógicos eran muy parecidos unos a otros», recuerda Incorvati, «una vez que una oficina de tráfico contrataba un proveedor, en cierto modo se 'casaba' con él, pero en el nuevo escenario para nada es así.»

Tras los atentados en el metro de Londres en marzo de 2003, los responsables de Seguridad tuvieron que visualizar horas y horas de videovigilancia para unir las evidencias sobre el incidente, lo que supuso varios días de trabajo. Con los sistemas IP, los investigadores que están buscando incidentes en los sistemas de transporte públicos

pueden ahora obtener las evidencias de forma instantánea. Las autoridades aeroportuarias, los sistemas ferroviarios y otras grandes organizaciones de transporte se han aferrado a la tecnología y, actualmente, la mitad de las agencias de tránsito en Estados Unidos están instalando cámaras IP. Para 2016, se espera que esta cifra crezca hasta el 80 %.

En cuanto a los problemas de uso y desgaste de las cámaras IP, los proveedores están buscando formas de garantizar que resistan no solo golpes y vibraciones constantes en un vehículo móvil, sino también actos vandálicos y temperaturas extremas.

## Más que seguridad

Moti Shatai, vicepresidente de Operaciones de Seguridad para el Transporte en Nice Systems, explica que los clientes están buscando sistemas que les proporcionen seguridad para los pasajeros y les ayuden a optimizar las operaciones. Mientras algunas cámaras están vigilando las vías y los trenes para asegurarse de que nadie pase por los raíles, otras cámaras contabilizan el número de pasajeros para garantizar que las líneas de tren están funcionando eficazmente y evitar embotellamientos.

Los desarrolladores de software necesitan, por un lado, conocer qué quieren los clientes y, por otro, ajustar los sistemas para obtener el máximo rendimiento. Sin embargo, el principal reto para la tecnología es detectar un incidente en tiempo real, mientras se resuelven los problemas de tipo ambiental que afectan a las cámaras, desde nieve y niebla a grandes sacudidas o fuertes vientos.

## Evolución tecnológica continua

Los sistemas de seguridad han pasado de la mera detección de movimiento a generar analíticas sobre lo que se está viendo. Las cámaras necesitan determinar si los movimientos son de animales o personas, y por qué el objeto está en movimiento, para comprender lo que se está viendo y reducir el número de falsas alertas. Los sistemas utilizan un conjunto de algoritmos para el auto-aprendizaje como parte de las analíticas de comportamiento, de tal modo que las cámaras puedan determinar por qué alguien está corriendo en una estación mientras otras personas están andando, y aprender qué puede considerarse un comportamiento normal. «El tiempo de aprendizaje es muy rápido: no se tardan días ni meses, sino minutos», señala Shatai.

Existe un software de reconocimiento de comportamientos, que graba los problemas operativos y riesgos de seguridad potenciales, además de documentar y analizar el comportamiento, para que los proveedores de tráfico tengan una imagen más amplia de lo que está pasando en su sistema. Permite a los responsables de Seguridad y de Tránsito no solo ver lo que pasa en el sistema sino comprender por qué se producen determinadas acciones.

Por otro lado, otra compañía ha desarrollado el acceso móvil al vídeo, lo que permite a los empleados de tráfico y responsables de Seguridad acceder a los datos a través del smartphone u otros dispositivos. También permite que estos dispositivos se transformen en cámaras para suministrar aún más flexibilidad al grabar.

Y nuestra compañía ha desarrollado una cámara capaz de filmar en condiciones de poca luz de hasta 0.05 lux. Las cámaras pueden ahora detectar actividades sospechosas y leer automáticamente las matrículas para encontrar vehículos. Algunos usuarios de los sistemas IP incluso presumen de que ningún ojo humano está pendiente ya de las cámaras. Así, el personal de seguridad está en las estaciones, donde deben estar, en lugar de sentado frente a una pantalla de ordenador. ●

> «En los últimos años, los responsables de las agencias de tránsito han apostado por las cámaras para la seguridad en estaciones, trenes y autobuses»

Fotos: *Archivo.*

**Frente a sus predecesoras analógicas, las redes de cámaras IP no son sistemas cerrados.**

Contactos de empresas, p. 7.


**JOSÉ LUIS ROMERO.** GENERAL MANAGER SPAIN & PORTUGAL DE SAMSUNG TECHWIN EUROPE

# Soluciones de seguridad para infraestructuras críticas

LAS consecuencias de un ataque con éxito a una infraestructura crítica (bien una planta de tratamiento de aguas, una línea de ferrocarril, una central nuclear, una central eléctrica…) van más allá de los posibles costes financieros por la reparación de daños: estamos hablando de actos que pueden incidir de forma directa en el día a día de la sociedad y suponer, en algunos momentos, una seria amenaza para las personas.

Para estos casos, marcas en seguridad profesional como nuestra compañía ofrecen soluciones de seguridad integradas, sacando provecho de la tecnología más reciente e incorporada a los sistemas de videovigilancia, la protección perimetral y los sistemas de control de accesos. Ahora, se puede supervisar la actividad de una ubicación en tiempo real las 24 horas del día, tanto desde una sala de control in situ como de forma remota desde cualquier punto del planeta mediante un ordenador conectado a la red, lo que permite que el personal de seguridad y los directores de operaciones respondan rápida y eficazmente ante cualquier incidente o emergencia en desarrollo.

La mayoría de infraestructuras críticas ya cuentan con un alto nivel de seguridad que, probablemente, incluya cámaras de seguridad. Los avances tecnológicos más recientes han facilitado, no obstante, una sencilla vía de actualización y modernización de lo que puede ser un sistema analógico tradicional a una solución basada en red, brindando la oportunidad de controlar y supervisar el sistema desde cualquier punto. Y lo que es más importante: la grabación en vídeo se puede guardar en cualquier ubicación de la red y recuperarse después desde cualquier ordenador mediante usuario autorizado. Por tanto, se puede introducir un alto nivel de redundancia al elegir grabar y almacenar vídeo de forma simultánea en múltiples ubicaciones.

La generación más reciente de cámaras megapíxel HD ofrece funciones de Análisis de Vídeo Inteligente (IVA): detección de movimiento, detección de entrada/salida, detección de línea virtual, aparición/desaparición de objetos... El IVA también cuenta con una función de detección de sabotaje por cambio de escena creando una alerta si, por ejemplo, se pulveriza pintura en la lente de una cámara o se produce un movimiento no autorizado de la cámara que la aparte de su campo nor-

**La mayoría de las infraestructuras críticas ya cuentan con un alto nivel de seguridad que, probablemente, incluya cámaras de seguridad.**

**Sala de Control donde supervisar la actividad.**

mal de visión. Todo ello en la propia cámara, sin necesidad de licencias.

## Seguridad en edificios públicos

Las autoridades locales y los ministerios de los gobiernos de todo el mundo reconocen desde hace tiempo el papel fundamental que los sistemas de videovigilancia y control de accesos pueden desempeñar a la hora de garantizar que los ciudadanos vivan seguros. Detectar, evitar actividades delictivas y comportamientos antisociales, hacer cumplir las normas y gestionar grandes aglomeraciones son sólo algunas de las formas en las que los sistemas integrados de control de accesos y videovigilancia pueden ser útiles en la seguridad de las personas, al ofrecer una respuesta eficaz ante cualquier amenaza o comportamiento peligroso.

> «La mayoría de infraestructuras críticas ya cuenta con un alto nivel de seguridad que, probablemente, incluya cámaras de seguridad»

En el entorno económico actual debe aceptarse que los gobiernos probablemente pongan en práctica restricciones presupuestarias pero, sin embargo, la necesidad de contar con sistemas de videovigilancia sigue siendo igual de importante que antes... si no más. Afortunadamente, marcas como nuestra compañía ofrecen una amplia gama de productos de seguridad, a fin de dar soluciones asequibles y rentables para prácticamente cualquier proyecto.

Existe una amplia variedad de cámaras y domos, que incluye modelos antivandálicos instalables en el exterior, capaces de rendir eficazmente con independencia de las condiciones medioambientales. Entre las prestaciones principales destacamos la tecnología de «ampliación del rango dinámico» (Wide Dynamic Range), que garantiza que se pueden grabar imágenes de alta calidad incluso en condiciones de iluminación complejas, y la tecnología Súper Rango Dinámico de Samsung (SSDR), una progresión de la compensación de retroiluminación que destaca automáticamente los detalles de las zonas oscuras de toda una escena para revelar los objetos escondidos en la sombra. La tecnología DIS (Estabilización Digital de Imagen) es otra característica innovadora que puede corregir los resultados

de una cámara poco estable por efectos del viento o de posibles vibraciones.

La mayoría de nuestras cámaras y domos más recientes también ofrecen multistreaming, con una variedad de métodos de compresión (MJPEG, MPEG-4 y H.264) adecuados para el ancho de banda disponible, lo que permite transmitir imágenes simultáneamente a múltiples ubicaciones y equipos y a distintas resoluciones. Así, los distintos usuarios autorizados pueden supervisar las imágenes de una ubicación en vivo, al tiempo que siguen grabando pruebas en vídeo de otra. Recordar también que pueden grabarse imágenes en una tarjeta de memoria SD, y enviar notificaciones de posibles incidentes por correo electrónico a un Smartphone o Tablet.

Por último mencionar la tecnología de escaneado progresivo (Progressive Scan) integrada en un gran número de cámaras y domos, a fin de optimizar la grabación de vídeos de alta calidad de objetos en movimiento lo que permite, por ejemplo, que se puedan leer con nitidez las matrículas de los coches,

**La generación más reciente de cámaras megapíxel HD ofrece funciones de Análisis Inteligente de Vídeo.**

Contactos de empresas, p. 7.

ya que la imagen no se desenfoca aún cuando exista movimiento.

Las opciones híbridas disponibles incluyen codificadores: un método económico y de fácil implantación a la hora de añadir cámaras analógicas a un sistema de videovigilancia basado en red. Disponemos también de un programa continuado de integración con proveedores en software de gestión de vídeo (VMS), que ofrecen un software «abierto» y diseñado específicamente para facilitar la integración de los equipos y los sistemas de distintos fabricantes. Así, ofrecemos a los clientes también la flexibilidad de poder elegir la combinación perfecta de productos de seguridad que satisfagan sus necesidades.

## Tecnología al rescate

Las cámaras megapíxel HD ofrecen mucho más que sólo imágenes de calidad. También incorporan características que facilitan a los operadores responder eficazmente ante cualquier acto sospechoso o de emergencia. La mayoría de estas características de «valor añadido» están incorporadas en el conjunto de chips DSP de la cámara.

Además de capturar imágenes con todo lujo de detalles, las cámaras megapíxel tienen la opción, entre otros beneficios, de transmitir simultáneamente imágenes de baja resolución, que incluyen QVGA (320 x 240), VGA (640 x 480) y SVGA (800 x 600): distintos usuarios autorizados pueden controlar simultáneamente imágenes en directo de un lugar, grabar pruebas en otro o bien visualizar imágenes grabadas o en directo desde un Smartphone o Tablet.

Al mismo tiempo, se pueden adjuntar imágenes JPEG de un incidente a una notificación de alarma enviada por correo electrónico con su correspondiente pre/post alarma previamente grabado en una tarjeta de memoria SD.

En algunos casos los usuarios no necesitan trabajar con las resoluciones más altas: es vital entender los requisitos operacionales a fin de proponer soluciones que satisfagan los requisitos específicos del proyecto. Por lo general, un sistema de seguridad comprende cámaras HD megapíxel para necesidades concretas, específicas, junto con cámaras de resolución estándar para fines de visualización general.

Escaneado progresivo (Progressive Scan). Hasta hace poco un problema común, que a menudo puede resultar frustrante, ha sido que los usuarios finales que han invertido en cámaras domo PTZ observen que las imágenes grabadas con la cámara en movimiento no tienen la claridad deseada u ocasionan lo que se conoce como zonas borrosas. Si el usuario final es un aeropuerto o un puerto, o se encuentra inmerso en una misión crítica, su confianza hacia el sistema de videovigilancia se verá mermada ante grabaciones de baja calidad, pues espera que ofrezca imágenes que le permitan identificar objetos y personas de forma clara. Los estacionamientos y parkings, las propiedades industriales y los centros comerciales son entornos donde las cámaras PTZ se instalan con frecuencia y en los que las imágenes borrosas pueden tener un impacto negativo en la capacidad del personal de seguridad a la hora de tomar decisiones rápidas y eficaces en caso de incidentes o emergencias.

Afortunadamente, una vez más, la tecnología ha acudido al rescate. Una prestación conocida como escaneado progresivo (Progressive Scan) optimiza la grabación de vídeos en alta calidad y ofrece imágenes más nítidas. La mejora se puede apreciar sobre todo en imágenes pausadas lo que facilita (como hemos mencionado con anterioridad), entre otras aplicaciones, la lectura de matrículas. ●

Fotos: *Archivo/Samsung.*

# PENSAMIENTO INTELIGENTE

## WisenetIII CON DETECCIÓN FACIAL FRONTAL Y DE PERFIL

### La opción más inteligente para los profesionales...

- Detección facial: detecte rostros de frente y de perfil
- P-iris: el control de iris preciso mejora la resolución, el contraste y la claridad
- Multi-Cropping: destaque y seleccione hasta 5 áreas de interés y disfrute de un uso eficiente del ancho de banda
- Antiniebla: mejore la calidad de las imágenes grabadas en condiciones meteorológicas adversas
- Detección avanzada del movimiento: mejora la inmunidad al ruido, cree máscaras de áreas e ignore aquellos objetos que no satisfagan los requisitos especificados
- Detección avanzada del sonido: mejora su eficiencia gracias a que la cámara reconoce sólo los ruidos atípicos y contribuye a reducir el número de alarmas
- Instalación rápida: nueva estructura de cableado extraíble que permite una instalación rápida
- SSLE (Sistema de incremento de la sensibilidad de Samsung)
- WDR mejorado: aumenta la calidad de las imágenes, con menos zonas borrosas y un procesamiento más eficaz de las imágenes claras
- Salida de imagen: salida de dos imágenes Full HD a 1080p simultáneamente

www.samsungsecurity.co.uk

SAMSUNG

SAMSUNG TECHWIN

**JORDI ALONSO.** JEFE DE PRODUCTO DE CCTV. CASMAR


# Protección perimetral de infraestructuras críticas con análisis de vídeo

## Éxito garantizado

LAS infraestructuras críticas requieren una protección perimetral de muy alta fiabilidad. Como consecuencia de los estándares internacionales de homologación, podemos garantizar que el vídeo-análisis es una tecnología útil, fiable y eficaz al estar certificada para su uso en infraestructuras, siendo además, flexible y fácil de instalar.

### Protección de perímetros con la máxima fiabilidad

Hoy en día es fácil encontrar un gran número de soluciones capaces de proteger perímetros (barreras de microondas, barreras de infrarrojos, cable sensor de valla, cable enterrado, etc.), pero cuando se trata de hacerlo con la máxima fiabilidad, el binomio de cámaras térmicas y vídeo-análisis se muestra como la solución más solvente. Si, además, las distancias crecen, el coste de implantación de las propuestas habituales crece en la misma medida, algo que no sucede con la tecnología térmica y el vídeo-análisis.

Un sistema de protección perimetral eficaz debe ser capaz de filtrar todos aquellos elementos que hacen fallar a otras tecnologías como, por ejemplo, la lluvia, el viento o la niebla. Si hablamos de grandes perímetros debemos añadir a esta lista nuevas necesidades: la mayor longitud del perímetro dificulta la labor de los vigilantes, por lo que es necesario incluir un sistema capaz de detectar el acceso no autorizado de personas o vehículos al perímetro, permitiendo distancias de detección muy superiores a las habituales (para no encarecer la solución y conseguir que sea viable) pero con total fiabilidad.


Las infraestructuras críticas requieren una protección perimetral de muy alta fiabilidad.

La combinación de cámaras térmicas y análisis de vídeo permite detectar intrusos con la máxima fiabilidad, y nos ofrece la posibilidad de cubrir grandes superficies con pocos sensores, permitiendo distancias de detección de más de 450[1] metros con una sola cámara. De esta forma se consigue un ahorro económico en material, costes de obra civil y mantenimiento. En el contexto actual, con los presupuestos de seguridad en contención, ésta es sin duda la mejor opción. Pero su implantación no se limita solo a este tipo de perímetros, y son cada vez más los clientes que eligen esta tecnología para proteger perímetros de menor tamaño gracias a su mayor eficacia. Además, la utilización de hardware estándar homologado por grandes fabricantes de electró-

[1] Para las cámaras térmicas de Flir junto con el vídeo análisis de Davantis.

# Red Inteligente + Seguridad M2M:

## La solución integral para las comunicaciones de su CRA

En ALAI somos especialistas en garantizar la SEGURIDAD de las comunicaciones de nuestros clientes. Más de ocho años de experiencia en la operación de comunicaciones críticas nos avalan como el Operador Global de Telecomunicaciones del sector SEGURIDAD.


**www.alaisecure.com**

Alai Secure

Soluciones profesionales para empresas de Seguridad

Condesa de Venadito, 1
28027 Madrid · España
T. 902 095 195 · F. 902 095 196

nica en la construcción de los equipos de analisis de vídeo garantiza su estabilidad y robustez, reduciendo así los costes de mantenimiento.

## Homologación del Ministerio del Interior del Reino Unido

La presencia en el mercado de sistemas con diferentes niveles de fiabilidad motiva la necesidad de un sistema de homologación independiente, así que el Ministerio de Interior del Reino Unido, a través de su departamento de Desarrollo Científico, puso en marcha en 2007 el primer programa de certificación de análisis de vídeo, realizado por una entidad independiente sin ánimo de lucro. El objetivo es homologar sistemas de análisis de vídeo para su uso en infraestructuras gubernamentales: recintos militares, centrales nucleares, prisiones, centros petroquímicos, puertos, aeropuertos, etc.

El programa de homologación i-Lids valora la fiabilidad y eficacia tecnológica de los sistemas de análisis de vídeo. Mide la capacidad de detección de intrusos y el nivel de falsas alarmas de cada sistema. Se definen dos niveles de homologación: Principal y Secundario. Principal significa que el sistema de Vídeo-Análisis puede funcionar como sistema único de alarma anti-intrusión. Secundario, significa que requiere de otros productos complementarios para proteger un perímetro de forma fiable.

La homologación garantiza la eficacia y fiabilidad tecnológica de los sistemas, y en el caso del Reino Unido, es un requisito imprescindible para su instalación en centros públicos gubernamentales o militares, pero fuera de este país es también útil para valorar el nivel de fiabilidad de cada sistema.

## Vídeo-Análisis para Centros de Control

Además de la fiabilidad del sistema, uno de los puntos importantes es la gestión de alarmas de su software para centros de control.

Un sistema que «mira» automáticamente nuestras instalaciones tiene ventajas evidentes. Por una parte, es difícil escapar de él, ya que la visión de una cámara cubre una gran superficie. Por otro lado, por su propia naturaleza, las alarmas de estos sistemas son videoverificadas, lo que permite respuestas más eficientes a las alertas reales. Si además tienen la capacidad de enviar las detecciones a Centros de Control, tendremos una solución de altas prestaciones con un coste mucho más competitivo que un vigilante privado.

La combinación de estos sistemas con cámaras de visión térmica reducen al mínimo los falsos positivos, aumentando considerablemente su eficacia respecto a las cámaras convencionales. Junto con una buena herramienta de gestión de alarmas para el Centro de Control, convierten en eficaz y rápido el trabajo de los operadores.

Algunos productos permiten que el Centro de Control pueda prestar servicios avanzados. Por ejemplo, la combinación de Vídeo-Análisis con un Centro de Control permite activar sirenas o encender luces rápidamente cuando el operador ha verificado que se ha producido una intrusión real. De esta forma tenemos un sistema activo con capacidad disuasoria.

## Facilidad de uso

La facilidad de uso es un valor añadido para el cliente y para su Centro de Control. Hay características imprescindibles, como: la activación mediante teclado de alarma convencional, y la videoverificación mediante grabación inteligente.

La activación de los equipos de vídeo-análisis mediante el teclado de alarma convencional facilita su uso. Un usuario autorizado puede armar y desarmar el equipo cuando entra o sale del perímetro vigilado. De esta forma, se evita el envío innecesario de alarmas al Centro de Control, reduciendo el coste de operación.

La videoverificación mediante grabación inteligente con indicador de intrusiones es imprescindible para optimizar el funcionamiento del Centro de Control. En caso de intrusión, el operador puede ver inmediatamente el vídeo de la grabación, con un recuadro indicando el motivo de la alarma. Y todo con un solo clic en el ordenador. El vídeo inteligente con prealarma proporciona mucha más información que una cámara en directo o una grabación indicadores de intrusión. ●

El binomio de cámaras térmicas y vídeo-análisis es la solución más solvente para proteger perímetros.

Fotos: *Casmar*

Contactos de empresas, p. 7.

# Agility™3

Perfectas imágenes vía radio

## Controle su seguridad Estando Appsolutamente conectado


El sistema de seguridad inalámbrico **Agility™3** combina la más avanzada tecnología de verificación visual con una interesante Aplicación para Smartphone. Esto permite a la CRA y al usuario controlar remotamente el sistema de seguridad y verificar si realmente se está produciendo una intrusión o la señal se debe a una falsa alarma.

App Store Play Store iRISCO

Para más información acerca de **Agility™3** llame al: 91 490 21 33

riscogroup.es

RISCO Group Iberia | Tel: 91 490 21 33 | Fax: 91 490 21 34 | E-mail: sales@riscogroup.es

RISCO GROUP

Creating Security Solutions. With Care.

**JORGE SANZ SESMA.** REGIONAL SALES MANAGER IBERIA. TYCO SECURITY PRODUCTS

# Gestionar la seguridad de manera eficiente

## Las infraestructuras críticas deben ser protegidas de forma muy especial debido al superior riesgo general que entrañan

EL concepto de infraestructuras críticas resulta ser un poco subjetivo; para todos nosotros nuestras infraestructuras, sean del tipo que sean, son críticas. Pero, por otro lado, todos también entendemos que hay algunas que por razón de su naturaleza, en el caso de sufrir algún tipo de incidente, el perjuicio que puede provocar va mucho más allá de la propia entidad que gestiona y explota esa infraestructura, resultando perjudicada en general la sociedad en cualquiera de sus facetas.

Estas infraestructuras críticas deben ser protegidas de forma muy especial debido precisamente al superior riesgo general que entrañan y, por supuesto, hay que ampliar la evaluación de riesgos hasta los niveles máximos, contemplando cualquier detalle y amenaza por pequeña o remota que pudiera parecer.

Para cubrir de forma adecuada todos estos riesgos y amenazas extendidos, hay que desplegar una serie de medidas de prevención de muy alto nivel y políticas de gestión muy avanzadas. Como es lógico los equipos a cargo de gestionar la seguridad de estas instalaciones necesitan trabajar con niveles de eficacia y responsabilidad más altos de lo normal, ya que las consecuencias de concretarse algún riesgo son muy superiores, y deben ser por ello tremendamente eficaces a la hora de resolver cualquier incidente que se produzca. El secreto del éxito para obtener unos niveles de eficacia acorde con las expectativas necesarias se basan en aunar lo mejor de dos mundos: los mejores medios humanos y los mejores medios técnicos.

**INTEVO, plataforma hardware y software de gestión integral.**

Un eficaz equipo de seguridad asegura la realización con éxito de sus funciones de protección. Pero por supuesto, hoy en día, debido a la infinidad de amenazas existentes en la actualidad, son imprescindibles una serie de medios técnicos que complementen y eleven la eficacia de ese equipo hasta los niveles de precisión y eficacia exigida para estas infraestructuras.


**Sistema unificado de Dirección de seguridad Ccure 9000 y Victor.**

Todos hemos conocido de forma no poco dolorosa que los equipos humanos cometemos errores y que además las máquinas, teóricamente infalibles, también, o no siempre están ahí para avisarnos y solventar los problemas por nosotros. Por esto el diseño del sistema de seguridad de estas infraestructuras críticas debe contar con una infraestructura que integre de forma lo más perfecta posible a los responsables y gestores del sistema de seguridad con los mejores medios técnicos disponibles, y no dejar ningún resquicio para que se produzca cualquier fallo, ya sea técnico o humano, que desencadenen la serie de pequeños incidentes que pueden ocasionar un accidente más grave.

Los directores de Seguridad de una instalación crítica no deben conformarse con sistemas de seguridad electrónica, que simplemente presenten una información aséptica en unas pantallas

# Soluciones que marcan la diferencia

tyco Integrated Fire & Security

Como la empresa de seguridad electrónica más grande del mundo, **Tyco Integrated Fire & Security** cuenta con los conocimientos técnicos necesarios para integrar soluciones de seguridad y protección contra incendios.

**Tyco Integrated Fire & Security** ofrece diferentes niveles de servicios de integración que van desde la integración sencilla de múltiples productos de seguridad hasta la integración más compleja de infraestructuras TI y aplicaciones de procesos empresariales, combinando soluciones físicas y lógicas. Sepa más sobre cómo podemos proteger su negocio en *www.tyco.es*

**916 313 999**
**www.tyco.es**

tyco Integrated Fire & Security

procedentes de un complejo manojo de cables de algo que aparentemente pueda estar ocurriendo al otro extremo de la instalación. No deben aspirar sólo al mero sistema de aviso de una «alarma» para que los vigilantes la comprueben.

Hoy en día la evolución de los modernos sistemas de seguridad permite ir mucho más allá en la gestión electrónica, y pueden dotar a los profesionales de la seguridad de herramientas extremadamente eficaces, de cara a gestionar cualquier incidente en una instalación crítica pudiendo contemplar cualquier tipo de supuesto de riesgo actual, así como hacer evolucionar el sistema a medida que la experiencia nos obligue sin restricciones de ningún tipo.

Para implementar este tipo de sistemas de seguridad electrónica, sólo podemos contar con fabricantes con una dilatada experiencia en la fabricación y desarrollo de estos eficientes sistemas. Experiencia no solo referida a la evolución activa de estas tecnologías a lo largo del tiempo, sino también experiencia en su implementación en un mundo globalizado en todo tipo de instalaciones, regiones y ambientes, aunando e integrando todas las diferentes tecnologías disponibles para la protección de cualquier instalación.

Estos sistemas van más allá de integrar de manera más o menos elegante las diferentes tecnologías y mostrarlo todo conjuntamente en una sola pantalla, sino que unifican la información enlazándola y proporcionando a los operadores y al equipo de seguridad un mensaje claro de lo que está ocurriendo, apoyándose en imágenes, mapas, áreas, y niveles de riesgo, de tal manera que la forma de enfrentarse a los incidentes cambia de forma radical. Ya no hay que pasar por sistemas en donde hay que averiguar qué está tratando de decirnos el monitor de turno y después averiguar que está pasando: Un sistema «Unificado» nos comunica claramente qué está pasando, cuándo, cómo y dónde, e incluso adicionalmente puede iniciar políticas de seguridad activa en la instalación para prevenir otros incidentes, informar en diferentes instancias e indicar protocolos concreto de actuación a todos los implicados. En la práctica la denominación específica de un sistema de estas características es la de «Software de Dirección de Seguridad».

> «Hoy en día la evolución de los modernos sistemas de seguridad permite ir mucho más allá en la gestión electrónica»


**Software de Dirección de Seguridad. software House Ccure 9000.**

## ¿Cuáles son las claves de estas nuevas herramientas para la dirección y gestión de seguridad?

Una de las claves más importantes es que se trata de un sistema que unifica los diferentes medios técnicos que habitualmente utilizamos para proteger una instalación. El sistema reside en una sola máquina, o en varias, pero funciona como una sola y desde ella se controlan todos los componentes útiles del sistema.

**CCTV:** El sistema puede gestionar de forma indiferente el vídeo procedente tanto de un sistema de grabación digital analógico como los más potentes y modernos sistema de grabación de cámaras de alta definición IP, pasando por las tradicionales matrices de conmutación de vídeo. Pero todo ello de forma transparente para el operador, este visualizará las imágenes que necesite para la gestión de la instalación, sin tener que saber de qué dispositivo electrónico se trata. El sistema presentará el vídeo de una forma concreta y al operador concreto, ya sea de forma manual mediante un mapa o de forma automática provocado por un evento, y si fuera necesario indagar más allá de la cámara en cuestión implicada y entrar en modo investigador para realizar búsquedas inteligentes en las cámaras adyacentes hasta localizar los orígenes del incidente. Las instalaciones normalmente están vivas y pueden tanto crecer como evolucionar, necesitando más puntos de control visual y cámaras de cualquier tecnología, con lo que no tendremos ninguna limitación a la hora de hacer crecer este sistema y sin restricciones en su arquitectura.

**Control de accesos y personas:** Por supuesto el propio sistema tiene moni-



# LA LLAVE DE UN CONTROL DE ACCESOS INTELIGENTE

CONTROL DE ACCESO SIN CABLEADO

LOCKEN
Simple key • Smart access

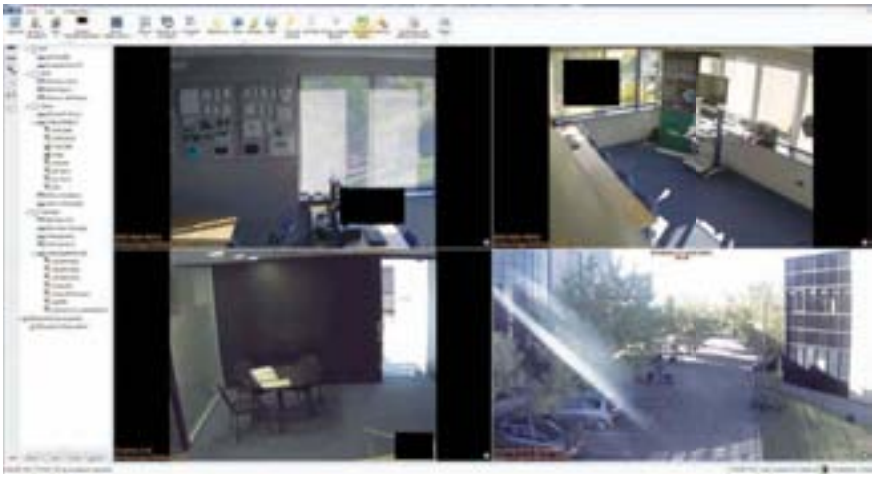
LOCKEN - CALLE JOSÉ BARDASANO BAOS, 9 - 28016 MADRID - ESPAÑA - TLF : (+34) 91 353 39 42 - WWW.LOCKEN.ES

torizado y controlado todos los elementos críticos de accesos, y a las personas asociadas a la instalación. Ninguna puerta o ventana se queda abierta o cualquier personal no autorizado accede a zonas restringidas, llegando al punto de poder monitorizar áreas y personal sin tener que limitar los accesos de forma física con puertas y cerraduras. En el caso de un acceso no autorizado a un área específica, el sistema ejecutará una actuación automática mostrando al operador con todos los datos necesarios para corregirla e incluso registrar el resultado del incidente para su posterior análisis y fiscalización. La capacidad ilimitada de crecimiento en puntos de monitorización y control de accesos nos asegura la posibilidad de expandir y multiplicar los niveles de seguridad en función de las necesidades presentes y futuras.

**Intrusión:** Este sistema hace propio los sistemas anti intrusión, que debido a la legislación específica que les vincula necesitan de un hardware específico certificado. Pero todas las señales de los diferentes sistemas anti intrusión pasan a formar parte del sistema principal, e interactúan con el resto de componentes del sistemas exactamente igual que si partieran del propio sistema principal, de hecho el sistema puede, para facilitar al operador el manejo de estos dispositivos, imitar el teclado físico del panel de intrusión en forma virtual en la pantalla de un puesto de operador, para no duplicar los procesos de aprendizajes y gestión. Los niveles en los que nos encontramos de integración con estos paneles nos permite no solo integrar paneles de alarma de forma individual, sino llegar incluso a gestionar varios de estos paneles como si se haría en una central receptora de alarmas, pudiendo contar con líneas alternativas de back up para las centrales receptoras de alarmas, así como para los diferentes puesto de control de las propias instalaciones.

**Sistemas de detección de incendios:** Al igual que ocurre con los sistemas anti intrusión la legislación es incluso más restrictiva, por lo que la interactuación con estos sistemas se limita a las labores de apoyo, aportando información adicional a los parcos sistemas de detección de incendios. Si salta un detector en un área específica, un mapa nos debe decir dónde está exactamente esa área y mostrarnos el vídeo en vivo de forma automática, para que junto con el listado de presentes y las instrucciones específicamente diseñadas para esa situación determinar el nivel de riesgo concreto. Si por cualquier razón el sistema no recibiera confirmación por parte del operador sobre el incidente en concreto, el propio sistema podría iniciar un protocolo de actuación de forma automática, reportando el evento en otras diferentes instancias.

**Cliente Unificado de Gestión de Vídeo Victor.**



## ¿Cómo puede ser fácil para un operador de seguridad trabajar con un sistema tan potente?

Muy sencillo, cada operador específicamente solo recibe los mensajes exclusivos para él y para sus funciones. Solo tiene que interactuar con los elementos puramente de seguridad: Puertas, personas, vistas de vídeo de zonas de riesgo, no con los medios electrónicos que le envían la información. Estos que pasan a ser totalmente transparentes. De esta manera un sistema extremadamente potente puede servir de forma personalizada y sencilla a cualquier tipo de operador en función de sus atribuciones. Si algo que ha recibido el operador no está claro, incluso con las diferentes instrucciones que le puede presentar el sistema, este puede enviar la incidencia a otro puesto de control para que ellos le apoyen o lo gestionen directamente ante cualquier duda. En este tipo de instalaciones mejor chequearlo más de dos veces.

Finalmente, y como parte no menos importante de estos sistemas, está su sistema de reporte de información. Absolutamente todo lo que ocurre en el sistema queda archivado para su posterior estudio llegado el caso. Todos los cambios que se realicen de forma autorizada quedan también registrados. Esto nos permite fiscalizar cualquier cambio introducido en el sistema especialmente cuando ha sido de forma errónea. En el caso de que se produzca algún incidente, siempre podremos revisar lo que ha ocurrido e introducir mejoras en el protocolo de actuación y evitarlo en el futuro. ●

Fotos: Tyco


# DVR PEGASO

## Mucho más que un videograbador

TU LOGO

### Tu empresa se merece su aplicación.

Avanza un paso más, sabemos que **tu empresa** se merece trabajar con sus propias herramientas, te proponemos que tengas **tu aplicación**, a tu medida, personalizada con **tu imagen y tu logo**, disponible para descargar en iTunes y PlayStore, lista para que **tus clientes** la instalen y trabajen con **tus videograbadores.**

Diferénciate de la competencia, regístrate en **www.iptecno.com**

iPTECNO®

BARCELONA
C/Pla del Ramassar 52
08025 Granollers

CANTABRIA
Av. Santander 23B
39180 Noja

T. 902 502 035
F. 902 502 036
**www.iptecno.com**

**ÓSCAR CABRAL SIERRA.** PRODUCT MANAGER DE SISTEMAS Y SOLUCIONES DE SEGURIDAD. TECOSA

# Elección de UAS en las infraestructuras críticas

## Sistemas Aéreos no Tripulados

La compleja situación económica que atraviesa nuestra nación está obligando a una revisión de las estrategias corporativas en materia de seguridad, con el fin de racionalizar los recursos técnicos y humanos y tratar de adecuarlos al contexto socio-económico vigente.

La respuesta a esta situación debe liderarse alentando la puesta en escena de soluciones innovadoras, con una barrera de entrada asumible por las empresas, y que permita una rápida amortización de la inversión sin menoscabo de las prestaciones técnicas. Una de las soluciones a esta compleja ecuación dentro del contexto de las infraestructuras críticas, la brinda el empleo de Sistemas Aéreos no Tripulados (Unmanned Aircraft Systems o UAS). En este artículo desgranamos algunos de los conceptos más relevantes a la hora de seleccionar el UAS que mejor se adecue a las necesidades de nuestra instalación.

La seguridad debe constituir uno de los criterios esenciales de su diseño.

Se trata de una tecnología con un protagonismo creciente en el entorno civil, compuesta por un vehículo aéreo sin tripulación a bordo, en el que es posible distinguir un segmento «aire» y un segmento «tierra». El segmento aire comprende la plataforma de vuelo, la carga de pago o carga útil (cámaras de vídeo, sensores de medida…) adecuada a la misión encomendada, y el sistema de comunicaciones. El segmento tierra comprende el sistema de control de la aeronave y de su carga útil, los equipos de comunicaciones y la estación que permite transmitir la información obtenida con los sensores.

Entre sus características más relevantes, suele ser habitual prestar atención a parámetros tales como su peso máximo en el despegue (en inglés Maximun Take-Off Weight o MTOW), el rango de vuelo o el tipo de aeronave. En este sentido y por sus múltiples aplicaciones en el contexto de la seguridad en infraestructuras críticas, nos centraremos en los UAS con peso no superior a 5 Kg de tipo quad-rotor (con despegue vertical) y alcance LOS (Line Of Sight).

Entre las consideraciones más importantes a la hora de seleccionar el quad-rotor más adecuado, resulta muy importante tener presentes los siguientes aspectos.

**Condiciones de Vuelo**. Según datos de la Agencia Estatal de Meteorología, en un lugar como Madrid hay 63 días al año con precipitaciones iguales o superiores a 1mm, 16 días de tormenta o 4 días de nieve, lo que suponen 83 días de condiciones meteorológicas adversas anuales, o lo que es lo mismo, una probabilidad de un 22% de posible inoperatividad de los sistemas UAS por inclemencias atmosféricas, aspecto éste que puede resultar desalentador para los responsables de un departamento de Seguridad. Por este motivo resulta imprescindible analizar detenidamente las características constructivas de la unidad de vuelo, tales como la estanqueidad de la unidad de vuelo frente a lluvia o nieve o la resistencia al viento. En el segmento de los micro y mini UAS, un valor estándar de resistencia al viento del segmento aire está en los 25 Km/h, valor que puede resultar insuficiente en muchas zonas de España, donde se producen vientos sostenidos de intensidad superior a 25 Km/h, lo que incrementaría aún más la tasa del 22% de inoperatividad previamente estimada. Resulta por tanto esencial seleccionar sistemas micro o mini UAS en los que el fabricante avale la usabi-

lidad de la unidad en condiciones de lluvia, nieve o viento.

**Tiempo de vuelo**. La mayor parte de los fabricantes de micro UAS publican en sus hojas de características técnicas tiempos de vuelo similares. Sin embargo, resulta clave determinar si la información proporcionada incluye la unidad de vuelo con carga de pago y bajo qué condiciones de vuelo (viento, temperatura…). Una carga de pago adosada a la unidad de vuelo puede reducir el tiempo de vuelo en un 50%.

**Seguridad**. La seguridad debe constituir uno de los criterios esenciales de su diseño, de forma que su manejo no represente una amenaza para los usuarios ni para el resto de la población. La operación segura de estas unidades requiere la posibilidad de:

- Conocer el estado de carga de la batería, informar al piloto y, en caso necesario, regresar al punto de despegue (o a la posición «home»).
- Indicar en todo momento la velocidad de viento registrada por la unidad de aire, y en caso de que se sobrepase el umbral permisible, forzar su aterrizaje.
- Establecer un radio máximo de seguridad en torno a la posición de despegue, de manera que en caso de que la unidad no sea capaz de retornar a la posición de despegue, ésta aterrizará automáticamente en el momento en que se sobrepase dicho alcance máximo.
- No posibilitar la operación del vehículo en caso de que se detecte cualquier fallo en la unidad.
- Respuesta inteligente en caso de fallo de comunicación, con retorno a la posición de despegue.

La disponibilidad de estas funciones de seguridad posibilitan que el operador se pueda centrar en la misión encomendada.

**Coste**. El coste de la unidad de vuelo y subsistemas de control representa sólo una parte de la inversión necesaria para la adquisición de un sistema UAS. Deben considerarse como parte de la misma la formación, práctica en el manejo del sistema o su mantenimiento. Se ha comprobado que una interfaz de usuario basada en una pantalla táctil, disminuye de manera muy significativa el tiempo de aprendizaje requerido con esta tecnología. Un interfaz de usuario sencillo e intuitivo resulta imperativo en caso de que no se emplee la unidad de manera continuada, a fin de evitar la necesidad de cursos de refresco. Desde el punto de vista del mantenimiento, resulta deseable que el sistema haya sido diseñado de manera modular para eliminar o reducir al máximo la necesidad de mantenimiento, reduciendo los costes directos de dicha tarea y los costes indirectos derivados de no poder emplear el sistema durante el periodo de mantenimiento.

**Número de operadores para su manejo.** Muchos de los sistemas comercializados actualmente requieren más de un operador. La posibilidad de que el sistema sea manejado por un solo operador representa una ventaja en términos de rapidez de despliegue, fiabilidad y costes. En estos casos, el sistema debe proporcionar al operador la funcionalidad necesaria para asegurar el control del vuelo y de las cargas útiles, junto con la supervisión de los datos proporcionados por el sistema.

> «Se trata de una tecnología con un protagonismo creciente en el entorno civil, compuesta por un vehículo aéreo sin tripulación a bordo»

**Capacidades de red**. La capacidad para distribuir información (fotos o imágenes) a un centro de control o a otro órgano decisor es una de las cualidades que permite realmente extraer todo el potencial de esta tecnología, y sacar el máximo provecho a la inversión en aplicaciones de supervisión y de seguridad de instalaciones.

**Cargas útiles intercambiables en caliente**. Es probable que durante el transcurso de una misión cambien los requerimientos de la misma, derivando en la necesidad de cambiar el sensor embarcado. Resulta esencial en este caso poder efectuar dicha maniobra de manera rápida y sencilla, independientemente de las condiciones ambientales y de manera automática, de forma que no sea preciso reconfigurar el sistema para que la aplicación de control reconozca el nuevo sensor ins-

**Se puede disponer de mapas de la zona.**

talado y esté listo para su utilización en cuestión de segundos.

**Datos e imágenes**. Entre la gama de UAS disponibles hoy en día en el mercado, es posible discriminar entre aquellos que montan una cámara comercial en la parte inferior de la unidad de vuelo, y aquéllos que integran y ensamblan en la unidad de vuelo una cámara a medida para el objeto de la aplicación. El tipo de información proporcionada por el primer tipo consiste básicamente en fotografías, lo cual puede resultar suficiente para un buen número de aplicaciones. En caso de que se requieran metadatos asociados a las fotos o imágenes de vídeo, es necesario acudir a un sistema que disponga de una carga útil con esta funcionalidad integrada. Mediante esta funcionalidad es posible componer mapas de la zona de interés sin necesidad de obtener información complementaria a la proporcionada por el sistema.

**Despegue y aterrizaje vertical (VTOL)**. Es posible clasificar los UAS en 2 categorías, los de ala fija y los de despegue y aterrizaje vertical. Los UAS de ala fija permiten volar distancias más largas y durante más tiempo, pero requieren un espacio mayor para las maniobras de despegue y aterrizaje, además de no permitir detenerse sobre un punto fijo en el aire. Los sistemas con opción de despegue y aterrizaje vertical requieren un espacio muy reducido para dicha maniobra, al tiempo que suelen proporcionar un control muy preciso de dicha maniobra, lo que les permite volar a bajas alturas o suspenderse en un punto sobre el suelo para la supervisión o vigilancia de una zona.

**Portabilidad**. Todos los elementos necesarios para su utilización deben ser fácilmente trasportables en una maleta de reducidas dimensiones, que permita su traslado a mano o en un vehículo, de forma que su utilización no se relegue a ocasiones especiales.

> «Las posibilidades de uso de esta tecnología en el ámbito de la seguridad y la protección de infraestructuras resultan muy interesantes»

**Ensamblaje**. Otra característica deseable es la de poder ensamblar los elementos o módulos que integran el UAS de forma sencilla, rápida y sin requerir herramientas para dicha labor, de forma que la unidad esté lista para su operación en cuestión de minutos.

Estos son diez de los aspectos a tener en cuenta en la adecuada selección de un quad-rotor. En la actualidad multitud de fabricantes cumplen buena parte de las características reseñadas previamente. Cabe mencionar los sistemas quad-rotor Aeryon Scout y Aeryon SkyRanger distribuidos por Tecosa/Siemens, los cuales han sido concebidos para satisfacer todos los requerimientos mencionados en el presente artículo, y proporcionar una solución robusta, fiable, sencilla de utilizar y con un rápido retorno de inversión (ROI). Se puede pensar en el ahorro que puede suponer para labores de supervisión o vigilancia aérea frente al coste de contratar un piloto y un helicóptero.

Las posibilidades de uso de esta tecnología en el ámbito de la seguridad y la protección de infraestructuras resultan muy interesantes. Aplicaciones como la investigación de accidentes, labores de búsqueda y rescate, gestión de desastres, control de multitudes, incidentes NBQ, vigilancia táctica, protección personal VIP, protección perimetral, extinción de incendios son sólo algunas de las posibles aplicaciones de esta tecnología en este contexto.

También es importante mencionar que el marco regulatorio para el uso civil de esta tecnología está progresando hacia un marco legal que aborde definitivamente el uso de estos dispositivos.

Como conclusión, podemos decir que la aplicación de los micro-UAS puede aportar grandes beneficios desde el punto de vista de la seguridad en entornos altamente exigentes, como es el de las infraestructuras críticas, para lo cual resulta esencial considerar los aspectos técnicos, constructivos, funcionales y económicos referidos en este artículo, a fin de seleccionar el UAS que mejor se adecúe a las necesidades de la infraestructura a proteger. ●


Fotos: *TECOSA*

**Tiene aplicación en investigación de accidentes, labores de búsqueda y rescate.**


G-SCOPE


NET_PORTER

RE_PORTER

GEVISCOPE

GEVISTORE

# ¿ IP O ANALÓGICO ?
# NO DUDES ...

# GEUTEBRÜCK

SISTEMAS HÍBRIDOS - SISTEMAS IP - SISTEMAS ANALÓGICOS - MATRIZ VIRTUAL - LECTURA DE MATRÍCULAS
ANÁLISISDE VÍDEO - ALMACENAMIENTO RAID - OMNIBRID - SISTEMAS COMPACTOS - VIDEO FULL HD
SISTEMAS CENTRALIZADOS - VIDEO WALL - ONVIF - TECLADOS DE CONTROL - CPA - BASES DE DATOS

**F.F. Videosistemas S.L.**
www.geutebruckspain.com
Tel. 902 99 84 40
ffvideo@ffvideosistemas.com

distribuidor exclusivo:
FF Videosistemas

**JOSÉ ENRIQUE ARGIBAY DEL OLMO.** SALES MANAGER. SECURITY. THALES

# Protección de infraestructuras críticas en la industria Oil & Gas

EL abastecimiento seguro y fiable de energía es una pieza fundamental en las economías de los países. Dado su carácter estratégico, la seguridad siempre ha constituido una de las prioridades en la industria energética, y más concretamente petrolífera y gasista. Las instalaciones petroleras constituyen una parte importante del catálogo de infraestructuras críticas de una nación.

Informes de las agencias de inteligencia de los distintos países han identificado la industria de Oil&Gas como un claro objetivo de ataques terroristas, como el ocurrido en enero de 2013 en la planta de gas argelina de In Amenas, que se saldó con el dramático balance de 37 trabajadores muertos a manos terroristas.

La industria petrolera está sometida a estos riesgos por múltiples razones:

- Las propiedades de los materiales tratados y almacenados en la industria O&G tienen el potencial inherente de causar daños a poblaciones y ecosistemas con enorme repercusión mediática.
- El carácter estratégico y global de la industria de O&G hace que cualquier perturbación en las operaciones afecte gravemente la economía mundial.
- La identificación de las grandes compañías petroleras con los grandes ejes de poder e influencia mundial.

En la actualidad, la mayor amenaza para las infraestructuras críticas proviene de los «conflictos asimétricos»[1] . Los departamentos de Seguridad Corporativa de las petroleras se enfrentan hoy a «oponentes poco convencionales»: terroristas nacionales e internacionales, activistas, grupos de presión, fanáticos de causas concretas, empleados descontentos y hackers informáticos (ya sea organizados u oportunistas). Estos oponentes pueden utilizar ataques de diferentes tipos e intensidad, que pueden ser complejos y coordinados con el objeto de explotar cualquier vulnerabilidad: física, lógica (IT), organizativa, ambiental e, incluso, humana.

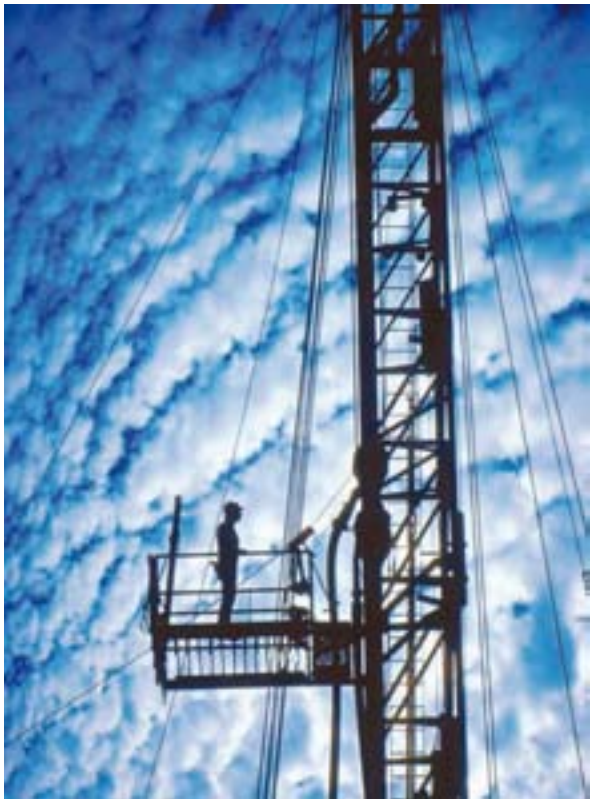
**En la actualidad la mayor amenaza para las infraestructuras críticas proviene de los «conflictos asimétricos».**

## Infraestructuras Críticas en Oil &Gas

El término «Infraestructura Crítica» se utiliza de manera habitual, especialmente desde los ataques terroristas del 11 de septiembre de 2001. Una primera versión del «Plan Nacional de Infraestructuras Críticas de Estados Unidos (también conocido como PDD-63)»[2] definía las infraestructuras críticas nacionales como «aquellos activos y sistemas –ya sea físicos o lógicos– tan vitales para la nación, que su destrucción o incapacidad de operación tendrían un

[1] «Conflicto asimétrico»: aquel en el cual las partes beligerantes difieren notablemente en su esencia, objetivos y poder de combate, utilizando tácticas y estrategias de ataque muy distintas.


El mundo es complejo.
Sus decisiones no tienen por qué serlo.
¿Seguridad urbana?
Detección inteligente combinada con respuestas de las agencias de seguridad
¿Protección de infraestructuras?
Desde gestión de alarmas a supervisión multi-emplazamiento
¿Ciudades inteligentes?
Infraestructura de información centrada en el ciudadano
¿Control de fronteras?
Autenticación de ciudadanos, e-fronteras y vigilancia del territorio
¿Seguridad aeroportuaria?
Optimización de las operaciones de seguridad cumpliendo con los estándares OACI
¿Ciber-seguridad?
Protección activa de los sistemas de información contra ataques
El mundo en que vivimos está basado en la movilidad personal, la libre circulación de capitales, bienes y servicios y en el acceso a la información. Pero estas libertades llevan consigo amenazas complejas. Nuestra misión es desarrollar soluciones integradas y robustas que ayuden a los gobiernos, autoridades locales y protección civil a preservar de dichas amenazas a los ciudadanos, datos confidenciales e infraestructuras. Al integrar todos nuestros sistemas, equipos y soluciones en nuestra Cadena de Decisiones Críticas, posibilitamos que los responsables de las tomas de decisiones dominen la complejidad inherente a las situaciones críticas y tomen las decisiones oportunas para obtener los mejores resultados.
Para obtener más información sobre nuestras soluciones de Seguridad, escanee el código QR o visite thalesgroup.es
THALES
Together • Safer • Everywhere



**La seguridad ha constituido una de las prioridades en la industria energética y más concretamente petrolífera y gasista.**

impacto debilitador importante en la seguridad nacional, la economía, la salud pública y seguridad de los ciudadanos e, incluso, sobre la moral nacional.»

Esta amplia definición engloba infraestructuras de muy diferentes sectores: alimentario, agua, energético, transporte, financiero, militar o logístico.

Los «Planes Nacionales de Protección de Infraestructuras Críticas» en cada país tienen como objetivo el identificar dichas infraestructuras (catálogo nacional de infraestructuras críticas), y establecer las medidas necesarias para su protección.

Si nos circunscribimos al sector de Oil&Gas, podríamos considerar la siguiente propuesta de categorización de infraestructuras críticas:

- Instalaciones industriales en la Cadena de Valor: Yacimientos, pozos, instalaciones de producción off-shore y on-shore, instalaciones de almacenamiento masivo, refinerías y plantas de procesamiento.
- Edificios: Cuarteles generales de las compañías petroleras y de servicios, oficinas dentro y fuera de las instalaciones industriales.
- Equipos: Unidades de proceso, instrumentación y control asociados a las unidades, tanques, tuberías, etc.…
- Sistemas auxiliares: Líneas eléctricas, líneas de gas, plantas de energía y cogeneración.
- Sistemas de transporte: Líneas de ferrocarril, terminales de carga y descarga, pantalanes, muelles, camiones, almacenamiento off-site, oleoductos y gasoductos, estaciones de compresión y bombeo.
- Sistemas informáticos: Sistemas de Control Distribuido, SCADAs, sistemas de Control Avanzado, redes, ordenadores, portátiles, PDAs, etc.

La industria petrolera debe adoptar medidas de seguridad y protección acordes al nivel de amenaza y sus posibles consecuencias. Todo ello en un entorno de optimización y reducción de costes. Para ello se hace necesario un programa corporativo de «Valoración de Riesgos de Seguridad», que tenga como fin último la definición y priorización de las inversiones que una compañía petrolera debe realizar para proteger su base de activos críticos.

## Un modelo genérico para la «Gestión de Riesgos de Seguridad»

Si bien existen diferentes metodologías para llevar a cabo la «Gestión de Riesgos de Seguridad», casi todas ellas comparten una serie de elementos y etapas. Todas pivotan alrededor de tres conceptos fundamentales: amenazas, vulnerabilidades y riesgos. El objetivo no es otro que identificar los recursos necesarios para reducir los riesgos a un nivel admisible y optimizando los costes de esta reducción.

La secuencia de elementos sería similar a la siguiente.

- Identificación de activos críticos.
- Clasificación de criticidad de los activos.
- Identificación y valoración de las amenazas.
- Valoración de la vulnerabilidad de los activos identificados frente a las amenazas específicas.
- Determinación del riesgo: Posibles consecuencias de la ejecución de las amenazas sobre los activos, combinado con su probabilidad de ocurrencia.
- Identificación de medidas para mitigar el riesgo.
- Adoptar una estrategia de reducción de riesgo que permita priorizar las actividades de mitigación.

## Soluciones para protección de infraestructuras críticas

En un sentido amplio, las «soluciones para protección de infraestructuras críticas» comprenden una combinación de tecnología, procesos y personal. Como ocurre en muchos otros campos, soluciones tecnológicas de primer nivel pueden fracasar en su implementación si no van acompañadas de las medidas organizativas adecuadas o de los cambios organizativos necesarios.

La **Figura 1** ilustra de manera esquemática los diferentes subsistemas

[2] Defending America's CyberSpace: National Plan for Information Systems Protection. Version 1.0. White House 2000

# COLOSO

EVOLUTION II

**NÚMERO 1 EN ESPAÑA**

## Renovamos la imagen de toda nuestra gama de DVR y NVR Coloso Evolution II

FULL D1 · Full HD 1080

## LITE, PRO, MAX

**Gama profesional**

Rack 1,5U, 2U

Capacidad para DVD-RW

Hasta 8 HDDs

## D-LITE, LITE-II

**Gama residencial**

Rack 1U, Mini-U

Hasta 2 HDDs

Distribuidor exclusivo

by demes

avanzando juntos hacia el futuro

San Fructuoso 50-56
08004 Barcelona
Tel. 934 254 960
Fax 934 261 904

AirSpace CCTV

y tecnologías que pueden encapsularse dentro de un proyecto de este tipo.

Como principio fundamental en el diseño de un sistema de protección debe tenerse en cuenta que el mismo debe funcionar como un «todo integrado y coordinado». No obstante, el sistema global de protección se compone a partir de numerosos subsistemas heterogéneos y de diferentes fabricantes, lo cual supone un importante reto a la hora de la integración.

Entre los principales subsistemas que conforman un sistema global de protección cabría destacar:

– **Videovigilancia:** Con frecuencia se distingue entre videovigilancia de seguridad y de proceso, dados los diferentes objetivos de ambas. Las instalaciones petroleras imponen en CCTV (y en otros susbsistemas); severas restricciones según las zonas clasificadas (ej. Eex Proof) que encarecen notablemente el equipamiento a utilizar.

– **Control de accesos:** Para controlar el acceso a las instalaciones -y dependencias de las mismas- a vehículos y personas. Una tendencia es complementarlos con soluciones de localización que permiten un seguimiento en tiempo real de activos críticos dentro de las instalaciones.

– **Detección de Intrusiones:** Sistemas de protección perimetral de la instalación para detectar accesos no deseados a las mismas. La tecnología empleada es muy diversa: sensores microfónicos, alambre tensado, sensores de fibra óptica, barreras de infrarrojos o microondas, etc.

– **Megafonía de aviso y emergencia** (Public Address / General Alarm (PA/GA)). Sistema fundamental en toda planta e instalación para la retransmisión de mensajes de aviso en eventos especiales, como puede ser la necesidad de evacuación de la instalación.

– **Interfonía:** Intercomunicación de voz entre personal de planta y Centro de Control a través de terminales fijos.

– **Radio:** Comunicación de voz entre personal de planta y Centro de Control a través de radioterminales portátiles.

– **Seguridad en Control y Comunicaciones / Ciberseguridad:** Sistemas para detectar y prevenir el acceso inadecuado a las redes de control o a las comunicaciones a través de diferentes medidas de protección (IDS/IPS, encriptación de comunicaciones, etc).

– **Sonares y radares:** Para detecciones submarinas o de larga distancia en circunstancias concretas pueden emplearse sonares y radares de medio-largo alcance.

– **Red de comunicaciones multiservicio:** Es la auténtica «columna vertebral» de la solución que permite la intercomunicación de los diferentes subsistemas, no sólo de seguridad sino también de comunicaciones y control. Dada su criticidad es usual utilizar un respaldo de comunicaciones para el caso de indisponibilidad de la red de fibra, que bien pueden ser comunicaciones satelitales mediante tecnología VSAT.

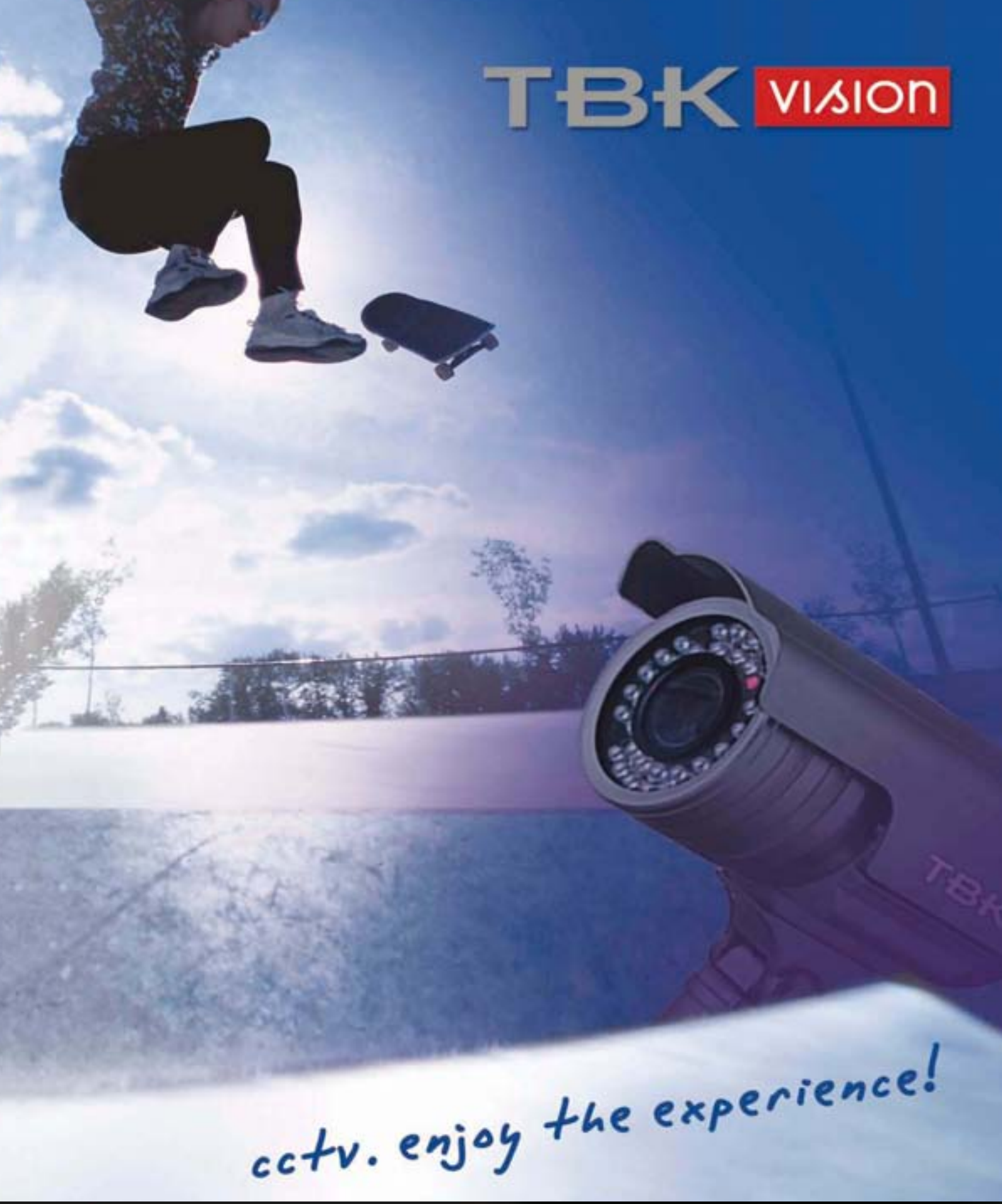
– **Centro de Mando y Control:** El «cerebro» del sistema de protección. Los sistemas de soporte permiten una visión integral de la seguridad del complejo, constituyendo una parte fundamental en la ayuda a la toma de decisiones.

La implementación de estas soluciones se traduce en proyectos complejos que exigen una importante capacidad de gestión de proyecto y servicios, que abarcan desde la propia ingeniería de detalle de la solución, identificación de las interfases, compra, documentación, entrenamiento, test de fabricación, embalaje y transporte de las mismas, instalación, test on-site y puesta en servicio de la solución; junto con unas necesidades de soporte tras la puesta en marcha.

Por todas estas razones es más que conveniente contar con un integrador especializado, conocedor del equipamiento y la tecnología, con capacidad de ingeniería, experiencia en gestión de proyectos complejos y capacidad operativa a nivel mundial. En este sentido, nuestra compañía es un integrador de seguridad global en este tipo de instalaciones, habiendo realizado proyectos para muchos de los principales operadores petrolíferos en todos los puntos del mundo. ●

**Figura 1.**


Fotos: *Thales/Archivo*




HOMMAX

www.hommaxsistemas.com

Avda. Alquería Moret, 9
Tel. +34 961 59 46 46 - Fax +34 961 59 29 56
46210 PICANYA (VALENCIA) ESPAÑA

**MIGUEL BALLABRIGA.** SALES MANAGER SPAIN & PORTUGAL. DALLMEIER

# El mundo en cambio

## De casetes analógicos VHS a modernos sistemas de sensores multifocales

La tecnología de videoseguridad se ha convertido hoy en día en un acompañante habitual. Sin embargo, ha sido un largo camino desde el primer grabador sencillo hasta los actuales sistemas de información de vídeo basados en IP. Un camino, que marcó la empresa alemana con sede Ratisbona de una forma determinante.

CÓMO comenzó todo...

Durante mucho tiempo, en las instalaciones de vigilancia se usaron grabadores analógicos que grababan en casetes VHS. Pero estos sistemas requerían mucho mantenimiento, se tenían que renovar periódicamente las piezas de desgaste y cambiar manualmente los casetes VHS en cuanto el almacenamiento estaba lleno. Por no mencionar la enorme demanda de espacio que era necesaria para guardar los casetes VHS. Si se querían recuperar secuencias de imágenes relevantes con fines de investigación, la búsqueda solía resultar muy laboriosa y requerir mucho tiempo: Los casetes de vídeo individuales habían de ser clasificados sucesivamente hasta encontrar la secuencia deseada. Al ver las cintas frecuentemente su calidad empeoraba más y más, lo que obligaba a recambiarlas a menudo.

El gran salto vino con los grabadores de vídeo digitales. El primer sistema de vídeo con detección de movimiento y almacenamiento digital de imágenes lo desarrolló la empresa de Ratisbona hace más de 25 años, en el año 1992. Al principio, la idea de emplear una memoria gráfica digital en la tecnología de seguridad no fue tomada muy en serio – más bien fue recibida con sonrisas. Debido a las entonces extremadamente bajas capacidades de los medios de almacenamiento, nadie quiso creer seriamente, que un día, los grabadores digitales de vídeo realmente pudiesen sustituir a los dispositivos analógicos de grabación. Si se pregunta hoy a Dieter Dallmeier, qué le ha impulsado en su trabajo durante todos estos años, contesta: «Sobre todo una cosa: Pasión y entusiasmo por los nuevos desarrollos y progresos de tecnologías visionarias. Tampoco en el pasado tuve miedo a tomar caminos no convencionales. Ha sido muy divertido durante todos estos años producir resultados pioneros en la tecnología de videoseguridad. Dar al mercado, una y otra vez, un nuevo impulso y ver qué consecuencias directas puedes hacer vivir a un sector entero, sigue siendo muy emocionante.»

Y el éxito le da la razón: la idea digital conectada con la tecnología correspondiente, debía posteriormente resultar precursora y revolucionar la videovigilancia. En comparación con los antiguos sistemas analógicos, convencieron especialmente tres puntos: una mejor calidad de imagen, una disponibilidad fiable y una mayor comodidad para el usuario.


**Los ciclos de desarrollo de nuevas tecnologías se acortan cada vez más.**

## Apuesta por la calidad a largo plazo


**La tecnología está siempre presente en los equipos de Dallmeier.**

Lo que hace 20 años todavía era impensable, hoy en día es un estándar muy extendido. Pero falta mucho aún para hablar de estancamiento: ideas y tecnologías innovadoras animan al mercado una y otra vez. Piense simplemente, por ejemplo, en las capacidades crecientes de los discos duros, los sistemas de análisis de vídeo cada vez más potentes, las posibilidades aumentadas debido a la tecnología de red o HDTV. En la mayoría de los casos no es fácil decidir qué es lo que a la larga va a imponerse. Ya que las tendencias –independientemente de si se trata de la bolsa o de la tecnología– muchas veces tienen una vida muy corta. Por esa razón, el fabricante y experto alemán en CCTV/IP apuesta desde siempre por una planificación dirigida al largo plazo y orientada sin concesiones a la calidad. «Muchas veces no es fácil reconocer a tiempo los cambios de tecnología y tenerlos en cuenta en el momento correcto para los propios planes de desarrollo. Siempre nos hemos dejado guiar por un único pensamiento: ¿Qué ventajas trae esta tecnología al usuario? A nosotros nos importa sobre todo una implantación óptima de innovaciones maduras y orientadas al futuro, que aportan realmente provecho al usuario y que trabajan de manera fiable», explica Dieter Dallmeier.

## Tecnología en proceso de cambio

De una manera análogamente precursora a lo que ocurrió con el primer DVR del mundo, el sistema de sensores multifocal también revolucionará el mercado y abrirá al sector de la videoseguridad posibilidades completamente novedosas.

Mientras otras firmas del sector libran una batalla incansable por unos valores de megapíxel más y más altos, la empresa germana presenta un concepto absolutamente nuevo. Con el patentado sistema de sensores multifocal, el fabricante de Ratisbona presenta una tecnología de cámara totalmente novedosa. Al contrario de las cámaras HD y megapíxel convencionales, que disponen de un único objetivo, este sistema trabaja con varios objetivos con diferentes distancias focales cada uno. Gracias a este nuevo concepto de sensores se pueden vigilar incluso superficies inmensas con un solo sistema - ¡y con grabación permanente de la imagen completa y, al mismo tiempo, máxima resolución de detalles, incluso a grandes distancias!

Con este sistema de sensores multifocal se puede vigilar desde un único punto de instalación la misma superficie para la que antes hacían falta varias cámaras (¡incluso de alta resolución!), lo que no sólo aumenta la eficiencia a la hora de evaluar las imágenes, sino que también ahorra considerablemente los costes, especialmente los que están relacionados con la infraestructura necesaria (postes, cables, etc.).

## La flexibilidad es todo

Los ciclos de desarrollo de nuevas tecnologías se acortan cada vez más, la seguridad de inversión se ha convertido en una palabra clave. Debido a la arquitectura abierta del sistema del fabricante alemán, la instalación de vídeo se mantiene flexible y escalable. Es posible llevar a cabo ampliaciones o adaptaciones futuras fácilmente, incluso un funcionamiento mixto con dispositivos de diferentes generaciones no causa ningún problema.

> «Las soluciones de CCTV/IP deben ser, sobre todo flexibles y abiertas a modificaciones y ampliaciones»

Las experiencias de los años pasados demuestran claramente que las soluciones de CCTV/IP deben ser, sobre todo, una cosa: flexibles y abiertas a modificaciones y ampliaciones. ●

*Fotos: Dallmeier*

Contactos de empresas, p. 7.

**JAIME MARTÍNEZ-AVIAL THOMA.** JEFE DE PRODUCTO DE LSB, S. L.

# Vigilancia IP, software y sistemas de grabación e interoperabilidad

En la videovigilancia en general, uno de los objetivos que se persigue es la visualización en directo y la grabación de imágenes, que permitan si se produce un determinado hecho, disponer de información visual sobre lo acontecido, que ayude a esclarecer cómo se produjo el hecho, e incluso que las imágenes grabadas puedan servir como prueba para los Cuerpos y Fuerzas de Seguridad o, en su caso, ante la Justicia. De aquí la importancia de que cualquier cámara IP pueda ser conectada a cualquier software IP o sistema de grabación IP, esto es lo que podemos llamar «Interoperabilidad».

LOS antiguos sistemas de vigilancia (sistemas analógicos de CCTV) permitían la interconexión de cámaras y grabadores de distintos fabricantes, ya que básicamente las únicas señales con las que se trabajaba eran la estándar de Video Compuesto (1 Vpp, 75 Ohm), y en algún caso las señales de telemetría (RS485); esta interoperabilidad no es tan sencilla en los sistemas de cámaras IP.

El rapidísimo desarrollo de la vigilancia IP, dio como resultado una cierta anarquía en los estándares y en los protocolos de comunicación de los dispositivos IP, resultando que cada fabricante quería crear «escuela», haciendo difícil o imposible la interoperabilidad de equipos.

**Las cámaras IP aparecen en el mercado aproximadamente en el año 2000.**

## Un poco de historia

Las cámaras IP aparecen en el mercado aproximadamente en el año 2000, y en aquellos días cada fabricante de cámaras suministraba un software propio para PC (gratuito la mayoría de las veces), con objeto de poder grabar y gestionar sus propias cámaras.

Los fabricantes de cámaras IP pusieron a disposición de los desarrolladores de software sus SDK (Software Development Kit,) con objeto de facilitar herramientas de integración a terceros y aumentar así la cuota de mercado de sus cámaras.

Por tanto, los desarrolladores de software comenzaron a crear software de vigilancia para distintas marcas de cámaras IP, integrando distintos modelos de cámaras de distintos fabricantes IP; esta solución de pago solía disponer de algunas características extra sobre el software gratuito de los fabricantes de cámaras IP. Resulta obvio que en el software no estaban integrados ni todos los fabricantes ni todos los modelos de cada fabricante.

La inclusión de nuevos fabricantes y de nuevos modelos de cámaras IP, se realizaba mediante actualizaciones periódicas del software, lo que suponía ciertas demoras para el usuario final en lo relativo a la operatividad de los nuevos modelos de cámaras.

Por otra parte, uno de los problemas frecuentes que se encontraban los usuarios en los comienzos de la videovigilancia IP, era la «Inestabilidad» de los sistemas de grabación, en este caso los

PC donde se instalaba el software de videovigilancia IP.

Muchas veces por ignorancia, otras por la competitividad de precios del mercado, los PC «clónicos» utilizados en estos sistemas no tenían todos sus componentes de la calidad y durabilidad necesarias. Hay que recordar que un sistema de grabación de videovigilancia debe estar operativo las 24h/365 días al año, y que tan importante como el procesador y la placa madre, y las memorias, son los HDD, la fuente de alimentación, el sistema de alimentación ininterrumpida, o los switch de red local. El fallo de alguno de los elementos descritos, podría inutilizar todo el sistema de videovigilancia.

Como consecuencia de lo anterior, y con el objetivo de dar estabilidad mediante un hardware fiable muy testeado para trabajar 24h/365 días, y mediante un software embebido evitar así posibles fallos achacables al usuario, algunos fabricantes de cámaras IP, fabricantes de unidades de Backup, y desarrolladores de software, presentaron en el mercado los NVR (Network Video Recorder).

Dependiendo de quién lo fabricara, si era el fabricante de cámaras IP, valían para su gama de cámaras, y si era los fabricantes de software o de equipos de grabación, eran «multimarca» para los modelos existentes en el mercado en ese momento y se integraban según demanda de forma individual.

## ONVIF y PSIA

Como consecuencia de la anarquía existente, son los propios fabricantes de hardware IP y software los que deciden la necesidad de unificar criterios para que todo el hardware IP pueda trabajar con todo el software IP, para lo cual crean en 2008 dos plataformas de trabajo abiertas a todas las compañías y organizaciones.

ONVIF (Open Network Video Interface).

PSIA (Physical Security Interoperability Alliance).

Ambos grupos de trabajo tienen objetivos similares, aunque a día de hoy parece que es ONVIF quien lleva la iniciativa.

Fundamentalmente ONVIF establece unos estándares para que las cámaras IP que cumplan «ONVIF Compatible», puedan ser reconocidas por cualquier software de gestión y grabación, o por cualquier NVR también compatible ONVIF, sin necesidad de que el fabricante o modelo de cámara esté nominalmente integrado en la lista de compatibilidad del Software/NVR.

Esta compatibilidad en general permite ver, grabar, ajustar ciertos parámetros de la cámara, aunque en la mayoría de las ocasiones no se obtiene el 100% del control o prestaciones de la misma, si bien en la mayoría de los casos se llega a un 80 o 90% de sus funciones.

> «En la actualidad no es posible la total interoperabilidad de cámaras IP y software/NVR IP»

## Segmentación del mercado de cámaras IP y disponibilidad de Software/NVR IP

En la actualidad la oferta de cámaras IP podría dividirse en cuatro grupos:

– Hogar, primer precio (Precio< 100€).

– Hogar, Pequeño comercio (100 < Precio >250€).
– Profesional Medianas Instalaciones.
– Profesional Grandes Proyectos.

En función de esta segmentación de las cámaras IP se puede deducir cuáles pueden trabajar con Software/NVR comerciales y cuáles no.

– El 1º apartado, que actualmente está creciendo de forma espectacular, si bien por la procedencia de los fabricantes (China) y el objetivo de mercado, se trata de una vigilancia «casera» bastante sencilla y elemental. Estos modelos, muy económicos, no suelen cumplir ningún estándar ONVIF/PSIA, por lo que solamente funcionan con su propio Software de Grabación/NVR.

Si la cuota de mercado del fabricante de la cámara aumenta considerablemente, siempre es posible que algún fabricante de NVR la integre en la marca o el modelo en algún modelo básico de NVR.

– En el 2º apartado, bastantes modelos cumplen ONVIF, por lo que además de su software gratuito original, pueden instalarse en software de pago de terceros, como un modelo ONVIF, o en NVR también como ONVIF.


**Uno de los problemas que encontraban los usuarios en los comienzos de la videovigilancia IP era la inestabilidad de los sistemas de grabación.**

Es habitual que existan NVR de la propia marca de cámaras IP y, por supuesto, NVR «multimarca» de terceros.

En los apartados 3º y 4º todas las cámaras cumplen el estándar ONVIF, pero también es verdad que al ser equipos más sofisticados, en la mayoría de las ocasiones disponen de funciones muy específicas no contempladas por el momento en ONVIF, lo que implica que para obtener el 100% de sus características, siga siendo necesaria la integración personalizada del modelo de cámara IP en el Software/NVR, mediante los SDK (Software Development Kit) del fabricante de la cámara IP.

Como conclusión, en la actualidad no es posible la total interoperabilidad de cámaras IP y software/NVR IP.

Si las cámaras IP son muy económicas solamente se podrán gestionar con su propio software y un PC.

**En las nuevas especificaciones ONVIF están recogidas entre otras las compatibilidades de movimiento PTZ, audio, streaming RTSP, etc.**

Si son semiprofesionales o profesionales encontraremos además del software del fabricante diversos software de pago, que nos permitirán sacar el 100% de prestaciones gracias a ONVIF o a la integración por terceros.

Si consideramos la gama profesional para proyectos, será necesaria la integración personalizada en software de pago para la obtención del 100% de prestaciones.

## Expectativas para el futuro

Los estándares ONVIF están en constante evolución, como ya hemos indicado anteriormente pretenden el desarrollo global de un interfaz de comunicación para todos los dispositivos de seguridad basados en IP.

Las especificaciones ONVIF definen un protocolo común para el intercambio entre dispositivos de vídeo en red, incluyendo la búsqueda automática de dispositivos, el streaming de vídeo y los metadatos.

En las nuevas especificaciones ONVIF, están recogidas entre otras las compatibilidades de movimiento PTZ, Audio, Streaming RTSP, etc.

Como conclusión final, para un futuro cercano, es previsible que gracias a los trabajos de estandarización que los fabricantes realizan dentro de ONVIF/PSIA se pueda llegar a niveles de interoperabilidad cercanos al 100% entre cámaras IP, sistemas de grabación, y sistemas de control de accesos. ●

*Fotos: LSB*

VIVOTEK
BUILT WITH RELIABILITY

Con la creciente demanda de imágenes
de calidad superior, las cámaras megapíxel
están encabezando el mundo de la videovigilancia.
VIVOTEK invita a los expertos en seguridad
de todo el mundo a participar en el importante
lanzamiento de nuestra completa línea de productos
de 5 megapíxeles y disfrutar
de la máxima calidad de imagen.

# Celebrando una nueva era en Megapixel

*Más Detalles, más Cobertura, más Seguridad*

FD8372

FE8172/72V

IP8372

IP8172/72P

## Principales Características

- H.264
- 5MP
- Full HD
- ePTZ
- ICR
- WDR Mejorado
- Sistema de enfoque inteligente
- EN50155 (FE8172V)
- P-iris (IP8172P)

ONVIF


cartronicgroup
• Tel: +34 916 588 760 • Sales:marketing@cartronic.es
• Fax: +34 916 588 769 • Web: www.cartronic.es

LSB
• Tel: +34 913294835 • Sales: jaime.avial@lsb.es
• Fax: +34 913290611 • Web: www.lsb.es/

VIVOTEK
www.vivotek.com
VIVOTEK INC.
6F, No.192, Lien-Cheng Rd., Chung-Ho, New Taipei City, 235, Taiwan, R.O.C. | T: +886-2-82455282 | F: +886-2-82455532 | E: sales@vivotek.com

**CHRISTOPHE FARROUILH.** DIRECTOR DE TEB IBERICA

# Nuevas funcionalidades para grabadores digitales

Varias tendencias vieron la luz en los últimos años, en cuanto a la grabación de vídeos. Entre ellas cabe destacar la aparición de nuevas técnicas de análisis de imágenes, que permiten compartir el uso de sensores y servidores numéricos, de cara a gestionar tanto la grabación, como la transmisión y tratamientos específicos de imágenes.

AHORA es posible proporcionar a los actores del retail, la logística e incluso de la banca, múltiples funcionalidades avanzadas utilizando un único servidor de All in One, que puede ofrecer conteo de personas, ANPR (lectura automática de matrículas), Tracking (seguimiento automático), o Función SCAN (control de trazabilidad de paquetes), con un único servidor de vídeo.

Las grabaciones de datos tienen una importancia primordial en el momento de aportar pruebas (recordemos que por motivos de seguridad, muchas instalaciones están bajo vigilancia las 24h y no pueden permitirse perder ninguna grabación). Por eso, la función RAID (copia de seguridad de discos) está siendo utilizada en el tipo de instalaciones sensibles.

Grabador Digital Digipryn.

Como consecuencia, los usuarios se pueden beneficiar de la mejor tecnología de análisis de vídeo, en su solución de grabación clásica. Esta forma inteligente de vídeo (i.e. conteo de personas) puede dar respuesta tanto a los responsables de Seguridad de las compañías, como a los departamentos de Marketing y Ventas. Los últimos avances en esta materia suponen una importante ayuda para estos departamentos, pues permiten evaluar los momentos de mayor afluencia de público, los puntos de mayor interés para los clientes o puntos calientes e, incluso, establecer un patrón en el comportamiento de los consumidores. Una vez analizada y tratada esta nueva fuente de datos, puede convertirse en una poderosa herramienta que permita optimizar, desde las acciones de Trade Marketing (eligiendo aquellos productos que, gracias al estudio de los comportamientos detectados en el vídeo, son los más demandados y por lo tanto colocarlos en los escaparates o zonas de paso de la tienda…), hasta la manera en que se gestionan los Recursos Humanos (delimitando los momentos de mayor necesidad de personal y en qué zonas serán necesarios, por ejemplo). En nuestra compañía venimos desarrollando este tipo de tecnologías desde hace varios años y actualmente ya están disponibles en nuestras últimas versiones de grabadores digitales Digipryn v6.

## Los sistemas capaces de transmitir vía IP están revolucionando el sector de la Seguridad

En la actualidad, es fundamental contar con soluciones que permitan la coexistencia de sistemas de cámaras analógicas con sistemas IP. De esta manera, se hace posible conservar las instalaciones existentes (en coherencia con las líneas de limitaciones presupuestarias), pero a la vez existe la posibilidad de añadir cámaras IP megapíxeles de alta resolución (que den respuesta a las nuevas necesidades de los operadores y mejoren la solución de los posibles incidentes).

Gracias a los grabadores multi-híbridos, estas opciones están disponibles en las últimas versiones del videograbador anteriormente citado, y admitiendo una total compatibilidad tanto con cámaras IP, como analógicas o HD-SDI.

Estas nuevas cámaras IP HD pueden obtener imágenes de alta calidad pa-

ra monitorear áreas estratégicas (por ejemplo, la entrada a las instituciones públicas, manejo de dinero en salas de conteo, leer las matrículas y controlar los parkings o el acceso a edificios sensibles, entre otras).

La integración de cámaras de visión 360 megapíxel en grabadoras digitales es, así mismo, una tecnología eficaz para el control integral, ya que pueden ofrecer una visión panorámica de una sala completa, a través de una única unidad. Para un uso óptimo de este tipo de cámara, es imprescindible una buena integración de software en el grabador digital. Obviamente, el software debe grabar toda la escena 360°, incluso si el operador elige algunas escenas específicas en Live View. En el momento de la revisión de las grabaciones, no sólo es posible ver las grabaciones en 360°, sino también las zonas o áreas específicas, en base a hechos pasados (sin perder información en función del área seleccionada para la monitorización). Hemos desarrollado un software que evita la pérdida de secuencias de vídeo, aunque el operador de vídeo este eligiendo un área concreta (la secuencia completa seguirá estando disponible en modo relectura).

Nuestra compañía destina un importante porcentaje de sus ingresos totales a I+D+i. Disponemos de un departamento propio, Prynel, integrado por un conjunto de ingenieros altamente cualificados y dedicados, en exclusiva, al desarrollo y mejora de software. Gracias a esto, hemos incorporado las últimas tecnologías en nuestros grabadores, adaptando nuestros productos para responder a las necesidades de los clientes. El objetivo es lograr la máxima optimización de su inversión en un sistema integral de videovigilancia, que ya no sólo desarrollará funciones de seguridad, sino que podrá ser útil en múltiples áreas del negocio.

**Las grabaciones de datos tienen una importancia primordial en el momento de aportar pruebas.**

Dedicamos un importante esfuerzo a incorporar los inputs del mercado en nuestros productos, y desarrollamos constantemente una tecnología cada vez más útil para la problemática diaria. El resultado de todo este trabajo nos permite tener, a día de hoy, los grabadores más completos del mercado. ●

*Fotos: TEB*

Contactos de empresas, p. 7.

**ALBERT CLAPÉS Y SERGIO ESCALERA, HUPBA GROUP.** UNIVERSITAT DE BARCELONA
Y CENTRO DE VISIÓN POR COMPUTADOR (CVC-UAB)

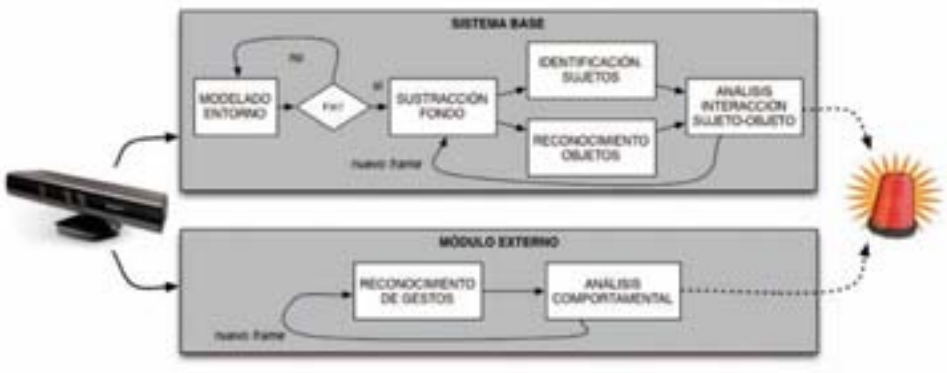
# SAMEC: Sistema automático de monitorización en entornos cerrados

## Proyecto presentado a los I Premios Security Forum

Hoy en día, la tecnología ha alcanzado un punto en el que instalar cámaras de videovigilancia resulta económico, mientras que la contratación de recursos humanos para desempeñar la tarea de «sentarse y mirar» la información captada por las cámaras resulta relativamente caro y poco eficaz (difícil monitorización visual sistemática 24 horas al día, con la consecuente fatiga visual causada). En este contexto, la automatización de sucesos (o eventos) ocurridos en la zona monitorizada para facilitar la tarea del observador resulta extraordinariamente útil, tanto desde el punto de vista de optimización de recursos, como desde el punto de vista de fiabilidad.

La automatización ha de permitir descartar eventos irrelevantes a la vez que ha de indicar la existencia de elementos de riesgos en un determinado contexto, clasificar la información visual por prioridades y almacenar inteligentemente la información captada para su posterior visualización.

**Figura 1.** Esquema general del sistema.




La llamada «Visión por Computador», uno de los principales subcampos de la inteligencia artificial, se encarga de la teoría que se encuentra detrás de los sistemas artificiales dedicados a extraer información a partir de imágenes. Es decir, una vez captada la información visual, un sistema inteligente es capaz de realizar razonamientos automáticos de alto nivel sobre lo «visto». Históricamente, las técnicas de «Visión por Computador» se han basado en el uso de imágenes de color (RGB) bidimensionales; sin embargo, la reciente aparición de los dispositivos multimodales RGB+Depth (o RGBD) —tales como Microsoft® Kinect™— han permitido grandes avances de técnicas clásicas de visión por computador y la aparición de nuevas metodologías. Concretamente, los dispositivos RGBD proporcionan una valiosa información adicional para cada píxel aparte del color y la intensidad lumínica: La profundidad respecto el plano de la cámara. Este hecho supone la enorme ventaja, respecto a las cámaras normales, de poder recuperar la tridimensionalidad de la imagen captada, disponiendo de

*1 http://www.maia.ub.es/~sergio/*

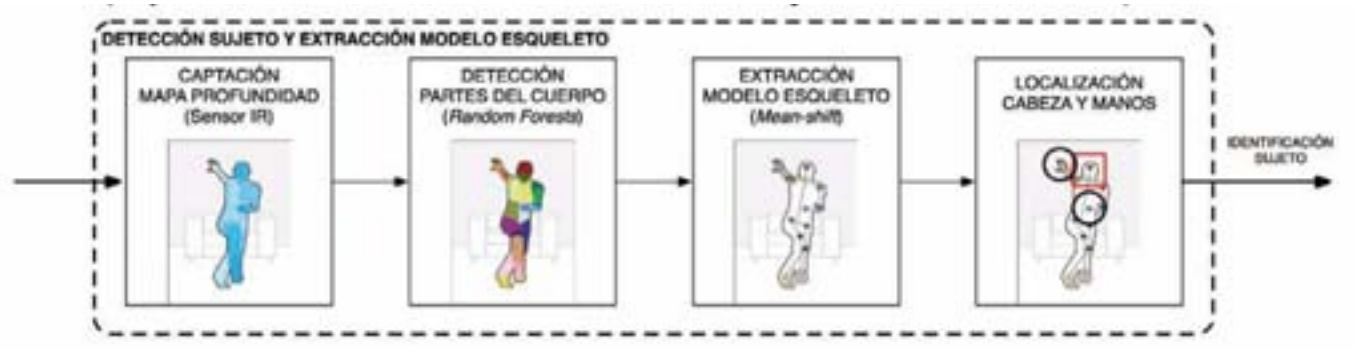



**Figura 2.** Identificación y descripción de sujetos. Primero se realiza la clasificación de partes de cuerpo (a nivel de píxel) a partir una imagen de profundidad captada mediante un dispositivo RGBD. A continuación, a partir de las regiones de partes extraídas se calculan las articulaciones del modelo esqueleto. A partir del esqueleto se conoce directamente la posición de la cabeza y las manos.

información de color y de profundidad sincronizada para cada píxel de la imagen a partir de sensores económicos y portables, siendo una tecnología robusta frente a cambios ambientales de iluminación. Dado este contexto tecnológico, resulta útil e interesante la aplicación de las técnicas de «Visión por Computador» en el ámbito de la videovigilancia. Por ello, en el grupo de investigación Human Pose Recovery and Behavior Analysis (HuPBA)[1] de la Universidad de Barcelona y del Centro de Visión por Computador de la Universidad Autónoma de Barcelona, los investigadores Albert Clapés y Sergio Escalera han implementado una nueva tecnología capaz de detectar e identificar sujetos y objetos presentes en la escena, para comprender y alarmar sobre posibles hurtos u otras actividades delictivas [4]. El funcionamiento del sistema se ilustra gráficamente en la **Figura 1**.

> «La automatización de sucesos (o eventos) ocurridos en la zona monitorizada para facilitar la tarea del observador resulta extraordinariamente útil»

El sistema desarrollado permite aprender el entorno, para posteriormente identificar nuevos sujetos u objetos que aparecen o desaparecen de la escena. Adicionalmente, los objetos detectados son asignados a un usuario propietario, permitiendo así realizar un reconocimiento automático de robos en caso de producirse. El sistema propuesto tiene una alta tasa de reconocimiento en entornos con poca iluminación, dado que los mapas de profundidad capturados y analizados se obtienen mediante el sensor de infrarrojos (IR) del dispositivo, invariantes a

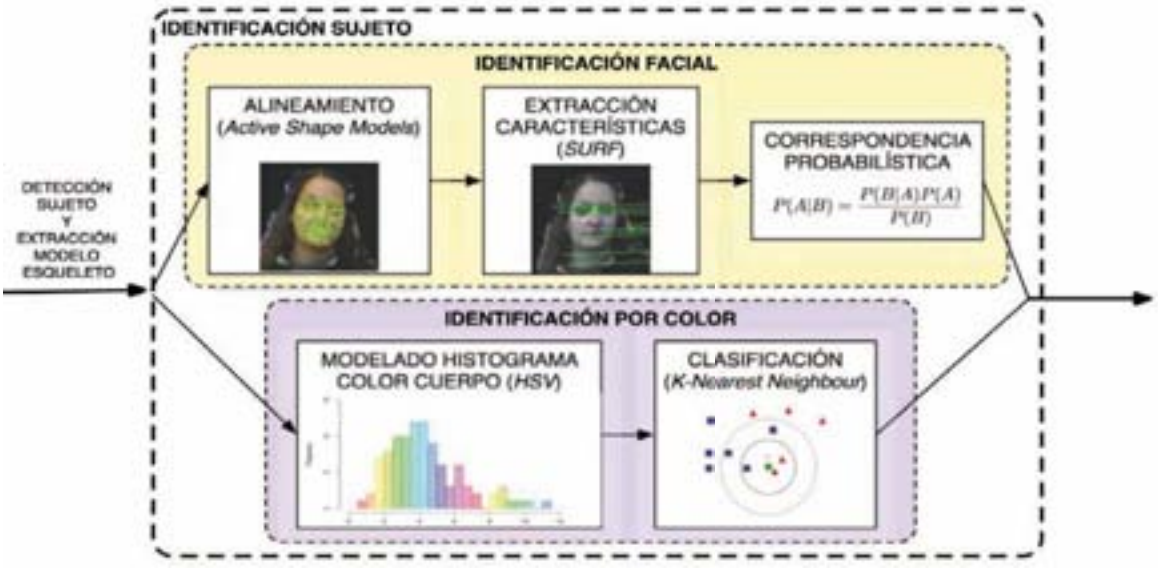



**Figura 3.** Módulo de Identificación de sujetos.

**Figura 4.** Procedimiento de correspondencia probabilística entre puntos faciales característicos extraídos mediante SURF. Los puntos verdes unidos con líneas ilustran una correspondencia exitosa, los rojos indican una mala de correspondencia, y los azules son outliers (no se encuentran candidatos en la imagen de la derecha). En (a) se puede ver como el resultado de la correspondencia (98.4%); mientras que en (b) se puede ver una correspondencia entre dos caras de dos sujetos diferentes (32.3%). La deformación que se aprecia en las imágenes izquierdas se debe a un preprocesado de alineación usado para mejorar la correspondencia.

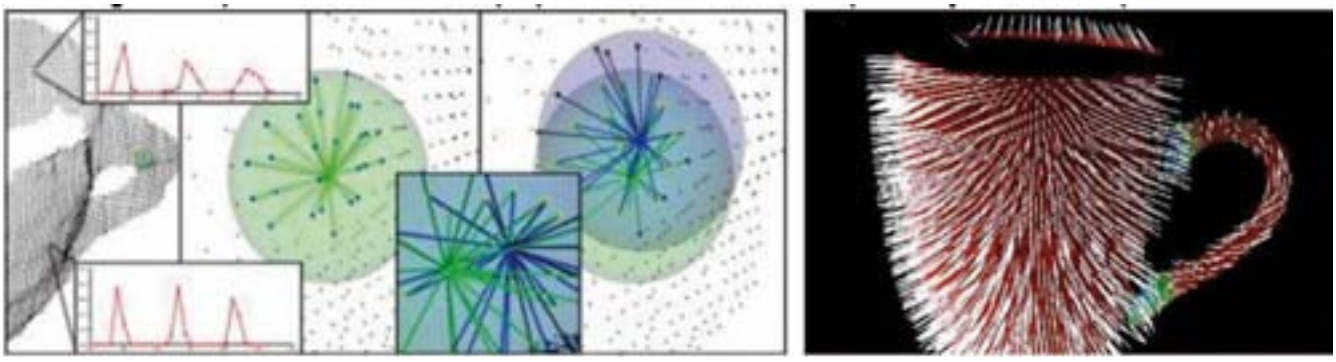
luz ambiental no direccionada al sensor de captación de datos.

**El entorno y su modelado**: Para el modelado del entorno, se requiere una secuencia inicial de frames, con la cual se aprende un modelo adaptativo para cada píxel de la escena. Una vez el sistema ha aprendido el entorno sobre el cual monitorizará, modelando la distribución que sigue cada píxel, se pondrá en funcionamiento la etapa de monitorización. Una vez el entorno se ha modelado, cada nuevo frame adquirido por el dispositivo es analizado para detectar zonas en las que el valor de los píxeles se desvíen respecto la distribución estadística aprendida, detectando así apariciones de objetos/sujetos que no eran parte del entorno o desapariciones de otros que lo eran.

> «Una vez captada la información visual, un sistema inteligente es capaz de realizar razonamientos automáticos de alto nivel sobre lo visto»

**Detección e identificación de sujetos**: Dadas las regiones segmentadas cabe determinar ahora para cada una si se trata de persona u objeto. Con este objetivo, se aplica una técnica de aprendizaje automático, Random Forests (RF), capaz de detectar y categorizar regiones (partes del cuerpo) pertenecientes a sujeto [3]. Una vez se han localizado las partes del cuerpo se extrae el modelo de esqueleto. Este modelo permitirá localizar la posición de la cabeza, y así aplicar el detector facial sólo en la región correspondiente a la cara (y reducir así la probabilidad de obtener falsos positivos), localizar también la posición de las manos para analizar la posible interacción del sujeto con objetos presentes en la escena, y también conocer la configuración de articulaciones y la variación de su posición en el tiempo, con el fin de aplicar las técnicas de reconocimiento de gestos oportunas. La **Figura 2** ilustra este proceso. Para la identificación del sujeto, la metodología se basa en la combinación de dos métodos complementarios: un modelado del color del cuerpo

**Figura 5.** Descripción tridimensional de objetos con FPFH. En la parte izquierda de la figura izquierda se aprecia medio mapa de profundidad de un objeto taza (la parte del asa) y dos descriptores (histogramas) extraídos de un par arbitrario de puntos. El descriptor expresa relaciones angulares entre los vectores normales a la superficie de los puntos (mostrados en la imagen de la derecha).



junto con un reconocimiento facial. En la **Figura 3**, se muestra conceptualmente el módulo.

Para la identificación facial se requiere primero realizar una detección facial usando en el algoritmo de Viola-Jones [5]. Una vez se han localizado con precisión las regiones conteniendo la cara de los correspondientes sujetos, éstas se describen mediante SURF (Speeded-Up Robust Features) [6]. Finalmente, se procede a hacer la correspondencia probabilística con las descripciones de caras de sujetos identificados y determinar con cuál se obtiene una mejor correspondencia **Figura 4**.

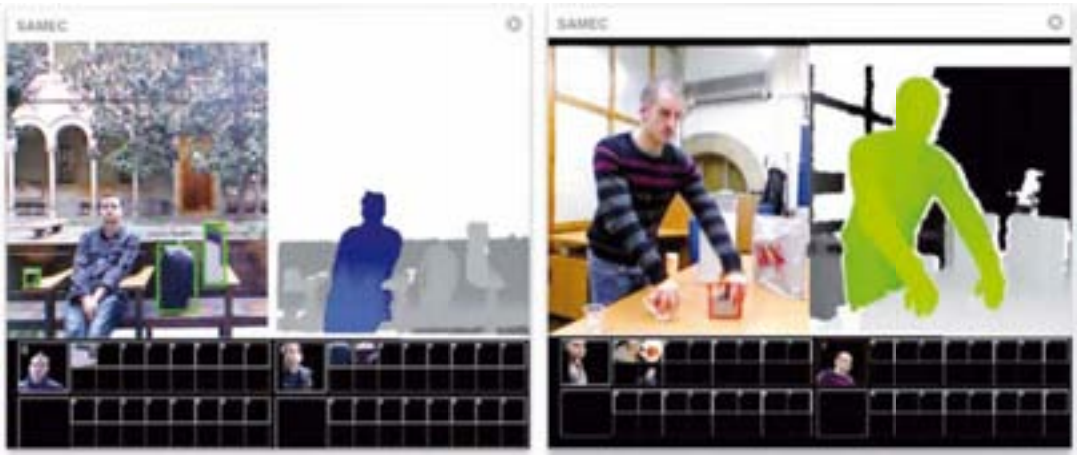


**Figura 6.** **(a) Ejemplo de funcionamiento del sistema. A la izquierda de la figura, la imagen de color captada por la cámara RGB. A la derecha, el mapa de profundidad construido a partir de la información captada por el sensor infrarrojo. Se encuentra en escena un segundo sujeto (ID1) propietario de dos objetos (una taza y una mochila), junto con un objeto perteneciente a un primer sujeto (ID0) no presente en escena. En caso de interacción del sujeto ID1 (u otro distinto a ID0) con el objeto del sujeto ID0 se procederá a activar la correspondiente alarma de seguridad. (b) Ejemplo de identificación de interacción usuario-objeto. Un sujeto (ID1) en escena (a la izquierda de la imagen captado por la cámara y a la derecha el mismo sujeto en el mismo instante de tiempo tal como es captado por el sensor IR) interactuando con dos objetos pertenecientes a otro sujeto (ID0), una taza blanca y una figura metálica. La interacción indebida con el objeto figura metálica se está indicando con un rectángulo rojo, mientras que la taza, después de haberse interactuado también indebidamente con ella, ha sido desplazada de su posición original, lo cual será considerado hurto por el sistema.**

**Reconocimiento de objetos**: Las regiones de la escena no consideradas sujeto son categorizadas como objeto. Así pues, dada la detección de una región objeto, se procede a describirlo para, posteriormente, compararlo con otros objetos previamente reconocidos y determinar así si se trata de un objeto previamente identificado o si por el contrario es desconocido por parte del sistema y se actualiza como nuevo objeto en la base de datos de elementos del entorno. La información de forma es directamente extraíble del mapa de profundidad adquirido por el sensor infrarrojo del dispositivo RGBD. Más concretamente, el descriptor al cual hacemos referencia se construye como un histograma que resume las variaciones de la orientación de la superficie en la vecindad de cada uno de los puntos que conforman la superficie visible del objeto para una vista particular (Fast Point Feature Histogram [4,5]) **(Figura. 5).**

Resulta evidente pensar que en videovigilancia no tiene sentido tener una pre-especificación de los objetos a ser monitorizados o, aún menos, de los sujetos que aparecerán en escena. Es por eso que se ha dotado al siste-

ma del dinamismo necesario para considerar cualquier sujeto que aparezca en la escena, reconociendo las instancias particulares de estos «en línea» (actualizando dinámicamente una base de datos de sujetos y objetos), y estableciendo las debidas relaciones de pertenencia sujeto-objeto.

> «El sistema se complementa con un módulo automático de análisis comportamental basado en el reconocimiento gestual»

**Interacción sujeto-objeto en detección de hurtos**: Este paso se basa en la definición de relaciones de pertenencia sujeto-objeto en el momento de aparición de un nuevo objeto, definiendo así quién será considerado su propietario. Así pues, dada una nueva interacción con el mismo objeto por parte de un sujeto, se revisa el histórico de relaciones de pertenencia para determinar si el sujeto que lleva a cabo la acción es o no el propietario y, si procede, activar la debida alarma. Un ejemplo de interacción mediante el uso del sistema se muestra en la interfaz de la **Figura 6b**.

**Análisis comportamental automático de sujetos**: El sistema se complementa con un módulo automático de análisis comportamental basado en el reconocimiento gestual, dotándolo así de la capacidad de realizar inferencias a alto nivel sobre el comportamiento de los sujetos, pudiendo detectar eventos anómalos y de riesgo en entornos de videovigilancia. Formalmente, se define un comportamiento como la concatenación de uno o más gestos. Y en concreto, definimos un gesto como una secuencia espaciotemporal que describe el movimiento de las articulaciones del modelo esqueletal de un sujeto a lo largo del tiempo. El reconocimiento de un gesto consiste en realizar una correspondencia entre dos secuencias o modelos espaciotemporales. En este trabajo se hace uso de un método desarrollado por parte los integrantes del equipo investigador de este proyecto: Probability-based Dynamic Time Warping (PDTW) [2], que mezclando otros enfoques del estado del arte permite modelar la apariencia de los gestos siendo invariante al tiempo de realización de los mismos y a la variabilidades inter e intra-gesto producidas por diferentes usuarios.

**Propiedades y escalabilidad del sistema de videovigilancia**: Dada la descripción técnica de la tecnología desarrollada, los puntos fuertes de ésta se podrían resumir en el siguiente listado: a) nueva metodología publicada por el grupo investigador, que permite fusión de nuevos descriptores visuales multimodales RGB+Depth, los cuales permiten detectar y analizar la apariencia y geometría de objetos, usuarios, así como sus comportamientos asociados incluso en entornos sin luz; b) metodología general que permite de forma adaptativa describir y reconocer nuevos y previos objetos presentes en la escena monitorizada; c) metodología de reconocimiento de eventos y gestos genéricos, lo cual permite establecer aquellos patrones de riesgo que puedan ser diferentes dependiendo de cada contexto a monitorizar; d) uso de sensores económicos, lo cual facilita su implantación y escalabilidad. No obstante cabe destacar que el software se limita a la distancia de captación del sensor IR, actualmente limitado a un máximo de 5 metros, lo cual debe ser tenido en cuenta para su implantación en el entorno. Por otro lado, estos sensores están apareciendo con más frecuencia en el mercado –y lo hacen con el empuje de gigantes del sector tecnológico (como Microsoft® o ASUS®)–, con lo cual se prevé un abaratamiento de sus costes y mejoras de la tecnología (incremento de resolución y distancia de captación).

## Referencias


1. Radu B. Rusu, N. Blodow, and M. Beetz. «Fast Point Feature Histograms (FPFH) for 3D registration». Robotics and Automation, 2009. ICRA '09. IEEE International Conference on , vol., no., pp.3212-3217, 12-17 May 2009.
2. Antonio Hernandez-Vela, Miguel Angel Bautista, Xavier Perez-Sala, Victor Ponce, Sergio Escalera, Xavier Baro, Oriol Pujol, and Cecilio Angulo, Probability-based Dynamic Time Warping and Bag-of-Visual-and-Depth-Words for Human Gesture Recognition in RGB-D, Pattern Recognition Letters, PATREC5825, DOI: 10.1016/j.patrec.2013.09.009, 2013.
3. J. Shotton, A. Fitzgibbon, M. Cook, et. al. Real-time human pose recognition in parts from single depth images. CVPR, 2011.
4. A. Clapés, M. Reyes, and S. Escalera, Multimodal User Identification and Object Recognition System, PRL, 2013.
5. P. Viola and M. Jones, «Rapid object detection using a boosted cascade of simple features», CVPR, vol. 1, 2001.
6. H. Bay, A. Ess, T. Tuytelaars, and L. Van Gool, «Speeded-up robust features (SURF),» Computer vision and image understanding, vol. 110, no. 3, pp. 346–359, 2008.

SEGURIDAD

SEGURIDAD INTEGRAL CANARIA SA

# *Líderes en seguridad*

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

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

+ Info: 902 226 047

GRUPO Ralons

UNE-EN 16082-2012

www.gruporalons.com

**JUAN JOSÉ MERLO.** COMITÉ SECTORIAL DE INSTALACION, MANTENIMIENTO E INGENIERÍA DE EQUIPOS Y SISTEMAS. TECNIFUEGO-AESPI

# Proteger contra incendios un Centro de Proceso de Datos

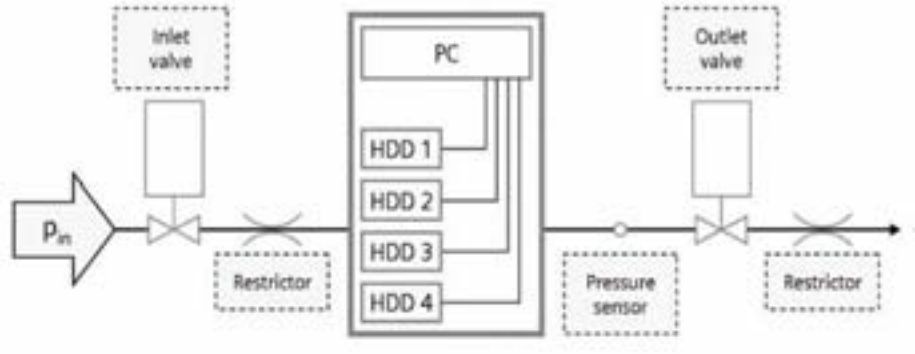
Los centros de proceso de datos (datacenters) y servidores se encuentran en el corazón del mundo de los negocios. Con una cantidad estimada de unos 35 millones de servidores en todo el mundo y una demanda creciente de proceso y almacenamiento de datos a través de una red mundial de millones de dispositivos, la necesidad de garantizar la continuidad del negocio y proteger los datos es esencial.

De acuerdo con la empresa de investigación de la tecnología Gartner, el gasto mundial en hardware de datacenter (servidores, almacenamiento y equipos de red) se esperaba que alcanzase los 98,9 mil millones dólares en 2011, un aumento del 12,7% respecto a 2010.

Gartner predijo que el gasto en hardware ascenderá a 106,4 mil millones dólares en 2012 y superar los 126,2 mil millones en 2015.

Gartner también predijo que la tendencia hacia la consolidación continuará. Consolidación significa la reducción del número de centros de datos de tamaño medio, y el aumento de los centros de mega datos de gran tamaño. En 2015, el 2% de todos los centros de datos contendrá el 60% de todo el espacio de datacenter y representará el 71% de todo el gasto en hardware del centro de datos. Esto significa que los centros de datos serán más pequeños pero más eficientes. La previsión para 2016 es que el 60% de los nuevos datacenters será un 40% más pequeño, mientras la carga de trabajo aumentará en un 300%.

**Figura 1**




## Los datacenters y sistemas de extinción

Los datacenters representan el 50% del mercado de extinción seca y por lo tanto uno de los mercados más importantes para las empresas que venden sistemas de extinción. Ellos representan un alto riesgo de incendio. Esto es debido a que el hardware del datacenter, la energía eléctrica y el extenso cableado proporcionan una constante fuente potencial de ignición. Especialmente bajo falsos suelos, mientras que los miles de componentes plásticos proporcionan fuentes de material combustible. Teniendo en cuenta que aproximadamente el 80% de los incendios son causados por fallos eléctricos, la necesidad de proteger los datacenters frente a los incendios, es esencial.

Según una aseguradora líder industrial en Alemania y el consultor de sistemas de seguridad HDI-Gerling, las compañías de seguros sobreviven a una ruptura completa de su infraestructura de IT sólo 5,5 días, las empresas industriales tienen que cerrar después de 5 días, los comerciales después de 2,5 días, ciertos bancos después de 2 días y los proveedores «just-in-time» en 24 horas.

En los datacenter de gran tamaño (>300m$^2$), se utilizan agentes extintores de gas inerte. Esto se debe a los gases inertes no crean residuos noci-

vos al reaccionar con el fuego, por lo que son seguros para los equipos electrónicos sensibles. Para los centros de datos más pequeños (<300m²), se utilizan con mayor frecuencia los agentes químicos.

Para algunas aplicaciones, tales como Grupos Electrógenos y SAI (suministro ininterrumpido de energía), se utilizan sistemas de agua nebulizada. Sin embargo, para los datacenters el uso del agua es un no-go. Esto es debido al hecho de que cuando los sistemas de agua nebulizada descargan unas finas capas de agua cubren todas las superficies dañando los equipos y creando un riesgo de choque eléctrico.

## Daño potencial a discos duros durante las descargas de los sistemas de extinción seca

En 2009, la industria de la protección contra incendios se dio cuenta de los posibles daños que ocurren en las unidades de disco duro (HDD) durante la descarga de sistemas de extinción seca. El daño causado varió desde una parada automática del disco a las perturbaciones más graves como las pérdidas de datos.

Las pruebas se realizaron en tres pasos para verificar la razón por la cual se dañan los discos duros durante las descargas. En primer lugar, las unidades de disco duro se expusieron a sobrepresión, a niveles generados típicamente durante las descargas de los sistemas de extinción seca. Durante la segunda prueba, los discos duros fueron expuestos a altos niveles de ruido. En el último test, sistemas de extinción reales fueron activados.

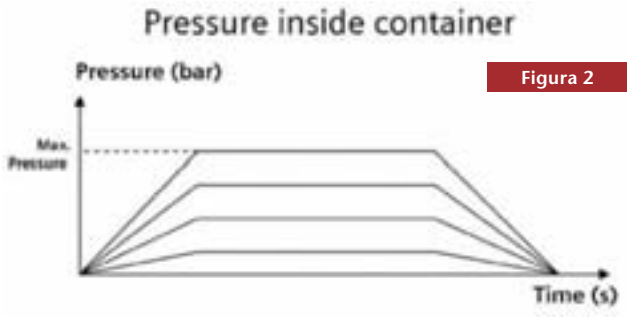


Figura 2

> «Los datacenters representan el 50% del mercado de extinción seca, y por lo tanto uno de los mercados más importantes para las empresas que venden sistemas de extinción»

La primera prueba demostró que ningún daño a HDDs es causado por exceso de presión creado por la extinción o por el gradiente de presión equivalente. Las segunda y tercera pruebas demostraron que el alto nivel de ruido creado por las descargas de extinción puede tener efectos negativos sobre los discos duros, que en el peor de los casos puede destruir los discos duros.

Basándose en los resultados había que desarrollar una extinción silenciosa, con una innovadora boquilla en su núcleo. De tal forma que el proceso de extinción sea diseñado de una manera tal, que el nivel de ruido permanezca por debajo del nivel que se encuentra en pruebas para suponer un riesgo a las unidades de disco duro.

De esta manera un innovador diseño lineal de la boquilla permite una

eficiente distribución del agente en el área protegida, al mismo nivel de rendimiento que un sistema convencional. Además, la descarga del agente, y por lo tanto el sonido, se centra en una dirección predefinida.

Adicionalmente hay que diseñar el sistema de extinción con una regulación de presión que descarga constante gas en la zona de las inundaciones. Esto elimina el pico al comienzo de la descarga y por lo tanto reduce el ruido máximo nivel.

> «En 2009, la industria de la PCI se dio cuenta de los posibles daños que ocurren en las unidades de disco duro (HDD) durante la descarga de sistemas de extinción seca»

## ¿El daño causado por sobrepresión?

La carga de una gran cantidad de agente extintor en una zona protegida dentro de un corto periodo de tiempo genera una sobrepresión en la habitación.

Los sistemas de extinción de gas inerte están fuertemente recomendados en los datacenters, debido a la alta sensibilidad de los equipos de las salas de servidores. Los gases inertes trabajan mediante la reducción de la concentración de oxígeno en volumen a un nivel en el que el fuego no puede continuar.

Dependiendo del riesgo de incendio, la concentración de oxígeno en volumen generalmente se reduce a entre un 14% y un 10%. La cantidad de gas inerte necesaria para proteger una sala es típicamente alrededor de la mitad del volumen de la habitación.

De esta forma los conductos de sobrepresión se utilizan para limitar la sobrepresión creada, permitiendo que cierto volumen de aire se desplace fuera de la sala. Dependiendo de la presión la resistencia de la sala, el criterio de diseño para las rejillas de sobrepresión es normalmente de 1 a 3 mbar en edificios normales.

Configuración de la prueba: Se llevó a cabo una serie de pruebas con HDDs típicos de varios fabricantes. La **Figura 1** muestra la configuración de la prueba con discos duros de 1 TB SATA de cuatro fabricantes diferentes. Para controlar los efectos en la prueba, las unidades de disco duro están en funcionamiento constante y los típicos parámetros de rendimiento son grabados. Durante las pruebas, la presión se aumentó a través de una boquilla abierta por una válvula de solenoide. La presión se controló luego por dos sensores de presión, uno para la presión absoluta y una sensible a la presión diferencial.

Entonces se realizaron una serie de pruebas con aumentos escalonados en la sobrepresión máxima y los gradientes, hasta una sobrepresión máxima de 170 mbar y una pendiente máxima de 30 mbar/s. **Figura 2**

Conclusión: Ningún efecto negativo se encontró en el rendimiento o daños causados en los discos duros. Adicionalmente, se retiró la limitación del flujo en la boquilla. Incluso a 220 mbar durante 3 s con un gradiente de hasta a 100 mbar/s no se registraron efectos negativos del rendimiento ni daños.

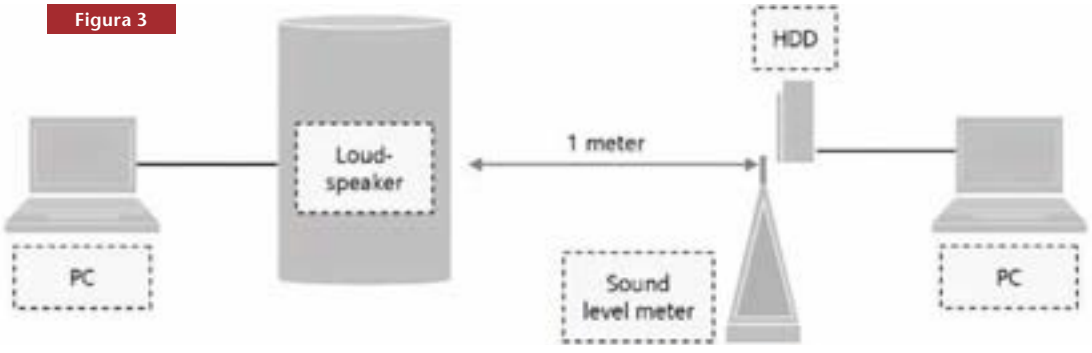
## ¿El daño causado por los altos niveles de ruido?

En los sistemas de extinción hay dos fuentes principales de ruido: los dispositivos de alarma acústicas utilizados para alertar a la gente a salir de la zona antes de que el agente se libera, y la descarga del propio agente extintor. En la segunda prueba se decidió medir los efectos sobre las unidades de disco duro cuando se expone a altos niveles de ruido.

Brevemente se resume que de acuerdo con las normas y reglamentos, los dispositivos de alarma para los sistemas de extinción seca deben generar niveles de ruido entre 90 y 120 dB.

Durante las descargas del sistema de extinción seca, los niveles altos de ruido se producen cuando el agente fluye a través de la boquilla en el área protegida. Para algunas aplicaciones, el nivel de ruido puede superar los 120 dB. Esto es cierto para los gases inertes, así como

Figura 3



para la agentes químicos, y también depende de varios factores de diseño.

Configuración de la prueba: La **Figura 3** muestra la configuración de la prueba utilizada para evaluar la sensibilidad al ruido de los discos duros. Las unidades de disco duro se colocaron y utilizaron de la misma manera como para las pruebas de sobrepresión, y el rendimiento fue medido de la misma manera.

Situado a una distancia de un metro de los discos duros, una generador de sonido con un altavoz creaba el ruido (banda ancha 500 Hz a 10 kHz) y 1/3 de octavas (353 Hz a 10 kHz). Los niveles de ruido fueron medidos a una distancia cercana en el disco duro.

La ventaja de usar un generador de sonido en lugar de un sistema de extinción seca fue la alta capacidad de control y la reproducibilidad de las condiciones de ensayo. Dado que los discos duros están directamente expuestos a la fuente de ruido sin estar montados en un bastidor o en un ordenador, las pruebas se llevaron a cabo bajo las peores condiciones posibles de impacto acústico.

La **Figura 4** muestra a lo que el nivel de sonido redujo el rendimiento de los discos duros (amarillo). Los resultados de la prueba mostraron que el ruido excesivo, a niveles de ruido perjudiciales para la salud humana, pueden tener efectos negativos en el rendimiento HDD, que temporalmente puede causar periodos en los que los discos duros están fuera de servicio (rojo). Este nivel suele comenzar a 120 dB, aunque ciertos tipos de HDDs y frecuencias comienzan ya por debajo de 110 dB.

La mayoría de los discos duros empiezan a ser sensibles al ruido en la gama de frecuencias de 500 Hz a 5 kHz. También se encontraron algunas frecuencias resonantes que pueden tener un impacto aún más fuerte (no se muestra aquí).

## ¿Son los resultados de laboratorio transferibles a los sistemas de extinción real?

Con el fin de observar los efectos cuando se expone a descargas reales de extinción, pruebas adicionales se realizaron utilizando la misma configuración de medición del rendimiento y unidades de disco duro.

Conclusión: Como era de esperar, se observa algunos de los efectos negativos sobre el rendimiento del disco duro.

Después de concluir que los altos niveles de ruido pueden provocar daños en los discos duros, se inició el desarrollo de la tecnología de una extinción silenciosa. El objetivo del proceso de desarrollo era crear un sistema de extinción operativo al mismo nivel de rendimiento que un sistema convencional, pero con un nivel de ruido significativamente menor que no dañe las unidades de disco duro.

Usando boquillas silenciosas en lugar de una boquilla convencional reduce el ruido emitido en aproximadamente 20 dB en el espectro relevante. La reducción de ruido de 20 dB es equivalente a una reducción de energía de ruido a una centésima, una significativa reducción. Adicionalmente usando sistemas de descarga constante el ruido nivel bajó de 8 dB. El uso de un sistema de extinción regulado en lugar de un sistema no regulado también redujo el nivel de ruido. ●

*Fotos: Tecnifuego-Aespi*

Figura 4

**JORGE SALGUEIRO-RODRÍGUEZ.** VICEPRESIDENTE EJECUTIVO DE AECRA Y ASESOR DE DESARROLLO NORMATIVO DE AJSE.

# Introducción al «Cloud» en la Seguridad Privada

La informática y la telemática son disciplinas en permanente evolución. La computación en la nube o cloud computing fue enunciada por primera vez por George Gilder en el año 2006 en un famoso artículo publicado por la revista Wired, bajo el expresivo título «Las fábricas de información». Un documento de enorme interés y referencia acerca de la computación en la nube lo constituye la Comunicación 2012/0529 realizada por el Comisión de la Unión Europea al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Relaciones, en relación al potencial de la computación en la nube en Europa de fecha 27 de septiembre de 2012.

EN dicho documento en su introducción se contempla una definición de la computación en la nube como «el almacenamiento, tratamiento y utilización de datos en ordenadores a distancia a los que se tiene acceso a través de Internet.»

El sector público tiene un papel importante que desempeñar en la configuración del mercado de la computación en la nube. En su calidad de mayor comprador de servicios informáticos de la UE, puede establecer requisitos estrictos respecto a las características, prestaciones, seguridad, interoperabilidad y portabilidad de los datos, así como al cumplimiento de los requisitos técnicos. También puede establecer requisitos para la certificación.

En relación a lo que es objeto de la introducción de este concepto en la realidad de la Seguridad Privada, decir que las empresas de seguridad deben tener en cuenta, a la hora de plantearse la contratación de un servicio de «cloud computing privado» comprensivo del almacenamiento y tratamiento de la documentación legal propia de su actividad, que parten de una situación propia de la exigencia normativa en la llevanza de dicha documentación, del tratamiento del documento en formato papel y no en soporte electrónico.

El sector público tiene un papel importante que desempeñar en la configuración del mercado de la computación en la nube.

Sustento de la presente afirmación lo constituyen los artículos 19 y 20 del Reglamento de Seguridad Privada, en cuanto a los requisitos formales fundamentales exigidos a las mismas como son los Libros Registro y los contratos de arrendamiento de servicios de seguridad privada.

Así el artículo 19 del Reglamento de Seguridad Privada que debemos poner en relación con el artículo 1 y artículo 14 de la reciente Orden INT 314/2011 de 1 de febrero de Empresas de Seguridad Privada, contemplan en el artículo 1 la vigencia de la sede electrónica para la relación de las empresas de seguridad con la administración competente, y en el artículo 14 procede a concretar y satisfacer el mandato expresado en el artículo 19 del Reglamento cuando se disponía que «el formato de los reseñados libros-registros se ajustará a las normas que respectivamente apruebe el Ministerio del Interior.»

De forma concreta, el artículo 14 de la citada Orden dispone: «1. Los Libros-Registro generales y específicos que se establecen en el Reglamento de Seguridad Privada y que deberán llevar las empresas de seguridad, se ajustarán a los modelos oficiales aprobados por Resolución del Secretario de Estado de Seguridad, y deberán conservarse durante un periodo de cinco años.

Los asientos o anotaciones podrán ser realizados por procedimientos informáticos o cualesquiera otros idóneos sobre hojas sueltas o separables, cuya confección se ajustará a las características de los modelos, y serán objeto de encuadernación posterior.»

El mismo artículo 19 del Reglamento, al aludir al depósito o almacenamiento de dichos libros cuya llevanza reitero, viene impuesta normativamente a las empresas de seguridad, establece de forma expresa que dichos libros no pueden ser archivados o almacenados por las empresas fuera de su sede principal o de sus delegaciones o sucursales, por lo que de su lectura parece desprenderse que se cierra la opción para la empresa de seguridad de contratación de un cloud computing privado que permita el traslado, archivo y depósito de dichos documentos en una nube.

En el mismo sentido, respecto a los contratos de servicio se manifiesta el artículo 20 del Reglamento de Seguridad Privada, al afirmar que 1.(…) El formato de los contratos y de las comunicaciones se ajustará a las normas y modelos que se establezcan por el Ministerio del Interior, sin perjuicio de la posibilidad de adición en los contratos, de pactos complementarios para aspectos no regulados en el presente Reglamento.

En cualquier caso, los contratos permanecerán en las sedes de las empresas de seguridad a disposición de los órganos de las Fuerzas y Cuerpos de Seguridad competentes en materia de inspección y control, durante un plazo de cinco años desde la finalización del servicio objeto del contrato.

**Es factor clave para poder utilizarse por las Empresas de Seguridad Privada el servicio de cloud computing, la existencia en el marco normativo de una disposición de carácter reglamentario reguladora de la Sede y Registro Electrónico en el ámbito de la Seguridad Privada.**

Por consiguiente, es factor clave para poder utilizarse por las empresas de Seguridad Privada el servicio de cloud computing, la existencia en el marco normativo de la Seguridad Privada de una disposición de carácter reglamentario reguladora de la Sede y Registro Electrónico en el ámbito de la Seguridad Privada, que ampare para cumplimiento de dichas obligaciones frente la Administración, la existencia del documento en soporte electrónico.

Además, y respecto al referido modelo aludido, tanto para los Libros Registro como para los contratos de servicios de seguridad, es preciso la aprobación de una Resolución de la Secretaría de Estado de Seguridad, que determine dichos formatos electrónicos respecto a los documentos mencionados.

Dicha afirmación viene ratificada por el contenido del artículo 16 apartado 1 de la Orden INT 314/2011 de Empresas de Seguridad ya meritada, respecto al modelo de contrato exigido a las empresas de seguridad cuando se establece literalmente:

«1. Los contratos en que se concreten las prestaciones de las diferentes actividades se consignarán por escrito, debiendo contener, con carácter general, los siguientes datos y cláusulas, acorde al modelo disponible en la sede electrónica de la Dirección General de la Policía y la Guardia Civil, ámbito del Cuerpo Nacional de Policía o, en su caso, de las Comunidades Autónomas competentes». ●

> «La computación en la nube es el almacenamiento, tratamiento y utilización de datos en ordenadores a distancia a los que se tiene acceso a través de Internet»

*Fotos: Archivo*

PROYECTO DE LEY DE SEGURIDAD PRIVADA

# El proyecto de Ley rubrica su examen en el Congreso de los Diputados

## Con el acuerdo entre PP y CiU

El ministro del Interior, Jorge Fernández Díaz, explicó en el Congreso de los Diputados el acuerdo alcanzado por el Grupo Parlamentario Popular y el de Convergència i Unió para modificar el contenido de algunos artículos del proyecto de Ley de Seguridad Privada, que fue enviado por el Gobierno a la Cámara Baja para su debate y aprobación.

ESTE acuerdo se presentó en el debate de las enmiendas a la totalidad que la Izquierda Plural y Convergència i Unió (CiU) habían presentado a este proyecto de Ley, elaborado por el Ministerio del Interior, y que modernizará e incorporará nuevas disposiciones que no estaban recogidas en la anterior normativa de 1992.

En este sentido, Jorge Fernández Díaz explicó que el proyecto abre «nuevos servicios a la seguridad privada que la sociedad está demandando», como la vigilancia de los polígonos, urbanizaciones, edificios públicos o joyerías, además de la seguridad exterior de las prisiones. El ministro del Interior recordó que este sector agrupa a casi 1.500 empresas, da trabajo a más de 85.000 personas y ha facturado en el último año más de 3.000 millones de euros.


Jorge Fernández Díaz, ministro del Interior.

El Grupo Parlamentario Popular (GPP) y el de Convergència i Unió (CiU), –que ha retirado su enmienda a la totalidad– han pactado siete cambios al articulado inicial del proyecto de Ley relativos fundamentalmente al control, inspección y sanción de las empresas de seguridad privada y de las agencias de detectives.

El ministro del Interior, Jorge Fernández Díaz, consideró «razonable» que las comunidades autónomas con estas competencias puedan inscribir en sus registros de seguridad privada a los despachos de detectives que trabajan exclusivamente en su marco autonómico. Asimismo, Fernández Díaz señaló que el falseamiento de la «declaración responsable» que se exige a las agencias de detectives privados, seguirá siendo una infracción administrativa que conllevará la correspondiente sanción.

Además, el ministro del Interior aseguró que con este acuerdo quedan subsanadas las dudas de constitucionalidad sobre la futura Ley de Seguridad Privada que habían surgido, debido a que el Estatuto de Cataluña establece que corresponde a la Generalitat la autorización de las empresas de seguridad privada, así como la inspección, sanción, autorización y coordinación de las actividades de la seguridad privada que se realicen en esta comunidad autónoma.

En virtud de este acuerdo, Jorge Fernández Díaz anunció que el Gobierno modificará los artículos 12 y 13 del proyecto de Ley de Seguridad Privada, y garantizó que con esta nueva Ley se mantiene la «irrenunciable preminencia de la seguridad pública a la privada y los principios de cooperación y corresponsabilidad». «No se trata en absoluto de privatizar la seguridad», ha afirmado el ministro.

*Fotos: MIR*

Visítenos en el Stand **3 F 002 de Cartes 2013** en París, Francia, del **19 al 21 de noviembre**

# iCLASS SE®
# La plataforma de control de acceso más inteligente


FUNCIONA CON MULTITUD DE TECNOLOGÍAS DE TARJETA

CONFIGURACIÓN REMOTA DE LECTORES

FUNCIONA CON MÚLTIPLES DISPOSITIVOS

MAYOR SEGURIDAD PARA CREDENCIALES

SEGURIDAD MEJORADA DE MICROPROCE-SADORES

**Equipada con una tecnología preparada para el futuro, que permite una identificación segura, desde el acceso físico al acceso digital. Un nuevo concepto de la seguridad, la usabilidad y el rendimiento.**

HID®

La plataforma iCLASS SE® de HID Global, compatible con multitud de tecnologías y medios, es una solución para una identificación segura, que está preparada para el acceso físico, para los dispositivos móviles y para la gama más amplia de entornos y aplicaciones convergentes. Para lograr la máxima interoperabilidad, iCLASS SE admite casi todas las tecnologías de tarjeta, incluidas las ya conocidas, lo que se traduce en actualizaciones rentables y sin complicaciones, que aumentan la seguridad y mejoran el rendimiento.

**Para más información, descarga el White Paper de iCLASS SE en el siguiente enlace: hidglobal.com/iclass-se-platform-cuadseg**

JORNADA ORGANIZADA POR EL OBSERVATORIO SECTORIAL DE LA SEGURIDAD PRIVADA

# Efectos de la crisis sobre el sector de la Seguridad Privada

Las organizaciones empresariales y sindicatos que conforman el Observatorio Sectorial de la Seguridad Privada han celebrado una jornada de análisis de los efectos de la crisis sobre el sector. El acto se centró en abordar las problemáticas de este segmento desde diversos puntos de vista, y contó con la participación de expertos de alto nivel para cada una de las áreas.

LA Fundación Sindical de Estudios de Comisiones Obreras (CC. OO.) acogió el acto, que fue moderado por el secretario general de APROSER, Eduardo Cobas.

El secretario general de la Federación de Servicios Privados de CC. OO., Jesús Fernández, dio la bienvenida a la jornada, que calificó de muy interesante. «Me gustaría animar al Observatorio para que sea una herramienta útil para situar al sector de la Seguridad Privada en el lugar en que tiene que estar, para establecer una seguridad con mayúsculas», señaló.

El presidente de Securitas España y de la División Iberoamérica de Securitas, Luis Posadas, analizó los efectos derivados de la crisis en los sistemas de contratación. Posadas abordó la situación desde la perspectiva de las empresas, y se mostró muy crítico con el actual funcionamiento de la contratación, especialmente la pública. «A la hora de la verdad, solo se tienen en cuenta criterios económicos, se opta por la oferta más barata y esto hace que se degrade muchísimo el sector», aseguró.

Además, destacó la necesidad de poner en valor los servicios de seguridad privada, ya que, según él, «la gente tiene que empezar a entender que prescindir de una seguridad privada de calidad no sale gratis.»

Un momento del encuentro del Observatorio Sectorial de la Seguridad Privada donde se analizaron los efectos de la crisis sobre el sector.

El ex-ministro de Administraciones Públicas y senior counsellor de PWC, Jordi Sevilla, analizó a fondo la situación económica del país. Sostuvo la tesis de que en España se está saliendo de la recesión pero no de la crisis, y para eso aportó numerosos datos macroeconómicos. En cuanto a la evolución de la cantidad y calidad del empleo, comentó que hemos pasado de un periodo caracterizado por EREs masivos, a uno de congelación salarial, entrando actualmente en otro de reducciones de salarios. Concluyó su intervención lanzando la siguiente cuestión: «¿Va a ser suficiente esta salida de la recesión para poner en marcha el tren?» o, en otras palabras, «¿ya estamos en el buen camino y solo toca esperar a que la situación mejore?». Él mismo reconoció tener dudas al respecto: «O cambiamos de políticas o es muy difícil que la salida de la recesión nos lleve a la salida de la crisis», señaló.

## Negociación colectiva

En el siguiente bloque se abordaron los efectos derivados de la crisis en la aplicación de la reforma laboral, en particular la negociación colectiva en los servicios empresariales, a cargo del catedrático de Derecho del Trabajo de la Universidad de Valencia Carlos Alfonso Mellado. Según él, la negociación colectiva es «un asunto estrella de este sector», al ser «intensivo en mano

de obra y destinado al consumo interno». En su opinión, «la última reforma laboral ha facilitado el descuelgue de las empresas del Convenio Colectivo», lo que aplicado a sectores como el de la seguridad «puede fomentar el dumping social y la competencia desleal.»

Por último, el comisario jefe de la Unidad Central de Seguridad Privada del Cuerpo Nacional de Policía, Esteban Gándara, aportó la perspectiva de la Administración en cuanto a intrusismo y competencia desleal. Gándara explicó las dificultades con las que se encuentran a la hora de luchar contra este tipo de prácticas: «El problema es que, para luchar contra el intrusismo y la competencia desleal –que son conceptos diferentes–, contamos con un marco jurídico insuficiente, no tenemos suficientemente definidos los procedimientos de actuación ni contamos con los instrumentos de ejecución que serían más eficientes. Sí tenemos la voluntad de luchar contra esta realidad, pero eso no siempre llega. El proyecto de nueva ley de seguridad privada supondrá un cambio radical en esta materia», aseguró.

> «Entre las conclusiones se destacó el importante deterioro cualitativo de los procesos de contratación tanto públicos como privados»

## Conclusiones

Por su parte, los miembros del Observatorio, entre sus conclusiones, destacaron el importante deterioro cualitativo de los procesos de contratación tanto públicos como privados; las consecuencias derivadas de una perversa utilización de la última reforma laboral, la necesidad de analizar con detalle los convenios de empresa y los procedimientos de descuelgue (aquellos que exclusivamente se originen para posicionar a algunas empresas en una situación de ventaja competitiva y, por lo tanto, de competencia desleal), así como la nueva dinámica en la lucha contra el intrusismo, entendiendo necesario a tal efecto el intercambio de información entre las distintas Administraciones Públicas implicadas, y formalizar acuerdos con los principales actores del sector, a tal efecto. ●

*Fotos: APROSER*

ENCUENTRO ORGANIZADO POR LA ASOCIACIÓN VALENCIANA DE DIRECTORES DE SEGURIDAD

# «Ciberseguridad en Infraestructuras Críticas»

Valencia se convirtió por unas horas en la capital de la Ciberseguridad y las Infraestructuras Críticas, gracias a la jornada «Ciberseguridad en Infraestructuras Críticas», organizada por la Asociación Valenciana de Directores de Seguridad (AVADISE) el pasado 19 de septiembre, y que sirvió para analizar las amenazas para la seguridad que pueden llegar desde el ciberespacio.

MÁS de 300 profesionales y expertos en la materia se dieron cita en el Paraninfo de la Universidad Politécnica de Valencia, en el que las ponencias se unieron a las demostraciones prácticas y las mesas de debate con el objetivo de abordar, de una manera integral, el amplio campo de la ciberseguridad en relación con las infraestructuras críticas.

El ciberespacio es el lugar en el que el crimen organizado y algunos países han buscado el amparo de los sistemas de justicia nacionales. De manera paralela, los ciberataques se han convertido en un tipo de amenaza para la seguridad, que cada vez está más presente en la sociedad debido a su dependencia de las tecnologías, directrices y métodos empleados para proteger los activos de una organización o de los usuarios.

De esta manera, entre los ponentes estuvieron presentes los principales Equipos de Respuesta ante Emergencias Informáticas (CERT´s), tanto a nivel nacional como autonómico, así como responsables de Seguridad de Infraestructuras Críticas de la Comunidad Valencia, representantes del sector educativo, especialista en TIC de la UPV, y de la OTAN en seguridad de la Información.

En este sentido, el senador por Valencia José María Chiquillo fue el encargado de inaugurar la jornada con una ponencia sobre la legislación para la protección de las Infraestructuras Críticas; a la que siguió la intervención de Roberto Peña, miembro de la División PIC de Grupo Control, que explicó en qué consiste un ciberataque y abordó una exposición sobre los vectores de ataque.

La jornada continuó con una mesa-debate sobre «La ciberseguridad y las infraestructuras», integrada por representantes de la OTAN en Bétera, de la Escuela Técnica Superior de Ingeniería Informática la UPV, la Autoridad Portuaria de Valencia, Iberdrola y el capítulo de ISACA en Valencia. Un debate que dejó de manifiesto la importancia que la disrupción de los servicios esenciales como luz, agua o comunicaciones pueden tener en una sociedad cada vez más dependiente de la tecnología, así como la necesi-

**Ponentes en la Jornada «Ciberseguridad en Infraestructuras Críticas».**


**Un momento de las intervenciones.**

dad de contar con perfiles específicos entre los profesionales de la seguridad.

La segunda mesa-debate del día se centró en «Los centros de respuesta a las Ciberamenazas», en la que participaron representantes del Centro Criptológico Nacional del Centro Nacional de Inteligencia, del Centro Nacional para la Protección de las Infraestructuras Críticas, del CSIRT de la Comunidad Valenciana, y del Grupo de Delitos Telemáticos de la Guardia Civil.

> «Estuvieron presentes los principales Equipos de Respuesta ante Emergencias Informáticas (CERT`s)»

Así, los ponentes explicaron a los asistentes los objetivos de trabajo de sus centros y cómo afrontan la problemática de la ciberseguridad, si bien un punto en común fue la necesidad de una mayor coordinación entre ellos. Esta segunda mesa dejó muestra de la importancia de la existencia de todos estos organismos a diferentes niveles y la contribución que hacen a favor de una mayor seguridad en la red.

La jornada finalizó con la intervención de Jacinto Aparicio, presidente de AVADISE, quien recordó la importancia que para la asociación tiene la realización de conferencias, charlas y coloquios de interés general para la seguridad pública y privada.

La jornada contó con el patrocinio de Grupo Control, a través de su División de Protección de Infraestructuas Críticas. ●

*Fotos y Texto: AVADISE*

**Vista general de los asistentes a la jornada.**

EL 26 DE ENERO DE 2012 SE LANZÓ LA PRIMERA ACCIÓN VÍA TWITTER

# La Policía Nacional alcanza los 600.000 seguidores en Twitter

La Policía Nacional española es el segundo cuerpo de seguridad del mundo –tras el FBI estadounidense- y primera institución pública de España en alcanzar los 600.000 seguidores en la red de información Twitter. El interés y apoyo de los ciudadanos a través de estas plataformas, no solo han convertido a la Policía en la institución española líder en redes sociales sino que han permitido desarrollar una labor de prevención, información, concienciación, atención al internauta y colaboración ciudadana, que han convertido a la Policía Nacional en el cuerpo de seguridad referente en el uso operativo de la web 2.0 y uno de los baluartes del plan estratégico Policía 3.0.

DESDE el 26 de enero de 2012, fecha en que se lanzó la primera acción vía Twitter, contra la droga y conocida como tweetredada, son muchos los éxitos policiales logrados gracias a los internautas y su colaboración a través de las redes sociales. Los últimos ejemplos son la desarticulación de una red de explotación sexual en Barcelona, gracias a la información recibida con la campaña #contralatrata; el contacto privado con un testigo clave en una violación recientemente esclarecida y conseguir su colaboración con el grupo operativo a través de @policia; paralizar la difusión por Internet de vídeos sexuales de menores gracias a la alerta privada de tuiteros; localización de varias víctimas de un abusador sexual con burundanga tras activar la búsqueda en Twitter; la detención de fugitivos tras viralizar un vídeo de «Los más buscados»; la detección y aviso de casos de amenazas, phishing, virus y fraude online o los más de 350 detenidos por narcotráfico tras recibir más de 12.000 correos electrónicos en antidroga@policia.es.

El fuerte impulso a la actividad del Grupo de Redes Sociales se enmarca en el Plan Estratégico de la Policía, denominado Policía 3.0, en el que la innovación y anticiparse a los retos de la seguridad del futuro y las nuevas tecnologías son ejes fundamentales.

El crecimiento exponencial en usuarios (en 20 meses se ha multiplicado su número por 10, hasta superar los 600.000 followers) se ha visto acompañado de una enorme participación de los internautas, con más de 1.500 menciones diarias a @policia y que los agentes gestionan con la resolución de consultas, y derivando cuestiones operativas a las unidades especializados o las comisarías locales correspondientes.

## Policía 3.0: resultados operativos a través de nuevos canales

A través de las redes sociales se han realizado acciones con una excelente acogida entre los ciudadanos, como la tweetredada; la tweetpatrulla, en la que se acompañaba en directo a agentes en su patrulla nocturna; tweetencuentros con los agentes de la Brigada de Investigación Tecnológica (BIT) y los responsables de las pruebas de acceso a la Policía; la selección, alertas y consejos sobre virus y fraudes en la Red o concursos con una participación masiva.

Además, la web 2.0 se ha mostrado como un potente altavoz para las campañas de concienciación en aspectos tan relevantes como el bullying o acoso escolar; el ciberacoso; la lucha contra la violencia de género; el tráfico de drogas; la seguridad en el ocio joven; el turismo sin riesgos; ...

La Policía española utiliza el nombre genérico en Twitter (@policia), como hace en otras plataformas online, como la web (www.policia.es) o Youtube (www.youtube.com/policia). El canal de la Policía Nacional en Youtube es el de mayor audiencia entre las instituciones públicas españolas, y en la actualidad cuenta con más de 200 vídeos visibles al público, que han sido reproducidos más de 3.940.000 veces.

La Policía cuenta también con una página en Facebook a través de la cual sus casi 60.000 usuarios pueden informarse de cuestiones vinculadas con la seguridad, de la actualidad policial y de cómo trabajan las distintas unidades de la Policía Nacional. ●

# ) eyevis

PERFECT VISUAL SOLUTIONS

## PROFESSIONAL VISUAL DISPLAY SOLUTIONS - MADE IN GERMANY

) DLP® Cube Series

### eyevis EC Rear Projection Cubes - The Widest Range on the Market

- ) Lamp-lit or LED-lit Projector Versions
- ) Resolutions: XGA, SXGA, SXGA+, UXGA, full HD and WUXGA
- ) Screen Sizes from 50" to 100"
- ) Automatic Colour and Brightness Control
- ) Ideal for 24/7 Applications

### eyevis Modular LCD Screens - The Slim Solution for Seamless Video Walls

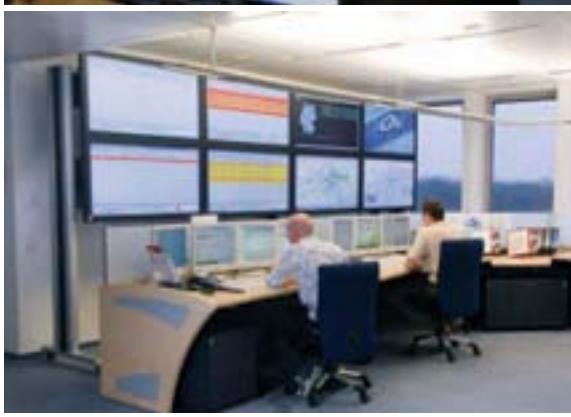
- ) Screen Sizes: 46", 55" and 60"
- ) Resolutions: WXGA or full HD
- ) Gap Active-to-Active <7mm
- ) New Versions with Direct-LED Backlight
- ) Many different Installation Possibilities

) Super Narrow Bezel LCDs

) LCD Monitor Series

### eyevis EYE-LCD Series - Professional Screens for any Application

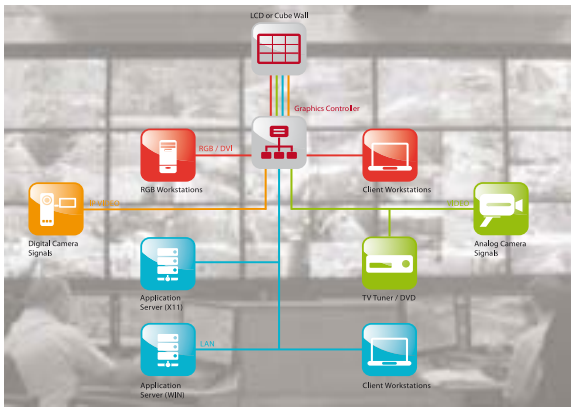
- ) Full HD LCD Monitors from 42" to 82"
- ) Ultra-HiRes Monitors with even higher Resolutions (Quad HD and 4K)
- ) New Versions with Edge-LED Backlight
- ) Stable industrial Design
- ) Various Stands and Wallmounts available



### eyevis Netpix Series - High-End Controllers for Display Systems

- ) Connectivity for any Signal Type
- ) Unlimited Inputs and Outputs
- ) Hardware Decoding for IP Video Streams
- ) Optionally available as redundant Version
- ) Perfectly compatible with eyevis Display Hardware and Software

) Netpix Graphics Controllers





**) eyevis GmbH**, Hundsschleestrasse 23, 72766 Reutlingen/Germany,
Tel.: +49 (0) 7121 43303-0, Fax: +49 (0) 7121 43303-22, www.eyevis.de, info@eyevis.de
**OFICINA EN ESPAÑA:** C/ Serrano 19 3ª dcha 28001 - MADRID evs@eyevis.com

INSTITUTO NACIONAL DE SEGURIDAD E HIGIENE EN EL TRABAJO

# Informe anual de Accidentes de Trabajo en España 2012

## Estudio realizado por el Observatorio Estatal de Condiciones de Trabajo

En el año 2012 se notificaron en España 471.223 accidentes de trabajo con baja; 408.537 de estos fueron accidentes en jornada de trabajo (86,7% del total) y 62.686 fueron accidentes in intínere (13,3% del total). Son datos que se desprenden del «Informe anual de Accidentes de Trabajo en España 2012», que elabora el Observatorio Estatal de Condiciones de Trabajo, en su labor por proporcionar y difundir el conocimiento riguroso de los factores que puedan influir en los riesgos laborales, así como realizar el estudio en profundidad de la siniestralidad laboral para orientar de forma más eficaz las políticas públicas preventivas y realizar el seguimiento y valoración de las mismas.

Habitualmente se utiliza el índice de incidencia para expresar la siniestralidad, pues se considera una forma sencilla y ajustada de valorar este fenómeno, ya que indica el número de accidentes que se producen en un periodo determinado por cada 100.000 trabajadores afiliados con la contingencia de accidente de trabajo y enfermedad profesional cubierta, relacionando de esta manera el número de sucesos con la población susceptible de padecerlos, tal y como indica el informe.

El colectivo de los trabajadores afiliados con la contingencia de accidente de trabajo y enfermedad profesional cubierta en el año 2012 incluye a los trabajadores afiliados al Régimen General y Minería del Carbón, al Régimen Especial Agrario, al Régimen Especial del Mar y a los trabajadores del Régimen Especial de Autónomos, que hayan optado voluntariamente por la cobertura de las contingencias profesionales.

A modo de resumen, a continuación detallamos algunos de los aspectos más destacados del estudio.

**Índice de incidencia por sector y gravedad**

El índice de incidencia del año 2012 fue de 2.848,9 accidentes de trabajo con baja en jornada de trabajo por cada 100.000 trabajadores afiliados, lo que supone un descenso del 19% respecto a 2011 **(Figura 1).**

El sector de actividad con mayor índice de incidencia fue Construcción, que con 6.296,9 supera en más del doble la media de los índices sectoriales. Le siguió el sector Industria, con 4.652, valor también muy superior a la media. Por debajo de la media se situaron los sectores Agrario y Servicios, que alcanzaron valores de 2.405,1 y 2.302, respectivamente.

Respecto al año 2011, la disminución del índice de Construcción e Industria fue similar, - 18,6 y -18,7%, respectivamente. El sector Servicios tiene una disminución inferior, pero también muy importante (-16,9%) y el sector Agrario es el que disminuye en menor proporción (-7,8%).


**Figura 1.** Índices de incidencia sectoriales. Fuente: Anuario de Estadísticas Laborales y de Asuntos Sociales 2012. MEYSS.

# Cámaras IP de Honeywell

## Posibilidades de integración ilimitadas con las nuevas soluciones IP de Honeywell

Nuestros sistemas IP poseen una mejor escalabidad e interoperabilidad e incluyen la compatibilidad con los estándares ONVIF, ONVIF S y PSIA. Además, son compatibles con otros fabricantes y con las principales plataformas de software de gestión de vídeo. Las nuevas soluciones IP de Honeywell ofrecen posibilidades ilimitadas para elegir la solución adecuada para cada instalación.

Esto le proporciona infinitas oportunidades de mejora y expansión en función de la evolución de su ecesidades de la empresa. Con excelente calidad de imagen, nuestra amplia gama de cámaras IP y el último MAXPRO® NVR le proporcionan soluciones completas para satisfacer todas sus necesidades de vídeo, lo que le permite tomar la decisión correcta en cada momento.
***Proteja su futuro con las nuevas soluciones IP de Honeywell.***

**Honeywell**

Para más información llame al teléfono 902 667 100
o visite www.honeywellipsolutions.com/es

**Índice de incidencia por división de actividad económica**

En el año 2012 solo las «Actividades relacionadas con el empleo» aumentaron notablemente su índice de incidencia, el 15,5%, y la «Pesca y Acuicultura» experimentó un discreto incremento del 0,4%.

El resto de las divisiones de actividad sigue la tendencia general de la siniestralidad laboral, con descensos de los índices de incidencia, en general bastante destacados.

**Índice de incidencia por sexo y gravedad**

Al igual que los datos obtenidos en años anteriores, la incidencia de accidentes de trabajo fue 2,2 veces mayor en los varones que en las mujeres. Considerando la gravedad de los accidentes, esta relación empeora conforme aumenta la gravedad de los accidentes de trabajo, llegando a ser la mortalidad por accidente de trabajo 19 veces mayor en los varones.

**Edad**

En el año 2012 la distribución de la población afiliada a la Seguridad Social con las contingencias cubiertas, según su edad, es la siguiente: los trabajadores más jóvenes, entre 16 y 24 años representan el 5,6%; en la franja de edad entre 25 y 49 años están el 70,2%; y el 24,2% de los trabajadores tienen 50 años o más. Estos datos, confrontados con los de 2011, están reflejando el aumento relativo de la franja de mayor edad, fundamentalmente debido a la disminución de los afiliados más jóvenes.

El índice de incidencia de los trabajadores más jóvenes fue superior al del resto de trabajadores: 1,2 veces mayor que el de los trabajadores con edades comprendidas entre 25 y 49 años y 1,3 veces mayor que el de los trabajadores de 50 años o más. Esta relación se ha demostrado estable durante años sucesivos en los que había distintas situaciones económicas, lo que constata que los trabajadores jóvenes deben ser considerados un grupo de especial atención en cuanto a su incidencia de accidentes de trabajo (**Figura 2**). Cuando se analiza la incidencia de accidentes de trabajo mortales la situación es completamente distinta, ya que los trabajadores de mayor edad presentaron un índice 3,8 veces mayor que los trabajadores más jóvenes y 2,4 veces mayor que los trabajadores con edades comprendidas entre 25 y 49 año.

**Tipo de contrato**

En el año 2012, la distribución de accidentes fue la siguiente: el 67% de los accidentes los sufrieron trabajadores con contrato indefinido y el 32,9%, trabajadores con contrato temporal.

En el año 2012 el índice de incidencia de los trabajadores temporales fue 1,6 veces mayor que el de los trabajadores indefinidos.

En todos los sectores de actividad se observa que el índice de incidencia de los trabajadores temporales es mayor que el índice de indefinidos. Los sectores en los que este resultado es especialmente destacado son Construcción e Industria.

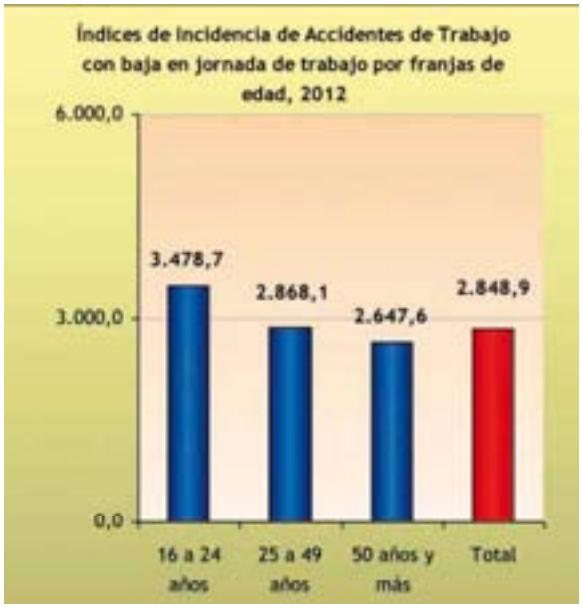



**Figura 2.** Índices de incidencia por edad. Fuente: Base informatizada de partes de declaración de accidentes de trabajo 2012. MEYSS.

**Tamaño de la empresa**

En el año 2012, la distribución de trabajadores inscritos en la Seguridad Social según el tamaño de la empresa para la que trabajaban era la siguiente: el 22,2% de los afiliados trabajaba en empresas de 1 a 9 trabajadores. El tamaño de plantilla de 10 a 25 trabajadores agrupa al 12% de los trabajadores y, en global, el 42,1% de los trabajadores estaba en empresas de menos de 50.

Las empresas con plantillas de 10 a 249 trabajadores presentaron una siniestralidad muy elevada en 2012, siendo el dato más destacado las empresas de 26 a 49 trabajadores con 4.810 accidentes por cien mil trabajadores afiliados.

La incidencia de accidentes graves fue muy importante en las empresas de 1 a 49 trabajadores, despuntando especialmente el dato de 45,5 accidentes por cien mil afiliados en empresas con plantilla de 10 a 25 trabajadores. Los accidentes mortales se agruparon especialmente en empresas de 10 a 49 trabajadores, siendo el dato más significativo 6,1 accidentes mortales por cien mil afiliados en empresas de 10 a 25 trabajadores.

**Mortalidad por accidente de trabajo**.

En el año 2012 sucedieron 452 accidentes de trabajo mortales en jornada de trabajo, que suponen un 0,1% de los accidentes de trabajo con baja de este año. La mortalidad por accidente de trabajo viene disminuyendo desde hace más de una década.

El índice de incidencia de accidentes de trabajo mortales fue de 3,2 para el año 2012, disminuyendo porcentualmente el -15,8% con respecto a 2011. El sector Construcción presentó el mayor índice de incidencia de accidentes mortales con un valor de 9,4.

VISUAL TOOLS


# La calidad de sus cámaras IP en su televisor HDMI

## DESCODIFICADOR INALÁMBRICO DE VÍDEO PARA CÁMARAS IP DE AXIS

AX-Tv es un dispositivo de pequeño tamaño, diseñado especialmente para el hogar y para oficinas, hoteles, clínicas, comercios y otros pequeños negocios, que permite ver hasta 16 cámaras AXIS instaladas en la propia red local o a través de Internet en un televisor HDMI.

No necesita PC, ofrece gran calidad de imagen, funciona vía red local o WIFI y, además, dispone de un mando a distancia con el que podrá poner a punto la configuración deseada y operar para ver las cámaras una a una, o en cuadrantes de 2x2, 3x3 y 4x4 cámaras.

AXIS COMMUNICATIONS
APPLICATION DEVELOPMENT PARTNER

más información en: www.visual-tools.com

C/ Isla Graciosa, 1 - 28034 Madrid - T: +34 91 729 4844 - F: +34 91 358 5236 - info@visual-tools.com

LA COMPAÑÍA CELEBRA SU PARTNER EVENT 2013

# Axis Communications: innovación en soluciones y productos

**El evento, que reunió a más de 180 profesionales, cierra el compromiso de la compañía hacia su red de integradores, consultores, desarrolladores de aplicaciones y partners**

Más de 180 profesionales acudieron el pasado 3 de octubre al Partner Event 2013 de Axis Communications, en una jornada en la que se dieron a conocer las últimas novedades tecnológicas de la compañía en materia de videovigilancia, así como se presentó la nueva solución de Control de Acceso Físico AXIS A1001.

MÁS de 180 socios de la filial española de Axis Communications fueron congregados en el Parque Warner en una jornada en la que el CEO de la compañía, Ray Mauritsson, y la directora regional del Sur de Europa, Edwige Maury –entre otros portavoces– dieron a conocer en diversas conferencias las últimas novedades de soluciones y productos de la compañía, seguidos de una serie de demostraciones prácticas dignas de ciencia ficción.

El evento cierra el compromiso de la compañía hacia su red de integradores, consultores, desarrolladores de aplicaciones y partners, sobre la que desarrolla toda una compleja campaña para su formación y certificaciones, manteniéndoles siempre actualizados sobre las posibilidades que ofrece a sus clientes su porfolio de productos y soluciones.

Como anuncio destacado, la compañía presentó durante el evento su solución de Control de Acceso Físico AXIS A1001, el sistema de control de puertas en red con software incorporado basado en la Web no propietario, inteligente y completamente escalable. Esta solución complementa el catálogo de Axis para productos de vídeo en red, posibilitando unas capacidades de integración únicas para sus partners y usuarios. La compañía la lanzará de momento en EEUU en el cuarto trimestre de 2013 a modo de laboratorio de pruebas, con expectativas de su comercialización a gran escala en un plazo de un año.

Durante la tarde la compañía llevó a cabo un simulacro de situaciones cotidianas fictícias, poniendo en práctica algunas de sus cámaras y aplicaciones con el plató del show «Loca Academia de Policía» del Parque Warner como escenario. Las simulaciones incluyeron el atraco a un cajero bancario, en el que gracias a una cámara Axis y la aplicación desarrollada por su partner Technoware, en base a una serie de algoritmos que detectan anomalías en el movimiento y la contabilización de individuos en el área, alertaron en

**Equipo de Axis Communications que participó en su Partner Event 2013.**


Un momento del simulacro en el plató del show "Loca Academia de policía".

cuestión de segundos a los agentes de policía logrando la detención del delincuente; así como infracciones de tráfico en líneas continuas del asfalto y salto de semáforos en rojo, que en este caso gracias a las aplicaciones de Infocom Sermar y una instalación básica de cámaras Axis, detectaron la infracción, identificaron el individuo y la sanción prevista.

Como cierre al evento, Axis procedió a la entrega de premios de sus ya habituales «Axis Oscars», con los que se pretende premiar a los mejores partners del año en diversas divisiones: Mejor partner del sector del retail, Mejor partner del sector de tráfico y transporte, Partner más proactivo e Instalación más compleja. ●

## Axis entra en el mercado del Control de Acceso Físico en EEUU

Axis Communications se abre paso en el mercado del Control de Acceso Físico con la presentación de su nueva solución AXIS A1001, el sistema de control de puertas en red con software incorporado basado en la Web. Esta solución complementa el catálogo de Axis para productos de vídeo en red, posibilitando unas capacidades de integración únicas para sus partners y usuarios.

El sistema de control de puertas AXIS A1001 es la primera solución no-comercial del mercado basada en tecnología IP. Se trata de una plataforma para dos soluciones diferentes. AXIS Entry Manager (AXIS A100 con software incorporado) es una solución lista para usar para pequeñas y medianas empresas, tales como oficinas, industrias y retailers – que por lo general cuentan con 10 puertas y requisitos básicos de control de acceso.

Para sistemas empresariales más grandes, la interfaz de aplicaciones abiertas de programación de AXIS A1001 habilita a las Aplicaciones de Desarrollo de Partners de Axis (ADP) a satisfacer las necesidades específicas del cliente. Los partners ADP de Axis, Aimetis, Genetec, IMRON, Milestone, NestLevel y OnSSI, están comprometidos con el desarrollo de soluciones que incluye integración de vídeo y funciones avanzadas de control de acceso.

Axis lanzará la solución AXIS A1001 en EEUU en el cuarto trimestre de 2013. Estados Unidos fue uno de los mercados pioneros en la adopción de tecnología de video en red, y constituye hoy en día un mercado de gran peso en el Control de Acceso Físico.

Contactos de empresas, p. 7.

I FORO DE DEBATE ATENEA-ADESYD

# «Mujer, paz y seguridad»

## Resolución 1325 del Consejo de Seguridad de Naciones Unidas

Analizar el papel de las mujeres en las misiones internacionales y comprobar el grado de implantación de la Resolución 1325 del Consejo de Seguridad de Naciones Unidas sobre mujeres, paz y seguridad, ha sido el principal objetivo de este I Foro de Debate, organizado por el Grupo Atenea en colaboración con la Asociación de Diplomados Españoles en Seguridad y Defensa (ADESyD). Un encuentro en el que se han abordado los principales desafíos en relación a la participación de la mujer en la prevención, mediación y resolución de conflictos.

Las mujeres, con las capacidades propias de su género, mejoran la eficacia de nuestras Fuerzas Armadas», aseguró el teniente general Juan Antonio Carrasco, jefe del Estado Mayor Conjunto, durante el acto de inauguración del I Foro de Debate Grupo Atenea & ADESyD, donde además se ha recordado que en la Resolución 1325 se instaba a los estados miembros a velar por el aumento de la representación de la mujer, en todos los niveles de adopción de decisones de las instituciones y mecanismos nacionales, regionales e internacionales, para la prevención, gestión y solución de conflictos. El encuentro –que fue moderado por Antonio Núñez García Sauco, embajador de España– contó con las intervenciones del Teniente Coronel Jesús Ignacio Gil Ruiz, jefe de la Oficina de la OTAN sobre perspectivas de género, quien hizo un recorrido por diferentes documentos en los que se abordan aspectos de «Mujer, paz y seguridad». «No se trata de una cuestión de mujeres, es de todos».

Por su parte, Cristina Gallach, responsable de Relaciones Públicas del Consejo de la Unión Europea, destacó que es preciso «integrar las perspectivas de género en las misiones de acción exterior», al tiempo que matizó que «el compromiso de la UE con la agenda de "Mujeres Paz y Seguridad" es total». En la actualidad, de las 14 misiones internacionales de la Unión Europea, sólo en nueve «se están supervisando las cuestiones de género y ninguna de ellas ha sido mandada por una mujer, explicó Gallach.

Acto seguido, Ismael Kasrou, jefe de la Secretaría Permanente de Igualdad del Ministerio de Defensa, analizó el Observatorio Militar para la Igualdad.

Para finalizar, Carlos Westendorp, secretario general del Club de Madrid, insistió en que «no existe una sociedad justa y plena, si el 50% de la población no está perfectamente integrada».

El acto contó con la presencia de Marian Caracuel, presidenta de ADESyD, y José Luis Cortina, presidente del Grupo Atenea.

Acto de inauguración del I Foro «Mujer, Paz y Seguridad».

Un momento de las intervenciones de los ponentes del encuentro.


Telefónica
Creciendo
juntos
cada día_
La seguridad es una de las fortalezas
de su negocio.
Nuestra tecnología lo hace posible.
www.telefonica.com/ingenieriadeseguridad
Ingeniería de Seguridad

SE PRESENTARON LAS ÚLTIMAS NOVEDADES DE LA COMPAÑÍA

# Mobotix celebra su National Partner Conference en España

## El encuentro contó con la presencia de más de 150 colaboradores del territorio español

Mobotix, fabricante mundial de sistemas en red de videovigilancia de cámaras megapíxeles, celebró del 22 al 24 de septiembre pasado su National Partner Conference en España. Un encuentro en el que estuvieron presentes más de 150 partners.

El evento ha sido calificado por la compañía como «todo un éxito», ya que contó con la asistencia de más de 150 partners de todo el territorio español.

Varias personas del equipo de Mobotix de Alemania se trasladaron a Madrid durante esos días para exponer a los partners las principales novedades que ha lanzado la compañía al mercado durante estos meses, así como adelantarles algunas de las que quedan por llegar.

El Dr. Magnus Ekerot, anterior CSO, que acaba de pasar a ocupar el cargo de CEO de Mobotix desde el pasado 1 de octubre, insistió en que Mobotix tiene mucho que decir ya que está en constante evolución y desarrollo de nuevos productos.

Además de las diferentes charlas, los propios partners aprovecharon la ocasión para mostrar sus casos de éxito de los que están más que satisfechos.

La jornada finalizó con una cena de gala y con la entrega de diversos galardones a algunos de los partners que más han trabajado durante este año: Premio a la mejor solución de seguridad a la empresa Informática del Este, al mejor proyecto del año a Conexiona, a la mejor estrategia de crecimiento a Amtel S. L, y al partner del año a Grupo Security. ●

**Algunos de los asistentes a la National Partner Conference en España.**

**Dr. Magnus Ekerot, CEO de Mobotix, junto a Jesús Garzón, director Sur de Europa de Mobotix (a la dcha.).**

Porque existen instalaciones cuyo funcionamiento es indispensable...

Vigilant le asegura un control eficiente, en infraestructuras críticas y estratégicas.

El novedoso lector Vigilant m2m es un sistema on-line que garantiza productividad e inmediatez en la gestión de los datos. Optimiza el tiempo y los recursos. El responsable tiene todo tipo de información en tiempo real. Los equipos se envían listos para funcionar, sin necesidad de instalar ni programar nada.

Disfrutará de la tranquilidad de tenerlo todo bajo control. El cliente percibe eficiencia, cercanía, transparecia, tecnología y mucha calidad en el servicio.

Controles de RONDAS y PRESENCIA On-Line "SIN INSTALACION"

VIGILANT®

**Si necesitas control, piensa en Vigilant.**

**www.vigilant.es - info@vigilant.es - Telf: 965 856 457**

**Mª INMACULADA LÓPEZ NÚÑEZ, LOURDES LUCEÑO MORENO, JESÚS MARTÍN GARCÍA Y EVA Mª DÍAZ RAMIRO.** LABORATORIO DE PSICOLOGÍA DEL TRABAJO Y ESTUDIOS DE SEGURIDAD DE LA UNIVERSIDAD COMPLUTENSE DE MADRID

# La promoción de la salud en el trabajo (II)

## Factores motivadores para el empresario

En un artículo anterior (Cuadernos de Seguridad, 278, Mayo 2013) pusimos de manifiesto cómo los «Programas de Promoción de la Salud en el Trabajo» son una de las prioridades de la estrategia comunitaria de salud y seguridad en el trabajo. Dicha estrategia, hace hincapié en que los efectos positivos de las políticas de prevención de riesgos en el lugar de trabajo, pueden ser reforzados mediante el fomento y el apoyo a los trabajadores, para que adopten estilos de vida que puedan mejorar su estado general de salud. Este trabajo requiere el esfuerzo conjunto de empresarios, trabajadores y de toda la sociedad en general. Por lo tanto es importante conocer los factores que motivan tanto a empresarios como a trabajadores a llevar a cabo medidas de promoción de salud en el trabajo.

EN este trabajo queremos poner de manifiesto los principales factores que motivan a los empresarios para llevar a cabo iniciativas de promoción de la salud laboral. Dichos factores se pueden clasificar en factores motivadores internos (los que están dentro de la organización) y factores motivadores externos (los que están fuera de la organización). **Cuadros 1 y 2.**

### Factores motivadores internos

**– Mejora de la productividad**

Existe evidencia de que programas de promoción de la salud en el lugar de trabajo, pueden tener un impacto real y significativo en las tasas de productividad individuales y la producción en general. En el Reino Unido, la encuesta de ausencia por enfermedad realizada en 2007 encontró que el 90% de los encuestados identificaron la pérdida de producción como el mayor coste derivado de los problemas de salud de los empleados. Los autores concluyeron que un programa de promoción bien implementado de salud laboral, puede provocar cambios importantes y significativos en los factores de riesgo

para la salud y las tasas de productividad entre los empleados, lo que puede dar un rendimiento positivo de la inversión de una organización en materia de salud laboral.

En el Reino Unido, la encuesta de ausencia por enfermedad realizada en 2007 encontró que el 90% de los encuestados identificaron la pérdida de producción como el mayor coste derivado de los problemas de salud de los empleados

**– Disminución de las bajas por enfermedad y el absentismo**

Las bajas por enfermedad y el absentismo laboral tiene claras implicaciones para las organizaciones en términos de pérdida de producción, plazos incumplidos, insatisfacción del cliente, la tensión entre los compañeros de trabajo, problemas de reclutamiento y formación de personal, etc. Para el empresario, los costos relacionados con las bajas se pueden dividir en costos directos (administrativos) y costes indirectos (pérdida de la producción, de clientes, horas extras de los demás empleados, etc.). Los costos más importantes son, en primer lugar, la pérdida de la productividad, seguido por el costo de la enfermedad por sí misma, y el del personal.

Diferentes estudios han puesto de manifiesto que las bajas por enfermedad se reducen significativamente como consecuencia de aplicación de Programas de Promoción de la Salud, así por ejemplo, en un estudio llevado a cabo en Alemania, se comprobó que los días de baja por enfermedades musculoesqueléticas se redujeron a la mitad, y la tasa de rotación de personal se redujeron en un 40% durante un período de dos años como resultado de la promoción de la salud en el trabajo.

Las bajas por enfermedad se reducen significativamente como consecuencia de aplicación de Programas de Promoción de la Salud.

**– Disminución del presentismo y del deterioro del trabajo**

La razón principal de los trabajadores a ausentarse del trabajo es sin duda la mala salud. Sin embargo, la enfermedad no significa necesariamente la ausencia del trabajo, ya que algunos empleados van a trabajar aun cuando no están en condiciones óptimas. Este fenómeno se denomina «presencia de enfermedad» o «presentismo». Según la última encuesta de trabajo europea sobre condiciones de trabajo, el porcentaje de empleados que declararon haber ido a trabajar en condiciones de salud no adecuadas se estimó entre un 50% a 70%. Las principales razones dadas tienden a relacionarse con un sentido del deber con los clientes o compañeros de trabajo, pero también se relacionan con las consecuencias económicas sobre el individuo y el temor a perder el empleo. Los principales factores relacionados con el presentismo son: la insatisfacción en el trabajo, problemas de salud y estrés. Las investigaciones muestran que este fenómeno es enormemente costoso para los emplea-

> «Algunos empleados van a trabajar aun cuando no están en condiciones óptimas; este fenómeno se denomina "presentismo" y repercute en el deterioro del trabajo y de la organización»

**Cuadro 1 y 2.**

| FACTORES MOTIVADORES INTERNOS |
|---|
| Mejora de la productividad |
| Disminución de bajas laborales y del absentismo |
| Disminución del presentismo y del deterioro del trabajo |
| Mejora de la satisfacción laboral y el compromiso organizacional |
| Prestigio organizacional y retención de empleados |
| Reducción de accidentes y riesgos laborales |
| Rentabilidad y retorno de la inversión |

| FACTORES MOTIVADORES EXTERNOS |
|---|
| Mejora de la fidelidad de los Clientes |
| Mejora de la imagen corporativa |

dores, no sólo en términos económicos sino en el deterioro del trabajo y del clima en la organización, y el lugar de trabajo las medidas de promoción de la salud puede ser una estrategia útil, no sólo para abordar y gestionar el presentismo, sino también para contribuir al desarrollo de trabajadores más motivados y comprometidos.

**– Mejora de la satisfacción laboral y el compromiso organizacional**

Un gran número de estudios científicos han demostrado un vínculo entre los niveles de satisfacción laboral en los trabajadores y su salud y bienestar. Mejorar la salud y el bienestar de los empleados a través de programas de promoción de la salud puede dar lugar a mayores niveles de satisfacción en el trabajo y el compromiso organizacional.

La aplicación de programas de promoción de la salud en el trabajo se ha asociado con mejoras en la satisfacción laboral, la autoeficacia y el estrés. **Cuadro 3**

Diferentes trabajos han demostrado que los trabajadores tienen una mejor actitud para trabajar y mayor satisfacción en el trabajo cuando participan en Programas de Promoción de la Salud en el Trabajo, incluso aquellos que participan de vez en cuando frente a los que no participan nunca.

**– Prestigio organizacional y retención de empleados**

La implementación de medidas relativas a la Promoción de la Salud en el Trabajo demuestra que el empleador se preocupa por el bienestar de sus empleados, y da lugar a una cultura de eficacia organizativa y mejora en la retención del personal. Iniciativas de salud en el trabajo son fundamentales para la creación de una cultura de la empresa y, en consonancia, con el desarrollo de una fuerza de trabajo sana y comprometida. Esto, a su vez, es probable que tenga un impacto directo en la productividad y la producción. Una encuesta sobre las actitudes y opiniones de los empleados de la fuerza de trabajo del Reino Unido indicó que más de la mitad de los trabajadores esperan que sus empleadores inviertan en la salud y el bienestar, a pesar de ello, sólo el 16% dijo que su compañía había invertido dinero en la salud y el bienestar de todo el personal.

**– Reducción de accidentes y riesgos laborales**

Las iniciativas de salud en el lugar de trabajo tienen un impacto indirecto positivo en los costos relacionados con accidentes y riesgos ocupacionales, al reducir las probabilidades de accidentes de trabajo y lesiones. Es por ello que existe una tendencia creciente a integrar las iniciativas de seguridad laboral con la promoción de la salud en el lugar de trabajo. Los empresarios están obligados a tomar medidas para prevenir los riesgos laborales, según consta en la legislación (LPRL 31/1995), y una buena medida de implementación es que sean estimuladas con iniciativas de promoción de la salud. Las iniciativas obligatorias en materia de Seguridad y Salud Laboral y las iniciativas voluntarias

**Cuadro 3.**

| Efectos de la aplicación de programas de promoción de la salud en la satisfacción laboral de los empleados |
|---|
| Aumento de la productividad |
| Reducción del absentismo laboral por enfermedad |
| Reducción de la rotación de personal |
| Aumento de la motivación de los empleados a realizar el trabajo |
| Mejora de las relaciones entre empleadores y los empleados |

de Promoción de la Salud en el Trabajo pueden ser perfectamente integradas para mejorar la reducción de accidentes y riesgos laborales.

**– Rentabilidad y retorno de la inversión**

La mayoría de las iniciativas de promoción de la salud en el trabajo muestran un retorno positivo de la inversión. En EEUU, Programas de Promoción de Salud en el trabajo han demostrado un retorno, de 3 a 6 dólares por cada dólar invertido. Curiosamente, la mayoría de los estudios sólo examinó una variable económica (por ejemplo, gastos médicos), lo que puede estar dando lugar a una subestimación del impacto económico total y el retorno de la inversión. Si se toman en cuenta los gastos de bajas, indemnización, gestión de incapacidades, absentismo etc., es probable que obtuviésemos una evaluación más realista y elevada del retorno de inversión.

## Factores Motivadores Externos

**– Mejora de la fidelidad de los clientes**

Los Programas de Promoción de la Salud en el Trabajo no sólo mejoran el bienestar del empleado sino que tienen el beneficio indirecto de mejorar el servicio y, por tanto, su fidelidad.

La fidelidad del cliente es muy importante ya que tiene el potencial de aumentar la cuota de mercado de una empresa. Las actitudes y el compromiso de los empleados de una empresa pueden influir en la lealtad del cliente. Los empleados que no están comprometidos con su trabajo pueden no estar dispuestos a cooperar con los clientes, lo que tiene un impacto negativo en la satisfacción y fidelidad.

**– Mejora de la imagen corporativa**

Las organizaciones que cuentan con Programas de Promoción de la Salud en el Trabajo son vistas como atractivas y socialmente responsables. Empresas que integran en su política directiva planes y programas para promover la salud y el bienestar de los empleados tienen mejor imagen corporativa que aquellas que no. Un beneficio adicional de una buena imagen corporativa aumenta la posibilidad de reclutamiento, fidelidad y compromiso ya que la organización es percibida como un lugar atractivo para trabajar, debido a su compromiso visible y la inversión en sus empleados y sus familias.

Los Programas de Promoción de la Salud en el Trabajo pueden jugar un papel importante en la mejora de la imagen corporativa, y, a su vez, ser una ventaja significativa en la contratación y retención de talento

En conclusión, las iniciativas e inversiones en la salud y bienestar de los trabajadores a través de los Programas de Promoción de la Salud en el Trabajo, deben ser una actividad central de la cultura organizacional ya que tienen un impacto directo en la productividad, conduce a tener trabajadores más sanos y motivados, una mejor retención de los empleados, reducir las bajas por enfermedad, mejorar el rendimiento, los niveles de satisfacción y el compromiso organizacional. ●

> «Las bajas por enfermedad se reducen significativamente como consecuencia de aplicación de programas de promoción de la salud»

*Fotos: **Archivo***

**Mejorar la salud y bienestar de los trabajadores a través de Programas de Promoción de la Salud en el Trabajo aumenta los niveles de satisfacción laboral y el compromiso organizaciones.**

EL ENCUENTRO SE CELEBRÓ EN OCTUBRE EN LA FERIA DE VENECIA

# Security Solutions Show, una apuesta por la innovación

La primera edición de Security Solutions Show, celebrado en la Feria de Venecia acogió una amplia muestra de las más innovadoras soluciones para seguridad. Los grandes operadores de esta industria tuvieron la oportunidad durante tres días de poder conocer las últimas novedades en soluciones anti-robo, anti-intrusión, videovigilancia, control de accesos, protección contra incendios, domótica, automatización de edificios, así como la tecnología IP aplicada al campo de la seguridad.

UN evento nuevo que el recinto ferial de Venecia quiso desarrollar y consolidar, junto con las principales asociaciones de la industria de seguridad, donde encontrar las respuestas a la demanda de este mercado. Y ha sido este formato vanguardista el que ha proporcionado lo último en tecnología, adaptándose al modelo que el sector demandaba. Los profesionales han tenido acceso a numerosas oportunidades de negocio, a través de convenciones y seminarios técnicos, pero también han podido intercambiar puntos de vista sobre los temas más actuales.

Security Solutions Show ha contado con la participación de 44 empresas líderes –un 25% extranjeras–, logrando aunar aspectos de información, presentación y demostraciones, pero también gracias a dos acontecimientos consolidados que se han desarrollado simultáneamente: MEB (exposición dedicada a suministros eléctricos) y Todo Digital (Foro Profesional sobre Tecnologías Digitales), creando una sinergia de visitantes de sectores cada vez más integrados.

Security Solutions Show fue aún más internacional por la participación de las delegaciones de profesionales extranjeros, minoristas e importadores de España, Alemania, Gran Bretaña, Francia, Polonia, Hungría, República Checa y Balcanes.

Muchos de los productos fueron presentados en exclusiva en la feria: desde soluciones de seguridad para la banca y el sector de la joyería, hasta un nuevo sistema de detección de incendios y nuevas tecnologías de vigilancia de vídeo.

Ahora la organización ya trabaja en la próxima edición de 2015, con el fin de ofrecer un modelo de evento mejorado que muestre las últimas novedades.

ORGANIZA / *ORGANISED BY*

IFEMA
Feria de Madrid

25-28
**FEBRERO**
February
**2014**

# sicur

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

www.sicur.ifema.es


**LINEA IFEMA / *IFEMA CALL CENTRE***

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

# Cepreven: plataforma e-learning

CEPREVEN ha apostado por el vídeo marketing para impulsar su plataforma de e-learning, una herramienta de formación online cada vez más extendida, que permite el acceso de los usuarios a sus cursos de seguridad y prevención con total flexibilidad de horarios y desde cualquier punto geográfico.

Esta modalidad de formación surge como complemento a la enseñanza presencial de Cepreven. Entre otras ventajas, la plataforma de e-learning de Cepreven ofrece la posibilidad de crear ediciones de cursos personalizadas para empresas, adaptadas a las necesidades de cada caso. Además, a través de la formación a distancia, los estudiantes pueden actualizar sus conocimientos sobre Prevención y Seguridad de forma práctica y accesible en cualquier momento.

Personalizada, económica, flexible y constantemente actualizada, así es la plataforma de e-learning. Todo ello con la garantía de contar con una formación acreditada por una entidad independiente como Cepreven.

# FES: nueva junta directiva y presidente

LA Federación Empresarial Española de Seguridad, FES, celebró el pasado 3 de octubre la Asamblea General Extraordinaria para la elección de su Junta Directiva, y posteriormente tuvo lugar la reunión de la misma para elegir de entre sus miembros a su presidente y otros representantes orgánicos, siendo elegido con todos los votos a favor, salvo una abstención, como nuevo presidente de FES, Ignacio Carrasco.

Para el Comité Ejecutivo fueron elegidos por unanimidad: Encarnación Ortiz como vicepresidenta; Mariano Agüero como tesorero; Javier Grasa, Enrique López del Estal y Federico Sánchez como vocales, y como presidente de la Comisión de Sistemas e Instalaciones, Antonio Domínguez. Los restantes miembros de la Junta Directiva, a falta de la asignación a las nuevas comisiones y grupos de trabajo son Esteban Granero, Eugenio Morales, Jorge Rodríguez, Antonio Toledano, Rafael Tinoco, Ángel Huete y Jaime Villares, y como secretario general, Luis González Hidalgo.

# Eulen participa en la constitución del Grupo Food Defense Soluciones

Eulen Seguridad, empresa decana en el sector de la seguridad perteneciente al Grupo Eulen, especialista en nuestro país en la prestación de servicios generales a empresas, ha participado en la constitución del Grupo de Trabajo Food Defense Soluciones.

La creación de este Grupo de Trabajo es una iniciativa de Eulen Seguridad, S21Sec, Masscomm, WAF y OCA Cert, que tiene por objetivo dar una solución global, así como promover, crear y difundir la cultura de Food Defense en el sector alimentario.

Food Defense (Defensa Alimentaria) no es lo mismo que Seguridad Alimentaria, sino que se trata de la protección de los alimentos contra la contaminación deliberada mediante sustancias químicas, agentes biológicos u otras sustancias nocivas.

La participación de Eulen Seguridad en el Grupo de Trabajo de Food Defense Soluciones se enmarca dentro del modelo de seguridad integral (Convergencia de la Seguridad) que lleva impulsando la compañía desde el año 2008.

# Siemens: nombramiento

JESÚS Daza es el nuevo director general de la división Building Technologies dentro del Sector Infraestructure&Cities de Siemens en España, en sustitución de Luis Dueñas, que ha dejado la compañía tras su jubi-

lación. Daza se incorporó a Siemens en 2001 y, desde entonces, ha desarrollado funciones de director de la unidad de negocio Building Automation y de la delegación de Siemens en Madrid. Ha desarrollado su carrera en el ámbito de las tecnologías para la edificación y las infraestructuras.

Su objetivo principal es que Siemens juegue un papel importante en la modernización de las ciudades e infraestructuras españolas para hacerlas más eficientes y seguras.

## Prosegur, galardonada

PROSEGUR, una de las principales compañías de seguridad privada a nivel mundial y en España, ha sido reconocida en la IV edición de los «Premios a las mejores prácticas en Recursos Humanos», en un acto organizado por la consultora de formación Cegos, en el Casino de Madrid. La Compañía ha sido galardonada en la categoría de Gestión Organizacional y Consultoría, por el proyecto «Premios Excelencia», una iniciativa anual, que tiene como principal objetivo poner en valor la función social que los profesionales del sector de la seguridad privada desempeñan en su labor diaria. En concreto, el jurado ha destacado la apuesta de Prosegur por potenciar conductas y valores positivos entre sus empleados.

Los «Premios Excelencia» valoran la profesionalidad de sus trabajadores y su compromiso con la protección y el bienestar de las personas. La Compañía, que considera que la figura del vigilante de seguridad merece un reconocimiento acorde con el servicio que realiza, premió, en la pasada edición, a más de 40 empleados que desarrollan su labor en ciudades españolas como A Coruña, Barcelona, Bilbao, Madrid, Mallorca, Mérida, Sevilla, Tenerife, Valencia y Valladolid. Durante el evento, la directora de Formación, Selección y Desarrollo de Prosegur en España, María Antonia Gómez, explicó en primera persona el proyecto y resaltó que, «esta iniciativa pone de manifiesto nuestro compromiso con la dignificación de la profesión. Al mismo tiempo, creemos que el reconocimiento y el ejemplo, nos ayudan a ofrecer modelos de comportamiento a nuestros trabajadores y convertimos su actuación en un referente para el resto de compañeros.»

## Tecnifuego-Aespi firma un convenio de colaboración con AJSE

Tecnifuego-Aespi ha firmado un Convenio con la Asociación de Jefes de Seguridad (AJSE) para promover el desarrollo de actividades conjuntas relacionadas con la formación continua y sensibilización en materia de seguridad contra incendios.

Algunos de las acciones propuestas para incrementar la colaboración son:

- Promover Congresos o Jornadas Técnicas sobre seguridad contra incendios.
- Intercambiar información de interés sectorial, mediante revistas, boletines o diferentes comunicados para difundir entre los asociados de las dos entidades.
- Unificar esfuerzos para la mejora del sector de la seguridad contra incendios, a través de acciones formativas, etc.

Durante la firma del convenio, Vicente Mans, presidente de Tecnifuego-Aespi, y Antonio Cedenilla, presidente de AJSE, destacaron la necesidad de aumentar las relaciones entre usuarios y fabricantes e instaladores de seguridad contra incendios para promover la formación e información de nuevas tecnologías y normativa aplicable.


## Milestone Systems y Bosch intensifican su colaboración

DURANTE los días 9 y 10 de octubre Bosch Security Systems ha participado en el evento para partners de Milestone, Partner Open Platform Days 2013, con un stand donde mostró sus soluciones de videovigilancia más recientes

controladas con el software de gestión de vídeo de Milestone. Los asistentes pudieron comprobar in situ el fantástico funcionamiento de las cámaras Starlight de Bosch en condiciones de poca luz.

Milestone Systems y Bosch Security Systems han establecido una alianza estratégica global con el objetivo de una integración completa de los dispositivos de vídeo IP de Bosch con el software de gestión de vídeo IP XProtect de Milestone. Como parte de la cooperación, Milestone forma parte como socio premium del programa Integration Partner Program (IPP) de Bosch. El IPP está diseñado para asegurar la interoperabilidad de los productos de vídeo de Bosch con las principales soluciones de software.

## enerTIC: nombramiento

DESDE su fundación en el año 2011, enerTIC se ha ido consolidando como la Plataforma de referencia en el ámbito de las TICs y la Eficiencia Energética, agrupando en torno suyo a las principales empresas del sector.

Una vez finalizados los objetivos del Plan Estratégico 2011-13, se hace necesario seguir creciendo hacia nuevos retos. Por este motivo, José Antonio González Hernández se incorpora al equipo de Francisco Verderas como director de Desarrollos Estratégicos, para aportar su experiencia en el diseño y desarrollo del nuevo Plan Estratégico 2014-16.

José Antonio González Hernández es Ingeniero Industrial del ICAI, especialidad en Electrónica, por la Universidad Pontificia Comillas, y ha realizado un Programa de Desarrollo Directivo en el IESE Business School, por la Universidad de Navarra. Profesional con 16 años de experiencia, se inició en empresas de ingeniería y telecomunicaciones, donde llegó a ocupar los cargos de director técnico y director comercial para la zona centro, antes de ejercer los

## Tyco Integrated Fire & Security inaugura su Retail Experience Centre

Tyco Integrated Fire & Security, ha presentado su primer Retail Experience Centre en Europa, que proporcionará a los minoristas una visión de los beneficios empresariales que aportan al negocio la amplia variedad de soluciones, que permiten al minorista total visibilidad en tiempo real de su inventario (tanto en tienda como en almacén) y la perspectiva necesaria para asegurar la disponibilidad de sus productos, satisfacer la demanda del comprador de manera rápida y efectiva, y optimizar su rentabilidad. El Retail Experience Centre se encuentra en la Fashion House de Düsseldorf, uno de los destinos destacados en Europa para fabricantes y distribuidores textiles de todo el mundo.

El Retail Experience Centre ofrece un recurso accesible a los minoristas de toda la región de EMEA para que experimenten con la innovadora plataforma de rendimiento en tienda de Tyco, que proporciona un amplio abanico de soluciones inteligentes basadas en el software True Vue. Estas soluciones permiten al minorista el suministro multicanal (tienda física, online, etc.) ofreciendo de un solo vistazo la totalidad de existencias, productos y promociones disponibles en tienda y que permiten ofrecer a los clientes una experiencia de compra de 360º en un mercado tan competitivo como el actual.

La instalación comprende más de 130 metros cuadrados y ha sido construida recreando una tienda de ropa real, evocando un entorno donde los minoristas pueden experimentar de primera mano cómo son puestas en marcha una serie de tecnologías para ofrecer una solución completa e integrada. Tyco ha desarrollado diversos escenarios que sirven para demostrar cómo las soluciones inteligentes de medición de datos (inventory intelligence, traffic intelligence y EAS intelligence) pueden combinarse a la perfección para dotar a los minoristas, con un uso fácil y eficaz, de un importante apoyo para las operaciones del día a día.

«En todas nuestras conversaciones con minoristas nos ha quedado claro que buscan soluciones innovadoras que les ayuden a mejorar el rendimiento en tienda y ofrecer una experiencia al cliente que resulte interesante» dice Ricardo Arroyo, presidente de Tyco Integrated Fire and Security en España y Portugal.

últimos 10 años como secretario general de FENIE, la Federación Nacional de Empresarios de Instalaciones Eléctricas y de Telecomunicaciones de España, con más de 15.000 empresas asociadas.

## Checkpoint, en las tiendas Familiy Dollar

CHECKPOINT Systems, especialista mundial en soluciones de disponibilidad de mercancía para el sector minorista, ha llegado a un acuerdo de varios años con la cadena de tiendas Family Dollar. La cadena minorista implementará la solución de vigilancia electrónica de artículos (EAS) EVOLVE P10 ECO de Checkpoint en todas las tiendas actuales, así como en las que se pongan en marcha en el futuro. La instalación en los 7.900 establecimientos que Family Dollar tiene en funcionamiento se espera que esté finalizada en diciembre de 2014. Durante los últimos tres años, Checkpoint y Family Dollar han realizado pruebas en distintas tiendas del país. Basándose en los resultados obtenidos, la cadena decidió instalar la solución EVOLVE P10 ECO, diseñada para reducir las pérdidas, así como los costes de energía.

Per Levin, presidente y director comercial de Checkpoint Systems, afirma: «Estamos encantados de formar parte de la exitosa trayectoria de Family Dollar. Se trata de un programa probado, con un ROI significativo, así que nuestra atención se centra en llevar a cabo una aplicación rápida y eficiente. Además, este programa significa una plataforma estratégica de futuro».

«Somos uno de los minoristas que más rápido ha crecido en el país y en ese sentido continuamente buscamos ampliar la oferta para nuestros clientes», comenta Chris Nielsen, vicepresidente-Prevención de Pérdidas de Family Dollar.

## Nace la Cátedra UDIMA-ANTPJI de Informática Forense

El Rector de la Universidad a distancia de Madrid UDIMA, José Andrés Sánchez Pedroche, y el presidente de la Asociación Nacional de Tasadores y Peritos Judiciales Informáticos, ANTPJI, Ángel Bahamontes Gómez, han firmado en la sede del rectorado, el acuerdo de colaboración que permitirá la creación de la Cátedra UDIMA-ANTPJI de Informática Forense, la primera que nace de la interrelación de esta entidad profesional de investigación de la Informática Forense de referencia nacional e internacional con una institución académico-científica. A través de ella se fomentarán la cooperación en materia de investigación, desarrollo e innovación (I+D+I)y transferencia, con el fin de potenciar la capacitación científico y tecnológica de estudiantes, trabajadores, investigadores y peritos informáticos.

La cátedra, UDIMA-ANTPJI, tiene como objetivos principales incrementar la actividad conjunta, tanto en el ámbito de la investigación y áreas de especialización tecnológica de la informática forense, como en la formación de alumnos, acogida de becarios y captación de profesionales, fomentando la docencia, el emprendimiento, la innovación tecnológica y la investigación en torno a la informática Forense, divulgando, facilitando y transfiriendo el intercambio de conocimientos y experiencias entre los profesionales, investigadores y los científicos de ambas entidades; participando conjuntamente en futuras convocatorias públicas nacionales y europeas.

Asimismo, en virtud del acuerdo, se pretende apoyar la organización de actividades docentes de cursos de formación continua, post grados de especialista y experto, Master y de Jornadas, Seminarios y Congresos, la difusión de las investigaciones mediante publicaciones y otras acciones de comunicación, y la realización de prácticas en la entidad profesional y las empresas asociadas por parte de los alumnos que faciliten su inserción profesional.

Esta nueva alianza de colaboración incluirá, entre otros aspectos, el desarrollo de programas formativos (Master, Cursos de Post Grado y Formación Continua); fomento de trabajos científicos y becas para el desarrollo de proyectos TIC; promoción para la realización de libros, manuales, guías, estudios y trabajos de investigación en el ámbito de la Informática Forense; realización de jornadas, seminarios y congresos de carácter científico-técnico, etc.

**Un momento de la presentación de la Cátedra y del acuerdo ANTPJI y Unisys, durante el V Curso Básico de Perito Informático.**

# Documento sobre Infraestructuras Críticas

EULEN Seguridad, empresa decana en el sector de la seguridad perteneciente al Grupo EULEN, especialista en nuestro país en la prestación de servicios generales a empresas, ha colaborado activamente en la elaboración del documento «La protección de Infraestructuras Críticas y la Ciberseguridad Industrial», que ya está disponible para su descarga tanto en la versión pública como en la de pago.

Este documento ha sido desarrollado por el Centro de Ciberseguridad Industrial (CCI) y pretende ser un análisis de la realidad actual de ambos conceptos para aclarar su significado y establecer las diferencias y puntos comunes entre ellos. Asimismo, ha sido desarrollado desde el conocimiento, la experiencia, el consenso y la máxima representatividad de los principales actores, públicos y privados, de la industria del país.

En la publicación -la primera de este tipo que existe en nuestro idioma- se recogen las principales iniciativas, problemas encontrados, responsables y metodologías de análisis de vulnerabilidades de los dos ámbitos. Se puede descargar el documento «La protección de las Infraestructuras Críticas y la Ciberseguridad Industrial» en el siguiente enlace: www.cci-es.org/DOC_PIC_CI.

# Casmar abre una nueva compañía en Portugal

Después de más de 35 años presentes en el mercado español y de 8 años en Portugal, primero a través de la presencia directa de un departamento Comercial y después con la apertura de la delegación de V. N. de Gaia, Casmar Electrónica S.A. inaugura una nueva etapa de plena integración en el mercado portugués de seguridad electrónica, a través de la creación de una nueva empresa de régimen jurídico portugués: Casmar Electrónica - Unipessoal, Ltd.

Esta decisión se basó en la confianza en el mercado luso y en sus clientes, así como en la fuerte conexión comercial de Portugal con los países africanos de lengua portuguesa, los cuales están experimentando un gran crecimiento económico, ante los que Casmar no podía permanecer indiferente. Casmar pretende con ello dar respuesta a una serie de nuevas oportunidades de negocio, con el objetivo de generar riqueza interna y contribuir al crecimiento de la economía nacional.

Esta nueva etapa en la vida empresarial de Casmar Electrónica es mucho más que un nuevo estamento jurídico; implica una nueva estrategia comercial, beneficiando a sus clientes con un mejor servicio, agilizando el proceso de envío de pedidos y con la disponibilidad de material en su almacén de V. N. Gaia.

# La App de CUADERNOS DE SEGURIDAD, un nuevo canal de información

Leer CUADERNOS DE SEGURIDAD nunca fue tan fácil. La App CUADERNOS DE SEGURIDAD, para Apple y Android, permite a los profesionales del sector de la Seguridad tener acceso a todas las novedades del sector, en cualquier momento y lugar. Ahora, la información en un sorporte más actual y dinámico acorde a las necesidades actuales de los profesionales de un sector que demanda continuamente contenidos especializados.


CUADERNOS DE SEGURIDAD siempre estará disponible para su consulta, con un acceso cómodo y fiable desde las dos plataformas más extendidas, Apple y Android. Busca la aplicación CUADERNOS DE SEGURIDAD en la AppStore o en la Play Store y podrás acceder fácilmente a toda la información de nuestra publicación cuando quieras, desde donde quieras y de forma rápida y sencilla.

Un nuevo canal para que CUADERNOS DE SEGURIDAD esté al alcance de todo el sector de la seguridad.

## Thales y Schneider Electric: acuerdo comercial

LA empresa de tecnologías aplicadas a la Defensa, Aeronáutica, Seguridad, Transporte y Espacio, Thales, ha firmado un acuerdo de cooperación comercial con Schneider Electric, para el desarrollo de soluciones y servicios de ciberseguridad para los sistemas de mando y control ante posibles ciberataques. Con este acuerdo Thales y Schneider Electric pondrán a disposición tanto de operadores industriales como de organismos de defensa, de las últimas tecnologías de seguridad y defensa contra las actuales amenazas a las que se enfrentan en materia de ciberseguridad.

Thales, como actor clave europeo de la seguridad de los sistemas de información y comunicación, pondrá a disposición de los diferentes operadores su experiencia y conocimiento en auditoría, consultoría, desarrollo e integración de soluciones y servicios de ciberseguridad. Por su parte, Schneider Electric, aportará su conocimiento en el diseño, así como su organización de servicios cercana a todos los clientes nacionales.

En el catálogo de soluciones que ofrecerán ambas compañías, se encuentran la gestión de riesgos, el análisis de vulnerabilidades, la definición de arquitecturas de seguridad, la implementación de medidas de seguridad y vigilancia, así como el mantenimiento de la seguridad y la gestión de respuesta a incidentes, entre otras.

Todas las soluciones ofrecidas cumplen con la normativa nacional e internacional en el área de la seguridad de sistemas digitales de mando y control y se adaptan a los sistemas de automatismos y mando y control de clientes tanto de Thales como de Schneider Electric.

## Grupo Álava Ingenieros: jornada sobre «La opción inteligente para los profesionales»

El Grupo Álava Ingenieros, en colaboración con sus socios tecnológicos Samsung y Genetec, organizó una jornada técnica bajo el epígrafe «La opción inteligente para los profesionales» con el objetivo de exponer los últimos avances tecnológicos a nivel mundial dirigidos al campo de la seguridad. Al evento, que tuvo lugar en el Hotel Holiday Inn, acudieron cerca de un centenar de asistentes, entre los que figuraban profesionales de empresas del sector, así como responsables de seguridad tanto del ámbito público como el privado.

Tras una presentación inicial de las tres compañías organizadoras de la jornada, tanto Samsung, proveedor de soluciones globales de seguridad, como Genetec, especialista en tecnología IP para videovigilancia, control de accesos y reconocimiento de matrículas, detallaron las características y aplicaciones de las soluciones que han desarrollado para mejorar la seguridad de clientes. Entre ellos se encuentran compañías públicas y privadas nacionales e internacionales de primer nivel.

La jornada fue de gran interés para los asistentes, en especial para los instaladores que cuentan con proyectos tanto dentro como fuera de España y que necesitan estar al corriente de los últimos avances tecnológicos en el ámbito de la seguridad.

## Radwin, en el puerto de Richmond

RADWIN, el proveedor global de soluciones inalámbricas de banda ancha sub-6 GHz, anuncia que el Puerto de Richmond, ubicado en Virginia (Estados Unidos), ha instalado su red de vigilancia inalámbrica que redundará en una mejora en la seguridad de sus 49 hectáreas de instalaciones portuarias. Radwin se ha asociado con la empresa integradora de sistemas CelPlan para diseñar e implementar la red de vigilancia inalámbrica. Los sistemas inalámbricos Radwin 5000 y Radwin 2000 suministran la más alta capacidad para largas distancias. Al brindar el nivel de servicio requerido para la transmisión de vídeo de alta definición, los sistemas soportan las necesidades de conectividad de estas extensas instalaciones portuarias. Las radios incorporan tecnología avanzada que permite un rendimiento superior bajo condiciones climatológicas adversas en el puerto y sin línea de vista (NLOS)».

# D-Link: mydlink, con un millón de usuarios

La plataforma mydlink™ cloud, que permite el acceso a las cámaras IP, routers y equipos de almacenamiento NAS de D-Link a través del portal mydlink o desde dispositivos móviles con sistema iOS y Android con aplicaciones gratuitas, también está ahora disponible para móviles con sistema Windows Phone. Además, mydlink™ está de celebración, ya que ha alcanzado el millón de usuarios a nivel global.

Los primeros pasos en mydlink no pueden resultar más sencillos. Todas las Cámaras IP, Routers y NAS disponen de un asistente que realiza la configuración de forma transparente al usuario. Una vez que el dispositivo está reconocido por la red (ya esté conectado por cable o por Wi-Fi al router) es el momento de crear una cuenta mydlink en el mismo proceso de instalación (definiendo un nombre de usuario y contraseña de acceso) o añadir el dispositivo a una cuenta ya existente. Es posible añadir hasta 99 dispositivos. A partir de ese momento ya es posible acceder al dispositivo por Internet, bien por Wi-Fi o por 3G/4G.


La plataforma mydlink se reforzó recientemente también con nuevas funcionalidades en las apps, como zoom táctil que sustituyó a los iconos para acercar o alejar la imagen y ahora se realiza con el gesto habitual de ampliar una foto o texto, lo que facilita notablemente su control.

# Interpol España, cooperación policial y judicial

La Oficina Central Nacional de INTERPOL, integrada en la División de Cooperación Internacional de la Policía Nacional, ha colaborado en lo que va de año en la investigación de 226 homicidios, 90 agresiones sexuales, 539 desapariciones, 43 casos vinculados a la explotación sexual o 115 operaciones contra la inmigración ilegal.

La Policía Nacional es la responsable de gestionar el trabajo de INTERPOL en España, uno de los 190 países que forman parte de esta organización cuyos orígenes se remontan a 1914. Entre sus cometidos destaca la cooperación policial y judicial, tanto a nivel nacional como internacional, en investigaciones relacionadas con la seguridad pública, la lucha contra el terrorismo, el crimen organizado, tráfico de drogas, armas o personas, el blanqueo de dinero, la pornografía infantil, delitos económicos o la corrupción.

Los representantes y altos mandos policiales de los distintos países que integran esta organización se han reunido en la 82ª Asamblea General de INTERPOL desarrollada en Cartagena de Indias (Colombia). Los asistentes han analizado la lucha policial contra el tráfico de estupefacientes, el crimen organizado, el terrorismo, el tráfico de seres humanos y el cibercrimen.

El director general de la Policía española, Ignacio Cosidó, fue uno de los ponentes en esta Asamblea y destacó el proyecto Policía 3.0 y su utilidad para detectar de manera proactiva conductas delictivas y anticiparse al crimen. «Necesitamos ofrecer una respuesta global y construir entre todos un INTERPOL 3.0», ha afirmado el director.

En lo que va de año, INTERPOL España ha colaborado además en la investigación de 117 operaciones de blanqueo de capitales, 460 estafas, más de 1.100 fraudes relacionados con medios de pago o 56 casos de robos de obras de arte.

La OCN INTERPOL España está formada por 43 agentes de las distintas escalas que, en su trabajo diario para combatir la delincuencia internacional, trabajan a través de una serie de notificaciones o avisos internacionales que sirven para informar en tiempo real a todos los países miembros, –mediante el Sistema I-Link-, de las personas buscadas, presuntos terroristas, delincuentes peligrosos o riesgos potenciales diferenciados por claves de colores. Notificaciones que son recibidas en el CENCI, Centro de Comunicaciones Internacionales, las 24 horas del día los 7 días de la semana. La Policía Nacional es la responsable de gestionar, coordinar, responder y canalizar los requerimientos procedentes de la red de oficinas de INTERPOL en los 190 países, o desde la Oficina Central en Lyon, y transmitir la información o petición correspondiente al resto de Fuerzas y Cuerpos de Seguridad españoles para ofrecer una respuesta coordinada y eficaz.

Contactos de empresas, p. 7.

# Vivotek lanza el grabador de vídeo en red NR8401 con 16 canales y montaje tipo rack

Vivotek ha lanzado el grabador de vídeo en Red (NVR) NR8401 con Linux integrado, 16 canales y montaje tipo rack, el cual opera independientemente de un PC, proporcionando a los usuarios finales un sistema de grabación estable y eficiente, con una amplia variedad de opciones de gestión de red y configuración del sistema. Toda la gama de cámaras de red de Vivotek, incluyendo los últimos modelos de ojo de pez de alta resolución, funcionan a la perfección con el NR8401.

A diferencia del tradicional DVR, un NVR se puede conectar directamente con otros dispositivos de red a través de Internet. El NR8401 de Vivotek, una versión mejorada de productos NVR anteriores, no sólo se puede conectar directamente con el software de gestión central como el VAST de Vivotek, sino que también es compatible con la aplicación iViewer, lo que permite acceso remoto al NR8401 en dispositivos portátiles. El monitoreo en tiempo real y la gestión de grabación y de datos se pueden realizar simultáneamente a través de la simple y práctica interfaz del navegador web y, particularmente, el NR8401 cuenta con una consola web dewarp, compatible con modos dewarping 1O, 1P & 1R para cámaras de ojo de pez.

# Nice: solución de videovigilancia NiceVision Net 2.7

NICE Systems, especialista mundial en sistemas de seguridad y con presencia en España, ha anunciado la salida de la nueva versión de su solución de videovigilancia NiceVision Net 2.7. Entre otras, las nuevas funcionalidades de Net 2.7 son: el soporte de cámaras con grabación de vídeo integrada en caso de fallo en la red; mejoras del cliente Web (exportación de vídeo, reproducción sincronizada, visualización 3x3...); integración de más aplicaciones terceras de vídeo analítica; mejoras en aplicación de conteo de personas; soporte de RAID-6.

Net 2.7 viene en línea con la política de NICE de sacar una nueva versión de mejora aproximadamente cada seis meses.

La versión previa, NiceVision Net 2.5 UP2, proponía la nueva grabadora SVR 9050 de 4 canales con 400GB o el servidor de media gama SVR 9425 con 128 canales y 256 Mbps con almacenamiento interno de 33TB, además de otras nuevas funcionalidades de la aplicación de gestión de vídeos.

# Euroma: grabador digital de vídeo para móviles con calidad D1

Euroma Telecom, como representante de la firma Camtronics, ha lanzado al mercado el grabador digital de vídeo para móviles. El nuevo grabador digital de vídeo para móviles de la firma Camtronics, modelo DVR X5 MOVIL, ofrece la grabación de cámaras de vídeo en móviles.

EL DVR X5 MOVIL es un grabador de vídeo especialmente preparado para la grabación en móviles; desde su diseño ha sido concebido para soportar niveles de golpes y vibraciones típicos de este entorno hostil.

Tiene 4 entradas de vídeo que pueden ser grabadas a tiempo real en calidad D1, (720 x 576), además de poder definir hasta 8 niveles de calidad, esto proporciona una gran resolución de imagen poco habitual en unidades de grabación móviles analógicas. Puede también grabar 4 canales de audio simultáneamente.

Para la grabación dispone de un disco duro especial de 2,5" de 500 Gb. Ademas incorpora una tarjeta SD que hace funciones de «caja-negra», de tal manera que graba secuencialmente el último espacio de tiempo (máximo 60m); en caso de accidente o pérdida del disco duro, la última información no se perdera.

# UTC Fire & Security: centrales analógicas 2X de Aritech

Las centrales analógicas 2X de Aritech de UTC Fire & Security disponen de la funcionalidad de transmitir alarmas y averías basadas en la normativa de obligado cumplimiento EN54-21. Esta normativa está vigente desde el año 2007 y detalla las características que deben tener la transmisión y recepción de las alarmas.

Existen 3 vías de comunicación para realizar la transmisión: Teléfono, GSM o IP. Para las dos primeras es necesario colocar un transmisor en la central, para la transmisión IP viene por defecto en la central.

El protocolo de comunicación utilizado es el Contact ID (CID), el más introducido en las centrales receptoras de alarma (CRA). En la actualidad la mayoría de las instalaciones de detección de incendios transmiten únicamente una señal de fuego, con un contacto, a través de la central de intrusión, esto según normativa no es correcto, ya que la comunicación no está supervisada por la central de incendios. Con la transmisión CID ganamos un aspecto importante y crucial que es que la CRA dispondrá de información importante para comunicar a los bomberos, como es la zona o zonas que están en alarma, evolución del incendio, etc.

# Samsung: minidomo de red Full HD WiseNetIII

Samsung Techwin ha presentado sus nuevos minidomos de red Full HD WiseNetIII de 2 megapíxeles, antivandálicos y extremadamente resistentes a la intemperie.

El nuevo minidomo de red antivandálico Full HD WiseNetIII de 2 megapíxeles SNV-6084 de Samsung se ha diseñado para funcionar eficazmente en condiciones meteorológicas extremas y resistir ataques físicos.

El modelo SNV-6084, que es resistente a las inclemencias meteorológicas con carcasa IP66 y antivandálico IK10, puede soportar altas variaciones de la temperatura, desde -50°C a +55°C, con lo que es una solución de videovigilancia ideal, incluso en las condiciones ambientales más adversas. El bajo precio del modelo SNV-6084 hace que sea ideal para aeropuertos, puertos, aparcamientos, centros de negocios y espacios públicos abiertos que tengan necesidad de grabar, desde un gran número de cámaras, imágenes que sirvan de prueba.

# Gunnebo, el mobiliario de control de accesos de Casmar


Casmar Electrónica incorpora a su amplia oferta de soluciones de control de accesos, dos nuevas gamas de mobiliario de control de accesos del prestigioso fabricante Gunnebo. Gracias a este acuerdo, en el catálogo de Casmar se incluye la gama más completa de mobiliario de control de accesos para todo tipo de entornos y aplicaciones, tales como: edificios de oficinas, centros gubernamentales, recintos industriales, museos, gimnasios, etc.

La gama Alltech está dirigida a un mercado económico que no requiere muchas opciones de acabados o personalización, y está formada por torniquetes de tipo trípode con y sin caída de brazo, portillos motorizados y molinetes de diferentes alturas.

La gama Casmar by Gunnebo está dirigida a un mercado que demanda un mayor nivel de opciones en acabados, personalización y accesorios, así como en prestaciones. Esta gama se compone entre otras muchas opciones, de torniquetes simples y dobles con y sin caída de brazo, portillos motorizados bidireccionales circulares o de paso normal, tambores rotativos, así como pasillos motorizados, que combinan un gran flujo de paso con un sistema avanzado de detección y alarma ante intentos de paso no autorizado.

# Bosch Security Systems: familia de cámaras Autodome 7000 con tecnología inteligente de seguimiento

Bosch Security Systems ha presentado su familia de cámaras AUTODOME 7000 pan-tilt-zoom (PTZ) con funciones inteligentes que son un activo importante para la vigilancia de la seguridad. AUTODOME 7000 ofrece a los clientes un potente sistema de monitoreo automatizado que asegura el control de los riesgos de seguridad.

**– Inteligencia integrada:** El software integrado de Análisis Inteligente de Vídeo (IVA) de Bosch procesa automáticamente las señales de vídeo y alerta a los operadores acerca de los riesgos de seguridad.

**– Alto rendimiento:** AUTODOME 7000 lleva la proyección de imagen a un nivel más alto con la mejora de la nitidez, con la reproducción del color más exacto y con las imágenes de poca luminosidad más detallada.

**– Diseñadas para su fácil uso:** Las AUTODOME 7000 se usan y se instalan fácilmente. Vienen con cinco ajustes previamente configurados para capturar una calidad de imagen óptima en las aplicaciones más comunes y 256 posiciones preestablecidas para la visualización de las áreas de control críticas con sólo tocar un botón

**– Soporte e integración del sistema de gestión de vídeo:** Las cámaras Bosch IP estándar y de alta definición, los codificadores y los sistemas de análisis funcionan perfectamente con una amplia gama de software de seguridad y soluciones de grabación de Bosch y de otros proveedores de sistemas de gestión de vídeo.

**– Un funcionamiento seguro en una completa gama:** La familia de cámaras AUTODOME 7000 incluye cámaras domo de interior y exterior con un rango de resistencia a temperaturas de funcionamiento que va de -40 a 55 grados Celsius.

# Tyco IF & S: los sistemas de seguridad evolucionan hacia el cuidado de las personas mayores

Según datos estadísticos, en España hay más de 8,2 millones de personas de 65 años o más. Andalucía, Cataluña y Madrid son las comunidades autónomas con mayor cifra de ancianos. En la mayoría de los casos viven en pareja o junto a sus hijos, destaca un 20% que vive en soledad. Atendiendo a las actuales necesidades específicas de las personas mayores, los sistemas de seguridad y alarma en hogares de Tyco Integrated Fire & Security  han evolucionado más allá de la simple protección ontra intrusiónes hacia otros usos avanzados y útiles.

Existen en el mercado nuevos accesorios que complementan los sistemas de seguridad de Tyco/ADT instalados en el hogar, fácilmente instalables y manejables, que permiten detectar y prevenir situaciones de riesgo dentro del hogar idóneas para la seguridad de las personas mayores.

- Alerta médica para emergencias sanitarias: Al pulsar el usuario este botón, el personal autorizado responde de forma inmediata contactando con los servicios médicos.
- Alerta por coacción y botón de pánico: Presionando el botón de coacción o introduciendo un código de alarma diferente al habitual se envía una alarma silenciosa que alerta a la Central Receptora de que el usuario está siendo coaccionado.
- Detector de escapes de gas natural: Este dispositivo da aviso temprano de fugas de gas natural (metano CH4).
- Detector de escapes de monóxido de carbono: Activa un aviso sonoro y luminoso cuando se detectan niveles de monóxido de carbono, un gas inodoro altamente tóxico, que puede provocar daños a los órganos vitales e incluso la muerte.
- Detector de inundaciones: Este detector inalámbrico sirve para detectar la presencia de agua a nivel del suelo en sótanos, aseos y cualquier otra zona de la casa.
- Detector de cambios de temperatura demasiado bruscos: Este accesorio controla la temperatura ambiente en el hogar y envía alarmas al panel de control al detectar temperaturas extremas de calor o frío. El frío y el calor intensos pueden ser peligrosos para las personas con problemas de salud, especialmente para las personas mayores. Además, el frío extremo puede provocar que se congelen las tuberías, provocando importantes daños.

# Lilin anuncia la integración total de la serie NVR Touch con Control4

En enero, Lilin anunció la integración de sus productos IP con los sistemas de Control4. Ahora, Lilin ha anunciado que los usuarios de los sistemas de Control4 cuentan con la integración del NVR Touch mediante el uso de Control4® remote.

El lanzamiento del driver gratuito Extra Vegetables significa que ahora los usuarios del NVR Touch contarán con el control total del NVR, desde la misma plataforma desde la que controlan el resto de dispositivos de su casa o su negocio, todo mediante su Control4 remote. El SDDP de Control4 identifica y carga automáticamente el controlador correcto para el NVR Touch, realizando la instalación de manera instantánea. El NVR innovador Touch permite a los usuarios beneficiarse de una solución de grabación de vídeo en red independiente, es decir, los usuarios de Control4 pueden ver 16 canales Full HD (1080p) de vídeo IP de forma simultánea a 25 fps a través de HDMI. Los usuarios pueden disfrutar de las fantásticas imágenes en tiempo real de las cámaras Lilin de las pantallas de todo el hogar, incluyendo varios controles matrix de movimiento. Con el uso del interfaz de usuario de Lilin, los usuarios también pueden gestionar las numerosas características del NVR, incluyendo el control de imágenes en directo y el acceso a todos los menús del NVR y reproducción. Las cámaras conectadas al NVR tienen PTZ (Pan Tilt Zoom), los usuarios pueden controlar estos datos. Con sólo seleccionar la pantalla completa de la cámara y, a continuación, utilizar el interfaz de usuario, las imágenes se pueden ajustar mediante las teclas de navegación.

# Stanley Security Europa: hosting eVideo Cloud

Stanley Security Europa ha lanzado la solución de eVideo Cloud Hosting en 14 países de toda Europa. Después de la adquisición de Niscayah, Stanley Security ha experimentado un crecimiento significativo en todos los países de Europa Occidental, donde es considerada la primera elección para llevar a los clientes europeos al eVideo Cloud.

Esta solución proporciona un rendimiento seguro y fiel para el vídeo de alta calidad en la nube, sin las molestias y los costes de los equipos de grabación local en la instalación y mantenimiento. Stanley eVideo puede ser utilizado como apoyo en las operaciones de vigilancia y seguridad en los diferentes negocios.

Esta solución ofrece una forma sencilla y rentable de grabar y monitorizar el vídeo desde cualquier lugar con acceso a internet, desde un ordenador, una tableta o un smartphone. Stanley eVideo Cloud Hosting está basado en la tecnología de vídeo de red pionera a nivel mundial de Axis Communications, que utiliza el software Axis Video Hosting System (AVHS) como servidor de las cámaras de vigilancia IP.

# Hikvision: cámaras de red para el mercado PYME

Hikvision ha optado por ampliar su cartera de cámara de red del IR con la introducción de DS-2CD2032 -I 3MP Mini bala cámara con IR y el DS-2CD2132 -I 3MP Mini domo cámara, ambos de los cuales están especialmente diseñados para aplicaciones que requieren iluminación adicional en la noche (tiendas, edificios de oficinas, comunidades residenciales, etc.). Las dos cámaras contienen una variedad de excelentes características, incluyendo imágenes de alta resolución de vídeo, el rendimiento estupendo con poca luz, DWDR, y 3D DNR. Todos aseguran que una calidad de imagen es capturada y registrada, independientemente de la iluminación o las condiciones ambientales.

El DS- 2CD2032 -I y DS-2CD2132 -I incorporan un filtro de corte IR conmutable para la operatividad de día / noche. Equipado con mejores LEDs de IR, las dos cámaras son capaces de ofrecer imágenes de vídeo con una visibilidad a largo plazo de hasta a 30 metros en entornos completamente oscuros.

# Tyco Integrated Fire & Security: nuevos accesorios para detectar escapes de gas, monóxido de carbono...

Tyco Integrated Fire & Security, empresa especializada en soluciones de seguridad y protección contra incendios, ha lanzado una nueva gama de accesorios para sus sistemas de seguridad para el hogar, capaces de detectar escapes de gas, monóxido de carbono, inundaciones o cambios de temperatura. Los nuevos sistemas de alarma de Tyco incorporan además un nuevo teclado con pantalla táctil, más cómodo e intuitivo.

Los nuevos accesorios se conectan mediante tecnología vía radio bidireccional al sistema de alarma de Tyco/ADT instalado en el hogar. Los dispositivos pueden configurarse y gestionarse desde el panel de control del sistema de alarma y lo activan cuando detectan situaciones de peligro específicas:

· Detector de Gas Natural: Este dispositivo proporciona un aviso temprano de fugas de gas natural (metano CH4), el gas utilizado habitualmente para cocina y calefacción, mediante una alarma sonora y luminosa.

·Detector de monóxido de carbono: Activa un aviso sonoro y lumisono cuando se detectan niveles de monóxido de carbono, un gas inodoro altamente tóxico que puede provocar daños a los órganos vitales e incluso la muerte.

· Detector de inundaciones: Este detector inalámbrico está diseñado para detectar la presencia de agua a nivel del suelo en sótanos, aseos y cualquier otra zona de la casa o comercio. El dispositivo se conecta con el sistema de alarma del hogar y alerta en caso de producirse una inundación.

· Detector de temperatura: Este accesorio controla la temperatura ambiente en el hogar y envía alarmas al panel de control al detectar temperaturas extremas de calor o frío.

# Sony: cámaras HD inalámbricas


Sony ha anunciado que la pequeña, elegante y asequible cámara inalámbrica SNC-CX600W, diseñada para pequeños negocios, ya está a la venta en toda Europa. Sony también ha añadido la cámara de seguridad de alta definición (HD) SNC-CX600 a la gama de instalaciones con cables y con alimentación por Ethernet (PoE).

Las dos cámaras, con un amplio ángulo de visión y una calidad de imagen de 720p, suponen un gran avance en el mercado ya que se trata de productos de imagen muy sofisticados, pero con un precio razonable y una variedad de funciones muy fáciles de implantar. Se trata de soluciones perfectas no solo para grandes empresas públicas y privadas, sino para todo aquel que desee instalar un sistema de seguridad eficaz en sus tiendas, oficinas y almacenes.

# Schneider Electric: detectores de presencia Argus

Schneider Electric, especialista global en gestión de la energía y en eficiencia energética, ha renovado su oferta de detectores de presencia Argus con una nueva gama, que tiene como objetivo conseguir un mayor ahorro en la factura de la luz, añadiendo máxima funcionalidad y mejores prestaciones. La nueva gama incluye cinco nuevos modelos que van desde una y dos salidas relé, una salida 1-10V, una salida DALI y un detector esclavo, cubriendo todas las necesidades de cualquier instalación y garantizando el cumplimiento del Código Técnico de la Edificación.

Esta nueva oferta permite utilizar los detectores como autónomos o como parte de un sistema, entrelazándolos entre ellos con un cable adicional.

# Mobotix: sensor de 5 megapíxeles, más claro, más rápido y más nítido

Mobotix, el mayor fabricante mundial de sistemas en red de videovigilancia de cámaras megapíxeles, saca al mercado tres nuevos modelos de cámara equipados con un nuevo sensor de 5 megapíxeles, que ofrece una frecuencia de vídeo superior, una mayor fotosensibilidad y una mejor función de zoom.

Los modelos de cámara S15, D15 y V15 son versiones mejoradas de las series anteriores. Equipadas con un sensor de 5 megapíxeles, presentan claras ventajas para el usuario: «La mejora más evidente de la que se benefician nuestros usuarios gracias al sensor de 5 megapíxeles es la elevadísima calidad de imagen, incluso cuando las condiciones de luz son malas», afirma Dr. Ralf Hinkel, fundador de MobotixAG. «La fotosensibilidad es hasta cuatro veces superior, lo cual aumenta ostensiblemente la calidad de imagen, por ejemplo, cuando hace mal tiempo o está oscuro».

La resolución QXGA máxima es 2,5 veces superior a la Full HD. Otra ventaja importante es que la nueva tecnología de sensor, en combinación con la edición previa de los datos de las imágenes directamente en la cámara, alcanza una frecuencia para el flujo de vídeo de hasta 30 imágenes por segundo.

# FF Videosistemas, distribuidor exclusivo de Geutebrück

FF Videosistemas, fundada en 1992 como distribuidora exclusiva de la marca alemana Geutebrück, se ha consolidado en lo alto del mercado de sistemas de circuito cerrado de televisión a nivel nacional, siendo referente del sector de la Seguridad.

FF Videosistemas ha presentado el nuevo net_porter de Geutebrück, una solución única. Es un sistema de vigilancia que permite conectar hasta 16 cámaras IP PoE mediante bocas de red PoE integradas en el switch de alto rendimiento 180W PoE 1Gbit.

Control a distancia de la tensión de alimentación e indicadores del consumo de potencia actual para todas las cámaras PoE conectadas.

Geutebrück dispone de un software para la gestión de sistemas IP excepcional; puede usar las cámaras IP topline de Geutebrück sin licencia. Con la licencia correspondiente se puede usar las cámaras de los principales fabricantes.

Permite utilizar diferentes formatos de compresión de vídeo en el mismo equipo (M-JPEG, H.264, H264CCTV, MPEG4CCTV/MP).

En esta ocasión, Geutebrück ha creado un sistema todoterreno que integra su propio switch PoE siendo una solución completa para todas las aplicaciones de videovigilancia. Instalar y administrar las cámaras IP, de forma rápida, fácil y eficiente sin necesidad de hardware de red adicional.


net_porter hace que no sea obligatorio decidirse por un formato de vídeo concreto, ya que procesa todos los formatos.

net_porter integra todos los componentes en un único equipo: matriz virtual digital, grabador, switch y alimentación PoE.

Con net_porter se tiene un contacto para todo el hardware NVR.

# Axis Communications: nuevas cámaras de red fijas diseñadas para la captura de movimientos rápidos en alta definición

Axis Communications ha presentado las cámaras AXIS Q 1614 (para interiores) y Q1416-E (preparada para exterior). Se trata de cámaras capaces de capturar movimientos rápidos con el doble de fotogramas que de costumbre, y manejar escenas de iluminación compleja con altos contrastes y condiciones extremas de poca luz. Estas cámaras resultan idóneas para sistemas de vídeo destinados al control de tráfico, videovigilancia ciudadana y entornos industriales.

Las cámaras AXIS Q1614/-E proporcionan imágenes con resolución HDTV 720p a 50 o 60 fotogramas por segundo, el doble de la velocidad máxima convencional. Esto asegura la captura de movimientos rápidos en detalle para que, por ejemplo, los objetos de una línea de producción industrial puedan ser fácilmente identificados.

Wide Dynamic Range (WDR) con captura dinámica de Axis, es la tecnología que permite a las cámaras AXIS Q1614/-E manejar escenas con iluminación compleja y altos contrastes, como cuando la luz del sol crea zonas muy brillantes y otras muy oscuras. Bajo estas circunstancias las cámaras AXIS

Q1614 y AXIS Q1614-E ofrecen imágenes homogéneas sin contrastes bruscos. Las cámaras AXIS Q1614/-E también incorporan la exclusiva tecnología Lightfider, que permite el funcionamiento óptimo y eficaz de la cámara en condiciones extremas de baja iluminación.

# Dallmeier: cámara DDF4 22HDV Picodome


Mini, micro, pico: la cámara más compacta de Dallmeier, el Picodome®, vuelve, ahora en resolución HD 720p!

El Picodome® HD destaca no sólo por su pequeño tamaño y elegante diseño sino también por su rendimiento.

El Picodome® DDF4220HDV ofrece vídeo HD en tiempo real (720p/30) en formato H.264, que es actualmente el estándar más avanzado para una compresión de vídeo de alta eficiencia, y soporta resoluciones de hasta 1,3 megapíxeles. Junto a vídeo HD sobre IP, la cámara híbrida ofrece una salida de vídeo analógica SD (PAL/NTSC) simultánea por BNC (FBAS).

El Picodome® HD destaca por su muy amplio rango dinámico (Wide Dynamic Range – WDR) y permite imágenes con máxima fidelidad en el color y excelente reproducción de detalles, incluso en escenas con un rango muy elevado de contraste y mucha contraluz. El alto rendimiento Low-Light además suministra imágenes nítidas y con poco ruido, incluso bajo condiciones de poca luz.

# Tyco Security Products: teclado táctil M-Touch

El fabricante italiano Bentel Security, ha lanza su nuevo teclado táctil M-Touch compatible con su gama de paneles Absoluta. Con una gran facilidad de maniobra para el usuario final y para el instalador, el teclado de la pantalla táctil M-Touch, con un tamaño de 7 pulgadas, funciona con toda la serie de paneles Absoluta en sus versiones 3 en adelante, garantiza el control completo de todo el sistema pudiendo acceder rápidamente a todos los menús.

Gracias a su interfaz potente e intuitivo, este nuevo teclado ofrece al instalador y al usuario toda la información sobre el panel y sus accesorios en un formato muy agradable y fácil de acceder con un solo toque de su dedo.

Incorpora una ranura para tarjetas de memoria SD que permite el visionado aleatorio de archivos de imagen JPG, destaca la facilidad con la que se parametrizan botones de acción preprogramados, que

permiten la activación automática de multitud de escenas, como armados especiales de particiones, activación de salidas PGM, activación de secuencias de servicio, domótica, etc.

Contactos de empresas, p. 7.

# ÍNDICE

## MATERIALES, EQUIPOS Y SISTEMAS DE SEGURIDAD



## SERVICIOS DE SEGURIDAD



## ALARMA Y CONTROL

**EURODETECTION.com**

Detectores de Arco, detectores manuales, chalecos anti-balas y visión nocturna.

**EURODETECTION, S.L.**
Ctra. Canillas, 138-2ª ofic. 11-B
28043 Madrid
Tel.: 913 886 782 - Fax: 917 599 996
**info@eurodetection.com**
**www.eurodetection.com**

**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**

**ADT** ADT Always There

**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**

**TURSON** SEGURIDAD PERIMETRAL

**TURSON**
Corazón de María, 5
28002 Madrid
Tel.: 914 152 502 - Fax: 914 134 775
**info@turson.com**
**www.turson.com**

**bydemes**
avanzando juntos hacia el futuro

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

**AGÜERO**
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

**ISO 9001**

**casmar**
sistemas de seguridad

Accesos | CCTV | Incendio | Intrusión

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

**CIRCONTROL**
Identificación y Seguridad
Identification and Security

FABRICAMOS PRODUCTOS DE CALIDAD
PARA EL ESPECIALISTA EN FUEGO Y SEGURIDAD

C/ Innovació, 3 (Pol. Industrial Can Mitjans)
08232 Viladecavalls - Barcelona (Spain)
Tel.: +34 937 362 940 - Fax: +34 937 362 941

www.circontrol.com



## FORMACIÓN DE SEGURIDAD

**CETS**

Avda. Emperatriz Isabel, 5
28019 Madrid
Tel.: 91 460 88 69
Fax: 91 469 88 44
**cets@formacioncets.com**
**www.formacioncets.com**

## COMUNICACIONES

## CONTROL DE ACCESOS ACTIVO

**TESA** ASSA ABLOY

**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**

GENETEC

Centro de Negocios Ibercenter
C/ Velazquez, 157 • 28002 Madrid
Tel +34 91 524 57 70
Fax +34 91 524 57 71
**www.genetec.com**

DIGITEK primion

CONTROL DE ACCESO, HORARIO, TIEMPO Y PRESENCIA

C/Samonta 21
08970 Sant Joan Despi
tel +34 934774770
info@primion-digitek.es
www.digitek.es

biosys

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

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

bydemes
avanzando juntos hacia el futuro

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

WINKHAUS

**Aug. Winkhaus GMBH & Co. KG**
Bohlweg 43
D - 48147 Münster
Delegación España y Portugal
C/ de la Creativitat, 7
E - 08850 Gavá/Barcelona
Tel. +34 93 633 4470
Fax. +34 93 633 4471
**winkhaus@winkhaus.es**
**www.winkhaus.es**

RISTER
PRESENTCO®

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

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

SUMAT

**Sumat Electrosistemas S.L.**

C/ Pozuetakogaina, 15B-1
20305- Irun (Guipuzcoa)
Tel. 943 624 311
Fax 943 635 069
**sumat@infonegocio.com**

accesor

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

DDS

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

info@accesor.com
**www.accesor.com**

DORLET

**DORLET S. A. U.**

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

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

setelsa link
Sistemas Electrónicos y Telecomunicación S.A.

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

## DETECCIÓN DE EXPLOSIVOS

COTELSA

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

TECOSA

TELECOMUNICACIÓN, ELECTRÓNICA Y CONMUTACIÓN

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

TARGET TECNOLOGIA

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

## EXTINCIÓN DE INCENDIOS

## SISTEMAS DE EVACUACIÓN

BOSCH

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

## PROTECCIÓN CONTRA INCENDIOS. ACTIVA

STANLEY
Security Solutions

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

bydemes
avanzando juntos hacia el futuro

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

# MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

**PEFIPRESA, S. A**

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

**www.pefipresa.com**

**Oficinas en:**

**A CORUÑA**
info.noroeste@pefipresa.com

**ALGECIRAS**
Tel.: 618 959 420

**BARCELONA**
info.barcelona@pefipresa.com

**BILBAO**
info.bilbao@pefipresa.com

**MADRID**
info.madrid@pefipresa.com

**MURCIA**
info.murcia@pefipresa.com

**SANTA CRUZ DE TENERIFE**
Tel.: 618 959 414

**SEVILLA**
info.sevilla@pefipresa.com

**VALENCIA**
info.valencia@pefipresa.com

**LISBOA**
info.lisboa@pefipresa.pt

**Atención al cliente: 902 362 921**

NOTIFIER® by Honeywell

MORLEY IAS FIRE SYSTEMS by Honeywell

ESSER by Honeywell

ACKERMANN by Honeywell

**Honeywell Life Safety Iberia**

***Oficinas centrales***

C/Pau Vila, 15-19
08911 Badalona – Barcelona

Teléfono: 902 03 05 45
Tel. Internacional: +34 93 24 24 236
Fax: (+34) 934 658 635

**www.honeywelllifesafety.es**
**infohlsiberia@honeywell.com**

**Representación comercial en:**

Barcelona, Madrid, Bilbao, Sevilla, Valencia, Mallorca, Galicia y Lisboa

SIEMENS

**Siemens, S.A.**
**División Building Technologies**
**Área Fire Safety**

Ronda de Europa, 5
28760 Tres Cantos (Madrid)
Tel.: 91 514 80 00
Fax: 91 514 07 01
**www.siemens.es/buildingtechnologies**

aguilera

**GRUPO AGUILERA**

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

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

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

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

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

BOSCH

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

PROTECCIÓN CONTRA INCENDIOS. PASIVA

Promat

**PROMAT**
C/ Velázquez, 41
28001 - Madrid
Tel.: 91 781 15 50
Fax: 91 575 15 97

**info@promat.es**
**www.promat.es**

DICTATOR Española

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

ROCKWOOL
LA PROTECCIÓN CONTRA INCENDIOS

**Rockwool Peninsular, S. A. U.**

Bruc, 50, 3º. 08010 Barcelona
Tel. 93 318 90 28
Fax. 93 317 89 66

**www.rockwool.es**
**www.rockfon.es**

PROTECCIÓN CONTRA INTRUSIÓN. ACTIVA

SIEMENS

**Siemens, S. A.**
**División Building Technologies**
**Área Fire & Security Products**

Ronda de Europa, 5
28760 Tres Cantos (Madrid)
Tel.: 91 514 80 00
Fax: 91 514 07 01
**www.siemens.es/buildingtechnologies**

RISCO GROUP
Creating Security Solutions

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

JR Sistemas de Seguridad Security Systems

**JR SECURITY SYSTEMS**
Rosellón, 52-54
08029 Barcelona
Tel.: +34 934 948 440
Fax: +34 934 102 221
**jrsecurity@jrsecurity.com**
**www.jrsecurity.com**

BOSCH

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

Honeywell

**Honeywell Security España S. A.**
**Soluciones integradas de intrusión, vídeo y control de accesos**

Avenida de Italia, 7
C. T. Coslada
28821 Coslada
Madrid
Tel.: 902 667 800 - Fax: 902 932 503
**seguridad@honeywell.com**
**www.honeywell.com/security/es**

Tecnoalarm
Hi-Tech Security Systems

**TECNOALARM ESPAÑA**

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

## PROTECCIÓN CONTRA ROBO Y ATRACO. PASIVA

**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**

**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

**EYEVIS**
C/ Velázquez, 9.
28810 Los Hueros - Villalbilla
Madrid (Spain)
Tel.: +34 91 879 38 06
**evs@eyevis.com**
**www.eyevis.com**

**Samsung Techwin Europe Ltd**
P. E. Omega - Edificio Gamma
Avenida de Barajas, 24 Planta 5 Oficina 5
28108 Alcobendas (Madrid)
Tel.: 916 517 507
**STEsecurity@samsung.com**
**www.samsungcctv.com**

**HIKVISION EUROPE**
Tel. +31 23 554 27 70
**saleseuro@hikvision.com**
**www.hikvision.com**

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

**Siemens, S.A.**
**División Building Technologies**
**Área Fire & Security Products**
Ronda de Europa, 5
28760 Tres Cantos (Madrid)
Tel.: 91 514 80 00
Fax: 91 514 07 01
**www.siemens.es/buildingtechnologies**

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

**EUROMA TELECOM**
MADRID: C/ Emilia 55 - Local 4, - 28029 Madrid Tel.: 915 711 304 - Fax 915 706 809. **euroma@euroma.es**
BARCELONA: C/ Bogatell, 43-49. 1ª. 2ª 08930 S. ADRIÁ DE BESOS (Barcelona) Tel.: 933 812 458 - Fax 933 815 734
**barcelona@euroma.es • www.euroma.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**

**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**

**TEB Ibérica Videovigilancia, S. L.**
Avda. de la Industria, 37, 2ª Oficina 10
28760 Tres Cantos, Madrid
España
Tel. 91 806 38 97
**www.teb-online.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**

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

# MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

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

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

C/ 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

**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**

## ASOCIACIONES

**ASOCIACION ESPAÑOLA**
**DE SOCIEDADES DE PROTECCION**
**CONTRA INCENDIOS**
Serrano, 43 - 6º OF. 18
28001 Madrid
Tel.: 914 361 419 - Fax: 915 759 635
**www.tecnifuego-aespi.org**

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

**VISIOTECH**
C/ Severo Ochoa, 9 - Nave B7
28521 Rivas Vaciamadrid (Madrid)
Tel.: 911 836 285
Fax: 917 139 344
**visiotech@visiotech.es**
**www.visiotech.es**

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

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

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

**ASOCIACION ESPAÑOLA**
**DE LUCHA CONTRA EL FUEGO**
Jacometrezo, 4 - 8º, nº 9
28013 Madrid
Tel.: 915 216 964
Fax: 911 791 859

**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**

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

C/ Miguel Yuste, 21
28037 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**

## EVENTOS DE SEGURIDAD

C/ José Abascal, 44 - 1º
28003 MADRID

**aespri.correo@gmail.com**
**Tel.: 91 451 58 42 • Fax: 91 441 67 66**

**ADSI - Asociación de Directivos**
**de Seguridad Integral**
World Trade Center Barcelona
Moll de Barcelona, s/n - Ed. Este 2ª Pl.
08039 Barcelona • Tel.: 93 508 83 55
**info@adsi.ws**
**www.adsi.ws**

# MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

## ASEPAL

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

## ASIS INTERNATIONAL

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

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

## cepreven

**ASOCIACIÓN DE INVESTIGACIÓN PARA LA SEGURIDAD DE VIDAS Y BIENES CENTRO NACIONAL DE PREVENCIÓN DE DAÑOS Y PÉRDIDAS**
Sagasta, 18
28004 Madrid
Tel.: 914 457 566 - Fax: 914 457 136

## FES

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

## AJSE

**ASOCIACIÓN DE JEFES DE SEGURIDAD DE ESPAÑA**
Avd. Merididana 358. 4ºA. 08027 Barcelona
Tel. 93-3459682 Fax. 93-3453395
**www.ajse.es presidente@ajse.es**

# CENTRALES DE RECEPCIÓN Y CONTROL

## SPITZ

Certificación: ISO 9001

**ALARMAS SPITZ S. A.**
Gran Vía, 493 - 08015 Barcelona
Tel.: 934 517 500 - Fax: 934 511 443
Cdad. de Barcelona, 210 - 28007 Madrid
Tel.: 914 339 800 - Fax: 914 332 191
**Central Receptora de alarmas**
Tel.: 902 117 100 - Fax: 934 536 946
**www.alarmasspitz.com**

# INTEGRACIÓN DE SISTEMAS

## TECOSA

TELECOMUNICACIÓN, ELECTRÓNICA Y CONMUTACIÓN

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

# INGENIERÍA Y CONSULTORÍA



# ESTUDIOS DE MERCADO

## Instituto ITMS

**ITMS**
Datos de contacto:
Avda. de Manzanares 196 • 28026 - Madrid
Tel.: 91 476 80 00 - Fax: 91 476 60 57
**www.institutoitms.com**
**info@institutoitms.com**

# SERVICIOS AUXILIARES

## servicass

**Sede Central de la Compañía:**

**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

## STANLEY Security Solutions

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

## Telefónica Ingeniería de Seguridad

**TELEFÓNICA INGENIERÍA DE SEGURIDAD**
C/ Condesa de Venadito, 7
1ª planta • 28027 Madrid
Tel.: 917 244 022 • Fax: 917 244 052
**tis.clientes@telefonica.es**
**www.telefonica.es/ingenieriadeseguridad**

## AGÜERO

**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


**¿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 2013

# MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

## MATERIAL POLICIAL

**CIASIPROIND, S.L**
Autorizada por la D.G.P. con el nº. 3598
Avda. de Espartinas, 5 – Plg. Industrial PIBO
41110 Bollullos de la Mitación (Sevilla)
Tlfno. 902194814 – Fax. 954002319
**http://www.grupormd.com**
**email: comercial@gruporomade.com**

**SABORIT INTERNATIONAL**
Avda. Somosierra, 22 Nave 4D
28709 S. Sebastián de los Reyes (Madrid)
Tel.: 913 831 920
Fax: 916 638 205
**www.saborit.com**

**SECURITAS SEGURIDAD ESPAÑA**
C/ Entrepeñas, 27
28051 Madrid
Tel.: 912 776 000
**www.securitas.es**

**SEGURSERVI, S. A.**
**Empresa de Seguridad**
Moreno Nieto, 9
28005 Madrid
Tel.: 902 191 200 - Fax: 913 658 179
**segurservi@segurservi.es**
**Web: www.segurservi.es**
**Autorizada por la D.G.P. con el nº 1.833**

**SEGURIDAD INTEGRAL CANARIA**
Alfred Nóbel, 27
35013 Las Palmas de Gran Canaria
Tel.: 902 226 047 - Fax: 928 226 008
**laspalmas@seguridadintegralcanaria.com**
**www.seguridadintegralcanaria.com**

## PORTALES WEB

puntoseguridad.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 nº. 729
Sede Social: Avda. de Espartinas, 5 – Plg. Industrial PIBO
41110 Bollullos de la Mitación (Sevilla)
Tlfno. 902194814 – Fax. 954002319
http://www.grupormd.com
comercial@gruporomade.com
SERVICIOS EN TODA ESPAÑA

## TRANSPORTE Y GESTIÓN DE EFECTIVOS

**LOOMIS SPAIN S. A.**
C/ Ahumaos, 35-37
Polígono Industrial La Dehesa de Vicálvaro
28052 Madrid
Tlf: 917438900
Fax: 914 685 241
**www.loomis.com**

INSTAL SEC

Avda. Manzanares, 196
28026 Madrid
Tel.: 914 768 000 - Fax: 914 766 057
**publi-seguridad@epeldano.com**
**www.instalsec.com**

casesa
GRUPO GLOBAL SECURITY 2010

**Sede Central de la Compañía:**

**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**

**¿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 2013


Suscríbase

# CUADERNOS DE SEGURIDAD

**RELLENE SUS DATOS CON LETRAS MAYÚSCULAS (fotocopie este boletín y remítanoslo)**

Entidad: _____ N.I.F.: _____
D. _____ Cargo: _____
Domicilio: _____
Código Postal: _____ Población: _____
Provincia: _____ País: _____
Teléfono: _____ Fax: _____
Actividad: _____
E-mail: _____ Web: _____

**Forma de pago:**

❑ Domiciliación bancaria c.c.c. nº _____
❑ Cheque nominativo a favor de EDICIONES PELDAÑO, S. A.
❑ Ingreso en Banco Popular c.c.c. 0075 0898 41 0600233543
❑ Cargo contra tarjeta VISA nº _____ Caducidad _____

Firma

**TARIFAS** (válidas durante 2013)

**ESPAÑA**
❑ 1 año: 93€ ❑ 2 años: 165€ (IVA y Gastos de envío incluido)

**EUROPA**
❑ 1 año: 124€ ❑ 2 años: 222€ (Gastos de envío incluido)

**RESTO**
❑ 1 año: 133€ ❑ 2 años: 239€ (Gastos de envío incluido)



Peldaño

DEPARTAMENTO DE SUSCRIPCIONES: 902 35 40 45
Avda. del Manzanares, 196 • 28026 Madrid • Tel.: +34 91 476 80 00 • Fax: +34 91 476 60 57
suscripciones@epeldano.com • www.puntoseguridad.com

# Luis González Hidalgo.

Secretario General de la Federación Empresarial Española de Seguridad, FES.

# *«No concibo otra profesión que no sea servir a mi país»*

Gemma G. Juanes

NO es fácil encontrar hoy en día a alguien que haya concebido su vida profesional de total servicio a su país. Luis González Hidalgo, secretario general de la Federación Empresarial Española de Seguridad (FES), es prueba de ello. Tras media vida en las Fuerzas Armadas, donde alcanzó el grado de coronel y tuvo diferentes destinos: África, Madrid… e, incluso, en el Centro Nacional de Inteligencia (CNI) –antes conocido como CESID–, «aterrizó» en la seguridad privada. Su «otra media vida» en un sector, por entonces incipiente, comenzó con su incorporación a un centro de formación. Nada que ver con su etapa anterior, pero mucho que compartir: experiencia y conocimiento. «Hay numerosas cualidades que contempla y desarrolla el militar de carrera. Servimos para diferentes actividades», subraya con decisión.

De ahí a FES –allá por el año 2000– como secretario general con un claro objetivo: potenciar la presencia de la asociación en foros y en las diferentes comisiones e incrementar su número de asociados. Prueba superada. «Contaba con 20 empresas asociadas y llegó a alcanzar las 150, «ahora un poco menos, por la situación actual», matiza. Hoy estamos ante una asociación con una clara representación en toda la geografía española y en todas las actividades que contempla la seguridad. «Mi trabajo se convirtió en un reto personal, que creo que he cumplido». ¡Como para no cumplirlo!: una absoluta implicación y esfuerzo diario.

Pero el trabajo continúa, y «ahora más, con el momento que vivimos», indica. Una crisis –explica– que ha llevado a nuestro país a «perder una generación de jóvenes valiosos», a «la incredulidad en la gestión de los políticos», a «la incertidumbre diaria»… Sin embargo, Luis González sí ve la luz al final del túnel. Para él, España, «su país», es una nación con un marcado carácter emprendedor. «Yo se lo recalco a los empresarios del sector de la seguridad: de aquí se sale tirando para adelante. Estamos ante nuevos nichos de mercado. ¡Vamos a aprovecharlos!».

Y él seguirá «tirando» de un sector en el que «me siento feliz», donde cuenta con grandes amigos y del que no espera nada a cambio, salvo ser recordado como «un buen profesional que vino a ayudar y a aportar» y, sobre todo, como «una buena persona».

Una vida profesional y personal plena, a la que ha contribuido sobremanera una «maravillosa mujer» –son palabras exactas suyas– siempre a su lado y con la que tuvo cuatro hijos y, ahora, unos nietos que le han ascendido al grado de abuelo. Con una excelente salud, descubre que aún sigue practicando deporte (senderismo, esquí… y hasta hace poco footing). Y todavía le queda tiempo para la lectura y algunos viajes.

No es fácil encontrar hoy en día –terminamos como empezamos estas líneas– a alguien que te asegure, tras narrarte con verdadera pasión los vaivénes de una vida, que, pese a todo, «tengo más de lo que me merezco». Un café con… sí lo ha encontrado: Luis González Hidalgo. ●

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

# Pyronix®

www.pyronix.com

Descargue de aquí la lista completa de productos aprobados EN50131!

SERIE XD


Serie **KX**

Pyronix Remote Control App

Serie **PCX**

**export.sales@pyronix.com**

Secure House,
Hellaby,
Rotherham,
**UK.**

**www.pyronix.com**

# casesa

902.01.04.06
casesa@casesa.es

Trabajamos para conseguir la satisfacción del Cliente
aportando valor y soluciones para su seguridad