Interempresas.net

# seguridad

www.interempresas.net

Nº 1195/2015

- Retail
- Banca
- Infraestructura crítica
- Logística
- Tráfico

Conferencias y demostraciones

## Descubre un mundo de soluciones en el Axis Solution Conference.

Axis les presenta un nuevo concepto de evento con un formato dinámico y visual para que conozca un mundo de soluciones Axis a través de demostraciones en directo. Nuestros principales desarrolladores de aplicaciones se juntan para crear una nueva experiencia.

**¡Regístrese de forma gratuita para asegurar su lugar en el Axis Solution Conference!**
El espacio es limitado por lo que necesitamos que se registren para garantizar el óptimo desarrollo del evento.
**El plazo de inscripción finaliza el 15 de Octubre.**

**¡Esperamos contar con su presencia en la conferencia!**
**www.axis.com/events/es/solution-conference-es-2015**

Atentamente,
**El equipo de Axis Communications**

*Axis Communications se reserva el derecho de admisión.*

AXIS COMMUNICATIONS

# SIM M2M Alto Rendimiento

# Alai Secure


Especialmente diseñada **para comunicaciones M2M.**

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

- HUMEDAD
- VIBRACIONES
- GOLPES
- CORROSIÓN

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

# Alai Secure

**Operador M2M en Seguridad**

# AJSE

Asociación de Jefes de Seguridad de España

Somos especialistas en la realización de ***Auditorías, Planes de Seguridad, Operativas de servicios, Planes de emergencia y evacuación, Formación continua, Análisis, Estudios y trabajos técnicos a nivel Nacional e Internacional***.

## FORMACIÓN

Somos la única Asociación del sector de la Seguridad en España que cuenta con un Centro de Formación propio. Donde se imparten cursos de alto nivel formativo y de calidad, realizados por auténticos profesionales del sector.

- ✓ Acciones formativas gratuitas por la Fundación Tripartita
- ✓ Acciones Formativas a medida para las empresas
- ✓ Avalados por las mejores Universidades de toda España, Sudamérica y Europa.
- ✓ Los Programas de estudios se realizan conjuntamente con las Universidades.

Modalidades:

- ✓ Título de Consejero de Seguridad, ADR a nivel Nacional.
- ✓ Título de Técnico Superior en Protección Civil por la Escuela de Protección Civil de Madrid.
- ✓ Curso de Técnico en Protección de Datos.
- ✓ Los cursos de ISO 28000 y 27000, obtenido por IRCA, para auditar en todos los países del mundo.
- ✓ Cursos de Reciclaje, Escoltas, Explosivos, Guardas de Campo, Incendios, Rayos x, Emergencias y Evacuación, Perdida desconocida, etc.

## AUDITORIAS

- ✓ **Programas de Seguridad de la Organización** para evitar, reducir, eliminar o transferir el riesgo de pérdidas
- ✓ **Análisis de amenazas, debilidades y vulnerabilidad** para identificar y priorizar los peligros y riesgos potenciales,
- ✓ **Procedimientos de manejo de crisis** para que la Organización responda en caso de una emergencia (incendio, explosión, contaminación, secuestro etc.).
- ✓ Se desarrollan y ponen en práctica **Planes de contingencia y evacuación**, **Servicios de seguridad corporativa.**
- ✓ Se auditan y evalúan las **Instalaciones y Procedimientos de la empresa.** Si poseen y son acordes a las necesidades de seguridad, medios físicos y electrónicos para impedir, detectar o demorar el ingreso no autorizado por el perímetro de la empresa.
- ✓ **Programas de protección de ejecutivos:** Reducir los riesgos de seguridad, asegurar la viabilidad continua de la organización para saber cómo actuar en caso de secuestros, toma de rehenes o empleados en crisis, medidas de seguridad a tomar, protección de la información, etc.

Avda. Meridiana, 358 - 4º A - Barcelona 08007
D: 933 024 206 - F: 933 022 257 - M: 693 603 444
E: presidente@ajse.es - www.ajse.es

# Objetivo: paliar la desinformación bidireccional

La residencia de ancianos de Santa Fe, situada en Zaragoza, sufrió este verano un trágico incendio en el que perdieron la vida ocho personas. Tras el incidente, se ha vuelto a poner en entredicho la situación actual de las medidas de seguridad en edificios para prevenir este tipo de accidentes. La falta de inspección por parte de las autoridades competentes es uno de los aspectos que destacan los profesionales como uno de los principales puntos a mejorar para evitar hechos como el acontecido recientemente.

En este número de Interempresas Seguridad, el presidente de la Asociación Tecnifuego-Aespi, Vicente Mans, profundiza un poco más en este tema ofreciendo su opinión personal y la de las empresas a las que representa la Asociación, además de proponer alternativas más adecuadas a las que recurrir en estos casos. En este sentido, Tecnifuego-Aespi busca cubrir las necesidades básicas en materia de seguridad tanto para los usuarios como para los edificios.

La mejora de las instalaciones eléctricas, las mayores exigencias legislativas en cuanto a instalación de elementos de seguridad contra incendios en las viviendas o la concienciación desde la escuela de las ventajas de la protección, entre otras cosas, son algunos de los múltiples requisitos que Mans considera claves para reducir los incendios en las viviendas, aunque admite que todavía tendrán que pasar décadas para que éstos se cumplan. Para que estos aspectos se lleguen a cumplir en un período de tiempo más reducido, es esencial empezar desde la base, es decir, formando e informando al ciudadano sobre la importancia de la seguridad en todos los ámbitos que les rodean.

Son muchos los expertos que comparten opinión sobre un problema de falta de información generalizada en nuestra sociedad. El director de Seguridad del Grupo Casino Gran Madrid, Ángel Pérez Alcarria, considera que uno de los motivos de este desconocimiento es que ni las Empresas de Seguridad, ni los Departamentos de Seguridad, ni la Administración, ni siquiera ellos, han sabido 'vender' el trabajo que desempeña día a día el personal de Seguridad Privada. Cree que son muchas las personas las que llevan trabajando para sus empresas y colaborando activamente con la FFCC de Seguridad para ayudar a conseguir que el ciudadano se sienta seguro, protegido y libre, pero apenas se aprecia esta labor por la sociedad actual.

Por tanto, para paliar esta problemática se requiere un esfuerzo doble y en ambas direcciones para que empresas de seguridad, departamentos, etc., comiencen a dar a conocer su labor y relevancia social y, por otro lado, los ciudadanos tengan en cuenta que el objetivo de dichas entidades es, tal y como asegura Pérez Alcarria, que el ciudadano se sienta seguro y protegido.

En los próximos meses, así como en 2016, se llevarán a cabo diferentes ferias que abordarán éste y otros aspectos en materia de seguridad. La primera de ellas es el Salón Internacional de la Movilidad Segura y Sostenible, Trafic, organizado por Ifema, que celebrará su próxima edición del 29 de septiembre al 2 de octubre en Madrid.

Edita: Interempresasmedia

**Director**
Angel Hernández
**Director Adjunto**
Àngel Burniol
**Director Área Industrial**
Ibon Linacisoro
**Director Área Agroalimentaria**
David Pozo
**Director Área Obra Pública y Construcción**
David Muñoz

**Suscripciones**
A través de internet:
www.interempresas.net/suscripciones
Por correo electrónico:
suscripciones@interempresas.net
Por teléfono: 936 802 027

**www.interempresas.net/info**
redaccion_seguridad@interempresas.net
comercial@interempresas.net

grupo NOVAÀGORA

**Director General**
Albert Esteves
**Director de Estrategia y Desarrollo Corporativo**
Aleix Torné
**Director Técnico**
Joan Sánchez Sabé
**Director Administrativo**
Jaume Rovira
**Staff**
Angel Hernández, Àngel Burniol,
Ibon Linacisoro, Jordi Duran, Ricard Vilà

Amadeu Vives, 20-22
08750 Molins de Rei (Barcelona)
Tel. 93 680 20 27 - Fax 93 680 20 31

**Delegación Madrid**
Av. Sur del Aeropuerto de Barajas, 38
Centro de Negocios Eisenhower,
edificio 4, planta 2, local 4
28042 Madrid - Tel. 91 329 14 31

**www.novaagora.com**

**Medio colaborador de:** AECRA, cepreven

Audiencia/difusión en internet y en newsletters auditada y controlada por: OJD

Interempresas Media es miembro de: AEEPP



D.L. B-25.481/99 / ISSN 1578-8881

# Sumario

## Cepreven e Interempresas media firman un convenio de colaboración

Cepreven, asociación sin ánimo de lucro especializada en la prevención y la seguridad, e Interempresas Media, han firmado un convenio de colaboración por el cual ambas entidades se comprometen a desarrollar acciones conjuntas en el sector de la seguridad. Con este acuerdo, Interempresas Media, plataforma de comunicación industrial líder en habla hispana, reafirma su compromiso con el sector de la seguridad y fortalece su revista Interempresas Seguridad, al poder incluir como partner a una de las asociaciones más activas y con mayor prestigio dentro de este mercado.


## Knauf reitera su compromiso con la seguridad en el ámbito laboral al obtener el certificado Ohsas 18001


Knauf ratifica su compromiso con la seguridad en el ámbito laboral al obtener, un año más, el certificado Ohsas 18001 de gestión de la Seguridad y Salud en el Trabajo (SST). Este certificado, que concede Aenor, especifica los requisitos para obtener un sistema de gestión más eficaz, que controle sus riesgos para la seguridad y mejore su desempeño en el entorno de trabajo. El sello viene a sumarse a otras importantes certificaciones, como ISO: 9001 de Calidad, ISO: 14001 para todos sus centros de producción, ISO: 14006 de gestión de Ecodiseño para todos sus productos fabricados en España, que sitúan a Knauf GmbH a la cabeza de las empresas españolas en materia de calidad, sostenibilidad y seguridad en el entorno laboral.

# EN EL TRABAJO, NO VER BIEN, ADEMÁS DE MOLESTO ES PELIGROSO.

## Para la seguridad de sus trabajadores, las gafas de protección, mejor graduadas.

General Optica le ofrece la mejor **solución a las necesidades ópticas y de protección** de sus trabajadores, en todos los campos de uso. Nuestras gafas de protección les permitirán trabajar siempre seguros, en óptimas condiciones visuales y además, con la graduación específica de cada trabajador. Estamos muy cerca de usted, con más de 250 tiendas a su disposición que le ofrecen el **servicio personalizado** de una empresa **líder en el cuidado de la visión**.

Gafas de protección Graduadas certificadas C.E. Protección Ocular para todos los campos de uso.

**Oficina técnica: Andrade, 128 08020 Barcelona Tel. 93 303 79 70 e-mail: rree_central@general-optica.es**

General Optica

Tu mirada eres tú

AENOR ER Empresa Registrada ER-1670/2002

CERTIFIED IQNet MANAGEMENT SYSTEM

## EfficientIP amplía las capacidades de DNS Guardian en ataques DNS

EfficientIP, proveedor de referencia en el mercado DDI, ha ampliado las capacidades de DNS Guardian incorporando una gran innovación: su contramedida 'Rescue Mode' que atenúa las consecuencias de los ataques volumétricos, lentos o insidiosos sobre las funciones recursivas y de la caché. Así, EfficientIP puede asegurar una disponibilidad 100% del servicio de la caché durante cualquier ataque DoS. EfficientIP ha diseñado DNS Guardian con el objetivo de proteger la disponibilidad del servicio DNS bajo un ataque, garantizando la integridad de los datos y logrando una seguridad DNS más inteligente.

## El videograbador de red SRN-4000 de Samsung Techwin obtiene el galardón de 'Producto CCTV del año' en el Reino Unido

Los lectores de la revista PSI (Professional Security Installer) han elegido al videograbador de red SRN-4000 64 canales de Samsung Techwin como 'Producto CCTV del Año 2015'. Este prestigioso galardón se entregó en la cena PSI Premier Awards a la que acudieron más de 150 representantes de la industria de seguridad, celebrada en Stapleford Park, cerca de Melton Mowbray, el pasado 2 de julio de 2015. Estos premios son un reconocimiento a la innovación y la calidad, y en los que los galardonados en cada categoría son seleccionados por instaladores profesionales de seguridad. Los instaladores han valorado que el videograbador SRN-4000 minimiza el coste total de un sistema de videovigilancia al ofrecer una solución de grabación de vídeo basada en Linux que es extremadamente robusta y fiable.

## Siemens incrementa un 8% sus ingresos en el tercer trimestre hasta los 18.844 millones de euros

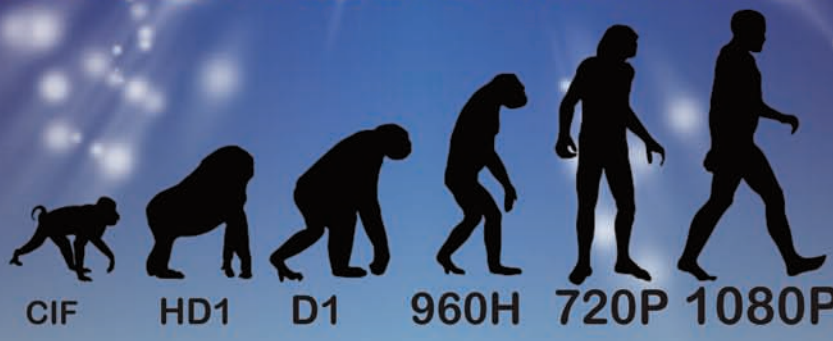
En el tercer trimestre de su año fiscal (del 1 de abril al 30 de junio de 2015), Siemens registró unos ingresos de 18.844 millones de euros, lo que supone un incremento del 8% respecto al mismo periodo del año anterior. "Esperamos mantener este ritmo y cerrar el año fiscal 2015 con sólidos resultados en el último trimestre", declaró el presidente y CEO de Siemens, Joe Kaeser. Estos datos se vieron influenciados por el efecto positivo del tipo de cambio. En términos comparables, los ingresos registraron un ligero descenso del 3%.

# Hoy el mundo se mira en HD

## Descubra la nueva tecnología AHD

CAMTRONICS

La evolución natural del vídeo tradicional




1. El DVR soporta a la vez cámaras estándar, AHD e IP (TRIHÍBRIDO)
2. Compatible con la anterior tecnología analógica sin cambiar de cables
3. Sistema abierto, no depende del futuro de un fabricante
4. Realiza un tratamiento avanzado de color. Mejora la imagen
5. Proporciona más del doble de calidad que el sistema de vídeo tradicional, 720p (HD) y 1080p (FULL HD)
6. No hay compresión, por lo que no hay pérdida de información
7. Permite instalación tanto con cable coaxial como con UTP con los conversores tradicionales
8. ¡Más económico de lo que imagina! Pregúntenos

AHD
Analog High Definition

€UROMA telecom

902 EUROMA
euroma@euroma.es
www.euroma.es

Madrid +34 91 571 13 04
Fax: +34 91 570 68 09
Barcelona +34 93 381 57 34
barcelona@euroma.es

## Francesco Della Mora, nuevo director de ventas para Europa Continental de Peli Products

Peli Products, multinacional destacada en el diseño y la fabricación de sistemas avanzados de iluminación portátil y maletas de alta protección, ha nombrado a Francesco Della Mora nuevo director de ventas para Europa Continental, función que desarrollará en su sede central para Europa, Oriente Medio y África, ubicada en Barcelona. "En este nuevo cargo, Francesco Della Mora será la persona responsable de dirigir nuestras actividades comerciales en todos los países y regiones de Europa Continental, abarcando desde Portugal hasta los países de la CEI", indicó Piero Marigo, director gerente de Peli Products.

## Mayor oferta y representación internacional en la próxima edición de Sicur

Sicur 2016, el gran referente internacional en España de la seguridad integral, celebrará una nueva edición entre los días 23 al 26 de febrero del próximo año, en Feria de Madrid. Una convocatoria, organizada por Ifema, que volverá a reunir a empresas, asociaciones, profesionales y usuarios de seguridad en torno a un escenario de alta representación sectorial, tanto desde el punto de vista de oferta como de demanda. Así lo confirman, los datos registrados en la pasada edición que congregó a 1.300 empresas participantes y 38.963 visitantes de 74 países, convirtiendo a Sicur en la plataforma por excelencia de esta industria, así como en el espacio donde tomar el pulso al mercado y conocer las novedades de vanguardia en materia de protección y prevención.


## Sando patenta un sistema para prevenir accidentes laborales en plataformas elevadoras

En línea con su política de Prevención de Riesgos Laborales e I+D+i, el grupo de empresas Sando ha desarrollado durante este último año un proyecto de investigación, denominado SAFE-PEMP, que ha dado como resultado la patente de un modelo de utilidad para evitar accidentes en Plataformas Elevadoras Móviles de Personas (PEMP). El modelo registrado en la Oficina Española de Patentes y Marcas consiste en una 'Cesta de seguridad para plataformas elevadoras' que reduce el riesgo de colisión y caída dentro de estas máquinas. Se trata de un sistema de seguridad activo, que señaliza y alerta a los responsables de la obra ante la falta de sujeción del trabajador o ante el riesgo de colisión, y que emplea sensores móviles, radiofrecuencia y ultrasonidos, resistentes a las inclemencias medioambientales y agresiones externas.

## Mycsa avanza en la distribución de sus embarcaciones semirrigidas Searib's

Varios contratos, con entrega en estos meses, de sus embarcaciones semirrigidas Searib's hacen que la gama Marina de Mycsa sea un referente en el sector. Uno de estos últimos contratos ha sido la entrega de seis embarcaciones, Searib'S modelo 860 Patrol al Servicio Marítimo de la Guardia Civil, a la unidad de actividades Subacuáticas (Geas) y que van a ser utilizadas por la unidad en la vigilancia y control del mar territorial Sur de España. El modelo 860 Patrol ofrece 8,75 m de eslora y 3,05 m de manga, fabricación en V profunda, para una navegación rápida y segura. La embarcación tiene una capacidad para 18 personas.

## Casmar Electrónica S.A. apuesta por el mercado de Chile y Colombia

Casmar Electrónica S.A., empresa española de distribución de material y soluciones de seguridad electrónica, con más de 35 años presentes en el mercado español y de 8 años en Portugal, inaugura una nueva etapa con la apertura de oficinas en Chile y Colombia. Esta decisión se basó en la apuesta de Casmar por el crecimiento de los países sudamericanos y la aportación de la experiencia de Casmar dentro del mundo de la seguridad. En los mercados chileno y colombiano hay una gran demanda de soluciones de seguridad para grandes proyectos y Casmar Electrónica, gracias a su experiencia en el mercado, y a los acuerdos estratégicos con una selección de los mejores fabricantes nacionales e internacionales, ofrece los mejores productos y soluciones para instalaciones de seguridad electrónica.

## Arsys se incorpora al proyecto europeo Tredisec de seguridad en Cloud

El proyecto Tredisec es una iniciativa de la Comisión Europea que cuenta con la participación de Arsys, entre otras firmas tecnológicas, para abordar de una manera integral los principales aspectos de seguridad del Cloud Computing y desarrollar procedimientos y soluciones que combinen seguridad, eficiencia y funcionalidades técnicas, facilitando la adopción de la Nube entre las empresas europeas. Esta iniciativa tiene como objetivo el desarrollo de soluciones tecnológicas que combinen los más elevados requerimientos de seguridad con otras características imprescindibles en un entorno Cloud, como eficiencia, fiabilidad y optimización de costes, tanto desde el punto de vista de negocio como de operaciones.

# Vicente Mans,
## presidente de Tecnifuego-Aespi

"En Tecnifuego-Aespi trabajamos por la calidad, el progreso del mercado y el cumplimiento legislativo"

Tecnifuego-Aespi es una asociación profesional sin ánimo de lucro que agrupa a diferentes compañías dedicadas a la protección contra incendios. Nació de la unión de las asociaciones existentes en 1992 conservando las garantías y la experiencia acumuladas por éstas durante más de 25 años. Tecnifuego-Aespi lleva a cabo su actividad dentro del territorio del estado español y extiende su participación a organismos de ámbito europeo e internacional. Interempresas Seguridad ha entrevistado a su presidente, Vicente Mans, quien ha opinado sobre la actualidad del mercado de la protección contra incendios.

**Mª Carmen Fernández**

***¿Cómo se estructura Tecnifuego-Aespi en la actualidad? ¿Qué ventajas le ofrecen a las empresas asociadas?***

La Asociación Española de Sociedades de Protección contra Incendios, Tecnifuego-Aespi, es una asociación empresarial de ámbito nacional y sin ánimo de lucro, que agrupa a los fabricantes, instaladores, mantenedores y otros servicios de seguridad contra incendios en España. Se estructura a través de comités sectoriales y grupos de trabajo donde se elaboran documentos, propuestas y todo tipo de actividades de mejora normativa, soluciones técnicas, difusión del sector, ética empresarial, divulgación de una cultura de protección, exportaciones y comercio exterior, formación en la innovación tecnológica, etc.

Además, el órgano ejecutivo es su Junta Directiva representada por los coordinadores de cada Comité y los vocales elegidos en la Asamblea general, directamente. Estar asociado a Tecnifuego-Aespi significa para las empresas un marchamo de calidad, ya que existe una continua actualización y formación en normativa, legislación, innovación, tendencia del mercado, oportunidades de negocio, exportación, apoyo a la investigación y el desarrollo, etc. Todo ello, bajo la garantía de un código deontológico, que en breve se materializará en un sello de 'empresa asociada'.

***¿Qué clase de actividades conjuntas llevan a cabo con sus asociados? ¿Y con la Administración Pública?***

Algunas de las actividades que desarrollamos son:

- Grupos de trabajo para la actualización y revisión de la normativa y legislación.
- Participamos en ferias y exposiciones tanto en el mercado español como internacionalmente, con el apoyo del Icex.
- Ostentamos la secretaría técnica del Comité Técnico de Normalización, CTN-23, que es el dedicado a seguridad contra incendios.
- Aportamos nuestras experiencias y participamos en grupos de trabajo junto a las Administraciones, como empresas fabricantes, ingenierías, instaladoras y mantenedoras en todo lo relativo a la legislación de seguridad contra incendios.
- Organizamos jornadas técnicas junto a las administraciones locales en diversas ciudades españolas, en lo que se ha dado en denominar el Día del Fuego, donde se debate "el estado del arte" en cada Comunidad Autónoma.

***¿Cuál es el objetivo de la Asociación para este 2015? ¿Cree que lo van a cumplir?***

Nos hemos propuesto varios objetivos y la mayor parte cumplidos en lo que va de año. Entre ellos, podemos destacar:

1. La creación de un nuevo subcomité en el CTN 23: Ingeniería para la seguridad contra incendios.
2. La gestión conjunta entre todas las asociaciones relacionadas. Hemos creado ya el primer grupo de trabajo para temas de protección pasiva contra incendios.
3. Seguimiento a los responsables del Ministerio de Industria para tener una información cierta y concreta del estado del Reglamento de Instalaciones de Pro-


Salida de emergencia.

Instalación de extintores en un edificio.

tección contra Incendios, Ripci, y de los planes de revisión del Reglamento de seguridad contra incendios en establecimientos industriales. El Ripci ha vuelto de Bruselas en agosto. Si no hay mayores problemas, verá la luz para la publicación a principios 2016.

4. En el área de Protección Pasiva estamos adelantando en el documento 'Sistemas de protección pasiva contra incendios en la edificación', una de guía de producto para una correcta instalación de los mismos. Una vez finalizado se continuará con el proceso para elevar el documento a Norma UNE e incluirlo en la legislación.

Algunas otras de las actividades que podemos destacar dentro de Tecnifuego-Aespi porque mejorarán notablemente el sector y la seguridad contra incendios en general, son: Desarrollo de un Registro de aplicadores de pasiva; Revisión, seguimiento y elaboración de normas UNE EN; Desarrollo de una Guía para la seguridad contra incendios en la interfaz urbano forestal (IUF), cuyo grupo de trabajo se mantiene en el Foro de SCI en IUF, etc.


Vivienda incendiada.

***En 2014 los incendios en viviendas provocaron un total de 116 muertes, un 11,5% más que el año anterior. ¿Considera que esas cifras se van a reducir este año?***

Para reducir los incendios en las viviendas se necesitan muchos requisitos que aún tardaremos décadas en ver cumplidos: concienciación desde la escuela de las ventajas de la protección, mejora de las instalaciones eléctricas y mayores exigencias legislativas en cuanto a instalación de elementos de seguridad contra incendios en las viviendas, como extintor, detector, rociador, BIE, protección pasiva (estructuras, puertas cortafuego, mobiliario ignifugado…), etc. En este sentido, estamos trabajando en el reforzamiento de la normativa para vivienda. Hemos solicitado al Ministerio de Fomento, que revise y amplíe la legislación (Código Técnico de la Edificación) exigiendo como primer paso la instalación de detectores de incendio, como ya sucede en Francia y otros países de nuestro entorno.

***¿Cuáles son las causas de incendio que más se repiten?***

Todos los años se repiten las mismas variantes: los fallecidos son personas mayores de 65 años, el mayor número de muertes se produce de noche, y el mayor número de incendios resulta en invierno. 'El calor barato', a

Detector de humos.

través de estufas, hornillos, braseros tiene mucha incidencia en los incendios habidos. Igualmente la sobrecarga eléctrica, descuidos en la cocina, fumar en la cama, etc.

***Tras el trágico incendio ocurrido este verano en la residencia de ancianos Santa Fe, en Zaragoza, donde fallecieron ocho personas, se ha vuelto a debatir sobre la seguridad en edificios. ¿Considera que el Código Técnico de la Edificación no contempla las suficientes medidas de seguridad para evitar incendios?***
Creemos que sobre todo hay una falta de inspección por parte de las autoridades competentes. El caso de la residencia Santa Fe es un ejemplo de ello: funcionaba sin las autorizaciones requeridas y sin las mínimas medidas de seguridad. En estos casos es necesario ser contundente y cerrar automáticamente este tipo de centros, además de ponerles fuertes sanciones. Con la vida no se juega.

***La detección de incendios en viviendas es obligatoria en muchos países de Europa. ¿Considera que España debería adoptar esta medida? ¿Cuáles más propone para mejorar la protección contra incendios?***
Sí, la detección de incendios en viviendas es exigible en Francia desde marzo y ya es una realidad en otros países europeos como Reino Unido, Holanda, Suecia y Alemania. En España debería exigirse igualmente al menos detectores autónomos que alertan de un incendio, pudiendo evacuar.

Otros medios de protección básicos y fáciles de instalar en una vivienda son los extintores, que pueden apagar un conato de incendio y evitar que se extienda el fuego. La boca de incendio equipada en el rellano de la escalera es otra de las medidas aconsejables. Los rociadores automáticos permiten sofocar el incendio con la acción directa del agua a través de los rociadores que son alimentados por tuberías. Se activan automáticamente. La ignifugación de los materiales se hace de fábrica en varios países de Europa en muebles, alfombras, cortinas, etc. Es muy importante la compartimentación y protección estructural, que todos los elementos constructivos cumplan con la resistencia al fuego que permita la evacuación de las personas y la intervención de los bomberos. El control de humos en la escalera y garajes, la señalización de evacuación y las puertas cortafuego completan la protección del edificio de viviendas para así mantener las vías de evacuación libres de humo, bien señalizadas y compartimentadas para que las personas puedan escapar del incendio.

***¿Cuáles son los retos de la Asociación de cara al futuro? ¿Y los del sector en general?***
Tenemos ante nosotros variados retos. Por un lado, trabajamos mucho en concienciar al usuario de que la búsqueda del "mejor precio", no debe descuidar la profesionalidad y la calidad de la instalación. Debemos encontrar vías para que las autoridades y/o organismos autorizados inspeccionen lo que se instala, con el fin de garantizar esa calidad y sobre todo la fiabilidad y eficacia de las instalaciones.
Otro tema que hay que mejorar es el de las normas de ensayo con que certificamos o calificamos nuestros productos, para que estén mejor definidas para que no sean "interpretables" y se eviten así problemas de competencia en el mercado. Este tema es común en la UE y estamos propiciando los caminos que mejoren esta situación. Tampoco podemos olvidar el apoyo e impulso a la actualización de la normativa vigente y evitar en el futuro retrasos en las publicaciones de reglamentaciones muy necesarias para el sector. Así, esperamos que la publicación del nuevo Ripci (que integra las nuevas normas UNE y otras actualizaciones necesarias) siga su curso y esté aprobado en los tiempos marcados. Igualmente, la instalación de protección pasiva necesita una certificación, y por ello el Ministerio de Fomento nos ha pedido que comencemos a trabajar en ello y en unas posibles guías de instalación de producto de protección pasiva.■

# Panda Security celebra su 25 aniversario en plena expansión internacional

Panda Security está de enhorabuena. La multinacional española de soluciones de seguridad para la protección de la vida digital de particulares y empresas cumple 25 años a la vanguardia de la seguridad TIC, no solo en España sino en todo el mundo.

Panda Security, que tiene presencia directa en más de 80 países y distribuye sus productos en cerca de 200, anuncia ahora la incorporación de Italia y Dinamarca a su red de filiales, que se convierten en mercados importantes para su negocio en Europa. Con estas dos nuevas incorporaciones, el número de filiales de la multinacional de seguridad asciende ahora a 16: España, EE UU, Francia, Alemania, Austria, Bélgica, Holanda, Suecia, Finlandia, Reino Unido, Brasil, Canadá, Portugal, México, Italia y Dinamarca.

Este proceso de internacionalización, que integra uno de los pilares del plan estratégico de la compañía a cuatro años vista, se completa además con un afianzamiento de su presencia en aquellos mercados en los que ya es fuerte, como Europa Occidental, Estados Unidos y Latinoamérica, destacando el ejemplo de Panamá donde la compañía acaba de aterrizar bajo el modelo de Country Partner.

Además, durante los próximos meses, la expansión internacional de Panda se completará también con el refuerzo de su presencia en otros mercados emergentes como China, Rusia o India.

### Nueva estrategia en su 25 aniversario

La compañía ha inaugurado recientemente el año de su 25 aniversario con nueva identidad corporativa que refleja el objetivo de Panda de hacer fácil lo complejo bajo la idea de 'Simplexity'. Un concepto que básicamente implica simplificar la complejidad creando nuevas y mejores soluciones que salvaguarden la vida digital de los usuarios.

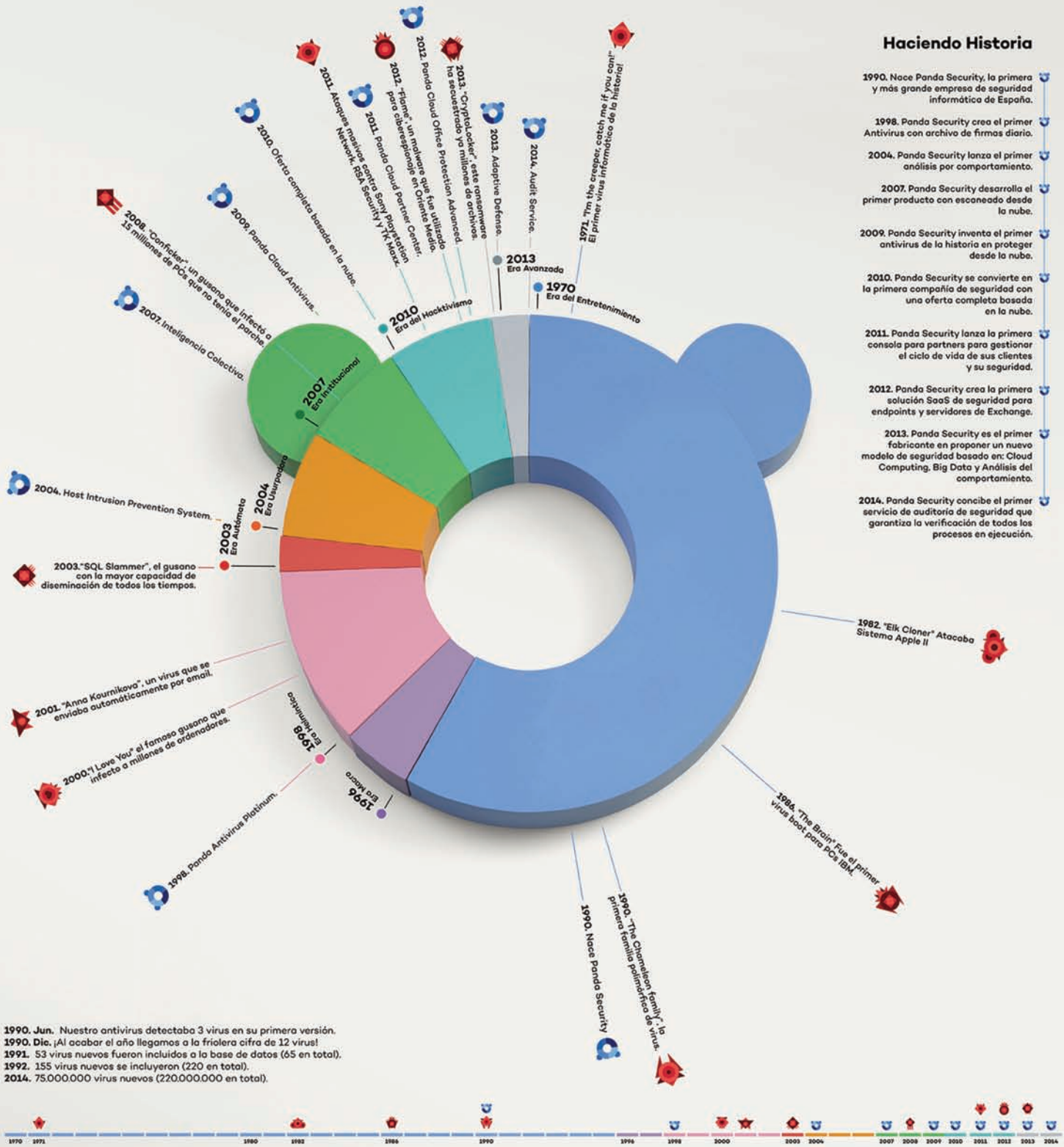
"Nuestra misión es ofrecer al usuario una solución fácil de usar, rápida y efectiva, y siempre sobre la base de la innovación. A lo largo de estos 25 años, Panda no ha dejado de innovar y de estar a la vanguardia tecnológica. Nos posicionamos como visionarios en la incorporación de tecnologías como Cloud Computing o Big Data que hace unos años eran totalmente disruptivas. Ahora vamos a por otros 25 años, repletos de entusiasmo y energía, y con la certeza de contar con todos los recursos necesarios para continuar siendo líderes", explica Diego Navarrete, CEO de Panda Security.

La compañía tiene previsto acometer un plan estratégico a cuatro años vista, centrado en la internacionalización, en mantener el ritmo de crecimiento tanto a nivel de ventas como de porfolio, y en impulsar nuevas tecnologías y alianzas estratégicas que respondan a tendencias de mercado como Internet de las Cosas, Big Data, Cloud Computing o movilidad.■

**Fundada en 1990, Panda Security es la empresa líder a nivel mundial en soluciones de seguridad basadas en la nube. Con sede en España, la compañía cuenta con presencia directa en más de 80 países, productos traducidos a más de 23 idiomas y millones de clientes en todo el mundo. Su misión es simplificar la complejidad creando nuevas y mejores soluciones para salvaguardar la vida digital de sus usuarios.**
**Como parte de su política de Responsabilidad Social Corporativa, Panda Security colabora con el Proyecto Stella para promover la inserción social y laboral de personas con síndrome de Down y otras discapacidades intelectuales.**

panda 25años

¿25 ya? Y parece que fue ayer cuando empezamos. Quién nos iba a decir entonces, cuando empezamos siendo un grupo de amigos en Bilbao, que estaríamos hoy en más de 80 países y compitiendo con los grandes. Han sido 25 años de reinventarse constantemente, de no dejar de aprender. Ahí está ese inconformismo que llevamos tan dentro, llevándonos a innovar en todo, adoptándonos a este mundo que ha cambiado más rápido que nunca antes. Desde la era pre-internet, cuando los virus se transmitían por disquetes, a hoy, rodeados de multitud de dispositivos permanentemente conectados, el Internet de las Cosas. Y siempre, Panda protegiéndonos en todo momento. **¡Vamos Panda, a por otros 25!**




## Haciendo Historia

**1990.** Nace Panda Security, la primera y más grande empresa de seguridad informática de España.

**1998.** Panda Security crea el primer Antivirus con archivo de firmas diario.

**2004.** Panda Security lanza el primer análisis por comportamiento.

**2007.** Panda Security desarrolla el primer producto con escaneado desde la nube.

**2009.** Panda Security inventa el primer antivirus de la historia en proteger desde la nube.

**2010.** Panda Security se convierte en la primera compañía de seguridad con una oferta completa basada en la nube.

**2011.** Panda Security lanza la primera consola para partners para gestionar el ciclo de vida de sus clientes y su seguridad.

**2012.** Panda Security crea la primera solución SaaS de seguridad para endpoints y servidores de Exchange.

**2013.** Panda Security es el primer fabricante en proponer un nuevo modelo de seguridad basado en: Cloud Computing, Big Data y Análisis del comportamiento.

**2014.** Panda Security concibe el primer servicio de auditoría de seguridad que garantiza la verificación de todos los procesos en ejecución.

**1990. Jun.** Nuestro antivirus detectaba 3 virus en su primera versión.
**1990. Dic.** ¡Al acabar el año llegamos a la friolera cifra de 12 virus!
**1991.** 53 virus nuevos fueron incluidos a la base de datos (65 en total).
**1992.** 155 virus nuevos se incluyeron (220 en total).
**2014.** 75.000.000 virus nuevos (220.000.000 en total).




## Eras del Malware

### 1971

Los virus se hacían por diversión, algunos muy dañinos, otros inocuos, pero no buscan nada más que sacar la sonrisa de su creador.
Su propagación era lenta (meses, incluso años) ya que era a través de disquetes.

### 1996

Internet empieza a popularizarse tímidamente y comienzan a popularizarse los virus que alteraban una macro para cambiar o neutralizar su acción. Estos virus viajan en documentos o se descargan al hacer clic en un banner o archivo adjunto de correo.

### 1998

Internet cada vez tiene más penetración, comienzan a aparecer los primeros gusanos de correo electrónico. La distribución de estos gusanos es limitada, pero en poco tiempo esto cambia, y "I Love You" llega a saturar Internet.

### 2003

Con "Blaster" se inaugura la aparición de los gusanos de red, que no necesitan la intervención del usuario para infectar otros ordenadores.

### 2004

En pleno auge de gusanos de red y de correo, comienzan a aparecer los primeros ejemplares de malware creados por ciberdelincuentes para conseguir ganancias económicas: los troyanos bancarios. Y se comienzan a producir los primeros ataques de phishing.

### 2007

En 2007 se produce el primer ciberataque masivo contra un país, Estonia recibe un ataque masivo que tira abajo páginas web y servicios del parlamento, bancos, ministerios, periódicos, etc. Tiene como origen Rusia.
Un año más tarde, antes de la invasión rusa de Georgia, se lanza un ciberataque que aísla completamente al país de Internet.

### 2010

Anonymous empieza una campaña contra diferentes organizaciones. Se comienzan a ver hackeos a grandes empresas (en 2011 hackeo y robo de cuentas de la PlayStation Network de Sony, RSA, etc.).

### 2013

Hoy en día todo está movido por el dinero y los intereses políticos: grandes compañías de ransomware (Cryptolocker, torrentlocker, ctb-locker, etc.), troyanos bancarios muy avanzados, robos a grandes empresas, incluyendo terminales de punto de venta, APTs (Advanced Persistant Threats), etc.

# Aslan ofrece las claves para la 'Seguridad y disponibilidad en la nueva red'

En su afán por estar al día de las últimas tendencias tecnológicas y mostrar las posibilidades que ofrecen a empresas y profesionales para que desempeñen un uso adecuado de estas herramientas, la Asociación Aslan organizó el pasado día 1 de julio un nuevo foro tecnológico en Madrid bajo el título 'Seguridad y disponibilidad en la nueva Red'. Representantes de importantes empresas como Microsoft, Panda Security o Aruba Networks ofrecieron charlas para dar una visión propia sobre los temas que conciernen este foro.

**María Fernández Peláez**

Para evolucionar de la mano de esta nueva 'sociedad conectada' de la que todos formamos parte, tenemos que adaptarnos a ella. Es por esto que aspectos como la disponibilidad y la seguridad son los que más preocupan tanto a empresas como a gobiernos al ser agentes que están inmersos en este proceso de transformación digital. En este sentido, la Asociación Aslan organizó el pasado 1 de julio el foro tecnológico 'Seguridad y disponibilidad en la nueva Red' para ofrecer una visión integral sobre las principales tendencias y soluciones en seguridad para afrontar esta nueva situación tecnológica.

Uno de los expertos en ofrecer soluciones para hacer frente a estas nuevas tendencias fue Federico de Dios, service line Manager de Akamai Technologies. En su conferencia 'IoT nuevos retos de Seguridad y Tendencias de ataques en Internet', de Dios contó lo que están viendo en Akamai en relación a la seguridad en Internet ya que su trabajo "está totalmente en Internet" y saben hacia donde se dirigen los ataques. "El IoT ha redirigido mucho los ataques: en los últimos 6-9 meses, hay muchos más ataques volumétricos en relación a los ataques específicos a nivel de aplicación ya que la capacidad de generar los primeros es demasiado alta y lo que hace es que sube la media", señaló de Dios tras asegurar que tanto el volumen como el número de ataques se multiplica año a año.

En este sentido, el profesional de Akamai hizo alusión a otra tendencia: el tiempo medio de duración de un ataque siendo, actualmente, la media de ataque superior a un día. Asimismo, de Dios aseguró que "el 50% de los grandes ataques actuales son multivector y hay dos tipos: multivector tecnológico y multivector de estrategia" y, en esta línea, ofreció unos datos escalofriantes y es que, a través de la Plataforma de Akamai (Akamai Inteligent Plataform) se han encontrado en pocos días con más de 120.000 ataques diferentes de sensor. "El hecho de atacar a dispositivos es mucho más fácil porque está todo conectado y por ello, hay que estar preparado ya que hay muchos más ataques en muchos sitios diferentes y con tecnologías diferentes" admitió este experto asegurando que es la Industria del juego online la que está situada en primera posición en ataques.

### Tendencias y principales problemas de los Data Center

Por su parte, Francisco Arcia, channel sales Manager iberia de Cyberoam, en su conferencia 'Mejorando la seguridad en los centros de datos' destacó los principales problemas de los Data Center y las tendencias que in-

Los asistentes al evento escuchando una de las ponencias.

tentan abrir en este aspecto ya que, al igual que el mercado de la seguridad está cambiando constantemente, también se observa una evolución en el Data Center, ahora mucho más segmentado. Arcia aludió a la seguridad y a la alta disponibilidad como los principales problemas de los Data Center. "Cuando empieza una empresa, quiere un modelo flexible para ajustar las soluciones a medida que crecen y vemos también una tendencia hacia la virtualización", admitió Arcia y afirmó que el 80% de los riesgos de ataque proceden del interior de la empresa, con lo que "hay que saber que los ataques pueden venir de muchos sitios".

Respecto al segundo de los problemas del Data Center –la alta disponibilidad-, este profesional aseguró que las empresas cuentan con una serie de soluciones que quieren que siempre estén funcionando, pero lo que hay que hacer es "buscar soluciones acordes a las necesidades de cada uno ya que hay soluciones que no tienen por qué estar en alta disponibilidad". En este sentido, hay que pensar en el diseño de la infraestructura para buscar las soluciones de conexión permanente porque hay que buscar medidas de seguridad dependiendo de cada Data Center.

Sobre 'Conexiones seguras y máxima disponibilidad a los servicios en cloud' se encargó de hablar el director general de Zertia Telecom, Félix García. El tema de este operador es la gestión de telecomunicaciones y, según una encuesta de la asociación a la que pertenece Zertia, la mayoría de los CEOs entrevistados tienen confianza en el nivel de respuesta de la aplicación. Además, García también nombró un concepto creado por Zertia: el NNI (Network Neutral Interface). Se trata de una interconexión cloud pública que no pasa por Internet pero es 100% segura.

Pilar Santamaría, directora de la división Cloud & Enterprise de Microsoft, se encargó de hablar sobre 'La privacidad y seguridad en la Nube' donde hay 16 billones de volumen de negocio. "En nuestras encuestas de Microsoft el resultado es que nuestros clientes tienen confianza en la seguridad en la Nube", afirmó Santamaría y confirmó que, aparte de cómo aplican la seguridad, tienen también al regulador, es decir, aunque no se produzca un fallo, se está actuando con la diligencia adecuada.

### Los tres pilares de Microsoft

Antes de continuar, Santamaría anunció los tres pilares que sostienen a Microsoft:

- Cultura de seguridad
- Inversión
- Lucha activa anti-cibercrimen

"Nuestra visión es aplicar la seguridad en base a los datos que tenemos para que sea eficaz", afirmó Santamaría y confirmó que, como parte de esa cultura, no utilizan los datos para el tema de publicidad ya que "pro-

porcionamos de forma transparente el código fuente y no damos el acceso directo a Gobiernos y es importante de cara a la regulación".

La experta dejó claro que desde Microsoft entienden que los datos es lo que hay que proteger y que se hace de extremo a extremo. "Nuestro compromiso es no perder el control de los datos porque los clientes son dueños de sus datos y nuestra filosofía es proporcionar herramientas de gestión".

### Seguridad y Movilidad con HP y Aruba

'Visibilidad y contexto: claves para implementar seguridad en movilidad' es el título de la ponencia que ofreció el director técnico de Aruba Networks, Carlos Vázquez. En este sentido y con motivo de la adquisición de Aruba por parte de HP, Vázquez marcó como tendencias la movilidad y el Cloud, siendo Aruba líderes de la primera de las tendencias y HP de la segunda. "En la parte de networking hemos unido fuerzas HP y Aruba cada uno siendo líderes en lo suyo. Aruba, en la parte de control de accesos, ha hecho algo nuevo. Tenemos una cultura abierta que es lo que nos ha dado la pista para unirnos con HP y comenzaremos a trabajar juntos en septiembre u octubre", explicó.

Vázquez resaltó también la importancia de la gestión de red y de acceso ya que consideran que aporta mucho valor tener una gestión de red multifabricante. Para el control de acceso, cuentan con la plataforma 'Clear Pass' que muestra la seguridad en el tema de movilidad. "Esta plataforma tiene contactos con la red y también es importante para securizar puertos de red. También compartimos contexto con los firewall y estamos desarrollando la integración de MDM", afirmó Vázquez y concluyó señalando que han pasado a un modelo totalmente impredecible, que es el de la movilidad, y por eso es imprescindible que haya un elemento -Clear Pass- que autentifique todo esto ya que "en el mundo móvil irremediablemente la seguridad pasa por la visibilidad y el contexto".

Finalmente, el vicepresidente de gestión de producto de Panda Security, Juan Santesmases, habló de 'La Seguridad como clave en Analytics of Things' y resaltó la necesidad de que los fabricantes de antivirus "estemos de acuerdo para coordinarnos" ya que "estamos ante una situación complicada". Santesmases aseguró que, según estudios de Panda, el 2014 puede considerarse como el año de los grandes ciberataques y de los robos de información a gran escala en algunas de las multinacionales más grandes del mundo.

Ante esta situación, las líneas de defensa que explicó este experto son el salto a la Inteligencia Colectiva y la llegada del Big Data. Así, el nuevo modelo de seguridad Cloud, se divide en tres fases:

1. Monitorización de cada una de las acciones que desencadenan los programas de los equipos.
2. Análisis y correlación de todas las acciones monitorizadas en todos los clientes gracias a técnicas de inteligencia basadas en Data Mining y Big Data.
3. Fortificación y securización de los equipos.

La tecnología utilizada es Adaptive Defense, un nuevo modelo de seguridad capaz de ofrecer protección completa para dispositivos y servidores mediante la clasificación del 100% de los procesos ejecutados en cada puesto y cada servidor del parque informático, supervisando y controlando su comportamiento.

En definitiva, todos los expertos aportaron su visión personal ante esta nueva situación tecnológica pero con un punto en común: garantizar la seguridad y disponibilidad en la nueva Red.■

# José Carlos Fuster,
## director de ventas de VPSitex

"A veces es difícil encontrar el equilibrio entre seguridad y protección de la intimidad, pero no diría que son incompatibles"


Interempresas ha entrevistado a José Carlos Fuster, director de ventas de VPSitex, empresa especialista a nivel mundial en la protección, mantenimiento y gestión de bienes inmuebles desocupados. Las nuevas tendencias tecnológicas, la legislación del mundo de la seguridad, o el equilibrio entre el derecho a la intimidad y la protección, son algunos de los temas que se han tratado, además de las principales novedades de VPSitex y sus principales retos para este 2015.

**Mª Carmen Fernández**

***¿Cómo valoraría la penetración que tienen las soluciones de seguridad de VPSitex en el mercado español? ¿Han ganado cuota de mercado durante los últimos años?***

Han representado una novedad que dinamiza el mercado inmobiliario. Las puertas y pantallas antiokupa han permitido una alternativa al tapiado o a las planchas soldadas, que no permitían la entrada para reformar o comercializar inmuebles. Por otro lado, el régimen de alquiler permite la protección temporal y supone un ahorro en seguridad. VPSitex es una empresa en constante expansión, y en el mercado español, en nuestros dos primeros años hemos protegido de forma temporal, más de 2.000 inmuebles.

***¿Cuáles son los principales retos que se han marcado para este 2015? ¿Cuáles van a ser sus principales líneas estratégicas durante este ejercicio?***

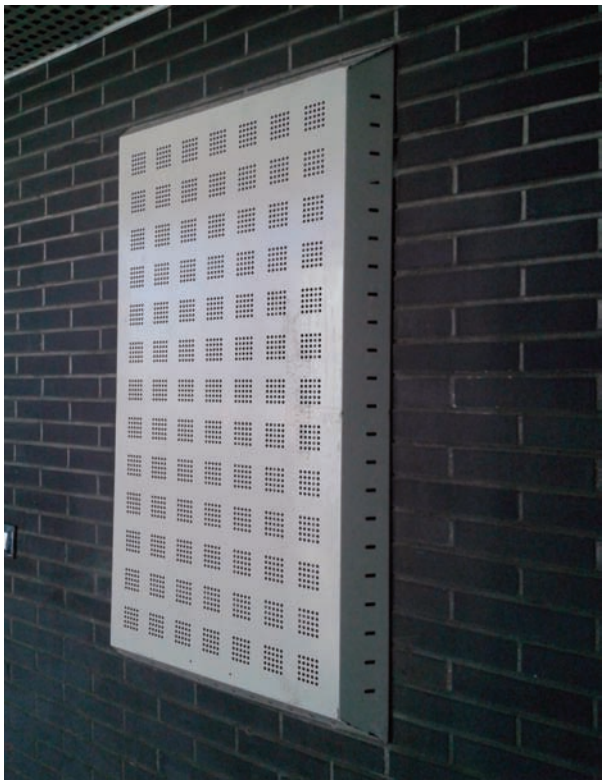
Nuestro principal reto es duplicar el volumen de inmuebles gestionados. Principalmente, vamos a ampliar la gama de servicios que VPSitex ya ofrece en otros países, incluyendo por ejemplo la instalación de alarmas sin cableado en alquiler. Otra línea estratégica es ampliar nuestra cobertura geográfica. Y finalmente, en el aspecto tecnológico, vamos a desarrollar una aplicación para que nuestros clientes puedan conocer el estado de sus pedidos en cualquier momento.

***¿Qué peso tiene la línea de negocio enfocada a soluciones de seguridad dentro de una mega-organización como es la de VPSitex? ¿Qué porcentaje de la facturación del grupo aporta su división?***

Tiene un gran peso, ya que VPSitex ofrece múltiples soluciones de seguridad dependiendo del tipo de inmueble, de los riesgos asociados, de las necesidades y de los recursos del propietario. De momento, es una pequeña parte, teniendo en cuenta que VPSitex es un grupo consolidado en Europa y llevamos poco tiempo en España.

***¿Podría resumirnos cuáles son las principales soluciones que ofrece hoy VPSitex en el mercado de la seguridad? ¿Qué peso tiene cada una sobre su actividad total?***

Globalmente, instalamos puertas, pantallas y paneles de acero, para proteger accesos y minimizar los riesgos asociados a la intrusión. También disponemos de alarmas sin cableado, cámaras, servicios de vigilancia, y la última solución que ofrecemos a ciertos clientes es la Smart Tower, una cámara que se instala en una torre portátil



Pantalla instalada en un piso bajo de Sevilla.

para controlar grandes espacios. Por otro lado, también ofrecemos servicios de inspección, cerrajería, limpieza y reforma de inmuebles vacíos. Dependiendo del país, unas soluciones se usan más que otras. En España e Italia, principalmente instalamos puertas y pantallas de acero. En Francia o Reino Unido, las alarmas están más extendidas.

***Centrándonos en el campo de la seguridad del inmueble vacío, y como especialistas que son en esta materia, ¿cuáles son las últimas tendencias tecnológicas que aprecian en este sector?***

Dejando a un lado los cerramientos de acero para proteger puertas y ventanas, también utilizamos otros materiales como el policarbonato, que respeta la estética de los edificios y se instala para proteger ventanales. En cuanto a las alarmas, los detectores con cámara y sin cableado son ya comunes, aunque el cambio legislativo encarece su uso al requerir un mínimo de 3 (2 en Cataluña) detectores por inmueble.

Puerta instalada en Torrejón de Ardoz (Madrid).

***¿Cuáles son los sectores que les están generando más actividad en este ámbito (bancos, centros logísticos, administraciones públicas, viviendas…)? ¿Trabajan más para empresas privadas o para entidades públicas?***

En general, nuestros clientes son los propietarios de inmuebles vacíos, ya sean empresa o particular. Les ayudamos a mantener el valor del inmueble reduciendo los riesgos de intrusión y facilitamos su comercialización. En España, los principales propietarios de inmuebles vacíos son los bancos y últimamente los fondos de inversión, aunque las entidades públicas también tienen un considerable patrimonio inmobiliario. Podríamos decir que el sector privado y el público tienen un peso similar entre nuestra clientela.

***Entiendo que los fabricantes de este tipo de dispositivos de seguridad siempre tienen que ir por delante de los conocimientos adquiridos por la delincuencia organizada. ¿Se está estrechando cada vez más este distanciamiento? ¿Cómo pueden aumentar los fabricantes los niveles de seguridad?***

Cuando sale un sistema nuevo, su grado de eficacia es inversamente proporcional al tiempo que tarden los delincuentes en encontrar sus puntos débiles y sabotearlo. Desgraciadamente, gracias a Internet, una vez se sabe cómo sabotear un sistema, los delincuentes lo tienen más fácil para compartir conocimientos. Lo vemos en todos los ámbitos: puertas blindadas, cajeros, banca online, etc.

Para aumentar el nivel de seguridad, la experiencia acumulada sobre las debilidades de los sistemas existentes y los tests a los nuevos productos y soluciones son factores clave para aumentar la efectividad inicial. Y obviamente, cuantas más soluciones y dispositivos nuevos se fabriquen, mayor será el grado de eficacia inicial.

***En algunos ámbitos, los sistemas de seguridad han creado cierto recelo en la sociedad por su complejo acople con el derecho de las personas a proteger su intimidad. ¿Considera que estos dos ámbitos son incompatibles? ¿Cómo se pueden encajar estas dos piezas?***

Efectivamente, a veces es difícil encontrar el equilibrio entre seguridad y protección de la intimidad, pero no diría que son incompatibles. Es cuestión de valorar las opciones, establecer prioridades, informar al ciudadano y regular el tratamiento de la información obtenida. Sin duda, los legisladores tienen trabajo por delante.

***Dentro del competitivo ámbito de la seguridad, ¿cuáles destacaría Ud. como los valores diferenciales de los productos y los servicios ofrecidos por VPSitex?***
La temporalidad, la fácil instalación y el efecto disuasorio, principalmente de las puertas y pantallas de acero.

***¿Podría decirnos algún trabajo relevante en el que haya participado recientemente VPSitex con sus soluciones de seguridad?***
Participamos en el Plan de Renovación de Viviendas del IVIMA en Madrid, facilitando la reforma y recuperación de viviendas que estaban tapiadas y ahora se adjudican a familias con escasos recursos. También hemos protegido edificios enteros en barrios conflictivos como La Mina en Barcelona o promociones públicas de nueva construcción como Nuevo Amate en Sevilla.

***¿En qué medida las nuevas tecnologías, las TIC, están cambiando el mercado de la videovigilancia, y de la seguridad en general?***
Los avances tecnológicos aplicados a la seguridad pueden facilitar su gestión, su control y el grado de eficacia. En nuestro caso vamos a instalar una aplicación que permita a los clientes conocer el estado de sus pedidos de forma automática.

***¿Cómo puede favorecer VPSitex la tendencia urbana hacia las 'smart cities'? ¿Están trabajando ya intensamente en este campo?***
Mediante la combinación de sistemas y personal cualificado, dotado con las últimas tecnologías de gestión.

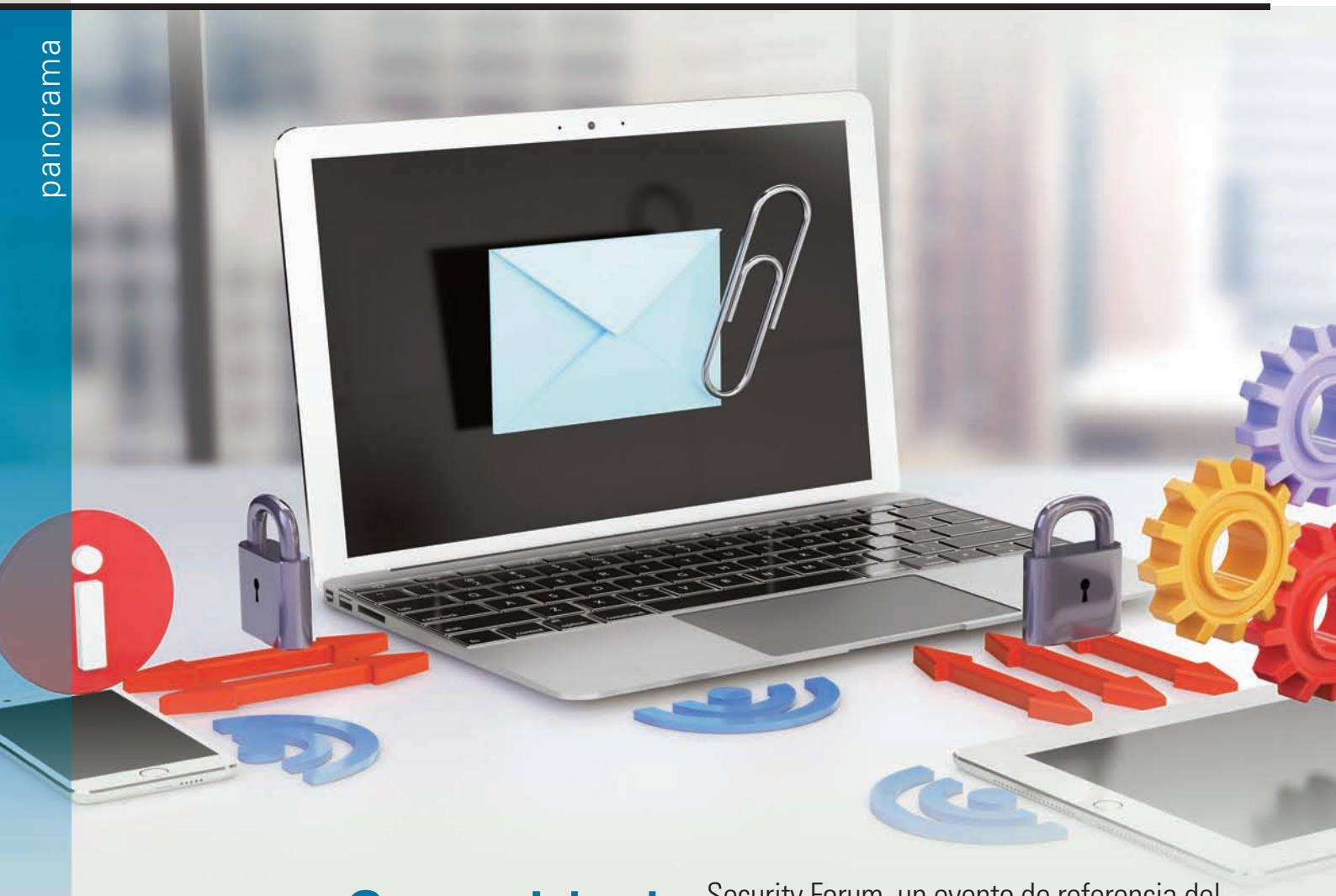
***¿Considera que el mundo de la seguridad está actualmente bien regulado en España? ¿Echa algo en falta en la legislación de nuestro país?***
El tema de la regulación debe ser dinámico y exige una participación de todos los sectores para evitar lagunas o un exceso de normativa. Quizás más rapidez en la adopción de cambios.

***De cara al futuro, ¿cómo cree que evolucionará el mundo de la seguridad? ¿Cree que todavía hay mucho por hacer en este ámbito en España?***
Actualmente hay una creciente preocupación por la amenaza terrorista y en los próximos meses es probable que surjan nuevas medidas y controles de seguridad en infraestructuras críticas, aeropuertos, etc. En España se tiene experiencia en la lucha contra el terrorismo local,


Puerta instalada en Barcelona.

pero los métodos y el sacrificio humano que llegan a emplear otros grupos requiere mayor control y precaución, sobre todo en la investigación y la prevención.

***¿Quiere añadir alguna cosa más antes de dar por finalizada esta entrevista?***
Simplemente recordar a los propietarios que si tienen un inmueble vacío y desean conservar su valor o reducir costes en seguridad, en VPSitex podemos ayudarles.■



# Seguridad Privada, eje de la tercera edición de Security Forum

Security Forum, un evento de referencia del sector de la seguridad en España, celebró su tercera edición los días 27 y 28 de mayo en el Centro de Convenciones Internacional de Barcelona. Esta edición, la más numerosa en número de expositores y visitantes, ha logrado unas cifras de récord: 5.512 visitantes, un 37% más que en la edición anterior, 245 congresistas acreditados para Diálogos Security Forum y 73 expositores. Así, Security Forum es ya un punto de encuentro para todos los profesionales de un sector vivo y en crecimiento.

**Nina Jareño**

"Security Forum es un evento consolidado que muestra como el sector de la seguridad empieza a remontar tras una dura crisis". Con estas palabras inauguró Security Forum el presidente del evento, Eduard Zamora, una feria que ha logrado unas cifras que son sinónimo de éxito. "España destaca a nivel internacional en el ámbito de la seguridad privada, facturando en 2014 3.300 M€. Vivimos en un entorno de superación donde las amenazas no entienden de fronteras, por lo que el sector debe centrarse en cuatro ejes: colaboración, conocimiento, negocio y networking", indicó.

"La seguridad privada ha vivido una gran evolución en España, es un sector maduro y profesionalizado con una legislación que ha servido de modelo inspirador para otros países. La nueva regulación es fruto de las exigencias de la sociedad, de la búsqueda de nuevas soluciones y un motor de dinamización de actividad económica, empresarial y laboral", señaló María de los Llanos de Luna, delegada del Gobierno en Cataluña. "El nuevo modelo legal de seguridad permite una eficiencia máxima y dota al sector del respaldo jurídico para evitar el intrusismo. La regulación sólo se entiende si va ligada a la colaboración y coordinación público-privada".

## Retos de la Protección de Datos en la seguridad privada

La nueva Ley de Seguridad Privada fue el eje de las jornadas y actividades paralelas que se realizaron durante el Secutiry Forum. Diálogos Security Forum, con 245 congresistas acreditados, abordó la Protección de Datos como un elemento fundamental de la sociedad actual. José López Calvo, subdirector general de Inspección de Datos de la Agencia Española de Protección de Datos, hizo balance de la nueva regulación de seguridad privada. "A pesar de que se establecen ciertas mejoras, hay 3 conclusiones que se extraen de la nueva regulación: hay varios conceptos jurídicos indeterminados en la ley, las medidas de seguridad han cambiado por la aparición de fenómenos como el cibercrimen y existe una necesidad palpante de adaptarse a los avances tecnológicos".

Para López Calvo, algunos artículos son poco concretos y pueden interpretarse de distintas formas. Por ejemplo, los límites de la utilización de imágenes en la vía pública (sólo legal si existe normativa específica) o privada por parte de los vigilantes o empleadores "no son específicos", así como el uso de carcasas o la adecuación de las actividades de detectives y servicios de investigación privada. "La libertad de información frente al derecho a la intimidad sigue siendo un choque de trenes, sobre todo cuando se trata de imágenes o videos en internet, por lo que debería haber límites temporales en ciertos casos".

España es el segundo país del mundo con más ciberataques, que ascendieron a 400.000 M€ en 2014. "Hay que tomar medidas de índole técnica y organizativa para asegurar la seguridad de los 3 millones de usuarios y 10.000 millones de equipos conectados al Internet del país", concluyó.

## Smart Cities, Seguridad Pública y Seguridad Privada: el camino hacia la optimización de recursos

Ramón Martín de Pozuelo, jefe de estudios de postgrado de Smart Cities de la Universitat Ramón Llul, destacó las ventajas de las Smart Cities como forma de administrar la seguridad. "No se trata sólo de tecnología, necesitamos colaboración público-privada para avanzar. El


Marta Reyero, periodista de Informativos Cuatro, fue la moderadora de Diálogos Security Forum.


Representantes de distintos Cuerpos y Fuerzas de Seguridad expresaron opiniones sobre la nueva normativa estatal.

paradigma ha cambiado y hemos pasado de un control físico a uno remoto. La ciudadanía está preocupada por su seguridad, por quién usa sus datos. Es un tema crítico que hay que abordar ya, su gestión debe estar planificada previamente por la administración para que no se usen de forma maliciosa".

Para Blanca Moreno, gerente de la consultoría Mètodes i Tècniques, "es necesaria una mayor transparencia. Hay que invertir en conocimiento y en estudios sobre Smart Cities porque en los entornos urbanos la masa crítica es cada vez mayor, lo que significa que la capacidad de gestión de la seguridad debe sincronizarse entre todas las fuerzas para obtener resultados. La sociedad tiene que ver a los Cuerpos y Fuerzas de Seguridad y a la legislación como un amigo, no como un enemigo, por lo que hay que cambiar mentalidades".

A este debate, May Escobar, coordinadora de la Red Española de Ciudades Inteligentes (RECI) añadió la importancia de "pensar en la seguridad desde el inicio de cada proyecto de Smart City, tener niveles de codificación podría ser una eje de futuro. Hay que cambiar la cultura, renovar la administración porque las estructuras de trabajo son antiguas. Precisamos más relación entre ciudadanos, empresas y entes públicos".

## El nuevo reglamento de Seguridad Privada: la visión de los Cuerpos y Fuerzas de Seguridad

La Ley de Seguridad Privada afecta directamente a los Cuerpos y Fuerzas de Seguridad del todo el Estado. Por eso, representantes de varios Cuerpos asistieron a un debate en el que ofrecieron sus distintos puntos de vista. Manuel Yanguas Menéndez, inspector del Cuerpo Nacional de Policía, destacó la eliminación de trabas burocráticas que supone el nuevo reglamento. "La legislación ayuda a evitar el intrusismo, recoge las demandas de los profesionales, apuesta por la formación continua y especializada y otorga mecanismos de organización institucional". Según datos ofrecidos por Yanguas, 119 empresas se dieron de alta durante el año pasado (91 en 2013 y 59 en 2012) y a 31 de diciembre de 2014 había en España 342.368 profesionales habilitados y 1.535 empresas de seguridad autorizadas (un 2,6% más que en 2013 cuando eran 1.495), 418 empresas de vigilancia y protección, 1.227 de instalación y mantenimiento, 156 centrales de alarmas, 46 de transporte de explosivos, 6 de transporte de fondos, 73 de protección de personas, 13 de depósitos de explosivos, 5 de depósito de fondos, 1.372 despachos de detectives y 27 sucursales. Asimismo, actualmete existen 1.057 centros de formación y 25 empresas no autorizadas.

César Álvarez, coronel jefe del Seprose de la Guardia Civil, indicó que "es tremendamente complejo desarrollar un reglamento, pero éste merece una felicitación. Aún así, falta una guía que desarrolle el camino a seguir ya que es difícil aplicar el reglamento en algunas ocasiones. La coordinación es fundamental, para no invadir competencias de otros Cuerpos o Fuerzas, y eso se echa en falta en el texto".

El jefe de la UCSP de los Mossos d'Esquadra, Carles Castellano, subrayó la agilidad y la simplificación de los trámites, así como la mejoría en seguridad informática. "La complementariedad que ofrece la colaboración entre la seguridad privada y la pública se debe aprovechar. Que la seguridad privada pueda actuar en terreno de la pública es positivo, siempre que se haga bajo sus instrucciones".

Por último, Francisco Llaneza, jefe de la USP de la Ertzaintza, afirmó que "el reglamento se ajusta a la realidad y es una herramienta de coordinación". En este sentido, el jefe de la USP explicó los objetivos que la Ertzaintza se marca con el nuevo reglamento: "Estamos preparando un decreto enmarcado en la Ley que recoja los atributos de las Comunidades Autónomas y determine los órganos dentro del Departamento de Seguridad a los que les corresponda ejercitar estas competencias, así como ejecutar las sanciones". Además de este decreto, el jefe de la USP indicó que la coordinación y la participación "son y serán elementos protagonistas en nuestra normativa. Crearemos una Comisión Mixta de Coordinación de la Seguridad Privada en Euskadi y una orden de menciones honoríficas, desarrollaremos el Plan Lagundu y llevaremos a cabo charlas sobre temáticas de interés como el islamismo radical, además de seguir apostando por centros formativos y despachos de detectives.■

AECRA

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

# AVALANDO SOLUCIONES GLOBALES PARA LA SEGURIDAD

- Consultoría legal en seguridad privada
- Programa global de Seguros
- Implantación y desarrollo de procesos de contratación electrónica
- Formación especializada de Seguridad
- Auditorías LOPD
- Gestión continua LOPD 365
- Copia Remota LOPD
- SaaS-Box
- Compliance Officer
- Defensa jurídica
- Planes de seguridad ante crisis

## Trabajando por la mejora de la seguridad privada desde el año 2006

Abogados ce consulting

evicertia · EVIDENCIAS CERTIFICADAS

VALVONTA Auditoría y Seguridad

SaaS spain

UNED Centro de Formación en Seguridad Privada

**CONTACTO e INFORMACIÓN**

Tel. 91 5339779 • servicios@aecra.org • www.aecra.org

# VideoXpert, nuevo sistema de gestión de vídeo de Pelco

VideoXpert es el nuevo sistema de gestión de vídeo de Pelco que gracias a su diseño intuitivo y su sencillo manejo permite a los profesionales de la seguridad tomar rápidas y eficaces decisiones para mejorar la eficiencia de su negocio. Su potente capacidad de integración posibilita hacer uso de la experiencia de terceros proveedores para personalizar sus funciones y lograr la máxima flexibilidad.

**Mª Carmen Fernández**

El objetivo de Pelco con VideoXpert es renovar su plataforma VMS, de modo que puedan responder a las necesidades de todos sus clientes con una nueva solución que se adapte a cualquier aplicación. VideoXpert es un nuevo sistema de gestión de vídeo que proporciona una experiencia de usuario única con un manejo sencillo e intuitivo. VideoXpert está marcando los estándares del mundo de la seguridad en este mercado. Está diseñado para ser un sistema flexible y adaptable a las necesidades del cliente en cada momento. Sus principales características son:

- Experiencia de usuario inigualable.
- Diseño intuitivo que requiere poca formación.
- Arquitectura abierta integrable con terceros mediante plug-ins.
- Escalable modularmente.
- Puede desarrollarse como una solución software o mediante el hardware de Pelco.
- Migración sencilla para usuarios actuales de Pelco.
- Diseñado para ser fiable.

"VideoXpert es un sistema escalable, podemos empezar con diez cámaras con un sólo operador y extenderlo. Cuando decimos que es expandible hasta niveles indefinidos, es porque tenemos un sistema beta de 1.500 cámaras y sistemas simultáneos. VideoXpert es sencillo. Podemos proporcionar estaciones de trabajo de hasta seis monitores que funcionan como un único sistema en el escritorio. Los monitores tienen un único procesador de manera que podemos visualizar 1080p en un sólo monitor. Cada monitor es flexible, podemos

visualizar cualquier cámara en cualquiera de ellos, arrastrar cámaras de unos a otros, etc. El principal potencial de Pelco está en la visualización de vídeo y en la recuperación de vídeo grabado", afirma Mark Pritchard, marketing director Emea de Pelco.

VideoXpert.

Por otra parte, Mónica Muñoz, technical sales engineer de España y Portugal de Pelco, añade: "No somos expertos en análisis de vídeo, ni somos una compañía de control de accesos. Trabajamos con una plataforma fácil SDKs que nos permiten integrarnos con éstas soluciones. A día de hoy, tenemos integraciones ya funcionando con sistemas de reconocimiento de matrículas, por ejemplo, y más sistemas que vendrán durante los próximos meses. VideoXpert ha sido concebido para aprovechar los sistemas Enduro que tenemos por el mundo. En Turquía se han instalado 56 sistemas por todo el país. Podemos integrar cualquier sistema en una única plataforma VideoXpert. Bajo el lema 'The Gateway to performance', VideoXpert es una plataforma desarrollada a través de la experiencia que hemos adquirido con nuestros clientes. Está basada en una arquitectura abierta para poder introducir otros sistemas de terceros que dan un único punto de trabajo para el operador".

## Reproducción síncrona

VideoXpert permite sincronizar el vídeo sobre la marcha de manera que añade dinámicamente nuevas cámaras a grupos que ya están sincronizados. Además, también permite otras funciones como mantener la sincronización mientras se conmuta entre vídeo en vivo y vídeo grabado. Por último, también cuenta con un único conjunto de controles de reproducción.

## Gestión de incidencias

Gracias al gestor de incidencias de VideoXpert, los profesionales cuentan con un modo de investigación para localizar y organizar rápidamente el vídeo, además de organizar dichos vídeos en listas de reproducción para crear una investigación completa. El sistema permite reproducir el vídeo de manera sincronizada para capturar la misma escena desde diferentes ángulos, además de permitir la exportación o almacenamiento de las listas de reproducción para una posible recuperación en el futuro.

> Los operadores tienen la posibilidad de filtrar etiquetas para encontrar rápidamente la cámara que buscan

## Etiquetado

Las etiquetas son una herramienta útil que permite al sistema clasificar de manera rápida las diferentes cámaras que estén operando. Dichas etiquetas específicas de cada sistema son configuradas y organizadas por los administradores desde el Admin Portal de VideoXpert. Además, los operadores tienen la posibilidad de filtrar etiquetas de manera que encuentren rápidamente las cámaras que buscan. Por último, también se asignan IDs a las cámaras para poder llamarlas por número.

Cámaras de Pelco.

### Mapping interactivo embebido

Este sistema de gestión de vídeo de Pelco permite:

- Importación de archivos de CAD, seleccionando las capas apropiadas.
- Exportación con archivo CAD con una nueva capa de cámaras.
- Mapas múltiples para representación de áreas críticas.
- Es posible mostrar capas en cualquier celda.

### Plug-ins de terceros

VideoXpert cuenta con una única interfaz y funcionalidades añadidas mediante la integración con partners como por ejemplo: Econnect proporciona superposición de datos de juego y POS, Platesmart captura matrículas de vehículos, Lenel registro de eventos de control de accesos y su asociación con el vídeo, y AgentVI, que permite la monitorización y búsqueda de eventos de Análisis de Vídeo.

### Configuración de seis monitores

VideoXpert mantiene la integridad del vídeo gracias a la decodificación distribuida entre monitores. Permite una gestión efectiva de su aplicación sin la carga que implica la decodificación de vídeo.

## VideoXpert mantiene la integridad del vídeo gracias a la codificación distribuida entre monitores

### Plan de migración a VideoXpert

Pelco propone unificar varias redes VMS en una única instalación y el acceso a cualquier cámara de sistemas agregados con VideoXpert. Con la migración y agregación de sistemas Endura y DS, Pelco pretende ofrecer un control total del sistema mediante la gestión centralizada.

### Agregación

VideoXpert permite la agrupación y gestión centralizada de múltiples sistemas, con acceso a cualquier cámara desde cualquier ubicación. También permite el acceso centralizado y la gestión de sistemas Endura y DS, a través de una aplicación de cliente de fácil manejo, proporcionándole a dicho cliente las funcionalidades que necesite. ■

Cuerpos de Seguridad · Policía · Bomberos
Antidisturbios · Motoristas · Tiro · Pilotos

# DRAGON
GLOVES


**Atención al cliente**
*Customer service*
**+34 947 47 42 26**

www.dragongloves.com
dragongloves@dragongloves.com

www.dragonhands.es
@DragonGloves
http://www.facebook.com/Dragon.Gloves


# Una nueva era para la videovigilancia

La revista BBC News acaba de publicar un artículo en su página web titulado "¿El fin de la era CCTV?" En el artículo se recoge la opinión de algunas autoridades locales del Reino Unido que se están cuestionando posibles inversiones futuras en videovigilancia.

¿Esto significa que nos acercamos al fin de un largo período de crecimiento sostenido para el sector de la videovigilancia? Peter Ainsworth, Head of Product and Marketing para la división de soluciones de seguridad de Samsung Techwin, afirma con plena confianza que no hay nada más lejos de la realidad.

"Si bien es cierto que en los últimos años las inversiones en videovigilancia del casco urbano han representado una gran fuente de ingresos para toda la cadena de suministro de soluciones de videovigilancia, tal y como afirma en el artículo de la revista BBC News un portavoz de la Asociación Británica de Seguridad (BSIA por sus siglas en inglés), el número de cámaras en el sector público es superior al número de cámaras en el sector privado en una proporción de 70 a 1.

El sector privado sigue invirtiendo y confiando en las soluciones de videovigilancia como una ayuda para detectar y evitar actividades delictivas. Además, la última generación de cámaras de red IP de alta definición goza de gran popularidad entre los usuarios que necesitan disponer de imágenes con calidad de prueba pericial.

## La plataforma abierta abre las puertas a una nueva era para la videovigilancia

La gran capacidad de procesamiento de los chipsets DSP integrados en la última generación de cámaras de alta definición ofrece grandes oportunidades para que los usuarios disfruten de un mayor valor añadido de sus sistemas de videovigilancia.

Es una situación en la que todos salen ganando, incluidos los fabricantes de cámaras y dispositivos de grabación, porque entienden el valor que aporta la colaboración entre empresas especializadas en desarrollos de software. Esto es, sin duda, una oportunidad para integradores e instaladores de sistemas de videovigilancia, tanto si trabajan en el sector de las tecnologías de la información como en el sector electrónico tradicional.

## Infinidad de posibilidades

Cada vez más oiremos hablar de la plataforma abierta porque es una clara oportunidad para beneficiarse de la capacidad de procesamiento del chipset DSP de una cámara, que descarga y ejecuta aplicaciones punteras de forma similar a cómo se añaden aplicaciones a un smartphone. Pero con una ventaja añadida: se reduce la necesidad de contar con servidores dedicados a la analítica de vídeo en hasta un 90%.

La mayoría de cámaras de plataforma abierta que están actualmente disponibles en el mercado solo pueden ejecutar una única aplicación. Sin embargo, la capacidad de procesamiento del chipset DSP WiseNetIII de Samsung Techwin ofrece a los clientes la opción de ejecutar múltiples aplicaciones a la vez.

## Soluciones de videovigilancia a medida

Poder usar aplicaciones integradas crea nuevas oportunidades para que las cámaras realicen múltiples tareas. Además, varios departamentos de un negocio u organización pueden recopilar y analizar simultáneamente información valiosa para la gestión empresarial mediante distintas aplicaciones especializadas en analítica de vídeo. También ofrece a los directores de operaciones la posibilidad de mejorar la eficacia en áreas como control de procesos, seguridad e higiene en el trabajo, marketing y gestión de recursos humanos, así como mejorar la capacidad de reacción del personal de seguridad para que actúen con rapidez y eficacia ante cualquier posible amenaza a la seguridad.

Los comercios minoristas, por ejemplo, pueden usar las cámaras con la plataforma abierta para integrarla con otros sistemas, softwares y tecnologías de la tienda como EAS, EPOS, control de accesos, reconocimiento automático de matrículas, reconocimiento facial, conteo de personas, mapas calientes y datos de recursos humanos. Y así analizar los patrones de flujo de clientes, gestionar colas o entender las implicaciones del comportamiento de los clientes en relación con la señalización de la tienda, su distribución y las promociones.

## Asegurando el futuro

Nuestro equipo de ingenieros de diseño está jugando un papel fundamental en la tarea de asegurar el futuro del sector de la videovigilancia porque ofrecen a instaladores e integradores de sistemas soluciones a medida, que satisfacen las necesidades de distintos sectores del mercado como, por ejemplo, el bancario, la educación y sanidad, el comercio minorista y el transporte, entre otros. Y por supuesto, para las autoridades locales que desean un mayor retorno de la inversión de sus sistemas de videovigilancia del casco urbano".■

# Francisco Arcia Ramírez, channel sales manager Iberia de Cyberoam

"Los incidentes de vulneración de datos y robo de credenciales son algunas de las tendencias de Ciberseguridad que van a predominar este año, sin duda"

Los constantes avances tecnológicos han permitido innumerables ventajas a los usuarios como la inmediatez y la mayor accesibilidad a cualquier tipo de información a través de Internet. Sin embargo, no hay que olvidar que esta facilidad de acceso a la red también puede ser utilizada con fines negativos, con lo que la seguridad se convierte en un elemento clave en la actualidad. Una de las empresas que se dedica a luchar contra estas amenazas es Cyberoam, una compañía que se encarga de mantener la seguridad de las organizaciones aprovechando la potencia de los procesadores multinúcleo. Su oferta de productos, los principales problemas de los Data Center o el origen de las amenazas son algunas de las claves que el channel sales manager Iberia de Cyberoam, Francisco Arcia Ramírez, ha explicado a Interempresas.

**María Fernández Peláez**

***La tecnología está en constante evolución, ¿qué es necesario para que los dispositivos de seguridad puedan mantener este ritmo tan cambiante?***

La seguridad será siempre un paradigma complejo, porque las amenazas están siempre cambiando, se reinventan y están en constante movimiento y trasformación. Los ecosistemas digitales están formados por elementos muy diferentes y las organizaciones requieren una respuesta dinámica en caso de que alguno sea afectado, la cual puede variar dependiendo de la metodología de ataque utilizado.

Cyberoam ofrece un conjunto de soluciones de seguridad que cubren diferentes tipos de amenazas, con la diferencia de que somos capaces de ofrecer esta protección integral en un único dispositivo en formato appliance. El enfoque se describe muy bien con las siglas UTM (Unified Threat Management, es decir, Gestión Unificada de Amenazas), siendo capaces de integrar varias capas tecnológicas que protegen las redes de las organizaciones, los dispositivos móviles y al usuario final en sí mismo.

Algunos fabricantes de tecnología de seguridad se han quedado estancados en la última década pero hoy en día hay que cambiar el enfoque de desarrollo de un producto e intentar entender y conocer los riesgos y amenazas avanzadas que sufren las organizaciones actuales así como las nuevas formas de negocio que demanda el mercado.

Son muchos los retos y tendencias que hemos visto en los últimos años como el Internet de las cosas (IOT) que ganará visibilidad tanto por sus avances como por sus vulnerabilidades. La Intervención Geo-Política es cada vez más habitual. Internet se ha convertido en una herramienta fundamental para las propagandas patrocinadas por el gobierno, espionaje y ataques cibernéticos. Los protocolos tradicionales siguen en la mira de las amenazas, algunos de ellos de código abierto, la transición de IPv4 a IPv6 trae brechas de seguridad latentes y además de las vulnerabilidades en los navegadores, también han aumentado los ataques del lado del cliente, explotando vulnerabilidades de las aplicaciones más utilizadas. Las pérdidas en el sector salud, el Malvertising y los ataques por email, iOS y Android están en el radar de los cibercriminales y los incidentes de vulneración de datos y robo de credenciales son otras de las tendencias de Ciberseguridad que van a predominar este año, sin dudas.

Uno de los mejores equipos de desarrollo, un roadmap agresivo, una filosofía de empresa acertada y una red de Partners que nos informa de lo que es útil y acertado en sus clientes nos ha permitido lanzar actualizaciones periódicas que incluyen entre otras cosas nuevas funcionalidades que solventan estos problemas y hacer de Cyberoam un producto cada vez más competitivo.

***Al igual que el mercado de la seguridad está en constante cambio, ¿se observa también una evolución en el Data Center? ¿En qué sentido?***

Para crecer en un negocio en expansión definitivamente hay que enfrentarse a la creciente demanda de consumo de recursos informáticos. Los equipos de IT están constantemente bajo presión para generar más potencia de cálculo con la actual infraestructura de servidores que tienen, una estrategia bastante común es apostar por la virtualización en estas organizaciones desembocando en la virtualización del Data Center.

La virtualización de un Data Center ayuda a las organizaciones a aumentar su eficiencia y rendimiento, además de ayudar a reducir la complejidad de su infraestructura, costes de administración, energía y refrigeración. Uno de los muchos beneficios de la virtualización es el uso inteligente de los principales servidores, utilizando los ciclos de CPU desaprovechados para hacer frente a un aumento de la demanda en lugar de añadir nuevos servidores.

En resumen, con la virtualización podremos aprovechar mejor el hardware, ya que un mal extendido en los Centros de Datos actuales es el gran número de servidores, muchos de ellos infrautilizados, además de tener otras ventajas respecto al aislamiento, flexibilidad, agilidad y portabilidad, pero….. ¿Qué pasa con la Seguridad?

***¿Cuáles son los principales problemas de los Data Center en la actualidad? ¿Qué soluciones existen para hacer frente a los mismos?***

Un Data Center actual puede experimentar problemas muy diversos entre los que quiero resaltar algunos de vital importancia:

- **Eficiencia energética:** Controlar el consumo de energía ayudará a un Data Center a ahorrar dinero y por ende a ser más competitivo en el mercado. Para reducir el consumo de energía, lo primero que hay que hacer es medirla teniendo en cuenta todos los elementos de consumo, equipos de IT, la infraestructura, ventilación, refrigeración, etc.
- **Monitorización:** Los posibles fallos del sistema requieren una respuesta proactiva, para ello se necesita una herramienta de visibilidad en tiempo real de todos los elementos críticos del centro de datos.
- **Capacidad de Planificación:** ¿Cómo saber si las instalaciones están realmente funcionando a su máxima capacidad? Una falta de visibilidad en este sentido desperdicia cientos de miles de euros en espacio no utilizado por no hablar de la pérdida de energía y refrigeración. Una correcta planificación y optimización permite explotar los recursos con todo su potencial ahorrando cantidades significativas de dinero. Por ejemplo, el conocer las fluctuaciones de temperatura en los pasillos fríos y calientes, el supervisar los generadores y su potencia de salida pueden proporcionar un indicador muy útil además de generar alarmas que se pueden enviar por e-mail, SMS, permitiendo establecer medidas preventivas que deben adoptarse para corregir los problemas antes de que se vuelvan críticos.

***¿Cuáles son las necesidades básicas de un Centro de Datos actual?***

Hay muchos tipos de Centros de Datos en la actualidad, y cada uno de ellos puede tener un objetivo y una visión diferente pero básicamente existen unos criterios básicos que deberían cumplir de forma general:

- Tendencia a la normalización y a la consolidación con el objetivo de lograr una mayor optimización de recursos y por ende un menor coste en el servicio ofrecido. Esto se logra reduciendo la cantidad de hardware, plataformas de software, herramientas y procesos dentro de un centro de datos. Normalmente se necesita disponer de tecnología de nueva generación que mejora la capacidad y el rendimiento actual teniendo en cuenta como un punto importante su usabilidad.
- Como ya hemos hablado anteriormente, la virtualización es un punto clave.
- La automatización en un centro de datos impacta directamente sobre el aprovisionamiento, las configuraciones, gestión de parches y versiones así como en el cumplimiento de normativas permitiendo una ejecución más eficiente.
- La seguridad informática en los centros de datos modernos es vital para la protección de las infraestructuras físicas y/o virtuales teniendo siempre en cuenta la seguridad física, la seguridad de la red y los datos así como la seguridad del usuario.

***¿Cuál suele ser el origen de las amenazas? ¿De dónde proceden? ¿Qué soluciones aporta Cyberoam contra las mismas?***

Entre las amenazas más comunes en los Centros de Datos se encuentran:

- **Ataques DDoS:** Básicamente son 'ataques distribuidos denegación de servicio' donde se ataca a un servidor desde muchos ordenadores para que deje de funcionar, casi siempre desbordando las peticiones que éste puede soportar. El verdadero origen de un ataque de este tipo es muy difícil de determinar ya que en muchas ocasiones se utilizan protocolos no orientados a la conexión permitiendo falsificar el verdadero origen de la conexión. Cyberoam ofrece un módulo Anti-DDos/DoS que protege las redes de las organizaciones ante ataques de este tipo tanto para el tráfico IPv4 e IPv6 mediante una configuración y ajustes adecuados en el Firewall.
- **Los ataques de aplicaciones Web:** Son los preferidos por los atacantes para infiltrarse en las redes corporativas y robar datos. Se utilizan técnicas como inyección SQL y cross-site scripting (XSS) que siguen siendo eficaces y fáciles de realizar. Cyberoam ofrece un Firewall de Aplicación Web mediante una suscripción más en sus dispositivos de seguridad de red (Next-Generation Firewalls / UTM) para proteger los sitios web y las aplicaciones basadas en entornos Web de las organizaciones contra los ataques, tales como la inyección SQL, cross-site scripting (XSS), URL parameter tampering, el secuestro de sesión, buffer overflow, y más, incluyendo las vulnerabilidades OWASP Top 10 de aplicaciones web.

- **Exploits para infraestructura DNS:** Los servidores DNS se han convertido en un blanco habitual por dos razones principales. En primer lugar, los atacantes saben que si interrumpen el acceso a los servidores DNS o envenenan las cachés DNS, pueden afectar el servicio de Internet que se ofrece a los usuarios. El segundo motivo es llevar a cabo ataques de amplificación DNS donde los atacantes falsifican la dirección IP de su verdadero objetivo para enviar respuestas mucho más grandes a la víctima y usando los servidores potentes para inundar la red de la víctima con el tráfico DNS. El sistema IPS (Intrusion Prevention System) de Cyberoam protege la red de conexiones maliciosas haciendo coincidir el tráfico de la red con las firmas de su base de datos del IPS. Estas firmas se desarrollan para aumentar significativamente el alcance de la detección y reducir las falsas alarmas.
- **Encriptación SSL:** Los atacantes están recurriendo cada vez más a la encriptación SSL para ocultar los ataques a los dispositivos de seguridad. Las organizaciones necesitan inspeccionar el tráfico SSL saliente de los usuarios internos, y el tráfico SSL entrante a los servidores corporativos, para eliminar este punto ciego. Cyberoam permite la inspección de certificados SSL junto con las políticas de filtrado para controlar el tráfico SSL.

Un modelo de Firewall Virtual como el de Cyberoam ofrece las mismas funciones de seguridad disponibles en sus dispositivos Hardware, solo que de forma virtualizada, utilizando además una tecnología de seguridad de Capa 8 basada en la identidad de los usuarios. Lo más importante para el tipo de entornos anteriormente detallados es analizar el tráfico entre máquinas virtuales y tener la posibilidad de un Firewall granular con aplicación de políticas de seguridad en este tipo de tráfico, además de permitir registros e informes, que permitan al Data Center tener una visibilidad de lo que ocurre en su red y cumplir con las normativas de seguridad más exigentes. Para garantizar una protección adecuada ante la gran diversidad de amenazas a las que se puede enfrentar un Data Center se recomienda contar con múltiples características de seguridad, como es el caso de un IPS o un Web Application Firewall, integrado en un único dispositivo virtual si es posible, para una mayor comodidad, gestión centralizada y ahorro de costes.

Por otro lado los administradores deberían poder segmentar la consola de administración en la DMZ, enrutando todo el tráfico a través de estos cortafuegos virtuales, y permitiendo separar las funciones de administración basándose en roles, es decir, definir hasta dónde puede administrar, controlar o tener visibilidad cada persona dentro de la organización.

Por último se debe tener en cuenta la posibilidad de poder escalar fácilmente dichas soluciones de seguridad y de ir creciendo a medida de que su negocio también lo hace, un modelo de licenciamiento que se basa en el número de CPU virtuales es muy recomendado. Se debería cuidar que la solución de seguridad elegida se pueda implementar en el sistema de virtualización actual, pero también en aquellos más usados por si en un futuro se decide cambiar, VMWare, Hyper-V, Xen Server y KVM son opciones a valorar sin dudas.

El origen de muchas de estas amenazas son, en ocasiones, los que operan y controlan una Botnet, Grupos Criminales, Hackers, Trabajadores Internos, Gobiernos, Phishers, Spammers, creadores de Spyware o malware y Terroristas.

"Las empresas ven el Modelo BYOX como una herramienta para aprovechar la inteligencia de los dispositivos inteligentes personales"

***Cada vez son más los usuarios que integran sus dispositivos personales al ámbito laboral. En materia de seguridad, ¿cómo se hace frente al denominado BYOD? ¿Cuáles son las ventajas e inconvenientes de esta tendencia en fase de crecimiento?***

Personalmente me gusta hablar más de BYOX que de BYOD. El Modelo BYOX es sinónimo de 'evolución de la forma de trabajo'. Además, las empresas ven el Modelo BYOX como una gran herramienta para aprovechar la inteligencia de los dispositivos inteligentes personales. Los soportes BYOX equipan a los usuarios para trabajar con la X de su elección, donde X puede ser un dispositivo, software, aplicaciones, servicios o un kit de herramientas.

Como resultado, las herramientas de trabajo personales han proliferado rápidamente en las culturas de todas las empresas. Antes de integrar el Modelo BYOX se deben tener muy en cuenta una serie de aspectos; es imprescindible para encontrar el equilibrio correcto de las soluciones de movilidad de usuarios y las necesidades de negocio de la organización.

Con la llegada del Cloud y la presencia de los dispositivos móviles personales, las redes corporativas están más expuestas a los ataques que conducen a la violación de datos o robo de datos. Un informe de 2014 del Instituto Ponemon e IBM sugiere: "El coste total promedio de una violación de datos para las empresas que participaron en esta investigación se ha incrementado un 15 %, hasta 3,5 millones de dólares. El coste medio pagado por cada registro perdido o robado que contiene información sensible y confidencial ha aumentado más del 9 % teniendo un precio de 136 dólares en 2013 hasta 145 dólares en la actualidad."

La Seguridad de la red era una preocupación significativa incluso con el legado de los dispositivos de IT, pero con el BYOX la amenaza tiene ahora una importancia mayor. A fin de garantizar una Continuidad del Negocio, las organizaciones permiten a los usuarios acceder a los recursos corporativos utilizando sus dispositivos personales. De esta manera, la responsabilidad de los datos críticos de la organización está en manos de los empleados. Intencional o no, la pérdida de datos a través de dispositivos personales de los empleados es el quid de la cuestión.

Utilizando la solución de Cyberoam con su tecnología Capa 8, siendo una firewall basado en la identidad del usuario, Cyberoam proporciona una seguridad perimetral absoluta a las empresas. Cyberoam apoya y potencia la implementación del BYOX con un enfoque de la seguridad basada en su mecanismo de identidad inteligente y ofrece información en tiempo real mediante una herramienta de monitorización que permite al administrador tener una visibilidad completa de dispositivos, datos y usuarios de la red.

- **Visibilidad de los Dispositivos:** La identificación del dispositivo o tipo de cliente proporciona un análisis detallado de los dispositivos BYOX, ayudando al administrador a asegurarse de que sólo los dispositivos autorizados accedan a la red de la empresa. Cyberoam no sólo detecta el tipo de dispositivo que se ha utilizado, incluso se podrían definir políticas corporativas basadas en el tipo de dispositivos en uso.
- **Filtrado de aplicaciones:** La tecnología de filtrado de aplicación en Cyberoam reconoce las aplicaciones móviles en diferentes plataformas. La visibilidad de las aplicaciones ayuda al administrador a comprender el uso de cada aplicación y la creación de políticas específicas para aplicaciones que usan los usuarios. El uso del motor avanzado de clasificación de aplicaciones en Cyberoam, basado en Micro-Apps HTTPS como el Chat de Facebook, permite una gestión y control de las subidas de video en Facebook o el Chat de Google por ejemplo. Estas funcionalidades permiten al administrador crear políticas granulares para un usuario en concreto o un grupo de ellos.
- **Conectividad y Continuidad:** Cyberoam ofrece una gama de opciones VPN que facilitan el acceso en cualquier momento, en cualquier lugar y desde cualquier dispositivo, asegurando operaciones comerciales de una forma ininterrumpida, una productividad mejorada y un menor coste de las operaciones, reduciendo al mínimo los gastos de viajes y de infraestructura.
- **Anti-malware y anti-spam:** Cyberoam ofrece una seguridad completa de correo electrónico, previniendo formas sofisticadas de amenazas de hora cero y ataques combinados que de spam, botnets, phishing, spyware y otros.Cyberoam adopta un mecanismo 2FA para asegurar la solidez de la autenticación donde se autorizan a los usuarios locales y móviles que acceden a los negocios a través de VPN.

"El Web Application Firewall de Cyberoam tiene la fortaleza en la capa de aplicación (Capa 7) frontal, salvaguardando así su servidor Web"

cepretec
Garantía de protección

# Todos nuestros servicios a tu alcance

## Auditoría y control

- Control de Nuevas Instalaciones
- Auditoría de instalaciones existentes
- Estudios de aplicación de reglamentación


## Planes de autoprotección

- Elaboración
- Auditoría / Revisión
- Implantación
- Mantenimiento

## Pruebas sobre instalaciones de PCI

- Recepción de instalaciones
- Prueba Door Fan Test
- Descarga real de gases con medición de concentración
- Pruebas de detección con humo real
- Endoscopias

SERVICIOS TÉCNICOS CEPRETEC, S.L
Av. del General Perón, 27 5ª planta - 28020 Madrid
Tlf.: 91 593 02 08 - www.cepretec.com

cepreven grupo

***La adopción de infraestructuras virtualizadas por parte de las organizaciones también es un fenómeno en crecimiento debido a la constante evolución tecnológica. ¿Cuáles son los pros y los contras de este hecho para la seguridad de las empresas?***

Las redes virtuales de un Data Center son propensas a ataques como hyperjacking y exploits que atacan vulnerabilidades en el propio hipervisor, la consola de administración y el sistema operativo para invitados; los riesgos de seguridad se derivan de la pérdida de la separación de funciones entre seguridad / seguridad de la red y operaciones; y entre los ataques a servidores virtualizados y las aplicaciones llevadas a un entorno web.

Un dispositivo externo de seguridad en formato hardware carece de la capacidad de escanear el tráfico entre máquina virtuales, dejando a las organizaciones inconscientes de cualquier violación de seguridad en su infraestructura virtualizada. Como las políticas de seguridad no se pueden aplicar entre entidades virtuales utilizando un appliance externo de seguridad en formato hardware, una sola máquina virtual comprometida puede infectar a todo el centro de datos, impactando directamente sobre el negocio. Además, la organización no tendrá registros e informes sobre el tráfico de red para soportar un análisis forense en caso de violación de la seguridad y mostrar si se cumple con la normativa de seguridad de una forma adecuada o no.

Lo ideal para proteger este tipo de entornos y ofrecer una seguridad adecuada es implementar un Firewall de Nueva Generación o UTM que ofrezca seguridad de red con tecnología puntera en la industria especialmente adaptada a Data Centers virtuales, y con un Modelo 'Security-in-a-Box' puesta a punto para empresas de tipo MSSP, y con un concepto 'Office-in-a-Box' fácil de implementar, configurar y desplegar.

***¿Cuál es el funcionamiento de los ataques DoS y DDoS? ¿Qué soluciones ofrece Cyberoam frente a estas amenazas?***

Los ataques de Denegación de Servicio (DoS) y ataques distribuidos de denegación de servicio (DDoS) han aumentado en número en los últimos años. En el pasado sólo las personas con conocimientos especializados y una buena cantidad de recursos eran capaces de lanzar este tipo de ataques de gama alta. Hoy en día, cualquier persona con acceso a Internet y un mínimo de conocimientos técnicos puede ejecutar muy bien un ataque de este tipo y tener éxito. De hecho, estos ataques se han convertido en una herramienta favorita no sólo entre las empresas criminales

y ciberdelincuentes, sino también entre clientes descontentos, ex empleados y manifestantes sociales.
Según las estadísticas, el 35% de las organizaciones experimentó un ataque DDoS en 2012. De los encuestados, un asombroso 39% eran minoristas y el 41% eran empresas de comercio electrónico. ¡Dichas interrupciones podrían costar entre 50.000-100.000 dólares por hora! Podemos ver que ya no es un fenómeno raro. Estos ataques podrían afectar a cualquier organización (grande o pequeña) y en cualquier lugar. La próxima víctima podría ser también su red.
Normalmente nos concentramos en fortalecer nuestras defensas contra posibles ataques, llenamos los agujeros, y comprobamos todos los rincones de nuestra red pero… ¿Alguna vez pensaste que podríamos ser los culpables? ¿Nuestros recursos pueden ser explotados, nuestras propias defensas pueden ser utilizadas contra nosotros para causar estragos en otras partes? Existen redes botnets donde las máquinas vulnerables están infectadas y convertidas en 'zombies', y luego controlados remotamente por botmasters para llevar a cabo sus actividades maliciosas. Bueno, ¿Y si los recursos dentro de la red o la totalidad de su propia red se han enrollado en una botnet? Cyberoam resuelve este problema de raíz mediante la prevención. Se niega el acceso a los robots (códigos maliciosos que infectan las máquinas vulnerables) en la misma puerta de entrada a la red. Lo hace con la ayuda de sus servicios como el Firewall basado en identidad de del usuario 'Capa 8', Web Application Firewall, Sistema de prevención de intrusiones, Anti-Virus, Anti spam, etc. El Sistema de prevención de intrusiones de Cyberoam está equipado con anti-spyware y firmas-DDoS que impiden que los robots entren en su red. Cualquier intento malicioso en la red, o cualquier recurso vulnerable que pueda convertir su red en una botnet se controla en la puerta de enlace. Más allá de eso, Cyberoam permite crear firmas IPS personalizadas usando en un umbral basado en origen y destino. Éstas te permiten diseñar defensas específicas para el tipo de tráfico que exista en su red.
Mayormente los bots infectan las máquinas con malware que vienen en enlaces de correos spam que conducen a sitios web maliciosos o mediante la descarga de aplicaciones maliciosas. Por lo tanto, el Gateway Anti-Virus de Cyberoam, Gateway Anti Spam y Web y los módulos de filtrado de aplicaciones proporcionan una capa adicional de protección contra malware, spam y sitios web maliciosos / apps respectivamente, previniendo la proliferación de todo tipo de robots en la red en la propia puerta de enlace.
Mientras el Anti Virus de Cyberoam y el Anti Spam protegen la entrada de los robots, el Web Application Firewall de Cyberoam tiene la fortaleza en la capa de aplicación (Capa 7) frontal, salvaguardando así su servidor Web. Basado en un detector de flujo intuitivo en el sitio web, el WAF garantiza la inviolabilidad de las Aplicaciones Web analizando la respuesta a las peticiones del servidor, protegiéndolos contra cualquier tipo de manipulación por parte de las entidades maliciosas.

Los sistemas heredados han demostrado ser insuficientes en contra ataques DoS y DDoS. Dichos ataques están tomando formas nuevas y cada vez están más evolucionados, las soluciones de seguridad de red tienen que prepararse para luchar contra ellos a múltiples niveles. Cyberoam, con su Firewall ofrece una inspección de los paquetes que llegan a su red, analizando las aplicaciones y la actividad del usuario. El Firewall permanece en un estado constante de alerta contra la entrada de cualquier tipo de tráfico sospechoso, evitando así el DoS, DDoS y ataques de IP Spoofing.
Cyberoam permite a los administradores configurar los ajustes de denegación de servicio a través del cual se pueden controlar los paquetes de entrada a su red. Esto permite prevenir contra las capas 3 y 4 contra ataques como SYN, UDP, TCP, ARP o ICMP flood, redirección de paquetes ICMP, etc. ■

Pueden leer la entrevista completa en
**www.interempresas.net**

# El Ayuntamiento de Vitoria-Gasteiz confía en Mobotix para proteger el acceso al casco medieval y a la Catedral Vieja

Mobotix, el mayor fabricante mundial de sistemas en red de videovigilancia de cámaras megapíxel, ha sido elegido para la puesta en marcha de un sistema de control de acceso al casco medieval de Vitoria-Gasteiz. La catedral de Santa María de Vitoria, conocida popularmente como Catedral Vieja, es un templo católico situado en Vitoria-Gasteiz, la capital de Álava. Es conocida como la Catedral Vieja, para distinguirla de la Catedral Nueva, dedicada a la Inmaculada Concepción de María y construida en el siglo XX en estilo neogótico.

En 1994 fue cerrada al público para llevar a cabo un proceso de restauración integral que finalizó en 2014. Así, 20 años después la Catedral Vieja vuelve a ofrecer cultos. Parte del proceso de restauración ha contado con la instalación de unas rampas y de un ascensor para facilitar el acceso a la catedral. Al mismo tiempo, se proporciona a los vecinos y visitantes del Casco Medieval de un elemento que ayuda a salvar el desnivel existente dentro del mismo. Debido a la existencia de antecedentes de actos vandálicos contra el mobiliario urbano se tomó la determinación de instalar un sistema de videovigilancia que pudiera proteger los elementos de la vía pública, concretamente las rampas y el ascensor que sirven para acceder a la catedral. Que además son elementos delicados y caros (el ascensor está realizado en cristal). Es ahí es donde entra en juego Mobotix.

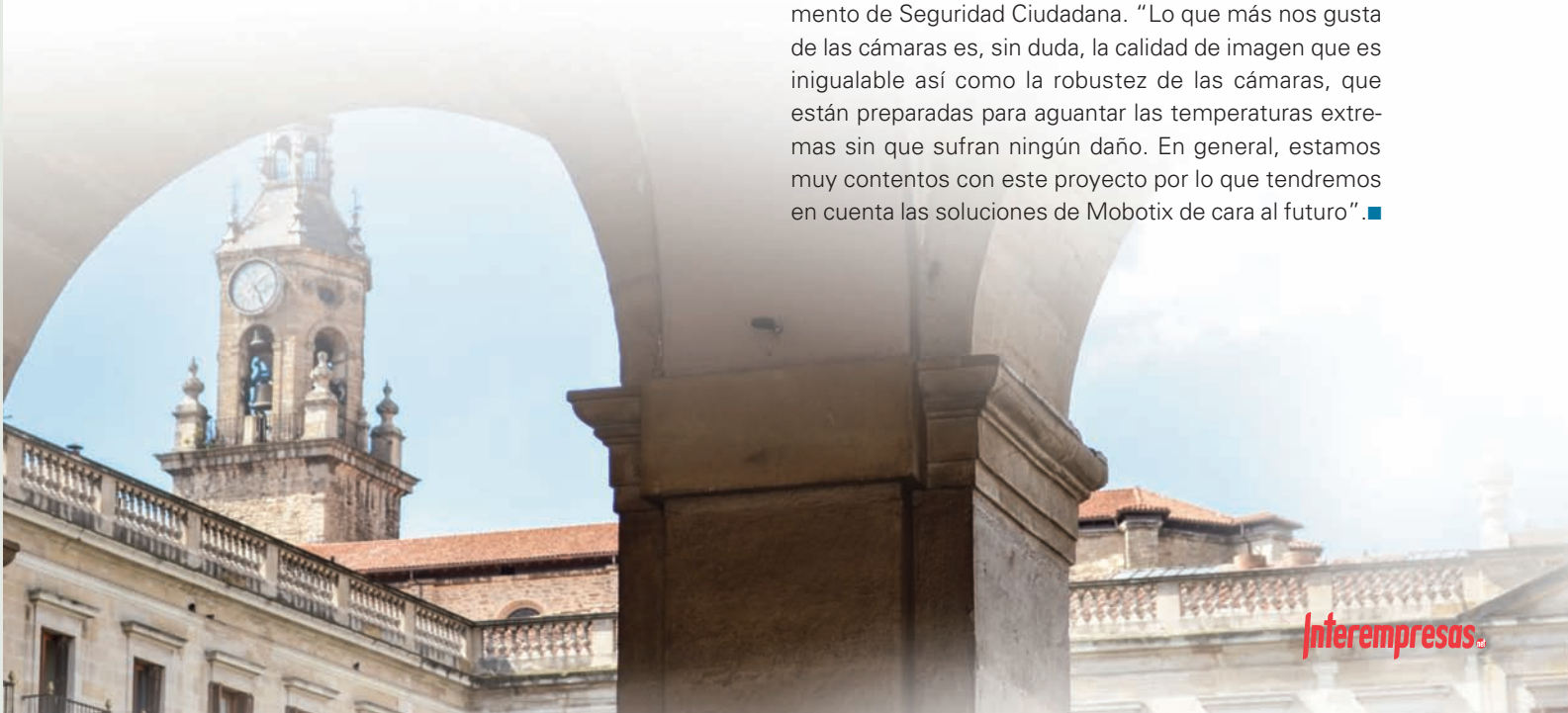
Su Ayuntamiento ha elegido a la compañía PCI Security Doctors, para la puesta en marcha de este sistema de control de acceso que es controlado por la Policía Municipal. "Se analizaron varias cámaras del mercado, tanto analógicas como IP y finalmente nos decantamos por las cámaras de Mobotix que nos parecieron las apropiadas", comenta Lorenzo González, socio director de PCI Security Doctors. "Sobre todo por la calidad de imagen, de la mejor del mercado, y también por la posibilidad de cubrir grandes espacios con pocas cámaras. Por último, pero no menos importante, el hecho de que las cámaras Mobotix son robustas y no tienen piezas móviles por lo que tienen una baja tasa de averías".

## El proyecto se cerró con éxito y actualmente las cámaras realizan su función a la perfección

El proyecto de instalación del sistema de videovigilancia en las rampas y ascensor del Cantón del Seminario del Casco Medieval de Vitoria-Gasteiz ha durado unos tres meses y ha constado de: licitación pública por invitación, toma de datos inicial, planos, planteamiento de instalación con número de equipos, realización de presupuesto, presentación, aprobación presupuesto, pedido materiales, ejecución de instalación, puesta en marcha, formación, entrega de obra y finalización.

Rubén Gómez, de SPC Telecom y Novatecno, ha sido el distribuidor oficial de las cámaras Mobotix. Y PCI Security Doctors ha sido la compañía que se han encargado de la implantación. Han instalado 4 cámaras en la vía pública, en concreto en zona del Casco Medieval de la ciudad. Se ha cubierto la zona de las rampas mecánicas y el ascensor utilizado para salvar el desnivel existente en el casco medieval. El proyecto se cerró con éxito y actualmente las cámaras realizan su función a la perfección. El cliente está tan satisfecho que no dudará en contar con las empresas implicadas y con Mobotix en el caso de tener que realizar algún otro proyecto relacionado con la videovigilancia.

"Hemos quedado muy satisfechos con este proyecto. Ha salido todo bien, sin ningún incidente y además en poco tiempo. Y las cámaras están cumpliendo su función a la perfección", comenta Adolfo Bueno, responsable de la Unidad de Informática y Comunicaciones del Departamento de Seguridad Ciudadana. "Lo que más nos gusta de las cámaras es, sin duda, la calidad de imagen que es inigualable así como la robustez de las cámaras, que están preparadas para aguantar las temperaturas extremas sin que sufran ningún daño. En general, estamos muy contentos con este proyecto por lo que tendremos en cuenta las soluciones de Mobotix de cara al futuro".■




La cámara SNC-VB632D resistente al agua.


Perfil de la cámara SNC-VB632D.

# Las cámaras de seguridad 4K alcanzarán su máximo esplendor en 2015

Muchos coincidirán en que una de las tendencias más importantes de 2014 ha sido la aparición del formato 4K; y ya hemos visto las primeras cámaras de seguridad Ultra HD en el mercado a precios excelentes. Durante casi diez años, Sony ha permanecido a la vanguardia de la tecnología 4K, siendo el único fabricante en ofrecer una completa solución de flujo de trabajo en 4K 'de la escena a la pantalla', tanto para el mundo cinematográfico como para el entretenimiento en el hogar, que ofrece experiencias increíbles para el espectador.

**Roger Lawrence, responsable de productos de videovigilancia de Sony Europe**

El formato 4K ofrece una resolución cuatro veces superior al Full HD (1080p), lo que da lugar a imágenes nítidas y detalladas. La importancia del 4K seguirá creciendo en todos los ámbitos relacionados con la generación de imágenes; en concreto, será de ayuda en el sector de la seguridad debido a la nítida resolución que proporciona y a la posibilidad de destacar y ampliar determinadas partes de una imagen, como rasgos faciales, imágenes de fondo o matrículas, a fin de no pasar por alto detalles esenciales.

### Un año lleno de innovaciones en seguridad

Durante este último año, Sony ha ampliado su gama de productos y ha incorporado una amplia variedad de funciones, formatos y niveles de rendimiento en aplicaciones de todos los campos de la seguridad y la vigilancia. Esto incluye:

- **Nuestras nuevas cámaras de la serie X (las SNC-XM636, XM637 y XM632):** cámaras minidomo compactas diseñadas para el sector del transporte pero que pueden usarse igualmente en cualquier entorno exigente o en exteriores, y su modelo inferior, la XM631, una variante para interiores.
- **Nuestra nueva cámara cilíndrica de la serie E, la SNC-EB602R:** se trata de nuestra cámara IP con infrarrojos (IR) más sensible hasta la fecha, que ofrece una amplia gama de opciones para seguridad y vigilancia en exteriores.
- **Por último, la SNC-VB632D resistente al agua:** la última cámara cilíndrica para exteriores con sistema de iluminación dual y función Día/Noche de Sony, ideal para una amplia gama de actividades de vigilancia y seguridad en entornos urbanos, vehículos y en el sector del comercio minorista.

La demanda de estas cámaras ha superado las expectativas, y esperamos que esto siga así a lo largo del 2015.

Las soluciones de videovigilancia de Sony han estado presentes en multitud de eventos y proyectos de todo el mundo, incluida la maratón de Nueva York

### Protección en la maratón más grande del mundo y en una de las capitales de la moda

Además, las soluciones de videovigilancia de Sony han estado presentes en multitud de eventos y proyectos de todo el mundo, incluida la maratón de Nueva York. Los organizadores de la maratón confiaron en las soluciones y cámaras de seguridad de Sony para el último tramo de la carrera y la línea de meta, ya que su intención era aumentar la seguridad y la conciencia de la situación para corredores y espectadores.

Las soluciones de Sony también fueron las elegidas para los cruces de ferrocarril de la ciudad de Milán, conocida por ser una de las capitales de la moda más importantes del mundo. Las cámaras de Sony se incorporaron como parte de un programa piloto con el integrador de sistemas Owls AG. En colaboración con la solución de iluminación de Owls, las cámaras PTZ (giro, inclinación y zoom) de Sony vigilan la zona desde ambos lados de la barrera y envían imágenes y vídeos al departamento de policía ya sea mediante una conexión LAN o una variante inalámbrica.

### De la seguridad en centros educativos a los estadios de la Copa Mundial de la FIFA

Cuando se trata de la seguridad de 28.000 alumnos, el distrito escolar de la ciudad de Bakersfield confía en Sony para proporcionar vigilancia en un área de 410 kilómetros cuadrados. Con más de 2.000 cámaras en red Ipela de Sony instaladas en 41 campus, se ha mejorado la seguridad de las instalaciones, además de obtener otros grandes beneficios. Se han reducido en gran medida los gastos en reparaciones de cristales rotos, pintadas y otras áreas problemáticas. Y, por último, se instalaron cientos de cámaras de seguridad con la tecnología más avanzada de Sony durante la Copa Mundial de la FIFA en Brasil.

En 2015, se espera que muchos de los principales fabricantes del sector de la retransmisión lo adopten por completo y creen líneas de productos que respalden la tendencia del 4K y el incesante aumento de la resolución de la imagen, incluido Sony. Esperamos que el formato 4K pase a ser la definición estándar del sector de la retransmisión de aquí a dos años aproximadamente. Para 2020, intuyo que el 4K se habrá convertido en el formato habitual dentro de la industria de la seguridad. El 4K será una solución rentable y eficaz que ofrecerá un nuevo estándar de seguridad y protección.■


# Claves de la seguridad online

La variedad y abundancia de incidentes de seguridad ocurridos en 2014 –desde el ciberespionaje y las campañas de cibersabotaje a las vulnerabilidades explotadas en todos los rincones de la web– hacen difícil elaborar un ranking de los principales eventos de seguridad que tuvieron lugar el año pasado. Pero, ¿qué suponen exactamente algunos de estos sucesos? ¿Qué desarrollos fueron simplemente interesantes y cuáles apuntan a importantes tendencias en el espacio de la seguridad online? ¿Qué amenazas son residuos del pasado y cuáles son indicaciones de lo que nos espera en el futuro? Para ello se han analizado algunos de los desarrollos más importantes en el campo de la seguridad online a lo largo del año pasado, lo que hemos aprendido (o lo que deberíamos haber aprendido) de ellos y lo que presagian para el futuro.

**Symantec Corporation**

Los principales expertos en seguridad de Symantec en Europa, Oriente Medio y África nos dan algunas claves de lo que ellos consideran que nos depararán los próximos años. Creen que debemos de tener en cuenta los siguientes puntos:

### Los métodos de pago electrónico estarán en el punto de mira

Vender en el mercado negro una tarjeta de crédito robada o los datos de la tarjeta de débito es un negocio muy lucrativo para los ciberdelincuentes. Dado que el sistema de chip y pin utilizado en la mayoría de tarjetas europeas ofrece una mayor seguridad que el de las tarjetas de banda magnética, es poco probable que veamos ataques a gran escala para obtener datos de pago de los clientes dirigidos a sistemas en el punto de venta (POS) que usan tarjetas con chip y pin. Sin embargo, las tarjetas con chip y pin (conocidas como "EMV" por las siglas de Europay, MasterCard y VISA) también son susceptibles de un uso fraudulento en las compras online.

Además, los métodos de pago sin contacto que utilizan la tecnología Near Field Communications (NFC) experimentarán probablemente un incremento en la adopción por parte de los consumidores, especialmente debido a que cada vez más smartphones soportan el estándar NFC. Los habitantes de grandes ciudades como Londres utilizan ya diariamente la tecnología NFC para pagar el transporte público. En los próximos 12 meses, los pagos sin contacto dejarán de ser una tendencia creciente y se convertirán en la norma para los consumidores de algunos mercados europeos.

Aunque los sistemas NFC son más seguros que las bandas magnéticas, se mantiene la posibilidad de que los hackers los exploten, aunque esto requeriría que los ciberdelincuentes se dirigiesen contra tarjetas individuales y nunca resultaría en brechas de seguridad o robos a gran escala como los que hemos visto en Estados Unidos. No obstante, la tecnología de pago utilizada no protegerá frente a los comerciantes que no estén almacenando los datos de las tarjetas de forma segura, por lo que se deberá mantener la vigilancia sobre la protección de los datos almacenados.

### Los ataques coordinados de ciberespionaje y cibersabotaje no muestran signos de decrecimiento

Las campañas de ciberespionaje y cibersabotaje apoyadas por determinados Estados, como las que vimos con DragonFly y Turla, respectivamente, en 2014, continuarán poniendo en riesgo las infraestructuras críticas nacionales y la propiedad intelectual. Dragonfly y Turla son solo un par de ejemplos de entre las muchas campañas de espionaje que vemos continuamente. Se trata de un problema global que no muestra signos de agotamiento, con ataques como el de Sandworm, que aprovecha las vulnerabilidades de día-cero para propagar programas backdoor (que abren "puertas traseras").

Dado que este tipo de campañas están diseñadas para minar la inteligencia y sabotear las operaciones, las organizaciones (incluyendo las del sector público) reconsiderarán su postura de ciberseguridad actual y harán de la seguridad una prioridad de inversión. La seguridad se convertirá así en una inversión estratégica, en lugar de táctica, diseñada no sólo para protegerse frente a intrusiones sino también para detectarla una vez que la intrusión ha tenido lugar, permitiendo a la organización responder de forma apropiada. También veremos proveedores de seguros que empezarán a ofrecer a las organizaciones soluciones de protección cibernética, un fenómeno que crecerá rápidamente en 2015.

### Los sectores público y privado mejorarán la colaboración para combatir el cibercrimen

Vayamos ahora con algunas buenas noticias: con los ataques internacionales, como los dirigidos Gameover, Zeus, Cryptolocker y Blackshades, 2014 fue testigo de cómo los equipos y fuerzas de seguridad adoptaban una postura más activa y agresiva contra el cibercrimen, incrementando la colaboración con la industria de seguridad online. Symantec firmó un acuerdo MoU con Europol para continuar coordinando sus esfuerzos. Aunque este fue un paso positivo para proteger a consumidores y empresas,

El aumento de adopción del cloud computing supone que muchas empresas realmente no saben dónde están todos sus activos de datos.

**La seguridad se convertirá en una inversión estratégica diseñada, no solo para protegerse frente a intrusiones, sino también para detectarla una vez que la intrusión ha tenido lugar.**

la realidad es que el cibercrimen no desaparecerá de un día para otro. Tanto el sector privado como las fuerzas de seguridad continuarán colaborando con el fin de lograr un impacto duradero y detener los planes de ataque de los ciberdelincuentes.

### Retos de cumplimiento normativo para las empresas de la UE, conforme se acerca la adopción de la legislación sobre protección de datos

Los próximos años veremos un foco y preocupación continua sobre la privacidad y el uso de la información, puesto que la UE tiene previsto implementar su nueva normativa sobre protección de datos. Con la expansión de Internet y el creciente número de dispositivos conectados que recogen y correlacionan datos, existe una enorme cantidad de información ahí fuera (se espera que ronde los 10 ZB al final de 2015, de hecho) que necesita ser adecuadamente protegida y gestionada. Uno de los principales retos para las empresas de la UE será saber dónde están ubicados todos sus datos y qué está pasando con la información que contienen.

El aumento de adopción del cloud computing supone que muchas empresas realmente no saben dónde están todos sus activos de datos y, de cara a recuperar la confianza de los consumidores tras las revelaciones de la NSA, las empresas tienen una necesidad y responsabilidad crecientes de saber qué es lo que ocurre exactamente con la información que guardan. Las organizaciones deberán hacer frente a nuevos desafíos en 2015, obligadas a hacer malabarismos para garantizar el cumplimiento de las nuevas regulaciones al mismo tiempo que siguen el ritmo de la economía mundial utilizando las vastas cantidades de datos existentes para impulsar nuevos servicios y fuentes de ingresos.

### Las plataformas de código abierto serán un flanco débil

Los próximos años traerán nuevas vulnerabilidades descubiertas en las bases de datos y plataformas de servicios web de código abierto, y también veremos cómo los hackers explotan estas vulnerabilidades impunemente. Como ocurrió con Heartbleed y Shellshock/ Bash Bug, estas vulnerabilidades representan potencialmente una nueva área para los atacantes. No obstante, el mayor riesgo sigue ligado a las vulnerabilidades ya conocidas, pese a lo cual ni las organizaciones ni los consumidores aplican los parches correctivos.

### El Internet de las Cosas (IoT) seguirá siendo el Internet de las Vulnerabilidades, pero los ataques serán limitados y aislados

Con el IoT generando grandes cantidades de datos, seguiremos viendo ejemplos de cómo los ciberdelincuentes pueden explotar las vulnerabilidades de software en los dispositivos conectados, incluyendo la tecnología wearable, los dispositivos domésticos conectados, como los televisores inteligentes y los routers (¿se acuerdan de los monitores de bebés del año pasado?) y las aplicaciones en los nuevos coches conectados. Es decir, no veremos ataques a gran escala contra los dispositivos IoT, sino ataques aislados.

### Las organizaciones se darán cuenta de que el tradicional sistema de registro/contraseña hoy ya no sirve

A finales de verano de 2014, saltó la noticia de que los perfiles de varias famosas en Estados Unidos habían sido hackeados y sus fotos posando desnudas habían sido robadas y publicadas online. Enseguida, Apple lanzó un comunicado en el que decía que "tras más de 40 horas de investigación, hemos descubierto que determinadas cuentas de famosas se han visto comprometidas por un ataque dirigido contra nombres de usuario, contraseñas y preguntas de seguridad, una práctica muy extendida en Internet".

Las contraseñas tienen muchos puntos débiles, pero normalmente pueden agruparse en tres problemas generales:

- Las personas utilizan contraseñas débiles que pueden adivinarse fácilmente –por ejemplo, "contraseña" o "123456"- o utilizan la misma contraseña para múltiples sitios, lo que significa que, si los ciberdelincuentes hackean una de tus cuentas online, tendrán también acceso a las otras.
- Los mecanismos para recuperar las contraseñas son defectuosos. Si pierdes u olvidas una contraseña, el método tradicional para recuperarla es contestar a preguntas de las que solo tú, el propietario real, debería saber la respuesta. Desafortunadamente, las respuestas a estas preguntas a menudo pueden deducirse de la información que puede encontrarse online fácilmente (especialmente, dada la proclividad de la gente a "compartir en exceso" en las redes sociales).
- Los ataques de phishing, con los que los usuarios dan directamente a los hackers sus claves, involuntariamente y bajo engaño.

Mientras las organizaciones intentan encontrar formas de acabar con las brechas de seguridad y proteger a sus usuarios finales, la buena noticia es que estamos empezando a ver alternativas al viejo sistema, incluyendo la autenticación de doble factor (2FA), que requiere no solo algo que el propietario real debería saber (por ejemplo, la contraseña) sino también algo que sólo él tiene (por ejemplo, su teléfono móvil). Sin embargo, conforme cada servicio empiece a implementar este tipo de medidas, los consumidores dependerán cada vez más de diferentes aplicaciones, números de teléfono y preguntas de seguridad (y, además, en múltiples plataformas), y les será cada día más difícil mantener todo en orden. ■


Con el IoT generando grandes cantidades de datos, seguiremos viendo ejemplos de cómo los ciberdelincuentes pueden explotar las vulnerabilidades de software en los dispositivos conectados.

# Eugeni Mulà,
## director comercial de Detnov

"Al cierre de agosto, Detnov prevé terminar el año 2015 con un crecimiento superior al 60%"

La compañía referente a nivel nacional en fabricación de productos específicos en la detección de incendios, Detnov, hizo público el pasado mes de marzo el nombramiento de Eugeni Mulà como nuevo director comercial de la marca en España. Mulà está a cargo de las operaciones comerciales y marketing a nivel nacional, además de contar con más de 20 años de experiencia en el sector, habiendo formado parte del equipo de otras empresas de referencia en seguridad electrónica y detección de incendios, como Mitsubishi Electric, Siemens, GE Security y UTC F&S. Interempresas Seguridad le ha entrevistado para conocer las principales tendencias del mercado de la protección contra incendios en la actualidad, las novedades que presenta Detnov, y sus objetivos en esta nueva etapa profesional.

**Mª Carmen Fernández**

***Recientemente se ha incorporado a Detnov para estar al cargo de las operaciones comerciales y marketing dentro del mercado nacional de la compañía. ¿Qué objetivos personales se marcó al llegar a la empresa?***
Detnov es un nuevo reto dentro de mi carrera profesional. La gerencia de la empresa ha confiado en mí para que desarrolle una estrategia de comercialización dirigida al mercado nacional y dando a conocer nuestra marca dentro del sector de la detección de incendios. El objetivo es la continuidad de mi carrera, más de veinte años en el campo de la seguridad electrónica, mantener el contacto con los colegas del sector, conocer nuevos clientes y aportar mi experiencia a la empresa, afianzar su crecimiento, así como aportar mi granito de arena al sector para potenciar la protección de incendios como parte social, ya que protegemos a nuestros seres queridos de posibles fatalidades generadas por un incendio.

Central CAD 150-4 de Detnov.

***A pesar de que la compañía se fundó hace poco tiempo, en 2007, a día de hoy es una empresa destacada en la fabricación de productos específicos en la detección de incendios a nivel nacional. ¿Cómo se estructura Detnov en la actualidad?***
Nuestro principal baluarte es la experiencia que acumulan los compañeros del Departamento de I+D, ya que, gracias a ellos podemos desarrollar nuevas tecnologías de detección y sacar productos novedosos al mercado. Disponemos de fabricación propia con importantes procesos de calidad. Además buscamos que nuestros proveedores externos sean de proximidad. Obviamente también disponemos de los Departamentos de Ventas, Atención al Cliente y Almacén para poder satisfacer las necesidades de nuestros clientes. Además de nuestra sede central en Sant Boi de Llobregat, en la provincia de Barcelona, tenemos delegación en Madrid, y un Departamento de Exportación que en estos momentos atiende a más de 25 países alrededor del mundo.

***En términos económicos, ¿cuál es el objetivo de Detnov para 2015? ¿Considera que van camino de cumplirlo?***
El objetivo marcado por la compañía era crecer un 30% su facturación con relación al año pasado. Al cierre de agosto ya estamos en una previsión de terminar con un crecimiento superior al 60%, por tanto, podemos decir que este año será muy satisfactorio. Asimismo, un objetivo no cuantificable era el que las empresas del sector contra incendios en España empezaran a conocer y familiarizarse con nuestra marca, que probasen nuestros equipos, etc. Quien nos prueba, repite debido a la calidad, facilidad de instalación y programación de éstos.

***En general, ¿cuál es la estrategia que se está siguiendo este año? ¿Van a seguir con la misma a largo plazo?***
La estrategia marcada por la compañía, a principios de año fue consolidar el crecimiento obtenido durante los últimos años en el mercado de exportación y empezar a ser un referente en el territorio nacional, además de invertir en I+D para seguir lanzado nuevos productos al mercado. A largo plazo, queremos expandir la red comercial creando más delegaciones tanto en España como en otros países.

***¿Qué tendencias sigue el mercado de la protección contra incendios en la actualidad?***
Desde mi punto de vista, la protección contra incendios tenderá a consolidarse dentro de nuestra cultura de seguridad, tomará mayor relevancia en nuestro día a día. Si nos fijamos en los anuncios de televisión, la seguridad contra robo es habitual pero, en cambio, de la protección contra incendios apenas hay propaganda. No hay que olvidar que más de 100 personas al año mueren en España a causa de incendios domésticos, y cada día hay muchas emergencias ocasionadas por incendios en viviendas y

Sistemas Detnov.

negocios. En muchos países europeos ya es obligatorio colocar detectores en las viviendas, por ejemplo desde el pasado mes de marzo en Francia empezó su obligatoriedad. Otra tendencia será tecnológica y vendrá de la mano de las telecomunicaciones. El conocer el estado de las instalaciones en tiempo real está tomando relevancia, tanto a nivel de gestionar alarmas como el del mantenimiento. Eso supondrá que los sistemas deberán estar conectados ya sea a un centro de control o incluso a nuestros teléfonos móviles.

***¿Qué consecuencias tiene la falta de mantenimiento o renovación de los sistemas de protección contra incendio?***

Una falta de mantenimiento en cualquier tipo de instalación de un edificio puede generar problemas a corto o a largo plazo. Si hablamos de la protección contra incendios lo que puede suponer un mal mantenimiento es que el sistema no funcione cuando se inicie un incendio. Esto conlleva la pérdida de un negocio, vivienda o incluso pérdida de vidas.

Tanto el mantenimiento correctivo como el preventivo hay que verlos como una inversión. Además, los equipos que llevan muchos años instalados pueden perder fiabilidad. Por ello, desde el sector recomendamos que se renueven las instalaciones cada cierto tiempo. La tecnología que usamos en la fabricación de los equipos de detección va evolucionando tanto por la inversión en desarrollo como a nivel normativo.

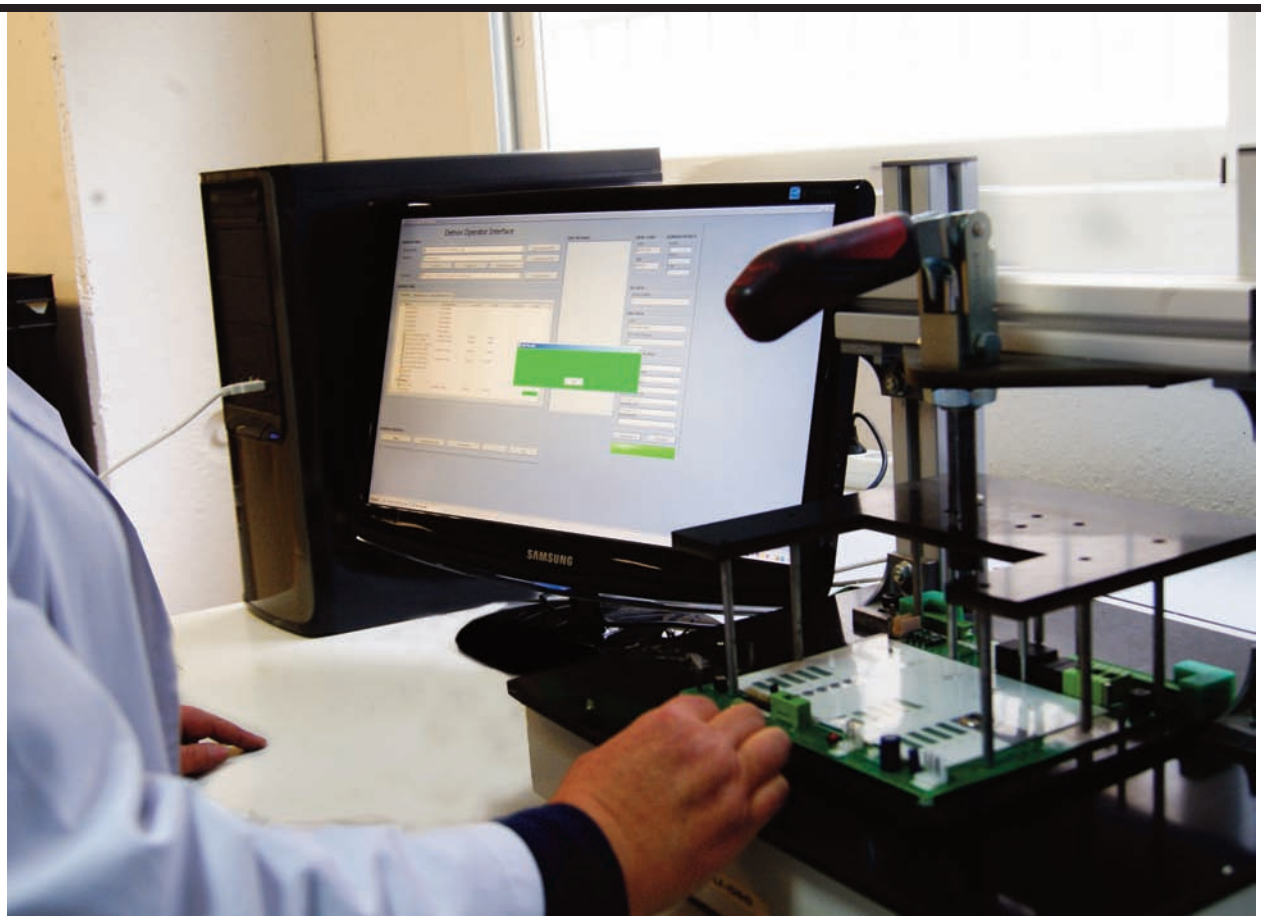
***¿Considera que se debe mejorar algún aspecto en cuanto a dichos sistemas? ¿Y en el sector de la seguridad en general?***

En el nuevo reglamento de protección contra incendios, que esperamos que salga en breve, ya se introducen algunas novedades en el campo del mantenimiento, como por ejemplo, la obligatoriedad de la renovación de los detectores cada cierto tiempo. Esto hará que las instalaciones se vayan renovando, manteniendo así el parque instalado en perfectas condiciones.

La protección de nuestras viviendas, en general, creo que también es un aspecto a mejorar. Tenemos que tomar más en consideración algunos aspectos básicos de seguridad como serían: planes de evacuación, simulacros en viviendas, instalación de detectores en zonas comunes o incluso dentro de las viviendas. Con relación al sector de la seguridad en general, creo que en España tenemos la suerte de disponer de unos servicios, tanto públicos como privados, con un nivel muy elevado de profesionalidad.

***¿Qué clientes contratan los servicios de Detnov con mayor frecuencia? ¿Qué servicios y soluciones le ofrecen a dichos clientes?***

Nuestros clientes son empresas instaladoras homologadas en detección de incendios así como, algunos distribuidores locales, que por proximidad, dan servicio a los instaladores. Prestamos un servicio de comercialización de nuestros productos, asesoría técnica en el caso de que nos lo soliciten. Obviamente, el dar un buen soporte




Los proyectos que actualmente está desarrollando Detnov son nuevas centrales de detección de incendios y de gases con nuevas prestaciones.

técnico y comercial es básico en nuestro día a día con los clientes. El porfolio de productos que ofrecemos va desde un sistema convencional hasta un sistema analógico con varias centrales en red, además de una gama completa de detectores y accesorios.

***¿Cuáles son las últimas novedades que han lanzado? ¿Tienen algún proyecto más en mente?***

Este año hemos empezado a comercializar una central de extinción certificada. Asimismo hemos incorporado detectores especiales ampliando así nuestro porfolio y ofreciendo a los instaladores una solución global de sistemas de detección de incendios. En octubre sacaremos al mercado una gama de detectores autónomos enfocados al mercado doméstico y también para los instaladores de seguridad. Los proyectos que en estos momentos estamos desarrollando son nuevas centrales de detección de incendios y de gases con nuevas prestaciones además de un diseño más moderno y funcional.

***¿Cómo ve al sector de la protección contra incendios dentro de cinco años?***

El sector de la protección contra incendios ha sufrido un impacto muy fuerte debido a la crisis de la construcción. Esto ha supuesto una reducción del volumen de negocio, con la consiguiente reducción de puestos de trabajo y un ajuste importante en los márgenes en la cadena de valor. Se empieza a ver una pequeña recuperación en el sector, el cual esperamos que en los próximos años se vaya consolidando. También vemos una oportunidad en la mejora de los servicios añadidos como podrían ser: el telemantenimiento, la conexión a Central Receptora de Alarma, así como la renovación del parque instalado.■


Conocer el estado de las instalaciones en tiempo real está tomando relevancia.


Manuel Martínez, coordinador del Comité Instalación, Ingeniería, Mantenimiento de Sistemas y Equipos en Tecnifuego-Aespi.

# Seguridad contra incendios en establecimientos industriales

Sistemas automáticos de detección de incendio, hidrantes exteriores, extintores de incendio, bocas de incendio equipadas o rociadores automáticos son sólo algunos de los sistemas y equipos de seguridad contra incendios en establecimientos industriales que encuentran en las normas UNE directrices que le son de aplicación. Además, están incluidos en el Reglamento de Seguridad contra Incendios en este tipo de establecimientos.

**Manuel Martínez, coordinador del Comité Instalación, Ingeniería, Mantenimiento de Sistemas y Equipos en Tecnifuego-Aespi**

Todos los establecimientos industriales nuevos, incluidos los almacenes, que cambien o modifiquen su actividad, se trasladen, amplíen o reformen deben cumplir los requisitos de seguridad contra incendios del Reglamento de Seguridad contra Incendios en los Establecimientos Industriales (RSCIEI). Este Reglamento establece y define los requisitos mínimos que han de satisfacer los establecimientos industriales y almacenes para su seguridad en caso de incendio, determinados por su configuración y ubicación con relación a su entorno y su nivel de riesgo intrínseco. La evaluación del riesgo intrínseco se determina calculando la densidad de carga de fuego de los distintos sectores de incendio que configuran el establecimiento industrial.

Para llevar a cabo un proyecto específico de protección contra incendios en este tipo de establecimientos, un técnico competente debe contemplar las características del edificio (superficie, configuración, tipo de construcción, etc.), altura del producto almacenado y disposición del almacenaje (apilado o en estanterías). Y, además, realizar un estudio en detalle de la densidad de carga del fuego ponderada y corregida; esto es, masa en kilogramos de los combustibles, poder calorífico de los mismos, etc.

El Reglamento de Seguridad contra Incendios en los Establecimientos Industriales contempla en este sentido que hay que tener en cuenta requisitos constructivos (Apéndice 2) atendiendo siempre a estos tres factores: configuración, ubicación y nivel de riesgo intrínseco. En cuanto a los materiales constructivos, las exigencias de comportamiento al fuego de los productos de construcción se definen determinando la clase que deben alcanzar suelos, paredes y techos siguiendo los siguientes criterios:

- Criterio de integridad 'E' / criterio 'E'. Criterio por el cual se evalúa la capacidad de un elemento de separación para evitar el paso de las llamas y los gases calientes.
- Criterio de aislamiento 'I' / criterio 'I'. Criterio por el cual se evalúa el aislamiento térmico.
- Criterio de soporte de carga 'R' / capacidad de soporte de carga. Criterio mediante el cual se evalúa la capacidad de un elemento constructivo o estructura para sostener una carga impuesta cuando se expone a un incendio.

El RSCIEI establece y define los requisitos mínimos que han de satisfacer los establecimientos industriales y almacenes para su seguridad en caso de incendio.

## Inspección de instalaciones

La Norma UNE 192005 'Procedimiento para la inspección reglamentaria. Seguridad contra incendios en los establecimientos industriales', en cuya elaboración ha participado Tecnifuego-Aespi ayuda a las labores de inspección y es una herramienta eficaz de trabajo para los Organismos de Control Autorizados (OCA). Detalla la metodología que debe seguir la inspección para la seguridad industrial y establece el proceso de actuación. La norma establece también la documentación final tras la inspección, como son el acta y el informe de inspección periódica. El qué y cómo se ha de inspeccionar se establece en los anexos A (comprobación de configuración y ubicación), B (comprobación del nivel de riesgo intrínseco), C (protección activa) y D (protección pasiva). El anexo F establece la formalización de la actuación inspectora.

Esta norma redunda en la eficacia y fiabilidad de los sistemas de seguridad contra incendios que se instalan en los establecimientos industriales. Por ello, es deseable y muy conveniente que el Ministerio de Industria, Energía y Turismo contemplara su aplicación en el marco del RD 2267/04 (Capítulo III, Artículo 6 y 7) cuando se publique la nueva versión del RSCIEI.

## Elementos constructivos

Las exigencias de comportamiento ante el fuego (EF) de un elemento constructivo portante se definen por el tiempo en minutos (60, 90, 120...) durante el que dicho elemento debe mantener la estabilidad mecánica (o capacidad portante). En riesgo bajo, según ubicación y configuración del edificio, se exige EF-120, EF-90, EF-60 y EF-30. En riesgo medio, EF-60, EF-90 y EF-120. En riesgo alto, EF-90, EF-120 y EF-180.

En el caso de la resistencia al fuego (RF) de elementos constructivos de cerramiento (o delimitadores) se definen por los tiempos durante los que dichos elementos deben mantener las siguientes condiciones: a) Estabilidad mecánica (o capacidad portante); b) Estanqueidad al paso de llamas o gases calientes; c) No emisión de gases inflamables en la cara no expuesta al fuego; y d) Aislamiento térmico suficiente para impedir que la cara no expuesta al fuego supere las temperaturas establecidas. La RF de los elementos constructivos delimitadores de un sector de incendio respecto de otros no será inferior a la estabilidad al fuego exigida. En toda medianería o muro colindante con otro establecimiento se exige en Riesgo bajo: RF-120. Riesgo medio: RF-180. Riesgo alto: RF-240.

La evacuación de los establecimientos industriales es otro aspecto que hay que contemplar. Si el número de empleados del establecimiento industrial es superior a 50 personas deberá contar con una salida independiente del resto del edificio. En riesgo alto, deberán disponer de dos salidas independientes y en riesgo medio dos salidas cuando su número de empleados sea superior a 50 personas. Las distancias máximas de los recorridos de evacuación no superarán en riesgo alto los 25 metros, los 35 en riesgo medio y los 50 en riesgo bajo.

Asimismo, la ventilación y eliminación de humos y gases de la combustión, y con ellos del calor generado en los espacios ocupados por sectores de incendio, debe realizarse de acuerdo con la tipología del edificio, así como en relación con las características que determinan el movimiento del humo. En concreto, los almacenes dispondrán de ventilación natural si están situados en planta bajo rasante y su nivel de riesgo es alto o medio; o en cualquier

Sistema de extinción por gases.

planta sobre rasante si su nivel de riesgo es alto o medio. En este sentido, la serie de Normas UNE-EN 12101 sobre sistemas para el control de humo y calor, y la UNE 23585 'Seguridad contra incendios. Sistemas de control de temperatura y evacuación de humos (SCTEH). Requisitos y métodos de cálculo y diseño para proyectar un sistema de control de temperatura y de evacuación de humos en caso de incendio' son de ayuda.

El RSCIEI señala que todos los aparatos, equipos, sistemas y componentes de protección contra incendios, así como los instaladores y mantenedores de las instalaciones cumplirán además el Reglamento de Instalaciones de Protección Contra Incendios (RIPCI). En cuanto a los sistemas y equipos de protección activa que son preceptivos, se pueden señalar los sistemas automáticos de detección de incendio; sistemas hidrantes exteriores; extintores de incendio; sistemas de bocas de incendio equipadas (BIE); sistemas de rociadores automáticos de agua; sistemas de agua pulverizada; sistemas de espuma física; sistemas de extinción por polvo; sistemas de extinción por agentes extintores gaseosos, y señalización fotoluminiscente. Todos estos sistemas y equipos cuentan con normas UNE que incluyen directrices que les son de aplicación.■

## Normas mencionadas

- UNE 192005 'Procedimiento para la inspección reglamentaria. Seguridad contra incendios en los establecimientos industriales'.
- Serie de Normas UNE-EN 54 sobre sistemas de detección y alarmas de incendio incluye directrices valiosas en este sentido.
- UNE-EN 14339 'Hidrantes contra incendios bajo tierra'.
- UNE-EN 14384 'Hidrantes de columna'.
- UNE-EN 3-7 de extintores portátiles de incendios.
- UNE-EN 14384 incluyen requisitos aplicables a estos extintores.
- Serie de Normas UNE-EN 671 sobre instalaciones fijas de lucha contra incendios contiene directrices de aplicación a estos sistemas.
- Norma UNE-EN 12845 'Sistemas fijos de lucha contra incendios. Sistemas de rociadores automáticos. Diseño, instalación y mantenimiento'.
- Serie de Normas UNE-EN 12259 de sistemas fijos de lucha contra incendios son de aplicación para estos sistemas.
- Serie de Normas UNE-EN 1568 sobre agentes extintores concentrados de espumas.
- Serie de Normas UNE-EN 12416 sobre sistemas de extinción por polvo.
- Serie de Normas UNE-EN 12094 sobre componentes para sistemas de extinción mediante agentes gaseosos.

"El ámbito de la seguridad privada no es un sector del cual el ciudadano medio esté plenamente informado"

# Óscar Tellez,

## director legal de Stanley Security Solutions

Óscar Tellez, director legal de Stanley Security Solutions y socio experto de Aecra en Seguridad Privada y Servicios, opina en esta entrevista sobre las consecuencias directas de la entrada en vigor de la nueva Ley de Seguridad Privada, el conocimiento que tienen los ciudadanos sobre la contratación de servicios de seguridad privada, y sobre la actualidad del mercado de alarmas-intrusión en general.

**Aecra**

***Después de la entrada en vigor de la nueva Ley de Seguridad Privada, ¿considera que va a producirse un aumento en la contratación de los servicios de gestión de alarmas?***

Lo cierto es que no. No vemos que la nueva normativa abra el campo de los servicios de conexión y gestión de alarmas a las empresas de seguridad más allá de lo que hasta la fecha estaba establecido. En todo caso, nos aventuramos a pronosticar que si se produce una variación, ésta sería negativa. Lo que sí se abre es el campo de la conexión de sistemas directamente a los equipos o medios telemáticos del propio usuario.


Instalaciones de Stanley Security Solutions.

Videowall de Stanley.

***Como jurista experto en las actividades y servicios de seguridad privada, ¿cree que éste nuevo marco legal plantea una mayor oferta de los servicios compatibles por las empresas de seguridad? ¿Ampliarán estas empresas su objeto social?***

En este caso, la respuesta sí se antoja positiva. Las nuevas actividades o actividades compatibles amplían el espectro de los servicios que las empresas de seguridad pueden llevar a cabo, tales como el control y seguimiento de señales técnicas, calderas, equipos de frío, suministro eléctrico, conteo de personas, control sobre telepeajes, etc. Es muy probable que gran parte de las empresas de seguridad y, en especial las más grandes, acaben ampliando su objeto social hacia este sentido.

***Como director legal de Stanley Security Solutions, ¿estima que el ciudadano tiene un conocimiento correcto del alcance y contenido del servicio de gestión de alarmas? ¿Considera que el ciudadano es consciente de las consecuencias de la contratación de los servicios de seguridad privada?***

De algún modo, la experiencia y la práctica de los últimos años, nos han llevado a la conclusión de que el ciudadano no cuenta con dicho conocimiento. El ámbito de la seguridad privada no es un sector del cual el ciudadano medio esté plenamente informado. Cuestión distinta es la relativa a los usuarios obligados a disponer de medidas de seguridad, así como los grandes usuarios que al contar con departamentos de seguridad propios y personal experto en seguridad en sus correspondientes entidades, sí cuentan con un profundo conocimiento en la materia.

***¿Cómo cree que debe ejercer una empresa de seguridad el deber de información frente a sus clientes? ¿Existen realmente servicios de atención al cliente en las Centrales Receptoras de Alarmas?***

En nuestro caso, ya desde hace años, se imparte formación interna al personal comercial y de atención al cliente para que estos puedan asesorar e informar correctamente al cliente en todas las cuestiones. Igualmente el contrato de seguridad que se firma con el cliente contiene ciertos aspectos informativos al efecto, así como la incorporación de un manual o protocolo de buen uso del sistema de alarma que está vigente desde el año 2009 con el fin de evitar posibles incidencias derivadas de manipulaciones, negligencias, etc., en el uso de los mismos.

En la misma medida se ha incorporado información en los propios certificados y documentación que se entregan a los clientes, así como en lo relativo al control de accesos y CCTV, en el cual se informa al cliente y asesora en relación a los requisitos y obligaciones que, en materia de protección de datos, debe cumplir como responsable del fichero.

***¿Considera que se va a producir un incremento de contratación en el número de operadores de seguridad por las empresas de seguridad? ¿Con qué perfil profesional debería contar dicho operador de seguridad? ¿Entiende que dichos operadores, como personal acreditado, deben tener conocimientos amplios en seguridad informática?***

No creo que vaya a producirse un incremento en la contratación de éstos, si bien sí consideramos que se eleva-

rán los requisitos de contratación en cuanto a su cualificación, perfil y formación. Las últimas novedades normativas ya contemplaban la necesidad de formar al personal operativo en relación a los procedimientos de verificación de señales de alarma, entre otros puntos. Sin duda, el Reglamento de Seguridad Privada, que en breve verá la luz, así como el posterior desarrollo del mismo, arrojarán más luz sobre este punto.

***¿Qué opinión le merece que las empresas Centrales Receptoras de Alarmas puedan subcontratar los servicios de instalación y mantenimiento de sistemas de seguridad conectados con este tipo de empresas de seguridad? ¿Desde el departamento legal que dirige han elaborado algún contrato tipo de subcontrata en dicho ámbito empresarial?***

Lo cierto es que este punto no supone una especial novedad como tal, puesto que esto ya se producía antes con la salvedad de que era requisito para dicha empresa el estar homologada para la prestación de los mismos, pudiendo así proceder a su subcontratación en otras empresas que también gozarán de dicha habilitación. Es una solución más a un problema real que muchas pequeñas empresas tenían, especialmente locales, y que bajo el espíritu de la flexibilización de requisitos, la nueva normativa ha tratado de paliar o actualizar a la realidad existente.

***¿Qué tipo de reclamación suelen formular sus clientes con más frecuencia?***

La mayoría de las reclamaciones derivadas de los clientes son cuestiones relativas a la facturación, cambios de denominación social, altas/bajas, etc. Nuestra empresa no es una compañía que reciba un elevado número de reclamaciones de clientes dado que un alto porcentaje de nuestra actividad está enfocado a grandes clientes y establecimientos obligados en lugar de a pequeños y medianos comercios, que también tenemos, pero en menor medida. Esto viene motivado por el tipo de sistemas de seguridad que desde nuestra empresa se oferta, vende, instala y conecta, ya que son más sofisticados y por ende, más seguros y fiables que la media, precisamente por el perfil de cliente al que van dirigidos.

***¿Existe mucho porcentaje de morosidad en el mercado de la seguridad privada? ¿Cómo cree que puede reducirse?***

Existe morosidad, pero no más que la que pueda producirse en otros sectores del ámbito servicios bajo el que nos movemos. Como es lógico, la crisis ha afectado a todos los mercados, y el de la seguridad privada no es una excepción, pero no son unos datos significativos en comparación con el resto.

***Nos consta que desde Stanley Security Solutions se ha realizado una inversión importante en nuevas tecnologías dentro de los servicios de las Centrales Receptoras de Alarmas. ¿Cómo piensa que puede acreditar sus buenas prácticas en la prestación del servicio o su especial diligencia frente a sus clientes?***

Efectivamente, así es. Desde Stanley Security se decidió apostar fuerte por la tecnología y se actualizó y modernizó, tanto las ubicaciones, como los sistemas desde los que se trabaja en nuestro SOC Security Operation Center (anterior CRA). Es innegable que las nuevas tecnologías y los avances en software facilitan los recursos y acciones a realizar en todas las materias. Las actuaciones en I+D en las empresas de seguridad y tecnología de sistemas han de fundamentarse en este tipo de acciones y recursos.

Actualmente los sistemas permiten realizar infinidad de acciones sobre los equipos de forma remota que dan lugar a la gestión, verificación, mantenimiento, certificación, etc., tanto de las señales de alarma o técnicas que pueden enviar los sistemas, como al correcto funcionamiento de los mismos. En especial, sirven de justificante de la buena praxis llevada a cabo al efecto, además de una herramienta más a valorar, y hasta utilizar por el cliente final para muchas más acciones y servicios de los que hasta ahora tradicionalmente acometía una central de alarmas.

***¿Aplica o tiene implantado algún tipo de certificado de calidad ISO 9001 o similar en su empresa?***

Stanley Security España cuenta en la actualidad con las siguientes calificaciones y certificaciones en materia de calidad y gestión:

- Certificado de Calidad según norma UNE-EN-ISO-9001:2008.
- Certificado de Sistema de Gestión Ambiental según norma UNE-EN-ISO-14001:2004.
- Certificado OHSAS 18001.
- Certificación de Seguridad y Salud Laboral para los trabajos en la AEQT. Calificación global 4 estrellas.
- Empresa clasificada en Cepreven en todas las categorías existentes. Representación en el comité técnico de calificación y auditorias de obras.
- Acreditación SGS para Estaciones de Servicio.
- Acreditación REA para Compañías Instaladoras.

***¿Cuál es contenido del servicio de acudas? ¿Cree que los costes económicos en la ejecución de estos servicios de acuda pueden reducirse a través de las nuevas tecnologías?***

En este punto hemos de diferenciar siempre dos tipos de servicios: nos encontramos por un lado con el servicio de verificación de alarmas (que puede ser exterior y/o interior) para aquellos supuestos en los que las señales recibidas en la central receptora, y los medios y mecanismos de comprobación llevados a cabo no se haya podido comprobar la veracidad de la alarma o tener la consideración de alarma confirmada (según la O.M. INT/316/2011), y por otro lado con la custodia de llaves. En nuestra opinión la verificación externa e interna de la alarma, se va a realizar cada vez más de forma telemática a través de la tecnología y en remoto desde los centros operativos, e incluso, la propia tecnología actualmente ya permite la apertura e iluminación en remoto de las instalaciones ante la llegada de las FF.CC.S. al lugar de comisión del delito.

***¿Le parece interesante la existencia de un código de buenas prácticas en el sector de las Centrales Receptoras de Alarmas frente a los clientes como garantía de la eficacia y eficiencia de dichos servicios?***

Por supuesto, este tipo de acciones son básicas para cumplir con compromisos y estándares de calidad y eficacia. Desde nuestra empresa, en este sentido, se pactan y redactan con nuestros clientes por escrito los distintos protocolos de actuación a partir del mínimo exigido por la normativa hasta llegar a puntos y niveles más allá de los contemplados en la propia norma. Estos protocolos nos sirven de compromiso de calidad en la actuación y respuesta de nuestra central receptora ante las señales recibidas.

***¿Qué estadísticas o datos cree que son necesarios extraer por la Administración Policial para una medición o evaluación real de los servicios prestados por las Centrales Receptoras de Alarmas?***

Sería conveniente contar con la media de datos relativos a números de elementos de seguridad por instalación, volumen de activación de los distintos elementos de los sistemas de forma individualizada y por sector o actividad, número de activaciones derivadas de deficiencias o descuidos por el usuario, incidencias acaecidas a consecuencia del mal funcionamiento de las distintas vías de transmisión, así como en qué supuestos el problema o la alarma derivaba de la propia instalación de seguridad, o la misma derivaba de las líneas o servicios de las empresas de telecomunicación, etc.

***¿Le parece que el porcentaje de acierto de las CRAs en su labor de verificación de señales de alarma es el adecuado para la prevención del delito? ¿Cómo cree que puede reducirse el porcentaje de avisos injustificados a las Fuerzas y Cuerpos de Seguridad competentes?***

En mi opinión, las Centrales Receptoras de Alarmas, o al menos las más importantes, han reducido en los últimos años de una forma drástica sus avisos a las FF.CC.S. mediante una mayor especialización de su personal, una mayor sofisticación de sus sistemas, y una concienciación a los usuarios. El filtrado de señales de alarma está

Videowall.

en torno al 98– 99% de señales recibidas, es decir, en la mayoría de los casos, de cada 100 señales de alarma, 99 se comprueban mediante los medios técnicos y humanos y se dispone que las mismas no son alarmas reales, por lo tanto, no generan un traslado o aviso a las FF.CC.S.
Una mayor colaboración entre la seguridad pública y privada, la realización de unos estándares o procedimientos de calidad y actuación conjuntas por parte de las centrales receptoras, la profesionalización del personal, y especialmente, la actualización y modernización del actual parque de sistemas de seguridad existentes que se encuentran conectados a centrales de alarma por unos equipos y software más modernos, completos y sofisticados, reducirían aún de forma más llamativa este volumen de filtrado al permitir de una forma efectiva y veraz comprobar la existencia o no de alarmas confirmadas.

***¿Le parece que el importe de las sanciones impuestas a las CRAs se adecúa a la gravedad o incidencia del hecho frente a la seguridad pública? ¿Qué formulas o soluciones piensa que se pueden desarrollar o implantar para disminuir el expediente sancionador frente a la empresa de seguridad en la presente normativa de seguridad privada?***

En mi opinión, nos encontramos ante diversas situaciones en función de la ubicación, el supuesto, el tipo de usuario, el tipo de delito perpetrado contra la instalación, etc. No deja de ser menos cierto que la nueva normativa que entró en vigor el pasado año ha elevado de forma considerable la cuantía de las sanciones. Si bien no es menos cierto que gracias al esfuerzo de las distintas unidades, las mismas no están ni de lejos en los números de expedientes sancionadores que se incorporaron a finales de la primera década de este siglo y que supuso una quiebra total que dio lugar a la necesidad de llegar a un consenso que diera solución a la situación que se produjo.
Creemos que ha de seguirse esa misma vía de la cooperación, la coordinación, la colaboración y entendimiento entre los distintos agentes del sector (empresas, personal, usuarios y Administración) para poder disminuir los expedientes sancionadores, mejorar en la prestación del servicio y perseguir y prevenir las posibles acciones delictivas a través del control, verificación, gestión y respuesta de las alarmas.

***¿Qué acciones, eventos e iniciativas entiende que, como socio experto de Aecra, puede emprender dicha Asociación este año 2015 en relación a los servicios prestados por las Centrales Receptoras de Alarmas? Enumérelas.***

- La realización de jornadas divulgativas de concienciación, adecuación y procedimientos de actuación por y para las centrales.
- El establecimiento de unos estándares de calidad y actuación a seguir.
- La formación del personal de los distintos centros y centrales de recepción de señales de alarmas, tanto para operadores como para vigilantes.
- La interlocución de forma directa con los distintos órganos de la Administración.
- La firma de convenios de colaboración con usuarios, aseguradoras, Administración, etc. ■

INEFCO INSTITUTO EMPRESARIAL
PARA LA FORMACIÓN CONTINUA

# Nuevo catálogo 2015

INEFCO INSTITUTO EMPRESARIAL PARA LA FORMACIÓN CONTINUA

**www.inefco.com/cursos**

**Tel. 902 090 372**

REF. NOMBRE CURSO

## MANAGEMENT
16 Dirección de proyectos (Project Management)
88 Como diseñar e implementar un plan de negocio
94 La gestión del cambio
90 Indicadores de gestión y medición de resultados
125 La creatividad en la gestión empresarial
126 La comunicación eficaz en la empresa
128 Orientación al cliente interno y externo
139 La negociacion eficaz. Convencer negociando

## DIRECCIÓN Y GESTIÓN DE EQUIPOS
50 Liderazgo y dirección de equipos
34 Gestión de equipos de trabajo
138 Equipos de alto rendimiento. Creación y liderazgo
136 Liderando reuniones efectivas
122 Trabajo en equipo: evaluación y feedback
123 Mejora de la eficiencia mediante gestión por objetivos
85 Cómo medir, evaluar y compensar el rendimiento del personal
82 Comunicación, incentivo y motivación (Balanced Scorecard)
61 Objetivo: ¡Tus objetivos! Taller de PNL
62 Gestión de la inteligencia emocional y la empatía (PNL)
35 Coaching: desarrollo del potencial humano
36 Coaching nivel II: el líder coach
59 Gestión y prevención de conflictos
130 Consolidación de equipos (Team- Building)

## CONSOLIDACIÓN DE EQUIPOS MEDIANTE JUEGOS Y EVENTOS
48 Outdoor team building

## MEJORA DE HABILIDADES PERSONALES
104 Planificación y organización personal
45 Gestión eficaz del tiempo
112 Técnicas para hablar en público
127 Dominio de las presentaciones en público
137 Preparación y control de las presentaciones
63 Gestión y prevención del estrés
46 La fuerza de la automotivación
44 Desarrollo de la inteligencia emocional
133 Pensar de manera efectiva y eficaz
131 Coaching y PNL para alcanzar tus objetivos

## ÁREA COMERCIAL
89 Presupuestos comerciales: desarrollo, implantación y seguimiento
88 Cómo crear y consolidar clientes
87 Estrategias para la captación de clientes
132 Mejora de habilidades para el trato con clientes
47 Las cinco claves de la atención al cliente
30 Técnicas para la fidelización del cliente
113 Atención al cliente: on line, personal y telefónica
49 La venta proactiva (técnicas de PNL)
129 Gestión de reclamaciones y quejas
86 Cómo rentabilizar la participación en Ferias
95 Merchandising. Mejora la gestión del punto de venta
141 Atención al cliente y resolución de conflictos
142 Técnicas de venta

## COMERCIO INTERNACIONAL
65 Gestión del proceso exportador
66 Potencial exportador y búsqueda de mercados de destino
107 El proceso de internacionalización de la empresa
108 Negociación internacional
109 Transporte internacional

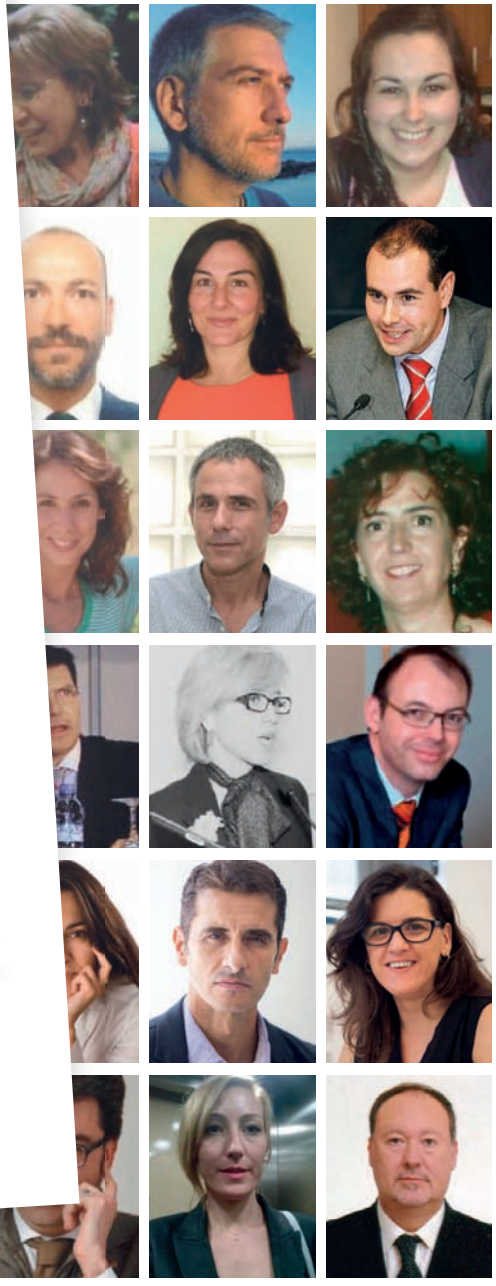
REF. NOMBRE CURSO

## COMUNICACIÓN Y MARKETING
33 Técnicas de marketing y comunicación
124 Cómo mejorar la comunicación escrita en la empresa
60 Mejora de la comunicación empresarial. Taller de PNL
91 Planes de comunicación y relaciones públicas
29 Estrategias de mejora en la atención al cliente
83 Cómo diseñar e implementar un plan de Marketing
106 Redacción publicitaria. Cómo escribir para generar respuesta
134 Organización de eventos
72 Protocolo y gestión de eventos
51 Fotografía e imagen de empresa
97 Cómo hablar en público sin miedos ni tensiones, con técnicas de interpretación
22 Gestión de patrocinios, mecenazgo y responsabilidad social corporativa
105 Cómo escribir un folleto comercial
73 Corrección de textos

## ÁREA FINANCIERA
75 Finanzas para no financieros
26 Finanzas para no financieros. Avanzada
135 Comprensión de los estados financieros
28 Análisis de estados financieros
27 Análisis de inversiones
32 Gestión de los impagados
76 Excel financiero avanzado: beneficios y potencialidades
77 Contabilidad económico-financiera. Nivel Iniciación
78 Contabilidad económico-financiera. Nivel Avanzado
79 Consolidación de estados financieros
80 Modelos y sistemas de imputación de costes
81 Bases y herramientas para el control de gestión
93 Elaboración rápida de las previsiones financieras
96 Negociación bancaria y fuentes de financiación

## COMPRAS, LOGÍSTICA, FABRICACIÓN Y MANTENIMIENTO
69 Organización, calidad y productividad
117 Introducción al Supply Chain Management (gestión de la cadena de suministro)
31 Gestión eficiente del Outsourcing
92 El margen de contribución: producir versus subcontratar
53 Gestión de calidad
114 Curso de Logística Inversa. Gestión óptima de devoluciones, residuos, embalajes y obsoletos
116 Gestión eficaz en el aprovisionamiento de MP y PA
118 Introducción y ventajas de las nuevas tecnologías en procesos logísticos
119 Organización óptima de almacenes y gestion del picking
120 Política y gestión óptima de stocks
121 Reducción de costes con tecnología RFID (Identificación por radiofrecuencia)
115 Curso de mozo y auxiliar de almacén
52 Curso de prevención de riesgos laborales
64 Medio ambiente en la empresa. Gestión ambiental y de residuos

## INFORMÁTICA, INTERNET Y REDES SOCIALES
71 Importancia de las redes sociales para la empresa
23 Aplicaciones empresariales de Linkedin
110 Cómo escribir para Facebook
111 Cómo redactar un emailing persuasivo
99 Curso de Excel básico
100 Curso de Excel intermedio
98 Curso de Excel avanzado
102 Curso de Power Point
102 Curso de Power Point avanzado
103 Curso de Word



* Fotos reales de formadores

# Usted elige el curso y el formador

## LOS MEJORES CURSOS CON LOS MEJORES FORMADORES

Formación presencial especializada para directivos y profesionales

Entidad de formación inscrita en: GOBIERNO DE ESPAÑA · MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL · SERVICIO PÚBLICO DE EMPLEO ESTATAL

Formación bonificable por: Fundación Tripartita para la formación en el empleo · Fondo Social Europeo

Feria Trafic.

# La movilidad socialmente responsable, a debate en el Foro Trafic 2015

El Salón Internacional de la Movilidad Segura y Sostenible, Trafic, organizado por Ifema y que celebrará su próxima edición del 29 de septiembre al 2 de octubre de 2015, en Feria de Madrid, está programando en su Foro Trafic una completa agenda de jornadas en las que las instituciones públicas y privadas más implicadas en la planificación y gestión de la movilidad urbana e interurbana abordarán las cuestiones más candentes en este ámbito fundamental de la sociedad actual.

El primer día de Feria, el martes 29 de septiembre, el Foro se centrará en las infraestructuras viales y su equipamiento, con sendas sesiones organizadas por el Comité de Seguridad Vial de la Asociación Técnica de Carreteras, ATC, y Foro Vial. El miércoles, 30, la Dirección General de Tráfico coordinará otra sesión sobre el vehículo conectado, que es el horizonte tecnológico de mayor alcance en la movilidad convencional, con grandes implicaciones tanto en la infraestructura como en la gestión del tráfico a medio y largo plazo.

Ese mismo día, en jornada de tarde, el Ayuntamiento de Madrid liderará un encuentro sobre Desarrollo Urbano y Movilidad Sostenible en el que participarán autoridades locales de las principales ciudades españolas, que plantearán la problemática actual en el ámbito de la movilidad urbana y las estrategias más adecuadas para abordarla.

El jueves, 1 de octubre, se celebrará la II Jornada sobre Seguridad Vial Urbana y el acto de entrega de los IV Premios de Seguridad Vial para Policías Locales, todo ello organizado por Unijepol, la Unión Nacional de Jefes y Directivos de Policía Local. También el día 1, distintas empresas de la Asociación Patronal de Empresas de Tráfico, Pemtra (Grupo Etra, Indra, Sice) expondrán sus casos de éxito, mientas que otros expositores de Trafic darán a conocer sus propuestas en materia de movilidad.

Finalmente, las Jornadas Técnicas del Foro Trafic 2015 concluirán el viernes, 2 de octubre, último día de Feria, con el Foro de la Movilidad Inteligente, bajo el lema 'Hacia una Movilidad Segura, Sostenible y Eficiente', organizado por ITS España.

También en el marco del Salón Trafic y enlazando con los temas del Foro, se celebrará el día 1 de octubre la Jornada Monográfica organizada por la Asociación de Talleres de Madrid, Asetra, sobre el impacto del vehículo conectado en el taller y en las relaciones de los talleres de reparación con sus clientes. ■

Feria Trafic.

## Trafic 2015 presenta los productos más vanguardistas

Los productos más vanguardistas en equipamiento para carreteras y seguridad vial vuelven a tener su espacio en la III Galería de la Innovación, dentro del Salón Internacional de la Movilidad Segura y Sostenible, Trafic.

Los productos de las empresas participantes en la feria seleccionados, se mostrarán durante los días de celebración de la misma, en un espacio habilitado al efecto, mostrando así el mejor perfil innovador de esta industria.

El Jurado, integrado por expertos del sector y representantes de las distintas asociaciones, seleccionó los productos, contemplando además en algunas categorías, en función de la calidad acreditada, algunas menciones especiales.

Es el caso de Safecross 2.0 (Cruce Inteligente con servicios 'Cloud' y 'Cooperative – ITS'), de la Sociedad Ibérica de Construcciones Eléctricas, S.A. – SICE, en la categoría de Infraestructuras Viarias; del Sistema Inteligente de Control Colaborativo y Asistencia a la Movilidad Urbana en las Intersecciones (Sherpa), de Electronic Trafic, S.A. (Grupo Etra), en el apartado de Sistemas Inteligentes de Transporte, y de Vivadén (Badén Inteligente Escamoteable), de Movivo Movilidad Sostenible, S.L., en Elementos y Productos para una Movilidad Sostenible, todos ellos distinguidos con su correspondiente mención especial. Además, en este último apartado, se ha incluido también el Sistema de Identificación de Bicicletas y Peatones – Sibicip, de Sistemas de Identificación y Mecanismos, S.L., Simec, y el ControlBike, de Tradesegur, S.A.

Asimismo, en la categoría de Seguridad Vial, la Solución Smartcam de Citilog, con cámaras IP de Axis Communications (Axernet Communications S.A.U); Fastrack City, presentado por Dow Europe GmbH; la Señal PF, expuesto por Sistemas de Prevención Vial S.L.U., y la Solución Lidar para el cálculo de visibilidad en carreteras, de Terrasolid Ltd, formarán parte también de esta III Galería de la Innovación.

Por último y entre las soluciones para Aparcamientos, se ha incluido el Icarous (Proyecto Icarous, S.A.), y el Smart Park, de Telecon Galicia, S.A.

# Ángel Pérez Alcarria, director de Seguridad del Grupo Casino Gran Madrid

## "Tras un año en vigor, todavía no se han visto los cambios tan esperados de la nueva Ley"

Ángel Pérez Alcarria, director de Seguridad del Grupo Casino Gran Madrid y socio experto de Aecra en Establecimientos Obligados e Infraestructuras Críticas, ha querido dar su punto de vista sobre la nueva Ley de Seguridad Privada en esta entrevista. Además, también ha opinado sobre los sistemas de prevención de delitos, el conocimiento que los ciudadanos tienen en la actualidad de los servicios de seguridad privada y sobre las futuras actividad que pretende llevar a cabo la Asociación Europea de Profesionales para conocimiento y regulación de las actividades de la Seguridad Ciudadana (Aecra) para el ejercicio 2015-2016.

***¿Después de haber transcurrido más de un año tras la entrada en vigor de la nueva Ley de Seguridad Privada, cuál es su valoración respecto de la misma?***

Qué duda cabe que la nueva Ley tan esperada por todos no ha logrado todavía los resultados deseados. El Reglamento que la debe 'aderezar' se está retrasando más de lo esperado. También considero que dicha Ley no ha modificado demasiado el cometido de los Departamentos de Seguridad. Los que en su día fuimos vigilantes jurados añoramos la consideración de agentes de la autoridad en el desempeño de las funciones, sin tener que estar actuando a instancias policiales. En resumen, después de un año en vigor, no se han visto de momento los cambios tan esperados.

***¿Estima que el ciudadano tiene un conocimiento correcto del alcance y contenido de los servicios de seguridad privada?***

Por supuesto que no. No se ha sabido 'vender' ni por las Empresas de Seguridad, ni por los Departamentos de Seguridad, ni por la Administración, el espectacular trabajo que desempeña día a día el personal de Seguridad Privada. Ni por nosotros mismos. Es una especie de complejo mal entendido el que tenemos, que parece que nos cuesta dar a conocer nuestro trabajo. Somos miles y miles de personas las que llevamos trabajando para nuestras empresas y colaborando activamente con la FFCC de Seguridad para ayudar a conseguir que el ciudadano se sienta seguro, protegido y libre, pero apenas se aprecia esta labor por la sociedad actual.

***¿Cree, como usuario que ha adoptado medidas de seguridad privada para protección de sus clientes y patrimonio, que dichas medidas son suficientes para la prevención del delito? ¿Considera que los servicios de videovigilancia y nuevas tecnologías aplicadas a la seguridad pueden beneficiar el desarrollo de su actividad?***

Por supuesto. Nuestra profesión así nos lo exige. El empresario que nos paga lo hace por este motivo. Tomamos todas las medidas de seguridad necesarias para prevenir el delito. A veces, teniendo que luchar contra viento y marea, ya que la crisis que estamos padeciendo ha hecho mucho daño en todos los sectores en general, pero particularmente en el sector de la seguridad. Esta crisis ha hecho que tengamos que multiplicarnos para conseguir, con menos medios técnicos y humanos, los mismos niveles de seguridad que teníamos en años de bonanza, con la particularidad que ha crecido la delincuencia y por motivos obvios, ha disminuido la presencia policial en nuestro entorno.

Referente a las nuevas tecnologías, gracias a ellas hemos podido 'suplir' la falta de recursos humanos que hemos padecido. Concretamente en el Casino Gran Madrid, las nuevas tecnologías como pueden ser las cámaras IP, el reconocimiento facial, la identificación de matrículas y el control de fichas por radiofrecuencia, han ayudado a incrementar exponencialmente la seguridad del casino.

***Como director de seguridad en una empresa dedicada a una actividad de riesgo de robo como son casinos de juego, ¿considera que las medidas de autoprotección que ha establecido son perfectamente compatibles con los servicios de seguridad privada que tiene contratados para protección de sus clientes y bienes?***

Totalmente. La seguridad integral se basa en un equilibrio entre las medidas de autoprotección adoptadas por la Dirección de Seguridad del Casino y los servicios de seguridad privada contratados. No es entendible que los servicios contratados no estén a la altura de esas medidas de autoprotección. Es más, la seguridad exterior existente en el casino es la imagen que se llevan nuestros clientes cuando nos visitan. Las medidas de autoprotección implantadas no se ven, pero no pasan desapercibidas para los que nos visitan con ánimos distintos a pasar una velada de ocio.

***¿Le parece interesante la existencia de un código de buenas prácticas en la ejecución de los servicios de seguridad privada frente a los usuarios de dichos servicios como garantía de la eficacia y eficiencia de dichos servicios?***

No es que me parezca interesante, es que lo considero imprescindible. Ha habido unos años que en algunas empresas de seguridad han considerado que el 'todo vale' es necesario para subsistir, y no es así. Al final, tanto para la empresa de seguridad como para el usuario, es necesario un código de buenas conductas. A ser posible, bidireccional.

***¿Qué acciones, eventos e iniciativas entiende que como socio experto de Aecra puede emprender dicha Asociación el próximo año 2015-2016 para la mejora de los servicios y protección de personas y bienes en el ámbito de los casinos? Enumérelas.***

En los casinos siempre tendremos el hándicap de la Ley de Protección de Datos, específica para nuestras empresas, así como la Ley de Videovigilancia. Somos establecimientos donde la vigilancia a través de CCTV es fundamental, debiendo estar al corriente de cualquier normativa al respecto. También la Ley de Espectáculos y el Derecho de Admisión son temas muy a tener en cuenta en nuestras organizaciones. ■

# Serafín Román,
## director general de HeiTel Dispositivos Electrónicos de Control

"El ciudadano sólo ha percibido cierta 'alarma social' ante la ampliación de las funciones y ámbitos de actuación de los vigilantes de seguridad"

Serafín Román, director general de HeiTel Dispositivos Electrónicos de Control S.L. y socio experto en nuevas tecnologías de la Asociación Europea de Profesionales para conocimiento y regulación de las actividades de la Seguridad Ciudadana, Aecra, ha opinado sobre la entrada en vigor de la nueva Ley de Seguridad Privada. Otros aspectos que se han abordado en esta entrevista son el nivel de conocimiento de los ciudadanos sobre los servicios de seguridad privada, el nivel tecnológico existente para la prevención de delitos y su opinión sobre la seguridad informática en general.

***¿Después de haber transcurrido más de un año tras la entrada en vigor de la nueva Ley de Seguridad Privada, cuál es su valoración respecto de la misma?***

La nueva Ley nos deja un camino muy importante que culminar. Es de agradecer que nos ponga a trabajar, pero también es una gran responsabilidad que ahora tiene que ser adoptada por los diferentes actores dentro de la Seguridad Privada. Estábamos acostumbrados a leer y cumplir y ahora tenemos mucho que aprender y que prepararnos para los nuevos retos de la seguridad. Por ahora ha sido el primer paso, esperemos que el futuro Reglamento nos aclare y puntualice las dudas que ha dejado la Ley.

***¿Estima que el ciudadano tiene un conocimiento correcto del alcance y contenido de las medidas y servicios de seguridad privada?***

No, en absoluto. El ciudadano no es consciente de la importancia que para la Seguridad Pública tienen las actividades realizadas por empresas y personal de Seguridad Privada. De los 72 artículos recogidos en la Ley 5/2014

de Seguridad Privada, el ciudadano sólo ha percibido cierta 'alarma social' ante la ampliación de las funciones y ámbitos de actuación de los vigilantes de seguridad en funciones siempre delegadas por Fuerzas y Cuerpos de Seguridad del Estado, cuando la realidad es que el nuevo texto legal pretende que la Seguridad Privada contribuya a completar la Seguridad Pública de la que forma parte en un plano de coordinación, en lugar de subordinación. Tampoco parece que esto sea un problema para los máximos responsables políticos. No se comprende cómo el Reglamento continúa sin ver la luz, y con elecciones generales, o puede que ésta sea la causa.

***¿Cree como prestador de soluciones y medidas para el mercado de la seguridad privada a nivel tecnológico que dichas medidas son suficientes para la prevención del delito? ¿Cree que los servicios de videovigilancia y nuevas tecnologías aplicadas a la seguridad pueden beneficiar el desarrollo de las actividades y servicios de seguridad privada? ¿Qué opinión le merece la seguridad informática?***

El marco normativo actual de la Seguridad Privada, a falta del Reglamento que desarrolle y complemente la Ley 5/2014 de Seguridad Privada, establece un catálogo de medidas a adoptar en las actividades de Seguridad Privada que indudablemente tienen una incidencia sustancial en la minoración del número de delitos. Sin embargo se precisan procedimientos que garanticen el correcto funcionamiento y la gestión eficaz de las señales. ¿Suficientes? Creo que este término es correcto hasta que los malos consiguen ganarte la partida. Es indudable que los servicios de videovigilancia están potenciando el desarrollo de servicios y actividades en el ámbito de la Seguridad Privada hasta tal punto que la Ley 5/2014 de Seguridad Privada dedica su artículo 42 a definir estos servicios, establecer en qué casos deben ser prestados por vigilantes de seguridad o guardas rurales y acotar los lugares donde no podrán utilizarse.

La Seguridad Informática hace mucho tiempo que ha dejado de ser algo ajeno a las actividades de las empresas y personal de Seguridad Privada. El apartado 6 del artículo 6 establece que también las empresas de seguridad privada pueden realizar "como Actividades Compatibles" tareas de Seguridad Informática, entendidas como el conjunto de medidas encaminadas a proteger los sistemas de información con el fin de garantizar la confidencialidad, disponibilidad e integridad de la misma o del servicio que aquellos prestan. Por su incidencia directa en la seguridad de las entidades públicas y privadas, se les podrán imponer reglamentariamente requisitos específicos para garantizar la calidad de los servicios que presten.

***¿Le parece interesante la existencia de un código de buenas prácticas en la ejecución de los servicios de seguridad privada frente a los usuarios de dichos servicios, y ello como garantía de la eficacia y eficiencia de los mismos?***

Me parece fundamental establecer un código de buenas prácticas que haga hincapié en las políticas de contratación, en la cualificación profesional del personal en plantilla y en la adecuación de los perfiles a los servicios que se van a desempeñar. Las empresas que se adhieran habrán de comprometerse a dar formación específica a sus trabajadores en centros homologados en función de las tareas que se vayan a asumir. También velará por que se dignifique el sector de la Seguridad Privada y porque las labores que desempeñen sus profesionales se rijan por los principios de buen gobierno, responsabilidad social y calidad.

***¿Qué acciones, eventos e iniciativas entiende que como Socio Experto de Aecra puede emprender dicha Asociación el próximo año 2015-2016 para mejora de los servicios de seguridad privada? Enumérelas.***

El trabajo que Aecra está haciendo ya es fundamental, por aportar alguna idea y en la parte tecnología de la seguridad, creo que presentarse en las academias – escuelas de formación profesional aportarían un conocimiento extra a los futuros trabajadores en tecnologías de seguridad, algo que hoy sólo se adquiere desde dentro de las empresa y con acuerdos de/por fabricantes. Fomentar esta formación técnica de calidad, que hoy no existe. ■

# Oriol Tinoco,

## director técnico de Worktocloud (WTC)

### "Nuestro software destaca por la medición objetiva y automatizada de la productividad laboral de cualquier empleado tanto dentro como fuera de la oficina"

Unas 10 empresas y alrededor de 300 personas ya se benefician de las ventajas que proporciona Worktocloud (WTC). Se trata de un software destinado a medir y mejorar la productividad laboral del que se pueden beneficiar, en especial, las empresas de seguridad privada –gracias, asimismo, a su APP 'WTC Security'-. Oriol Tinoco, director técnico de WTC, detalla dichos beneficios, entre las demás ventajas que proporciona este novedoso software.

**María Fernández Peláez**

***En líneas generales, ¿podría explicar brevemente qué es Worktocloud?***

Worktocloud es un software para mejorar los hábitos de trabajo y la productividad laboral. Es una nueva disciplina de trabajo con las últimas novedades en tecnología que ayuda a los empleados y a las empresas a encontrar el equilibrio entre eficiencia, eficacia y libertad laboral. Nuestro software destaca por la medición objetiva y automatizada de la productividad laboral de cualquier empleado tanto dentro como fuera de la oficina para diferentes tipos de trabajos: administrativos, comerciales, operarios y vigilantes de seguridad, entre otros.

***¿Hacia qué usuarios (empresas, personas...) está enfocado el software WTC? ¿Qué funciones pueden desempeñar con la misma?***

Cualquier empresa o/y autónomo que trabaje con ordenador o móvil puede utilizarlo, pero especialmente las empresas de seguridad privada ya que ellas pueden beneficiarse de todas las funcionalidades:

- Geolocalización de los vigilantes y control de rutas.
- Control de rondas con el móvil y volcado automático de los partes en la nube.
- Envío automático de los partes de servicio al cliente final por email.
- Integración de nuestra API en su web para que el cliente pueda ver los informes desde su web.
- Control de las llamadas realizadas en el servicio.
- Monitoreo de oficinistas y comerciales.

***¿Qué beneficios aporta Worktocloud a quien haga uso de sus servicios?***

- Ahorra tiempo y dinero en la realización y supervisión de los cuadrantes, del cálculo de horas, avisos de impuntualidad, etc…
- Simplifica la gestión de informes y rondas. Los partes del servicio se suben automáticamente a la web desde el móvil evitando los desplazamientos innecesarios para recoger los informes.
- Eficacia en el control de cualquier empleado. Control de horarios automático, online y en tiempo real. Desde su oficina/ casa sabrá lo que está ocurriendo en todo momento en su empresa.

***La compañía nació en mayo del pasado año, ¿qué retos se marcaron tras la creación de Worktocloud? ¿Cuáles eran los objetivos de la compañía?***

El primer reto era técnico, es decir, conseguir que todo funcionara como un único sistema integrado. Conseguir recopilar datos de muchos teléfonos móviles y de ordenadores simultáneamente, enviar los datos a la nube y visualizarlo todo en la web; implica trabajar con tecnologías muy diferentes y conseguirlo ha sido un gran logro tecnológico. Los objetivos de la compañía eran desarrollar el servicio, crecer y sobretodo consolidar a los primeros clientes.

***Actualmente, ¿cuántas empresas/personas se benefician aproximadamente de las soluciones que ofrece este software?***

Unas 10 empresas y alrededor de 300 personas aproximadamente.

***Recientemente han lanzado una APP - WTC Security dirigida exclusivamente al sector de la vigilancia y la seguridad. ¿En qué consiste esta aplicación?***

Además de lo mencionado anteriormente WTC Security se centra en el control de rondas de los vigilantes y en la elaboración automatizada de las partes de servicio así como el envío a los clientes. La ventaja es que se puede hacer todo con un simple teléfono móvil, en vez de los costosos dispositivos que se usan hasta ahora.

***¿Qué pasos tienen que seguir las empresas para empezar a utilizar WTC Security?***

Deberían ponerse en contacto con nosotros a través de la web www.worktocloud.es o enviando un email a oriol-tinoco@worktocloud.es para poderse beneficiar del mes de prueba gratis sin compromiso. Pero básicamente los pasos son los siguientes:

- Creamos la cuenta y configuramos los trabajadores, los servicios y asignamos los trabajadores a los servicios. (15 minutos de tiempo).
- Instalamos los puntos NFC (1 euro cada punto) que servirán para hacer la ronda en cada servicio (1 hora por servicio).
- Descargamos la aplicación WTC Security en el móvil y hacemos una primera ronda de prueba.
- Ya está, con estos sencillos pasos ya tendremos automatizado el control de un servicio.

***¿Qué coste anual le supone a una empresa el uso de esta herramienta?***

El precio es de 5 euros por usuario al mes.

***¿Cuánto dinero ahorraría al año utilizando WTC Security?***

Mucho dinero, evidentemente, depende del tamaño de la empresa. Pero solamente, el quitarse de encima la pesada tarea de: coger los lectores de fichas NFC y volcar los datos a un ordenador; elaborar los partes de servicio y enviar los partes al cliente ya sea por e-mail o en papel, ya es un ahorro de tiempo y de errores humanos enorme.

***¿Qué crecimiento pronóstica de la APP a corto y medio plazo?***

Es difícil de decir, pero extrapolando los datos actuales, esperamos doblar el número de clientes el año que viene.■

# Radar de estado sólido,

## una solución revolucionaria para protección perimetral y grandes áreas

Hasta hace poco el radar era una tecnología prácticamente reservada a usos militares y a la protección de infraestructuras críticas de alta seguridad. Los sistemas disponibles en el mercado eran caros, pesados y muy complicados de calibrar lo que hacía de ellos una solución poco atractiva para la mayoría de proyectos de seguridad. El radar de estado sólido SpotterRF comercializado en España por CCTV Center supone una alternativa revolucionaria, económica y flexible capaz de detectar objetivos móviles del tamaño de una persona a más de 1.200 m de distancia.

El radar de estado sólido SpotterRF destaca por su diseño compacto y reducido tamaño.

**Marta Tortosa,**

**responsable de Marketing en CCTV Center**


La unidad de radar puede integrarse fácilmente con otros radares y cámaras móviles PTZ.

La mayoría de sistemas de radar para seguridad se basan en radares giratorios capaces de cubrir 360º alrededor de la unidad. El planteamiento es bueno en la teoría pero, en la práctica, los radares giratorios plantean una serie de problemas que los convierten en sistemas caros, difíciles de gestionar y costosos de mantener.

Los radares de estado sólido SpotterRF comercializados por CCTV Center han sido diseñados para contrarrestar los inconvenientes de los radares giratorios ofreciendo una solución de detección por radar potente y fiable. El resultado es un sensor de radar compacto, de apenas 25cm, con un peso que oscila entre 700 g y 3 kg dependiendo del modelo y que puede instalarse en un poste o infraestructura existente sin necesidad de realizar obra civil.

## Fácil y rápida configuración

Frente a otros sistemas de radar muy complejos de calibrar que requieren la contratación de personal técnico especializado, el radar compacto SpotterRF puede configurarse en apenas 10 minutos sin necesidad de conocimientos especializados a través intuitiva interfaz web.

## Área de cobertura y distancia de detección

Los radares de estado sólido SpotterRF generan un área de cobertura elíptica con un ángulo de apertura de 90º de modo que, aunque no es posible cubrir 360º con una sola unidad, resulta muy fácil combinar varias unidades para cubrir eficazmente grandes áreas y perímetros.

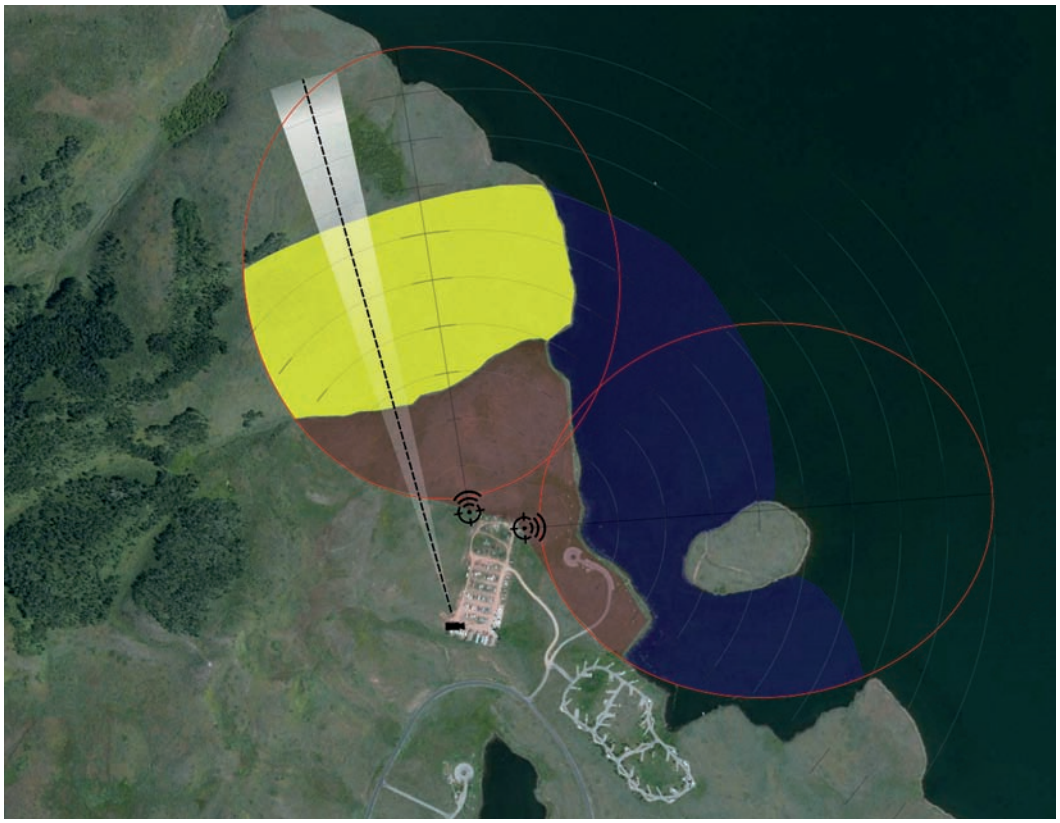
Un sensor de radar SP-C40 puede detectar y seguir un objetivo en movimiento del tamaño de una persona en

## Ventajas del radar de estado sólido

A diferencia de los radares giratorios que son pesados, complejos de configurar y sensibles a los desniveles del terreno y a los obstáculos, los radares de estado sólido SpotterRF destacan por su reducido tamaño que los convierte en equipos muy fáciles de instalar y reubicar. Las unidades pueden situarse a gran altura para aprovechar mejor el campo de visión y evitar obstáculos. De hecho, pueden orientarse para vigilar tanto el interior como el exterior del perímetro y, en el segundo caso, son capaces de detectar objetivos incluso a través de una alambrada.

Protegidos por una robusta carcasa de exterior, resistente al agua (incluso al agua a presión), los radares están catalogados con un índice de protección IP67 y pueden funcionar en rangos de temperatura de -30º a +65º. Además, como no disponen de partes móviles sujetas a desgaste, no requieren mantenimiento.


Los radares compactos SpotterRF generan un ángulo de cobertura elíptica que permite cubrir grandes áreas.



Interfaz de control NIO.

cualquier punto de la zona de detección a 350 m de distancia. Y puede hacerlo en tiempo real, tanto de día como de noche, con lluvia, niebla y nieve.

El modelo SP-C550 puede detectar objetivos del tamaño de una persona a una distancia de 850 m y del tamaño de un coche a 1.500 m. Con el modelo SP-C550-EXT la distancia de detección se amplía hasta los 950m (para personas). El SP-C950 (en trámites de homologación) es capaz de detectar un objetivo del tamaño de una persona a una distancia de 1.350 m.

### Integración con cámaras PTZ y otros radares

El sistema de radar SpotterRF está pensado para integrarse fácilmente con otros dispositivos de seguridad presentes en cualquier instalación de seguridad como cámaras domo PTZ móviles y otras unidades de radar. El servidor NetworkedIO (NIO) permite integrar múltiples radares SpotterRF y cámaras PTZ usando una interfaz de usuario georeferenciada que puede monitorizarse desde un navegador web convencional. Cuando el radar detecta una amenaza, el servidor NIO aplica los filtros de comportamiento, envía un comando de alerta a una cámara asociada para que siga el objetivo en movimiento y envía una alarma al centro de control para alertar al operador y poner en marcha el protocolo de seguridad.

El NIO armoniza los esfuerzos tanto de la cámara como del radar para ofrecer una seguridad completa en todo el perímetro. Además, pueden configurarse diferentes tipos de movimiento en zonas definidas por el usuario que pueden activar distintos tipos de notificaciones.

En definitiva, el radar de estado sólido SpotterRF es una excelente solución para proteger perímetros y grandes áreas ya que ofrece un sistema de detección eficaz a larga distancia, tanto de día como de noche, en prácticamente cualquier condición meteorológica sin los inconvenientes y costes de mantenimiento de otras soluciones. Por esta razón los sistemas de detección por radar SpotterRF están siendo usados para proteger infraestructuras críticas, puertos, aeropuertos, centrales nucleares, puentes, plantas industriales, huertas solares, subestaciones eléctricas o centros de datos en todo el mundo. ■

tecnifuego AESPI

# Asociación Española de Sociedades de Protección contra Incendios

## Trabajando por la calidad, la eficacia, la innovación, el cumplimiento legislativo y la inspección en el mercado de la seguridad contra incendios


Madrid - Secretaría General
C/ Doctor Esquerdo, 55, 1ºF.
28007 Madrid
Tel. 914 361 419
Fax 915 759 635

Oficina Barcelona
C/ Casanova, 195, entresuelo
08036 Barcelona
Tel. 932 154 846
Fax 932 152 307

info@tecnifuego-aespi.org
www.tecnifuego-aespi.org

# Escalera anticaídas sistema Faba A12

Para acceder en altura durante trabajos de mantenimiento de estructuras o trabajos en torres, edificios, antenas, postes, chimeneas y cisternas es necesario un dispositivo adecuado, cómodo, seguro y certificado. En algunas de las aplicaciones anteriormente citadas, durante mucho tiempo, se ha recurrido a las escaleras tipo 'jaula' o de 'gato', escaleras provistas de una protección circundante metálica. Como alternativa a éstas, hoy existen sistemas que sustituyen la 'jaula' por un raíl guía o un cable metálico de retención.

**Alex Comas Aguadé, product mánager Protección Anticaídas de Tractel**

Alex Comas Aguadé, product mánager Protección Anticaídas de Tractel.

### Conformidad respecto de las distintas normativas

Las escaleras tipo 'jaula' se ven todavía como dispositivos permitidos, tanto en el Real Decreto 486/1007, como en su Anexo I punto 8, donde se especifica que "en las escalas fijas la distancia entre el frente de escalones y las paredes próximas al lado de ascenso será, por lo menos, de 75 cm". A su vez, en la NTP 408 se menciona que el "diámetro máximo de jaula (es) 0,60 cm". De modo que ambas indicaciones sobre las medidas de la jaula no coinciden y contrastan con lo descrito en las siguientes normativas europeas:

1. La Norma UNE EN 547 01-02-03 del 2009-Seguridad de las máquinas-Medidas del cuerpo humano, que define los criterios antropométricos de referencia para la construcción de la maquinaria y prevé un espacio superior a 74 cm a su espalda en recorridos verticales.
2. La Norma EN ISO 14122-4: 2004-Seguridad de las Máquinas-Medios de acceso permanente a máquinas e instalaciones industriales-Parte IV: Escaleras fijas; en el punto 4. 5 se define que la distancia libre en el interior de la jaula debe estar comprendida entre 650 y 800 mm.

En cualquier caso, tanto con 60 cm, como con 74 cm de diámetro, no es posible llevar bolsa o maleta de herramientas. Las escaleras con jaula recientemente puestas a examen de la Comisión Europea han sido rechazadas como dispositivos anticaída. Entre los motivos adoptados por la Comisión se evidencia, de hecho, de forma experimental, que la caída no se detiene o, si se detiene, conlleva daños colaterales y dificulta la recuperación del accidentado. A continuación citamos extractos de los motivos en relación con la cuestión.

Faba ofrece un sistema de deslizamiento interno, único en el mercado.

## Decisiones de la Comisión Europea inherentes a las escaleras fijas con jaula

"Decisión de la Comisión 2006/ 733/ CE del 27 de octubre de 2006, relativa a la no publicación de la referencia de la Norma EN ISO 14122-4: 2004 «Seguridad de la Máquinas-Medios de acceso permanente a máquinas e instalaciones industriales-Parte 4: Escaleras fijas» de conformidad con la Directiva 98/37/CE del Parlamento Europeo y del Consejo [notificada con el número C (2006) 5062] (Texto importante para los fines del SEE) (DOUE L. 299 del 28. 10. 2006)".

Extractos de los motivos de la decisión:

- No respetan los requisitos esenciales 1.1.2 (b) (principios de integración de la seguridad) y 1.5.15 (riesgo de resbalones, tropiezos o caídas).
- El dispositivo anticaídas no impide la caída desde una escalera fija.
- Los dispositivos anticaídas presentan varias desventajas.
- Contrariamente al requisito esencial (omisones), sitúan los requisitos para las medidas de protección integradas (la jaula) al mismo nivel que los requisitos únicamente adecuados para riesgos residuales (EPI).

## Consideraciones de diseño para acceso seguro a través de escaleras

Las normas y notas técnicas de referencia, particularmente NTP 408 y la Norma EN 14122-4 para Europa, especifican que las dos alternativas principales para la protección contra caídas de los usuarios de escaleras fijas son las jaulas de seguridad y los dispositivos anticaída de tipo guiado como las líneas de vida verticales rígidas, éstas últimas certificadas con la norma EN 353-1. A continuación, exponemos brevemente los criterios de identificación que pueden guiar al diseñador a la elección de la más adecuada.

## Riesgo residual

El llamado 'riesgo residual de caída' que debe cumplir un usuario que se desplaza a lo largo de una escalera con protección circundante tipo 'jaula', radica en el hecho de que la caída puede no ser detenida por la jaula. En cambio, el uso de un sistema anticaídas tipo línea de vida vertical rígida, junto con el uso de un punto de anclaje al que pueda conectarse el usuario una vez haya llegado a la altura/nivel deseado, es un sistema capaz de eliminar este riesgo residual, ya que el usuario siempre está protegido de la caída en cualquier lugar.

## Número de personas que pueden utilizar la escalera a la vez

Este número no está definido en las normas. Los sistemas anticaídas o líneas de vida verticales rígidas permiten que varios usuarios suban al mismo tiempo. Esto es posible porque la distancia de frenado, en caso de una caída, queda definida, y las cargas y requerimientos de fijación del sistema están bien definidos. En el caso de los fabricantes de escaleras con protección circundante (jaula) deben indicar en su documentación si la escalera puede ser usada por una sola persona o varias personas a la vez.

Hoy en día existen sistemas que sustituyen la 'jaula' por un raíl guía o un cable metálico de retención.

### Procedimiento de uso y rescate. Obligación de uso de arnés

Para los sistemas anticaídas tipo línea de vida rígida está claramente definido que, para su uso, el usuario debe estar equipado con un arnés anticaídas. Este requisito es esencial para el procedimiento de rescate. En las escaleras con protección circundante o 'jaula' no hay indicaciones en este sentido: el usuario podría subir por la escalera sin el uso de ningún dispositivo anticaídas ni arnés; esto

requiere que se tenga en cuenta en la definición de los procedimientos de emergencia y de rescate del usuario herido, en caso de quedar atrapado en la 'jaula' tras una caída.

### Uso de casco de protección

En el uso de escaleras Faba de Tractel está previsto el uso del casco. Al no haber estructura detrás del usuario, no hay ningún riesgo de golpe. En cambio, en las escaleras tipo 'jaula' el usuario está expuesto a darse un golpe con los aros y elementos circundantes de la escalera. En este sentido, la Norma EN 397 especifica, en el punto 3.1, que el casco está destinado a "proteger la parte superior de la cabeza del usuario". La parte inferior de la cabeza o nuca no está considerada en la norma ni los posibles ensayos. En el punto 3.10 también habla de "accesorios de protección posterior del casco", pero no existen estos accesorios específicos en el mercado.

### Procedimiento de rescate de accidentados

En caso de caída, hay que rescatar al usuario en el menor tiempo posible. La forma más rápida para rescatar/descender al usuario accidentado es mediante un descensor de velocidad controlada EN 1496. El proceso de rescate requiere que el socorrista llegue hasta donde cayó el accidentado, se ubique por encima de su vertical, conecte al accidentado al descensor y, si es necesario, lo eleve ligeramente para luego descenderlo con precaución. En caso de escaleras provistas de línea de vida vertical rígida, este procedimiento de rescate funciona de forma rápida, incluso si el accidentado está inconsciente, ya que éste estará equipado con un arnés y conectado a la línea de vida vertical rígida mediante un dispositivo anticaídas. En el caso de una caída en una escalera con protección tipo 'jaula', el rescate puede plantear grandes dificultades. La primera es la composición del trabajo del equipo de rescate ya que, debido a que hay riesgo de daños colaterales graves, debe preverse la presencia constante de personal médico o paramédico. La segunda está relacionada con la presencia o no de un arnés al que conectar el descensor. La tercera, tiene que ver con el hecho de que el socorrista no tiene espacio para conectarse al accidentado.

### Sistema anticaída Faba A12

El uso de la protección anticaída Faba permite recorrer con total seguridad escaleras/vías de salida en instalaciones fijas.

En el uso de escaleras Faba de Tractel está previsto el uso del casco.

## Faba ofrece un sistema de deslizamiento interno único en el mercado

### Aplicaciones

En altura: torres eléctricas, repetidores, postes de telecomunicaciones, chimeneas, molinos, edificios, depósitos elevados, pilastras de puentes, andamios e instalaciones industriales. En profundidad: acceso a alcantarillas, estaciones de servicio y depósitos, minas, depósitos de agua y de estabilización y pozos y canales verticales en general.

### Ventajas

Gracias al carro anticaída (dispositivo anticaída móvil), el sistema permite subir y descender con seguridad a cualquier altura y profundidad. Faba ofrece un sistema de deslizamiento interno, único en el mercado. Esto significa que todos los rodillos del carro anticaída deslizan por el interior del carril. Por lo tanto, es posible compensar de manera óptima la tolerancia constructiva, y el carro está en todo momento listo para accionar el bloqueo. En subida, el carro desliza fácilmente, por lo tanto no hay ningún esfuerzo por rozamiento, como se ha podido confirmar de forma regular con profesionales que trabajan de forma cotidiana con este sistema. El sistema, de fácil instalación, incluye numerosos componentes combinables, con los cuales es posible satisfacer cualquier exigencia.

### Sistema A12, principio simple y seguro

1. Escalera anticaída Faba Sistema A12 con carril central fijado a la estructura.
2. Carro anticaída que corre por el carril fijo.
3. Arnés de seguridad conectado directamente al carro.
4. El sistema Faba es el único que tiene todos los mecanismos de deslizamiento dentro de la guía, garantizando siempre un perfecto y suave deslizamiento.

Todos los sistemas son conformes a la Norma DIN 18799 1 y 2, EN 353 1, VG11 CNB/P/11.073 y CEE 89/686.■

# Índice de anunciantes

TRAFIC

SALÓN INTERNACIONAL DE LA MOVILIDAD SEGURA Y SOSTENIBLE

29 SEPTIEMBRE A 2 OCTUBRE 2015
MADRID-ESPAÑA

ORGANIZA
IFEMA Feria de Madrid

CONECTIVIDAD

# TRAFIC 2015

SOSTENIBILIDAD

SEGURIDAD

APARCAMIENTO

INFRAESTRUCTURAS

## TECNOLOGÍA E INNOVACIÓN PARA UNA MOVILIDAD SEGURA, SOSTENIBLE Y CONECTADA

PROMUEVEN
MINISTERIO DE FOMENTO
MINISTERIO DE INTERIOR
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

COLABORAN
EUSKO JAURLARITZA GOBIERNO VASCO
SEGURITASUN SAILA / DEPARTAMENTO DE SEGURIDAD
servei català de Trànsit

www.trafic.ifema.es

LINEA IFEMA
LLAMADAS DESDE ESPAÑA
INFOIFEMA 902 22 15 15
LLAMADAS INTERNACIONALES (34) 91 722 30 00
trafic@ifema.es

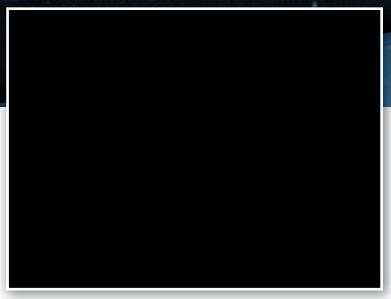

NUEVO

# FLIR TCX

## Cámaras térmicas bullet y minibullet

Las nuevas FLIR TCX abren un nuevo rango de aplicaciones gracias a su capacidad para ofrecer imágenes térmicas de alto contraste a un coste muy asequible y con una funcionalidad más que probada para detección a corta y media distancia.

- Imágenes nítidas incluso en total oscuridad
- Alto rendimiento 24/7 tanto de día como de noche
- Detección eficaz a corta y media distancia
- Eliminación de falsas alarmas
- Ideal para protección de zonas residenciales, casas, empresas, edificios públicos y locales comerciales



Visión normal

Cámara térmica

Tel. : +34 96 132 11 01
Fax : +34 96 132 11 08
E-mail : cctvcenter@cctvcentersl.es

CCTV CENTER
World Vision

www.cctvcentersl.es