CUADERNOS DE SEGURIDAD

Núm. 319 • FEBRERO 2017 • 10 euros

PUNTOSEGURIDAD.com

Seguridad en centros universitarios

Sistemas de Análisis de Vídeo

II CONGRESO NACIONAL DE JEFES DE SEGURIDAD

II Congreso Nacional de Jefes de Seguridad

Dahua Solución Inte

Banca y

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

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

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

ISO 9001:2000

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

grada de Seguridad

Finanzas

Centro de Seguridad

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

Video Wall

Plataforma de gestión de vídeo

Multi-lente Paronámica Cámara

Outdoor

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

Smart WDR IR Cámara

Entrada

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

Gestión avanzada de accesos

Cámara con tecnología ANPR integrada

· Válido para todas las matriculas europeas.
· OCR incluido, identificación de velocidad del vehículo <40km/h.
· Índice de captura >98%; tasa de acierto de matrículas>95%.
· Lista negra/blanca de acceso. Búsqueda de matrículas borrosas.
· La solución ANPR tiene una alta rentabilidad en aparcamientos, control de accesos y otros sistemas.

· ITC237-PU1A-HL/IRHL ·

· ITC217-PW1B-IRLZ10 ·

· ITC237-PW1A-IRZ ·

· NVR608-4KS2 ·

· DSS4004-T ·

CE FC UL RoHS **ISO 9001:2000**

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

bydemes · CCTV CENTER · iPTECNO

SECTOR DE LA SEGURIDAD PRIVADA

El sector ante nuevos desafíos

La seguridad del ciberespacio se ha convertido en uno de los grandes e inminentes desafíos del siglo XXI. La sociedad en general -y las empresas de cualquier actividad en particular- cada vez es más vulnerable a los nuevos retos de seguridad propios de un mundo interconectado y globalizado donde los delitos transpasan fronteras. Ha llegado el momento de unificar criterios, y normativas, entre todos los agentes sociales implicados para generar mecanismos y soluciones que hagan frente a este nuevo tipo de amenazas. Estamos ante un nuevo escenario social y delictivo que requiere de mecanismos e instrumentos adecuados para prevenir, y en su caso combatir, de manera efectiva las nuevas amenazas.

Amenazas y ciberataques por los que las empresas españolas pierden 1,4 millones de dólares al año; así se desprende de la Encuesta Mundial sobre el Estado de la Seguridad de la Información elaborada por PWC -cuyo resumen encontrará el lector en páginas posteriores-, donde, por otro lado, se revela que la digitalización de los negocios es el factor impulsor de la inversión en ciberseguridad de las empresas en España y en el mundo. Y este incremento de los presupuestos en ciberseguridad ha dado sus frutos este último año donde, según datos del informe, las compañías tanto a nivel global como en nuestro país, están viendo cómo los incidentes de seguridad se han reducido.

Y si de predicciones hablamos, Internet de las Cosas será el principal blanco de ataques cibernéticos en 2017, según el Informe de Trend Micro «Próximo Nivel- 8 predicciones de Seguridad para 2017», en el que además se adelanta que este año traerá consigo «una mayor amplitud y profundidad de los ataques, con agentes de amenazas maliciosas que diferenciarán sus tácticas para capitalizar el cambiante panorama tecnológico».

Ante estos nuevos retos y desafíos de seguridad, y adelantándose a las necesidades más apremiantes del sector de la seguridad, el próximo mes de mayo se celebra el 17 y 18 de mayo en Barcelona Security Forum 2017, y dentro de ese marco, el equipo de profesionales de Peldaño trabaja en la configuración de un congreso desglosado en dos grandes temáticas: Global Day y Ciber Day, donde además de analizar aspectos relacionados con la seguridad global, se potenciarán las temáticas enfocadas a la ciberseguridad con intervenciones sobre Ramsonware y otros malware en auge, la figura del CISO, o la coordinación estatal ante la Directiva NIS.

Previamente, el próximo 5 de abril, Barcelona será escenario del II Congreso Nacional de Jefes de Seguridad, encuentro profesional organizado por PELDAÑO y la Asociación de Jefes de Seguridad de España (AJSE), que tiene entre sus objetivos prioritarios crear un foro de debate y análisis que reúna al sector de la Seguridad en una jornada de trabajo, en la que se analizará de forma exclusiva la figura del jefe de Seguridad y sus funciones, sus retos ante las nuevas amenazas, así como su papel como colaborador entre la Seguridad Pública y Privada.

Dos citas imprescindibles para un sector que hará frente a inminentes desafíos.

3 EDITORIAL

— *El sector ante nuevos desafíos.*

8 IICONGRESO NACIONAL DE JEFES DE SEGURIDAD

— *II Congreso Nacional de Jefes de Seguridad, en marcha.*

10 SECURITY FORUM

— *Security Forum 2017,comienza la cuenta atrás.*

12 EN PORTADA

SEGURIDAD EN CENTROS UNIVERSITARIOS

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

© Jacob Lund – stock.adobe.com

ENTREVISTAS:

— **Carlos Baéz.** Director de Servicios Generales. Universidad de Alcalá. Alcalá de Henares. Madrid.
— **Juan Carlos Miranda.** Jefe de Servicios Generales. Universidad Francisco de Vitoria. Madrid
— **Ana Caro Muñoz.** Coordinadora de Proyectos de la Universidad Autónoma de Madrid.
— **Juan M. Uriarte.** Safety and Security Director, Laureate Europe (Laureate International Universities).
— **Marisol Diana Valiente.** Directora de Seguridad. Universidad de Alicante.
— **José Luis Reñón Castellanos.** Jefe del Servicio de Infraestructuras. Universidad de Cantabria.

ARTÍCULOS:

— Ventajas de la gestión de llaves en centros educativos, por **Fernando Pires.**

CUADERNOS DE SEGURIDAD

www.puntoseguridad.com

Nº 319 • FEBRERO 2017

Peldaño

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

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

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

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

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

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

— Sistemas centralizados, claves para la seguridad en centros univeristarios, por **Borja García-Albi Gil de Biedma.**
— Universidad: subir nota en Protección contra Incendios, por **Antonio Tortosa.**

44 SISTEMAS DE ANÁLISIS DE VÍDEO

ARTÍCULOS:
— Análisis de Vídeo, un mundo de nuevas aplicaciones, por **José Luis Romero.**
— Sistemas de Análisis de Vídeo Inteligente para todo tipo de negocios, por **Alfredo Gutiérrez.**
— Sistemas Inteligentes de Vídeo, por **Alberto Alonso**.

ENTREVISTAS:
— **Andreas Wolf,** Product Manager Intelligent Video Surveillance. Dallmeier

58 CIBERSEGURIDAD

— Más de 1.400 profesionales en las X Jornadas CCN-CERT.
— CyberCamp vuelve a batir récord de asistentes.

— Informe Trend Micro: El Internet de las Cosas, principal blanco de ataques cibernéticos en 2017.
— Informe PWC: Las empresas españolas pierden 1,4 millones de dólares al año por ciberataques.

66 SEGURIDAD

ENTREVISTAS:
— **Cristian Hernández Berzosa.** Jefe de Proyectos del departamento de Ingeniería, Proyectos y Grandes Cuentas. By Demes Group.

ARTÍCULOS:
— Reglamento General de Protección de Datos: mayor regulación menor seguridad jurídica, por **Ana Marzo**.
— Objetivos de la AEPD para 2017.
— Informe de la Fundación ESYS: el reglamento de Datos de la UE: una perspectiva empresarial.
— Balance Seguridad Vial 2016.
— Informe Checkpoint Systems: retos y perspectivas del comercio para 2017.

80 C.S. ESTUVO ALLÍ

— Cepreven celebra su 41 Encuentro Anual.
— Eurocloud evoluciona y ahora es Cloud Community Europe.

83 FERIAS

— HOMSEC 2017 con un Pabellón de China entre sus nuevos expositores.

84 ACTUALIDAD

— José Manuel Leceta, nuevo director general de Red.es.
— Synology redefine el concepto de almacenamiento en red NAS para hacer las pymes más competitivas.
— UGT solicita adelantar la edad de jubilación a los vigilantes, escoltas y guardas rurales.

— Ingram Micro distribuye las soluciones DynaScan para España y Portugal.
— Casmar presenta las soluciones Smart Home de Risco en ciudades españolas.
— La Ertzaintza lanza una app para mejorar la atención del ciudadano.
— LSB: Se endurecen los controles a empresas en relación a las horas realizadas por su trabajadores.
— Securitas Direct: Segovia, Soria, Ávila y La Rioja, las provincias más seguras en España en 2016.

96 EQUIPOS Y SISTEMAS

— Dallmeier: cámara 4K Ultra HD.
— Hanwha Techwin: nueva cámara ojo de pez 360 grados.
— By Demes anuncia la nueva generación de productos Hyundai.
— Dahua: el nuevo software Back-end ANPR amplía la solución ANPR con más calidad y fiabilidad.
— Etc.

114 AGENDA

— Ferias y eventos en el sector.

MARZO 2017 - Nº 320

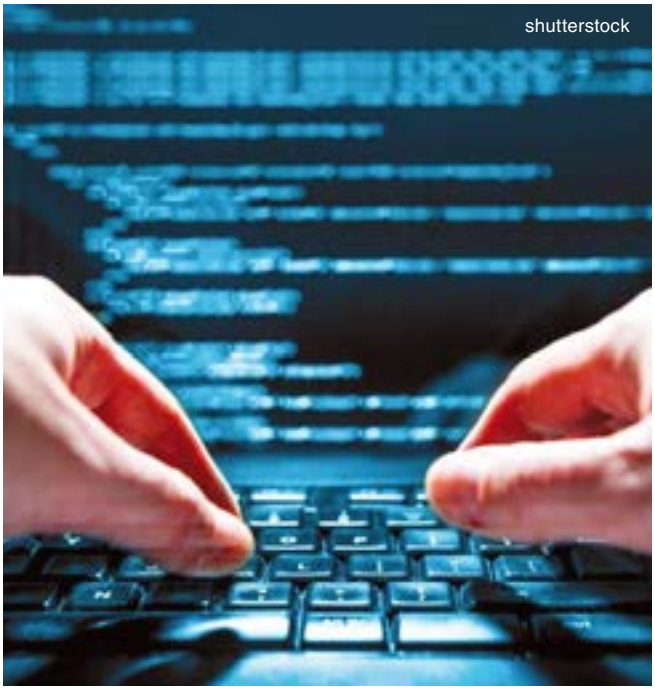
EN PORTADA

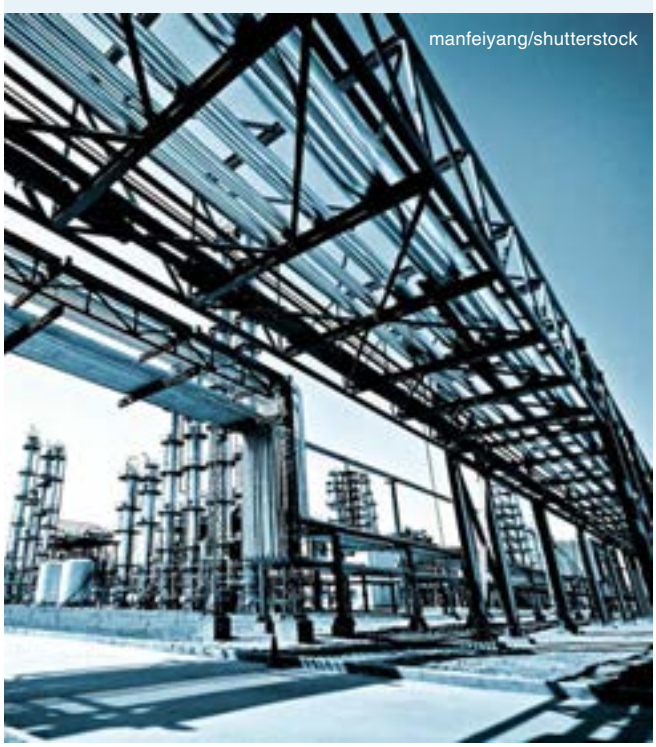
CIBERSEGURIDAD

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

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

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


shutterstock


manfeiyang/shutterstock

SEGURIDAD EN LA INDUSTRIA

La complejidad de la actividad industrial, el entramado legislativo en materia de seguridad, así como el ya más que conocido amplio catálogo de riesgos presentes, hacen preciso llevar a cabo un detallado estudio y análisis conjunto adecuado de todos estos aspectos, todo ello con el objetivo de poder acometer de manera adecuada y profesional un área tan importante como es el de la seguridad en la industria. Por ello, un elemento que no podemos dejar pasar por alto es el de la prevención, concepto que hoy en día está presente en todos los ámbitos y sectores de la sociedad. Además a todo esto hay que añadir, que ya disponemos desde hace años de una normativa concreta: el Reglamento de Seguridad contra Incendios en Establecimientos Industriales, y que tiene como objetivo conseguir un grado suficiente de seguridad en caso de incendio, concretamente en los establecimientos e instalaciones de uso industrial. Un tema que será analizado por responsables de seguridad y prevención de riesgos de diferentes compañías del entramado empresarial industrial español, que darán su visión profesional sobre la prevención y protección en esta área, así como expertos en seguridad.

Como en cada número de nuestra revista CUADERNOS DE SEGURIDAD incluiremos las secciones habituales fijas: Actualidad, Cuadernos de Seguridad estuvo allí, Seguridad...

ÍNDICE DE EMPRESAS CITADAS EN ESTA EDICIÓN

EMPRESA	PAG.	TELÉFONO	WEB
3M ESPAÑA	100	913216000	www.3m.com.es
ANATRONIC	101	913660159	www.anatronic.com
AVITOM	102	925516797	www.avitom.es
AXIS COMMUNICATIONS	48, 51,89, 92	918034643	www.axis.com
BOSCH SECURITY SYSTEMS	101	902121497	www.boschsecurity.es
BY DEMES GROUP	66, 99, 103	934254960	www.bydemes.com
CASMAR	88	933406408	www.casmar.es
CHECKPOINT SYSTEMS	78	914322500	es.checkpointsystems.com
DAHUA	Despl. Int. Cubierta, 100	917649862	www.dahuasecurity.com
DALLMEIER	41,54, 96	915902287	www.dallmeier-electronic.com
DETNOV	43	933716025	www.detnov.com
EUROMA	98	915711304	www.euroma.es
FF VIDEOSISTEMAS	23	902998440	www.ffvideosistemas.com
GRUPO IPTECNO	57,96	902502035	www.iptecno.com
GRUPO QUANTUM	53,94	935726218	www.grupoquantum.es
GRUPO VPS	73	930047035	www.vpsitex.es
HANWHA TECHWIN EUROPE	44, 97	916517507	www.hanwha-security.eu
HIKVISION	4ª Cubierta, 13	917371655	www.hikvision.com
HOMSEC	87	915945255	www.homsec.es
HONEYWELL	103	913136100	www.honeywell.es
II CONGRESO NACIONAL DE JEFES DE SEGURIDAD	9	914768000	www.congresojefesdeseguridad.com
INGRAM MICRO	88	902506210	es-new.ingrammicro.com
KASPERSKY	92	913983752	www.kaspersky.es
LILIN	104	902108533	www.meritlilinspain.com
LSB	90	913294835	www.lsb.es
MOBOTIX	46, 69,94, 98	911115824	www.mobotix.com
MORSE WATCHMANS	36	1159671567	www.morsewatchmans.com
PELCO By SCHNEIDER ELECTRIC	64,65,85	916245617	www.pelco.com
PWC	60	915684400	www.pwc.es
PYRONIX	19	917371655	www.pyronix.com
RISCO GROUP	38, 94	914902133	www.riscogroup.es
SABORIT	39,105	913831920	www.saborit.com
SECURITAS DIRECT	91	902195195	www.securitasdirect.es
SECURITY FORUM	3ª Cubierta	914768000	www.securityforum.es
SOPHOS	90	913756756	www.sophos.com
SYNOLOGY	102	33147176288	www.synology.es
TESA	104	943669100	www.tesa.es
TREND MICRO	62	913697030	www.trendmicro.es
TYCO IF & S	97	916313999	www.tyco.es
VISIOTECH	79	911836285	www.visiotech.com
VIVOTEK	99	886282455282	www.vivotek.com

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

ÍNDICE DE ANUNCIANTES

AXIS. 51
DAHUA . . . Despl. Int Cubierta
DALLMEIER 41
DETNOV. 43
FF VIDEOSISTEMAS 23
GRUPO QUANTUM 53
GRUPO VPS. 73
HIKVISION. . . 4ª Cubierta, 13
HOMSEC. 87
II CONGRESO NACIONAL DE JEFES DE SEGURIDAD . . . 9
IPTECNO 57
MOBOTIX. 69
PELCO. 64,65,85
PYRONIX 19
SABORIT INTERNATIONAL 39
SECURITY FORUM. . . . . 3ª Cubierta
VISIOTECH. 79

EL ENCUENTRO PROFESIONAL SE CELEBRARÁ EL PRÓXIMO 5 DE ABRIL

II Congreso Nacional de Jefes de Seguridad, **en marcha**

La jornada está organizada por PELDAÑO y la Asociación de Jefes de Seguridad de España

Ante la nueva realidad legislativa en materia de seguridad –y a la espera del desarrollo reglamentario de la Ley de Seguridad Privada– y los retos a los que se enfrenta la figura del Jefe de Seguridad, PELDAÑO y la Asociación de Jefes de Seguridad de España, organizan el II Congreso Nacional de Jefes de Seguridad, que tendrá lugar el próximo 5 de abril en Barcelona.

EL congreso, que se celebrará en el Colegio de Agentes Comerciales de Barcelona, tiene entre sus objetivos identificar y valorar la figura del Jefe de Seguridad, así como analizar las perspectivas y demandas ante el futuro desarrollo reglamentario de la Ley de Seguridad Privada. El encuentro, en su segunda edición, tiene entre sus objetivos prioritarios crear un foro de debate y análisis que reúna al sector de la Seguridad en una jornada de trabajo, en la que se analizará de forma exclusiva la figura del jefe de Seguridad y sus funciones, sus retos ante las nuevas amenazas, así como su papel como colaborador entre la Seguridad Pública y Privada.

Dirigido a jefes de Seguridad, directores y responsables de la Seguridad de entidades públicas y privadas, profesionales de empresas de Seguridad, así como a miembros de las Fuerzas y Cuerpos de Seguridad, la jornada se desglosará en diferentes ponencias y mesas de debate en las que se abordarán entre otros temas el «Jefe de Seguridad en el futuro Reglamento de Seguridad Privada», «Ciberseguridad & Jefes de Seguridad», «Presente y futuro del Jefe de Seguridad», entre otros.

Para finalizar se procederá a la entrega de los II Premios AJSE a la Seguridad Privada, en las categorías de: Premio Emprendedor del año; Premio Empresa Responsable; Premio Dedicación al Sector; Premio Tecnología de Seguridad, y Premio AJSE de Honor.

El I Congreso Nacional de Jefes de Seguridad se celebró hace ahora casi dos años, donde doscientos profesionales avalaron el éxito de un encuentro en el que se abordaron los nuevos retos a los que se enfrentaba el Jefe de Seguridad ante la nueva realidad legislativa, y otros aspectos como la cualificación profesional, la responsabilidad corporativa penal de la empresa de Segruidad y el Jefe de Seguridad, entre otros. ●

II CONGRESO NACIONAL DE JEFES DE SEGURIDAD

BARCELONA
05.04.2017

COACB

Salón de Actos del Colegio Oficial de Agentes Comerciales de Barcelona

AJSE
Asociación de Jefes de Seguridad de España

Peldaño

Más información e inscripciones:

www.congresojefesdeseguridad.com | info@congresojefesdeseguridad.com | +34 914 768 000

EL ENCUENTRO SE CELEBRARÁ EL 17 Y 18 DE MAYO

Security Forum 2017, comienza la cuenta atrás

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

A poco más de tres meses para su celebración, Security Forum 2017 empieza a tomar forma. Por un lado, las empresas del sector de la Seguridad continúan reservando sus espacios en el área de exposición, lo que augura los mejores resultados en lo que a número de expositores y visitantes se refiere, y los Premios Security Forum siguen recibiendo trabajos. Además, bajo el lema «Ver para Crear» el Congreso Security Forum 2017, se desglosará por primera vez en dos sesiones diferenciadas: Global Day y Ciber Day.

CONSOLIDADO ya como un espacio de networking, esta nueva convocatoria, que alcanza su quinta edición sigue apostando por la innovación y los nuevos valores empresariales en el sector de la Seguridad. Y es que a poco más de tres meses de su celebración Security Forum volverá a convertirse en un evento ágil, flexible y orientado a la innovación y desarrollo, que sigue respondiendo una edición más al espíritu emprendedor y audaz que caracteriza a las empresas y profesionales del sector de la Seguridad y que apuesta por reforzar el tejido empresarial de un sector en continua evolución, que demanda nuevos escenarios de plataformas de negocio e intercambio de conocimiento.

El encuentro contará de nuevo en esta edición con una zona de exposición con áreas sobre CCTV, integración de sistemas, seguridad física, seguridad lógica, control de accesos, IP/REDES,...; paneles de expertos, con

Ficha técnica

Fechas: 17 y 18 de mayo de 2017.

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

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

Periodicidad: Anual.

Carácter: Exclusivamente profesional.

Organiza: Peldaño.

Áreas de Exposición:

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

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

charlas de transferencia tecnológica entre las empresas que aportan soluciones tecnológicas y los profesionales de la gestión, consultoría e instalación de sistemas; etc.

Global Day y Ciber Day

Y respecto al Congreso, cabe destacar que se desglosará de nuevo en dos sesiones diferenciadas:

• Global Day: la primera jornada estará dedicada a la seguridad global. Los asistentes asistirán a conferencias y mesas de debate donde se abordarán los siguientes temas: «Vigilados por defecto», «Comunicación no verbal y análisis de conductas sospechosas como herramienta para el Director de Seguridad» o «Las nuevas guerras del siglo XXI».

• Ciber Day: la segunda jornada se centrará en la ciberseguridad. Temas como «Archivos secuestrados: ramsonware y otros malware en auge», «La robustez de los sistemas profesionales de CCTV frente a ciberataques», «Hacking & Cibersecurity for fun and profict», y mesas de debate bajo la temática «Ponga un CISO en su empresa» o «La coordinación estatal ante la Directiva NIS» centrarán el debate de esta edición.

Además, sigue abierta la fecha de recepción de los premios Security Forum, que pretenden promover y potenciar la investigación, el desarrollo y la innovación de la industria de la seguridad en España, a través del reconocimiento a los responsables de proyectos actuales de investigación en materia de seguridad, y a aquellos proyectos de carácter significativo ejecutados, que puedan ser modelo y escaparate internacional del amplio potencial de nuestra industria.

En la categoría Premio Security Forum I+D+i puede participar cualquier miembro o equipo de investigación de departamentos de universidades o escuelas de negocio españolas y aquellos investigadores o estudiantes, cuyos trabajos de fin de carrera o actividad investigadora no esté ligada a ninguna actividad empresarial.

«El plazo de entrega de los trabajos para los Premios Security Forum 2017 finaliza el próximo 31 de marzo»

En el Premio Security Forum al Mejor Proyecto de Seguridad realizado en España tendrán derecho a participar empresas que formen parte del propio proyecto y directores de seguridad.

Los premiados tendrán la oportunidad de realizar una presentación de su proyecto durante la celebración de Security Forum 2017, y el acto de entrega de premios se realizará el 17 de mayo durante una cena-cóctel.

La dotación de los premios será:

• Premio Security Forum I+D+i:
–Primer Premio: cheque valorado en 3.000 euros + trofeo conmemorativo
–Finalista: Trofeo conmemorativo.
• Premio Security Forum al Mejor Proyecto de Seguridad:
–Primer Premio: Trofeo conmemorativo.
–Finalista: Trofeo conmerativo.

Las memorias deben ser recibidas antes del día 31 de marzo de 2017. El fallo del jurado se producirá antes del 30 de abril. ●

Fotos: Xavi Gómez

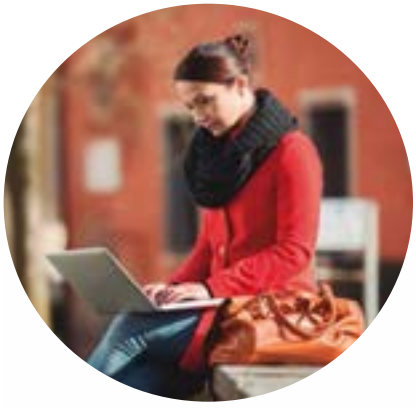
PREVENCIÓN Y SEGURIDAD

Seguridad en centros universitarios

Directores y responsables de Seguridad analizan la situación actual de las instalaciones universitarias desde el ámbito de la prevención y protección

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

De nuevo volvemos a destacar la figura del responsable de Seguridad en cuyas manos estará la conjunción de todos aquellos elementos para garantizar una satisfactoria seguridad para este tipo de instalaciones. Por ello en páginas posteriores, el lector encontrará entrevistas con directores y responsables de Seguridad y Prevención de diferentes centros universitarios, que analizan la seguridad en este tipo de instalaciones, cómo se encuentra organizado el área o departamento de Seguridad del que son sus máximos responsables, los medios y medidas con los que cuentan en su trabajo diario, así como su valoración profesional sobre la seguridad en este tipo de instalaciones. Además, diferentes expertos en la materia exponen, a través de artículos y tribunas, las últimas tecnologías utilizadas para la protección y prevención de este tipo de centros.



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

ALL-IN-ONE
SENCILLEZ Y VERSATILIDAD

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

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

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

CARLOS BÁEZ. DIRECTOR DE SERVICIOS GENERALES. UNIVERSIDAD DE ALCALÁ. ALCALÁ DE HENARES. MADRID

*«La mejor **seguridad** es la que dispone de los elementos pasivos de protección necesarios y **pasa desapercibida**»*

LAS nuevas tecnologías han jugado un papel fundamental e imprescindible para avanzar en la protección del patrimonio en instalaciones universitarias», así lo asegura Carlos Báez, director de Servicios Generales de la Universidad de Alcalá, quien además explica en esta entrevista las claves para una seguridad satisfactoria en este tipo de instalaciones.

—¿Podría explicarnos a grandes rasgos el origen de la institución universitaria, así como el número de alumnos, empleados, carreras, etc., que se imparten actualmente?

—La Universidad de Alcalá fue fundada en el año 1499 por el Cardenal Cisneros, aunque sus orígenes se remontan al Estudio General aprobado por el rey Sancho IV de Castilla en el año 1293. Actualmente cursan estudios en sus aulas casi 29.000 estudiantes de grado, posgrado y formación continua. La plantilla de la UAH está formada por 2.075 profesores e investigadores y 773 PAS (Personal de Administración y Servicio). En total, se imparten en la UAH 40 grados de todas las áreas (Ciencias Sociales y Jurídicas, Ciencias de la Salud, Ciencias, Arquitectura e Ingeniería y Humanidades).

—¿Cuál es la estructura e infraestructuras actual del área/departamento de Seguridad de la Universidad de Alcalá?

—Está integrada en la Unidad de Coordinación de Servicios Generales. Las tareas son realizadas por personal dependiente de la empresa adjudicataria del contrato de «Servicios de vigilancia, seguridad, atención a los sistemas de alarma y control de llaves». La plantilla adscrita a los servicios de vigilancia está controlada y coordinada por los mandos operativos de la empresa adjudicataria, mientras que el control de las tareas especificadas en el «Pliego Técnico» son gestionadas

por el personal de la Unidad antes citada. Para llevar a cabo este servicio y según se especifica en las condiciones técnicas del contrato, se realiza la supervisión de los mismos a los que la adjudicataria dedica alrededor de 65.000 horas de trabajo anuales de seguridad físicas, y hay conectadas a la Central Receptora más de 300 instalaciones de vigilancia pasiva repartidas en 40 edificios.

—¿Cuáles son las funciones concretas que lleva a cabo?

—Todas las relacionadas con el control operativo, administrativo y contable del contrato, así como la resolución de incidencias.

—A grandes rasgos, ¿podría explicarnos las medidas y medios de seguridad con que cuenta la instalación universitaria?

—Las descritas en el punto infraestructura.

—¿Cuáles son los riesgos más habituales a los que tiene que hacer frente el área de Seguridad de la Universidad de Alcalá?

—Los hurtos en horario de plena actividad. La falta de responsabilidad de los usuarios, al salir de despachos, instalaciones, etc., sin guardar las medidas mínimas de seguridad, como es cerrar la ventana y la puerta con llave, así como dejar los vehículos con las puertas y/o ventanas abiertas, o algunos materiales informáticos en los asientos, que pueden verse desde el exterior.

—¿Cuáles considera que son las claves para una seguridad satisfactoria en instalaciones como las de la Universidad de Alcalá?

—La actuación de los usuarios con sentido común. La seguridad es cosa de cada uno: «Tu ayuda es imprescindible para cuidar de lo tuyo».

—¿Cree que los alumnos, trabajadores... valoran las medidas de seguridad implantadas en las instalaciones de la Universidad o, por el contrario, se trata de un hecho que pasa desapercibido?

—Bajo mi criterio, la mejor seguridad es la que dispone de los elementos pasivos de protección necesarios, y pasa desapercibida.

—¿Qué papel cree que han jugado las nuevas tecnologías a la hora de mejorar la seguridad en instalaciones universitarias?

—Fundamental. Imprescindible para avanzar en la protección del patrimonio.

—¿Reciben algún tipo de formación en temas de prevención de riesgos laborales y seguridad los trabajadores de la universidad?

—Sí. Todos y de forma obligatoria.

Texto: Gemma G. Juanes.

Fotos: UAH

JUAN CARLOS MIRANDA. JEFE DE SERVICIOS GENERALES. UNIVERSIDAD FRANCISCO DE VITORIA. MADRID

*«Queremos un **campus seguro y tranquilo**, sin dar la percepción de que todo el mundo está vigilado»*

El equilibrio entre los medios tecnológicos y los recursos humanos es, en palabras de Juan Carlos Miranda, jefe de Servicios Generales de la Universidad Francisco de Vitoria, la clave para una seguridad satisfactoria en instalaciones universitarias. Así lo asegura en esta entrevista donde además explica los medios y medidas de seguridad implantados en el centro, entre otros aspectos.

—¿Podría explicarnos a grandes rasgos el origen de la institución universitaria, así como el número de alumnos, empleados, carreras, etc., que se imparten actualmente?

—La Universidad Francisco de Vitoria es una institución privada de enseñanza superior, cuya actuación se fundamenta dentro del respeto a los fines e ideales que la inspiran, en el principio de la libertad académica, manifestada en las libertades de cátedra, de investigación y de estudio. Fue reconocida como universidad en 2001 por la Comunidad de Madrid, tras comenzar su andadura como centro adscrito a la Universidad Complutense de Madrid en el curso 1993-94; forma parte de un sistema universitario internacional que integra instituciones

de formación superior en Estados Unidos, México, Europa y América del Sur.
Por su propia vocación y naturaleza, la Universidad Francisco de Vitoria promueve la formación humanística y cristiana desde su proyecto educativo de formación integral, tanto en sus alumnos como en profesores y personal de administración y servicios, basada en su Ideario, que apuesta por la persona tanto en su dimensión individual como social.
Con más de 20 años de andadura, la Universidad Francisco de Vitoria imparte 24 titulaciones de Grado y 15 de doble Grado, de diferentes áreas como Ciencias Jurídicas, Económicas y Sociales, Ciencias de la Salud, Ciencias de la Educación, Ingeniería y Arquitectura y Ciencias de la Comunicación. Además, la UFV apuesta por la innovación, la internacionalidad, la participación activa de todo el alumnado y la exigencia personal, con docentes de gran bagaje tanto académico como profesional. También cuenta con programas de prácticas con convenios en más de 3.700 empresas.

—¿Cuál es la estructura e infraestructuras actual del área/departamento de Seguridad de la Universidad Francisco de Vitoria?

—No existe departamento de Seguridad como tal. La seguridad del campus se engloba dentro del departamento de Servicios Generales en dependencia directa del Gerente de la UFV. Los recursos humanos de seguridad están externalizados en una empresa profesional seleccionada mediante concurso. Respecto a las instalaciones, además del puesto de trabajo propio del responsable de Servicios Generales, se cuenta con una garita en la entrada de acceso al campus en la que se centraliza el sistema de CCTV, así como alarmas anti intrusión y de incendios.

—¿Cuáles son las funciones concretas que lleva a cabo?

«El equilibrio entre los medios tecnológicos y los recursos humanos es la clave para una seguridad satisfactoria»

—Las propias de un responsable de SS.GG. En el caso de la seguridad, se trata de dimensionar y dirigir el equipo de seguridad en contacto directo con el responsable de operaciones de la empresa de seguridad subcontratada. Hacer cumplir en general las directrices que emanan de la Dirección de la universidad referentes a la seguridad, impartiendo instrucciones y apoyando al personal que presta el servicio de seguridad en el campus, atender todas las incidencias que se producen en el campus referentes a algún aspecto de la seguridad, como hurtos, golpes de tráfico, etc. Y lógicamente, la colaboración con los miembros de las Fuerzas y Cuerpos de Seguridad.

—A grandes rasgos, ¿podría explicarnos las medidas y medios de seguridad con que cuenta la instalación universitaria?

—Además de los elementos volumétricos anti intrusión que hay en todos los edificios, contamos con 158 cámaras, 6 videograbadores, una central CCTV, motocicleta eléctrica para desplazamientos rápidos por el campus, 9 walkies (además del personal de seguridad, cuentan con este aparato el jefe de SSGG, las recepcionistas y los bedeles, de manera que la comunicación de cualquier incidencia es inmediata), vigilante las 24 horas los 365 días del año, un vigilante de paisano que se mueve por todo el campus, personal auxiliar de servicio todos los días en número variable, dependiendo de los eventos que estén programados, pero como mínimo todos los días contamos con 2 auxiliares que cubren el servicio desde las 7:00 hasta las 23:00 hrs.

—¿Cuáles son los riesgos más habituales a los que tiene que hacer frente el área de Seguridad de la Universidad Francisco de Vitoria?

«Además de los elementos volumétricos anti intrusión que hay en todos los edificios, contamos con 158 cámaras, 6 videograbadores, una central CCTV...»

—Afortunadamente tenemos un campus tranquilo. Si tengo que mencionar algún riesgo, es el de la entrada de personas con ánimo de hurtar o robar, especialmente cuando estamos con obras, que se cuelan entre el resto de furgonetas y camiones de las obras. Cuando son detectados se les expulsa del campus y, aunque generalmente se marchan sin más, en alguna ocasión han puesto la situación algo tensa. Por otro lado, cuando nos visita alguna personalidad nos tenemos que coordinar con Policía y Guardia Civil, además de con los responsables de seguridad de sus respectivas embajadas o consulados. En un par de ocasiones nos hemos coordinado con el grupo antiterrorista de la Policía.

—¿Cuáles considera que son las claves para una seguridad satisfactoria en instalaciones como las de la UFV?

—El equilibrio entre los medios tecnológicos y los recursos humanos. Queremos un campus seguro y tranquilo, sin dar la percepción de que todo el mundo está vigilado con exceso de personal.

—¿Cree que los alumnos, trabajadores,... valoran las medidas de seguridad implantadas en las instalaciones de la Universidad o, por el contrario, se trata de un hecho que pasa desapercibido?

—Para nada pasa desapercibido. En las encuestas de satisfacción con los servicios del campus que cada año se realizan a alumnos, profesores y personal de administración y servicios, se les pregunta también por este servicio. Estamos en una media ponderada de 4,44 sobre 6, y mejorando lentamente cada curso. En el curso 2010 – 2011 esta media era de 3,89.

—¿Qué papel cree que han jugado las nuevas tecnologías a la hora de mejorar la seguridad en instalaciones universitarias?

—Sin duda nos ayudan. Soy consciente de que nos podrían ayudar más con mayor inversión, pero se consigue mucho con el presupuesto con el que se cuenta. ●

Texto: Gemma G. Juanes.
Fotos: Universidad Francisco de Vitoria

Detector Volumétrico de Exteriores de Triple Tecnología y Anti-masking

Pyronix
HIKVISION

XDH10TT-AM

Características

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

Para recibir más información, regístrese aquí

ANA CARO MUÑOZ. COORDINADORA DE PROYECTOS DE LA UNIVERSIDAD AUTÓNOMA DE MADRID

*«La **evaluación de riesgos** es el paso previo para llegar a una **prevención racional y efectiva**»*

LA UAM es una institución con baja siniestralidad laboral, no obstante trabajamos diariamente para reducir y actuar sobre aquellos peligros que nos ocasionan mayor siniestralidad laboral (accidentes in itinere, riesgos ergonómicos, etc.)», asegura Ana Caro Muñoz, coordinadora de Proyectos de la Universidad Autonónoma de Madrid, quien además añade que la institución es una universidad comprometida con la prevención de riesgos laborales y salud laboral, con la sostenibilidad, la cooperación, la internacionalización y las políticas activas de inclusión.

—¿Podría explicarnos a grandes rasgos el origen de la institución universitaria, así como el número de alumnos, empleados, carreras, etc., que se imparten actualmente?

—La Univerisdad Autónoma de Madrid se creo en el año 1968, por lo que pronto celebrará sus 50 años. Actualmente cuenta con 28.000 estudiantes, empleados (profesores 2.500) y (PAS 1.000). Los títulos que se imparten actualmente son (43 grados y 7 dobles grados), 74 másteres oficiales y 35 doctorados y más de 100 títulos propios.

—En pocas líneas, ¿cuál es su formación y experiencia profesional? ¿Qué cargo ocupa actualmente en la empresa?

—Licenciada en Derecho, Diploma de Práctica Jurídica del Consejo General de la Abogacía Española y Diploma de Estudios Avanzados. Profesional jurista, asesora y gestora pública desde hace veinte años. Actualmente ocupo el puesto de coordinadora de Proyectos de la Universidad Autónoma de Madrid y delegada del Patronato de la Fundación Parque Científico de Madrid. En su trayectoria profesional he sido jefe del Servicio Jurídico de la Universidad de Burgos, vicesecretaria General de la Universidad Autónoma de Madrid y directora General de Régimen Jurídico del Gobierno Vasco en la Consejería de Educación, Universidades e Investigación. Ponente habitual de foros de gestión administrativa, régimen jurídico y educación, he publicado más de medio centenar de artículos doctrinales, y más de una veintena de libros. Soy la secretaria General de la Asociación para estudio del Derecho Universitario y vicepresidenta de la Red Iberoamericana de Derecho Universitario.

—¿Qué sector del mercado abarca la empresa? ¿Qué productos y soluciones comercializa y qué actividades desarrolla?

—La Universidad Autónoma de Madrid (UAM) es una entidad de Derecho Público a la que corresponde, en el ámbito de sus competencias, el servicio público de la educación superior mediante la investigación, la docencia y el estudio.

Para cumplir con la prestación de estos servicios las funciones que desarrolla son las siguientes:

a) La creación, el desarrollo, la transmisión y la crítica de la ciencia, de la técnica, de la cultura y del arte, siempre orientadas hacia la libertad, el desarrollo humano sostenible, la justicia, la paz, la amistad y la cooperación entre los pueblos.

b) La preparación para el ejercicio de actividades profesionales que exijan la aplicación de conocimientos y métodos científicos, así como la actividad creadora en todos sus campos.

c) El apoyo científico y técnico al desarrollo cultural, social y económico en todos sus ámbitos, tanto nacionales como internacionales.

d) La difusión del conocimiento y de la cultura a través de la extensión universitaria y la formación permanente.

e) El desarrollo de un modelo de educación multidisciplinar y éticamente orientado hacia la búsqueda de soluciones concernientes a los derechos humanos, al medio ambiente, a las relaciones de género, a la atención a las personas con discapacidad, a la erradicación de la pobreza, y a la justicia económica y social entre los pueblos, a través de la promoción de conocimientos, valores, actitudes, habilidades y patrones de comportamiento comprometidos con un desarrollo humano sostenible.

—¿Cómo está estructurado el Servicio de Prevención de Riesgos Laborales de la empresa? ¿Cuáles son sus funciones básicas?

—Servicio de Prevención de Riesgos Laborales propio que denomina «Servicio de Salud Laboral y Prevención de Riesgos Laborales» asumiendo todas las especialidades preventivas. Tiene carácter interdisciplinario y, actualmente, cuenta con los siguientes recursos humanos:

- Especialidades técnicas: Cuenta con dos técnicos superiores de prevención con las tres especialidades y con un apoyo administrativo.
- Especialidad sanitaria: Cuenta con dos médicas y dos enfermeras todas especialistas en Medicina del Trabajo y con un apoyo Administrativo.

Del mismo modo, los directores o jefes de los distintos centros, departamentos y servicios, a propuesta del correspondiente Consejo, nombrarán coordinadores entre el Personal Docente e Investigador (PDI) o el Personal de Administración y Servicios (PAS), cuya función es la de asegurar la comunicación entre el SPRL y los departamentos en materia de seguridad e higiene en el trabajo.

Las principales tareas del Servicio de Prevención de Riesgos Laborales son:

- Garantizar el cumplimiento de la normativa vigente en materia de seguridad e higiene.
- Realizar las evacuaciones de riesgos de las diferentes facultades, escuelas, bibliotecas, talleres y otros edificios de la UAM.
- Llevar a cabo inspecciones periódicas de los distintos centros y, en especial, de los laboratorios docentes y de investigación y los almacenes de los centros experimentales.
- Elaborar los distintos planes de evacuación y coordinar los simulacros en los distintos edificios.
- Dar la formación adecuada al personal de la UAM en materia de seguridad e higiene en el trabajo. Así mismo, instruirá en materia de seguridad a los nuevos investigadores que se incorporen a los grupos de trabajo.
- Garantizar la retirada de residuos generados en los laboratorios facilitando su almacenamiento y retirada conforme la normativa existente.
- Informa además a los usuarios de la peligrosidad de los productos químicos utilizados, las medidas preventivas que deben adoptar y su posible sustitución por otros con menor riesgo para la salud y el medio ambiente.
- Coordinar la gestión de las instalaciones radiactivas de la Universidad.
- Evaluar y coordinar las dotaciones en infraestructura en seguridad de los laboratorios, talleres y aulas de la UAM.
- Desarrollar programas de vigilancia y promoción de la salud y evaluar los resultados derivados de los mismos.

—¿Cuáles son los principales riesgos laborales asociados a los trabajadores de la empresa? ¿Cómo se impiden?

—Los principales riesgos son los relativos a lugares de trabajo (caídas al mismo nivel), pantallas de visualización

de datos, los accidentes in itinere y los riesgos químicos, físicos y biológicos relacionados estrechamente con la actividad docente e investigadora.

Trabajamos para reducir estos riesgos a través de la correspondiente evaluación de riesgos y la planificación de la acción preventiva, que incluye medidas formativas e informativas, de mejora y adecuación de equipos de trabajo, de infraestructuras, etc.

—¿Qué equipos de protección individual se proporcionan a los trabajadores?

—Facilitamos todo tipo de EPIS entre los que se incluyen, guantes de protección (temperatura, riesgo químico, cortes, etc.), máscaras y mascarillas, protecciones oculares, protecciones auditivas, zapatos, mandiles, manguitos, fajas, etc. Estos equipos se facilitan siempre, como último recurso preventivo, ya que como todos sabemos los EPIS sólo se utilizan cuando el resto de medidas no son suficientes.

—Los riesgos psicosociales, tales como el estrés o el burnout, ¿cómo se impiden y se tratan? ¿Qué acciones se llevan a cabo para evitarlos y tratarlos?

—Uno de los compromisos de gestión de la UAM se corresponde con la promoción del bienestar de los empleados y empleadas mediante programas de evaluación de riesgos psicosociales.

Compromiso que se articula a través del Comité de Seguridad y Salud y del Servicio de Prevención de Riesgos Laborales.

Para abordar con eficacia y calidad esta actuación, el Comité de Seguridad y Salud articula su trabajo a través de un Grupo, en el que están representados tanto los delegados de Prevención de Riesgos como la parte Institucional.

Del mismo modo, los técnicos de prevención de riesgos laborales y la coordinadora de Proyectos de la Universidad, planifican, articulan y desarrollan los trabajos necesarios para llevar a efecto las evaluaciones aprobadas en el seno del Comité de Seguridad y Salud.

El test que utilizamos –aprobado por el Instituto de Seguridad e Higiene en el Trabajo– es un instrumento de evaluación orientado a la prevención. Identifica los riesgos al nivel de menor complejidad conceptual posible, facilita la localización de los problemas y el diseño de soluciones adecuadas.

Los resultados de la aplicación deben ser considerados como oportunidades para la identificación de aspectos a mejorar de la organización del trabajo. La evaluación de riesgos es un paso previo para llegar a una prevención racional y efectiva.

El método debe usarse para prevenir en origen (eliminar o disminuir los riesgos psicosociales y avanzar en una organización del trabajo más saludable)

Fruto de las evaluaciones de riesgos psicosociales se confeccionan informes en los que se determina, entre otras cuestiones, qué medidas han de ser adoptadas y quiénes han de ser los responsables de la implementación y el seguimiento.

Complementando estas actividades, y dentro de la planificación anual tanto del Comité de Seguridad y Salud como de la Unidad de Igualdad, se llevan a cabo cursos de formación específicos en la materia, para concienciar, dar elementos de conocimiento y juicio, y poner a disposición herramientas que sirvan a los empleados y empleadas en la prevención de estos riesgos.

En todo caso, cualquier persona que presta servicios en la UAM, o que cursa estudios en nuestras aulas, tiene a su disposición el Servicio de Salud y el Centro de Psicología Aplicada para ayudar a afrontar y superar supuestos y situaciones que puedan afectar a su salud física o psíquica.

—La vigilancia de la salud, ¿qué medidas conlleva (reconocimientos médicos, etc.)?

—La actividad sanitaria de los servicios de prevención incluye, entre otras y como principal actividad, la vigilancia de la salud que, mediante procedimientos adecuadamente validados, tiene como objetivo detectar sistemática y regularmente los síntomas y signos precoces de los daños derivados del trabajo, detectar las situaciones de riesgo, así como proponer las medidas preventivas necesarias. La vigilancia de la salud está integrada, por tanto, en la planificación de la actividad preventiva de la empresa.

En materia de vigilancia de la salud, la actividad sanitaria abarca:

1. Una evaluación de la salud de los trabajadores inicial después de la incorporación al trabajo o después de la

GEUTEBRÜCK

Excellence in Video Security

VISITENOS EN HOMSEC 2017 STAND C02

G-Tect VMX de GEUTEBRÜCK

Protección perimetral basada en análisis de video

CONTROL DE EXTERIORES

Revolucionaria solución de detección de movimiento de vídeo que ofrece protección perimetral fiable para instalaciones exteriores.

UN SOFTWARE CAPAZ DE APRENDER

Si un mismo objeto produce regularmente el mismo moviemiento ante la cámara sin ser marcado como peligroso, el sistema lo recordará y no generará alarma.

REDUCCIÓN DE ALARMAS NO DESEADAS

De esta manera se consigue un funcionamiento óptimo en diferentes condiciones meteorológicas. Filtrando la lluvia, vegetación en movimiento, cambios en la iluminación, pequeños animales...

Consiga más informcaión

F.F Videosistemas S.L.
www.ffvideosistemas.com
Tel. 902 99 81 10
ffvideo@ffvideosistemas.com

25 F.F. 1992 2017

distribuidor exclusivo

Videosistemas

GEUTEBRÜCK

asignación de tareas específicas con nuevos riesgos para la salud.

2. Una evaluación de la salud de los trabajadores que reanuden el trabajo tras una ausencia prolongada por motivos de salud (de 61 o más días naturales según última normativa), con la finalidad de descubrir sus eventuales orígenes profesionales y recomendar una acción apropiada para proteger a los trabajadores.
3. Una vigilancia de la salud a intervalos periódicos.

• La vigilancia de la salud está sometida a protocolos específicos con respecto a los factores de riesgo a los que está expuesto el trabajador.

• Los exámenes de salud incluyen, en todo caso, una historia clínico-laboral, en la que además de los datos del interrogatorio, exploración clínica, control biológico y estudios complementarios en función de los riesgos inherentes al trabajo, se hace constar una descripción detallada del puesto de trabajo, el tiempo de permanencia en el mismo, los riesgos (referidos) en el análisis de las condiciones de trabajo, y las medidas de prevención adoptadas.

• Consta igualmente en la medida en que se dispone de ello, una descripción de los anteriores puestos de trabajo, riesgos presentes en los mismos, y tiempo de permanencia para cada uno de ellos.

• El personal sanitario del servicio analiza los resultados de la vigilancia de la salud de los trabajadores y de la evaluación de los riesgos, con criterios epidemiológicos, y colabora con el resto de los componentes del servicio, a fin de investigar y analizar las posibles relaciones entre la exposición a los riesgos profesionales y los perjuicios para la salud y proponer medidas encaminadas a mejorar las condiciones y medio ambiente de trabajo.

• El personal sanitario del servicio de prevención estudia y valora, especialmente, los riesgos que puedan afectar a las trabajadoras en situación de embarazo o parto reciente, y a los trabajadores especialmente sensibles a determinados riesgos, y propone las medidas preventivas adecuadas.

El personal sanitario del servicio de prevención presente en el centro de trabajo proporciona los primeros auxilios y la atención de urgencia a los trabajadores víctimas de accidentes o alteraciones en el lugar de trabajo.

• Impulsar programas de promoción de la salud en el lugar de trabajo, en coordinación con el Sistema Nacional de Salud.

• Desarrollar programas de formación, información e investigación en su ámbito de trabajo.

• Participar en las actuaciones no específicamente sanitarias que el servicio de prevención realice en desarrollo de las funciones que tiene atribuidas («asesoramiento y apoyo»).

• Colaborar con el Sistema Nacional de Salud, para el diagnóstico, tratamiento y rehabilitación de enfermedades relacionadas con el trabajo, y con las administraciones sanitarias competentes en la actividad de salud laboral que se planifique.

• Colaborar con las autoridades sanitarias en las labores de vigilancia epidemiológica, provisión y mantenimiento del Sistema de Información Sanitaria en Salud Laboral. Y participar en cualquier otra función que la autoridad sanitaria les atribuya en el marco de la colaboración contemplada en los artículos 38 y 39 del Reglamento de los Servicios de Prevención.

Con carácter enumerativo las actuaciones son las siguientes:

– Se realizan exámenes de salud: Inicial tras la incorporación al trabajo; inicial tras asignación de nuevas tareas y/o cambio de puesto de trabajo; periodo específico y retorno al trabajo tras ausencia prolongada por motivos de salud.
– Y también se llevan a cabo protocolos de vigilancia de la salud específica: Agentes Biológicos, Altura, Musculo-Esquelético, Patología de la voz, Plaguicidas, PVD, Radiaciones Ionizantes, Radiaciones No Ionizantes, Riesgo Eléctrico, Riesgo Químico, Ruido, Silicosis, Temperaturas Elevadas, Turnos y Nocturnidad.
– Del mismo modo se realizan vacunaciones practicadas por riesgo de exposición a agentes biológicos, gripe y todas las vacunaciones distintas a Tétanos/Difteria, Hepatitis A y Hepatitis B o combinada de ambas.
– Por último, y no menos importante se desarrollan campañas de promoción de la salud: de Prevención de cáncer ginecológico y de prevención de cáncer prostático.

—¿Qué legislación se aplica en materia de seguridad y salud laboral? ¿Dispone la empresa de alguna norma específica?

—Las normas que se aplican en el ámbito

de la seguridad y salud laborales dentro de la UAM son las mismas que en cualquier otra institución o empresa, si bien también nos adecuamos a las exigencias recogidas en las leyes y normas específicas de aplicación para las administraciones públicas y para las universidades. De otra parte contamos, entre otras, con normas propias en materia de seguridad en el trabajo (organización de la seguridad en el trabajo, cadena de responsabilidades, normas generales de actuación en caso de accidente y evacuación, plan de emergencia y evacuación) y con normativa de seguridad en los laboratorios y talleres, expuestos a riesgo químico, físico o biológico.

—¿Cuántas horas de formación recibe cada trabajador? ¿Qué metodología se emplea para dicha instrucción? ¿Qué programas y contenidos se imparten?

—Desde el Comité de Seguridad y Salud, y bajo la articulación del Servicio de Prevención y Salud Laborales de la Universidad, anualmente se desarrolla una programación específica en materia de prevención y salud laborales. Los destinatarios son tanto el personal de administración y servicios, como el personal docente e investigador. Se abordan materias de toda índole: nutrición saludable, manejo de voz, uso de vitrinas de gases y armarios de seguridad, gestión y control del estrés, primeros auxilios, RCP, riesgos psicosociales, deshabituación tabáquica, actividad física, cursos básicos en la materia, etc. Formación a la que se debe añadir la específica que cada Centro puede impartir a los nuevos integrantes de las plantillas, o a los ya formados para reciclar, según corresponda a cada puesto.

—En cuanto a siniestralidad laboral, ¿cuál es la situación?, ¿qué medidas se aplican para reducirla y controlarla?

—La UAM es una institución con baja siniestralidad laboral, no obstante trabajamos diariamente para reducir y actuar sobre aquellos peligros que nos ocasionan mayor siniestralidad laboral (accidentes in itinere, riesgos ergonómicos, etc).

—¿La empresa ha logrado algún tipo de galardón o premio reconociendo el prestigio de su política de PRL? ¿Qué variables se han considerado y cuáles han sido los argumentos para su consecución?

—La UAM es una universidad comprometida con la prevención de riesgos laborales y salud laboral, con la sostenibilidad, la cooperación, la internacionalización y las políticas activas de inclusión, por ello, entre otras líneas de actuación, se implementan continuamente acciones que promocionan y facilitan a la comunidad universitaria la vida en nuestros Campus.

Por ello, y como resultado de estas políticas activas la UAM ha obtenido varios reconocimientos, entre otros:

- Finalista a la mejor práctica para el control del riesgo con la Normativa de seguridad en los Premios ASEPEYO 2013.
- Primer premio COAM 2013 por las medidas de accesibilidad del Edificio Plaza Mayor.
- Premio Reina Letizia 2015 de rehabilitación y de integración otorgado por el Real Patronato sobre Discapacidad.
- Premio a la mejor contribución preventiva de la representación institucional de trabajadores y empresarios, IV Premios ASEPEYO. Premio ex aequo: Universidad Autónoma de Madrid Protocolo y Reglamento por los que se regulan las medidas de prevención y el procedimiento de actuación en casos de acoso moral, sexual y/o por razón de sexo en el trabajo en el ámbito de la Universidad Autónoma de Madrid.

—¿Desea añadir algo más?

—La actividad en materia de prevención de riesgos y salud laboral, como ocurre en otras facetas y ámbitos de nuestra universidad, no sería de la calidad, eficiencia y eficacia, que demuestran día a día, si no fuera por las y los grandes profesionales que prestan servicios en ella. Desde aquí el reconocimiento y agradecimiento a todas y todos los que hacemos posible que nuestros Campus de Cantoblanco y Medicina sean todo un referente.

Fotos: UAM

JUAN M. URIARTE. SAFETY AND SECURITY DIRECTOR, LAUREATE EUROPE (LAUREATE INTERNATIONAL UNIVERSITIES)

*«La **seguridad** debe ser discreta y tiene que ser vista como un **servicio** que se proporciona a los **estudiantes** y **empleados**»*

LAS nuevas tecnologías son importantísimas a la hora de mejorar la seguridad en las instalaciones universitarias, ya que permiten gestionarla de una manera discreta», explica Juan M. Uriarte, Safety and Security Director, Laureate Europe (Laureate International Universities), quien además explica, en esta entrevista, que «permiten reaccionar de una manera rápida en caso de incidente».

—¿Cuál es la estructura e infraestructura actual del área/departamento de Seguridad de la Universidad Europea de Madrid?

—El departamento de Seguridad tiene un director de Seguridad y un Servicio de Prevención, Salud y Medio Ambiente compuesto por cuatro personas. Por encima estoy yo como director de Safety & Security para Europa, con responsabilidad en los diferentes campus que Laureate International Universities tiene en la región. Asimismo tenemos contratada una empresa de seguridad para la gestión de vigilantes.

—¿Cuáles son las funciones concretas que lleva a cabo?

—Nuestro departamento implementa las políticas globales de seguridad de Laureate International Universities sobre seguridad física, gestión de crisis, planificación de emergencias, recuperación de desastres, continuación de operaciones y gestión de viajes. Para ello estamos intentando implicar a todos los empleados en la aplicación de estas políticas, realizando formación y simulacros. Por ejemplo, cada año tenemos en marzo el mes del simulacro y en todas nuestras instituciones se hace un ejercicio de evacuación, simulando diversos escenarios como pueden ser fuego o amenaza de bomba.

—A grandes rasgos, ¿podría expli-

carnos las medidas y medios de seguridad con que cuenta la instalación universitaria?

—Disponemos de un centro de control en el Campus de Villaviciosa desde donde se gestiona la seguridad de las diferentes instalaciones. Disponemos de sistemas de CCTV y de control de acceso para aquellas dependencias en las que se considera necesario, como en las oficinas o lugares donde hay material de un cierto valor.

—¿Cuáles son los riesgos más habituales a los que tiene que hacer frente el área de Seguridad de la Universidad Europea de Madrid?

—En la Universidad Europea apenas se dan incidentes de seguridad, ya que se trabaja en la prevención, especialmente de hurtos de material. No obstante, tenemos que estar preparados para saber reaccionar ante cualquier tipo de incidente, sobre todo teniendo en cuenta la amenaza terrorista existente en Europa.

—¿Cuáles considera que son las claves para una seguridad satisfactoria en instalaciones como las de la Universidad Europea de Madrid?

—La clave para una seguridad satisfactoria en una universidad es mantener el equilibrio entre libertad y seguridad. Por ello la seguridad debe ser discreta y tiene que ser vista como un servicio que se proporciona a los estudiantes y empleados.

—¿Cree que los alumnos, trabajadores, etc. valoran las medidas de seguridad implantadas en las instalaciones de la Universidad o, por el contrario, se trata de un hecho que pasa desapercibido?

—En la última encuesta de clima se valoró muy positivamente la labor del departamento de Seguridad. Somos una unidad orientada a proporcionar un servicio a los estudiantes y trabajadores y eso hace que estemos bien valorados.

«Cada año tenemos en marzo el mes del simulacro y en todas nuestras instituciones se hace un ejercicio de evacuación»

—¿Qué papel cree que han jugado las nuevas tecnologías a la hora de mejorar la seguridad en instalaciones universitarias?

—Las nuevas tecnologías son importantísimas a la hora de mejorar la seguridad en las instalaciones universitarias, ya que permiten gestionarla de una manera discreta. Además permiten reaccionar de una manera rápida en caso de incidente. ●

Texto: Gemma G. Juanes.
Fotos: Universidad Europea

MARISOL DIANA VALIENTE. DIRECTORA DE SEGURIDAD. UNIVERSIDAD DE ALICANTE

*«Trabajamos para **mejorar** y **actualizar** los sistemas de **seguridad** para conseguir una universidad más **moderna y segura**»*

LA Universidad de Alicante tiene un historial con pocas incidencias relevantes, ya que en ella se puede observar un ambiente de tranquilidad y confianza, creo que motivado entre otras cosas, por la existencia de un departamento de Seguridad cercano y comprometido, que ofrece información, ayuda, soluciones y respuestas inmediatas a los problemas que se plantean», asegura Marisol Diana Valiente, directora de Seguridad de la Universidad de Alicante, quien además durante la entrevista analiza la estructura del área de Seguridad del centro universitario, y los medios y medidas de seguridad implantadas en el mismo, entre otras cosas.

—¿Podría explicarnos a grandes rasgos el origen de la institución universitaria, así como el número de alumnos, empleados, carreras, etc., que se imparten actualmente?

—La Universidad de Alicante se creó en octubre de 1979 sobre la estructura del Centro de Estudios Universitarios (CEU), que nació en 1968. Alicante recuperaba de esta manera los estudios universitarios suspendidos en 1834, tras el cierre de la histórica Universidad de Orihuela, con dos siglos de existencia, de la que actualmente la UA es heredera histórica.

El actual campus se asienta sobre las instalaciones del antiguo aeródromo militar de Rabasa, en sus viejos barracones. En aquellos años iniciaron sus estudios 230 estudiantes. Hoy en día la población universitaria alcanza los 40.000 habitantes entre alumnado, personal de administración y servicios y personal docente e investigador, además de las diferentes personas que trabajan en empresas de servicios como seguridad, hostelería, mantenimiento, limpieza, etc.

Actualmente se puede elegir entre 48 modalidades de títulos de grado, presenciales y no presenciales, dobles titulaciones y titulaciones simultáneas y 55 másteres oficiales, y más de un centenar de programas de formación propios.

Desde 1979 hasta ahora, no sólo el campus se ha convertido en un referente arquitectónico mundial con un millón de metros cuadrados, sino que algunos de nuestros grupos de investigación y de nuestros científicos, figuran en lugares de referencia internacional. No en vano, uno de nuestros científicos ha sido postulado este año al premio Nobel, en la categoría de Medicina y de Química.

En la actualidad, la amplia oferta formativa de la Universidad de Alicante se estructura a través de seis Facultades (Ciencias Económicas y Empresariales, Ciencias, Derecho, Educación, Filosofía y Letras, y Ciencias de la Salud), y una Escuela Politécnica Superior. Un amplio abanico de servicios, de centros de in-

vestigación e institutos universitarios, completan la oferta.

Además, la progresiva puesta en marcha de su Parque Científico denota su firme apuesta por la innovación, la tecnología y el emprendimiento, así como por la transferencia de conocimiento. Pero también la cultura, la extensión universitaria y la conservación del patrimonio son rasgos propios de una Universidad, que completa las infraestructuras del campus con un Parque Arqueológico en La Alcudia, un museo universitario, convertido en referente arquitectónico del siglo XX y una red de sedes y aulas universitarias diseminadas por toda la provincia de Alicante, con el objetivo de acercar la institución académica a toda la ciudadanía teniendo en cuenta las diferentes idiosincrasias de sus comarcas.

—¿Cuál es la estructura e infraestructura actual del área/departamento de Seguridad de la Universidad de Alicante?

—La estructura del departamento de Seguridad en la Universidad de Alicante es unipersonal, tan sólo está formado por la figura de director de Seguridad, encarnado, en el caso de la Universidad de Alicante por una mujer, la única que desempeña este tipo de funciones en una universidad española.

El personal de apoyo de seguridad está licitado a una empresa externa.

Las infraestructuras con las que cuenta el departamento son:

– Un centro de control de seguridad, atendido por vigilantes las 24 horas del día los 365 días del año.

  En este edificio, que es independiente, se encuentran integrados todos los medios técnicos que posee la Universidad (CCAA, CCTV, anti-intrusión, PCI, control de temperaturas, etc.).

  Es en este centro donde se recepcionan las alarmas y se ponen en funcionamiento los procedimientos establecidos.

– Una oficina de seguridad y objetos perdidos, que se encuentra abierta de lunes a viernes, donde se gestiona la recogida y entrega de objetos y se atiende e informa a los usuarios.

—¿Cuáles son las funciones concretas que lleva a cabo?

—Algunas de las funciones más importantes son analizar y evitar aquellos riesgos a los que la universidad está expuesta, bien por su actividad diaria o por el número de personas que estudian o trabajan en ella. La elaboración de procedimientos de actuación y operativas para actos o eventos que se realicen, y el estudio y la protección de las instalaciones optimizando los recursos, tanto en medios técnicos como humanos.

—A grandes rasgos, ¿podría explicarnos las medidas y medios de seguridad con que cuenta la instalación universitaria?

—La Universidad de Alicante cuenta

con unas medidas de seguridad adaptadas a las diferentes situaciones de riesgo, que pueden ser desde medidas disuasorias, protocolos específicos y formación contínua, tanto de los miembros del departamento de Seguridad como de los trabajadores de la universidad, en casos de emergencia y/o catástrofes naturales.

La Universidad también posee un Sistema Integral de Seguridad, dotado de medios técnicos, medios humanos, medios auxiliares y unos procedimientos de actuación que permiten actuar con eficacia y rapidez.

Entre los medios técnicos podemos destacar un moderno y actualizado circuito cerrado de televisión, formado por un gran número de cámaras de seguridad instaladas en las diferentes zonas del campus.

Un control de accesos con el cual es posible controlar las áreas o zonas restringidas.

Un sistema anti-intrusión que protege todas las instalaciones.

Un sistema de detección de incendios conectado con el centro de control de seguridad.

En medios humanos posee el personal operativo de la empresa de seguridad, adjudicataria del servicio: Coordinador de seguridad, responsables de equipo, vigilantes de seguridad y auxiliares de servicios.

En medios auxiliares se cuenta con varios vehículos, Segway, emisoras, megáfonos, DESA, etc.

Además, a través de un grupo de investigación propio, el GrupoM de redes y middleware de la Escuela Politécnica Superior, la Universidad de Alicante está implantando un moderno y pionero sistema de monitorización inteligente, un novedoso proyecto denominado Smart University que funciona a través de sensores y permite distintos monitoreos en tiempo real.

—¿Cuáles son los riesgos más habituales a los que tiene que hacer frente el área de Seguridad de la Universidad de Alicante?

—Como riesgos más frecuentes podríamos destacar el hurto o robo, el cual se produce la mayoría de las veces por descuidos de los propios estudiantes.

También el robo de bicicletas en las zonas peatonales del campus, algo que está sucediendo en todas las zonas de la ciudad de Alicante y es muy habitual en las grandes capitales.

Otro riesgo que se produce, pero con muy poca frecuencia podría ser algún pequeño conato de incendio o fuga de gases en zonas de investigación. También destacar algunos accidentes que se producen por colisión entre vehículos, así como la necesidad de actuar ante usuarios que sufren mareos, bajadas de tensión, ataques de ansiedad, sobre todo en época de exámenes. El moderno diseño del campus con amplias avenidas y el hecho de que sea peatonal hace que el tiempo de reacción sea muy inmediato porque no hay que lidiar con colapsos de vías, ni cuestiones similares.

—¿Cuáles considera que son las claves para una seguridad satisfactoria en instalaciones como las de la Universidad de Alicante?

—En realidad la Universidad de Alicante tiene un historial con pocas incidencias relevantes, ya que en ella se puede observar un ambiente de tranquilidad y confianza, creo que motivado entre otras cosas, por la existencia de un departamento de Seguridad cercano y comprometido, que ofrece información, ayuda, soluciones y respuestas inmediatas a los problemas que se plantean, así como con una preocupación constante por mantener los sistemas de seguridad en condiciones óptimas, asegurando además, la formación de todo el personal (PAS y PDI), para que tengan los conocimientos necesarios y saber cómo actuar en casos de emergencia, enfrentándose a las diferentes situaciones de riesgo.

—¿Cree que los alumnos, trabajadores,... valoran las medidas de seguridad implantadas en las instalaciones de la Universidad o, por el contrario, se trata de un hecho que pasa desapercibido?

—Nosotros intentamos que todas las medidas que se implementan, puedan llegar a toda la comunidad universitaria, ya sea vía cartelería con imágenes y colores atractivos, o con ejercicios prácticos de desalojos en casos de emergencia en edificios, accidentes graves de personas, etc., donde se les hace partícipes de ello, y pueden colaborar siempre que lo deseen.

Además contamos con un cuestionario de Seguridad, donde cualquiera puede hacer llegar al departamento de Seguridad sus sugerencias de mejora, así como con un Blog donde se dan consejos de seguridad y se cuentan anécdotas ocurridas en el día a día, tanto en nuestro campus universitario como fuera.

Por lo tanto yo diría que sí, que el personal en general valora los medidas de seguridad implantadas, ya que se puede observar una colaboración creciente y una cultura de seguridad que antes no existía.

—¿Qué papel cree que han jugado las nuevas tecnologías a la hora de mejorar la seguridad en instalaciones universitarias?

—Concretamente en la Universidad de Alicante han sido clave, ya que era necesario tener un control de accesos al campus, a las escuelas y facultades, a los laboratorios, aulas de informática, etc, sobre todo en periodos nocturnos y festivos, evitando con ello tanto accidentes como posibles hurtos, y en el caso inevitable de que sucediesen, revisar imágenes y poder esclarecerlos.

Hay que tener en cuenta que la universidad cuenta con salas de estudio 24 horas, 365 días al año y con personal de laboratorio que, por las características de sus investigaciones han de hacer uso de las instalaciones fuera de los horarios habituales.

Actualmente en el departamento de Seguridad estamos trabajando para actualizar y mejorar tecnológicamente los sistemas en nuestras instalaciones, con la idea de conseguir una universidad más moderna y segura.

—¿Reciben algún tipo de formación en temas de prevención de riesgos laborales y seguridad los trabajadores de la universidad?

—Anualmente se convocan cursos de formación para todos los empleados, en ellos se imparten módulos que engloban prevención de riesgos, primeros auxilios, plan de emergencia, extinción de incendios, uso y manejo de un desfibrilador, etc. En este sentido, por ejemplo, hemos de destacar que la Universidad de Alicante es una de las pocas en España y, además ha sido pionera, en constituirse como espacio cardioprotegido, lo que requiere, necesariamente, de la implicación y de la formación de nuestros equipos de seguridad.

Además se realizan simulacros de evacuación, donde se imparten charlas formativas para actuaciones según los diferentes riesgos existentes: incendios, inundaciones, terremotos, amenazas terroristas, etc.

Tras las mencionadas charlas formativas, se procede al desalojo físico y completo de todos los ocupantes del edificio, haciendo también uso de las técnicas de evacuación, para casos de personal con discapacidad. ●

Texto: Gemma G. Juanes.

Fotos: Universidad de Alicante

JOSÉ LUIS REÑÓN CASTELLANOS. JEFE DEL SERVICIO DE INFRAESTRUCTURAS. UNIVERSIDAD DE CANTABRIA*

«Los **sistemas** nos permiten facilitar a la comunidad universitaria un acceso más **fácil y seguro a sus dependencias**»

EL buen funcionamiento de todos los sistemas de protección y vigilancia instalados, así como la perfecta ejecución de los protocolos de actuación creados para el servicio, son las claves para una seguridad satisfactoria en este tipo de instalaciones». Son palabras de José Luis Reñón Castellanos, jefe del Servicio de Infraestructuras de la Universidad de Cantabria, quien además analiza para Cuadernos de Seguridad el papel que juega la tecnología a la hora implantar y mejorar la seguridad en las instalaciones universitarias.

—¿Podría explicarnos a grandes rasgos el origen de la institución universitaria, así como el número de alumnos, empleados, carreras, etc., que se imparten actualmente?

—La Universidad de Cantabria se fundó como institución independiente en 1972, bajo el nombre de Universidad de Santander. Hasta entonces era un campus de la Universidad de Valladolid que contaba con centros tan antiguos como las Escuelas de Comercio y Náutica (1829), la de Industrias y la normal de maestros (1915). Actualmente cuenta con cuatro institutos de investigación punteros en sus respectivas áreas de conocimiento: Prehistoria, Física, Biomedicina y Biotecnología e Hidráulica Ambiental. Actualmente cuenta con unos 14.000 alumnos que cursan alguno de sus 30 grados, 43 máster oficiales y 20 programas de doctorado, y cuenta con el distintivo otorgado por el Gobierno de España de Campus de Excelencia Internacional.

—¿Cuál es la estructura e infraestructuras actual del área/departamento de Seguridad de la Universidad de Cantabria?

—El Servicio de Seguridad involucra al Servicio de Infraestructuras (jefe del Servicio y director de la Unidad de Instalaciones y Seguridad), y una empresa adjudicataria (desde enero de 2017 Clece Seguridad).

Universidad de Cantabria.

Sala de Control de la Universidad de Cantabria.

—¿Cuáles son las funciones concretas que llevan a cabo?

—El cometido de nuestro Servicio de Seguridad es proteger, custodiar y vigilar las instalaciones y personal de la comunidad universitaria. También ejerce como de Punto de Información de todas las actividades y dependencias universitarias.

—A grandes rasgos, ¿podría explicarnos las medidas y medios de seguridad con que cuenta la instalación universitaria?

—En general, llevamos a cabo estudios de valoración de riesgos, control de las instalaciones de accesos a los edificios y aparcamientos. Asimismo disponemos de un CCTV y se realizan también rondas de vigilancia.

—¿Cuáles son los riesgos más habituales a los que tiene que hacer frente el área de Seguridad de la Universidad de Cantabria?

—El servicio de diurno atiende el control de tráfico y el control de los sistemas de vigilancia instalados. El nocturno, el control de los sistemas de seguridad y la protección de las instalaciones ante posibles intrusiones o vandalismo.

—¿Cuáles considera que son las claves para una seguridad satisfactoria en instalaciones como las de la Universidad de Cantabria?

—El buen funcionamiento de todos los sistemas de protección y vigilancia instalados, así como la perfecta ejecución de los protocolos de actuación creados para el servicio.

—¿Cree que los alumnos, trabajadores... valoran las medidas de seguridad implantadas en las instalaciones de la Universidad o, por el contrario, se trata de un hecho que pasa desapercibido?

—El personal comprende y utiliza las indicaciones de nuestras funciones. El alumnado, con el tiempo, va comprendiendo que es necesario utilizar las instalaciones y servicio con arreglo a las normas.

—¿Qué papel cree que han jugado las nuevas tecnologías a la hora de mejorar la seguridad en instalaciones universitarias?

—Se trata de un papel muy importante y que, además, se encuentra en continuo desarrollo. Los sistemas nos permiten facilitar a la comunidad universitaria un acceso más fácil y seguro a sus dependencias habituales.

—¿Reciben algún tipo de formación en temas de prevención de riesgos laborales y seguridad los trabajadores de la universidad?

—Además de la formación para la propia habilitación de los vigilantes de seguridad, el Servicio de Seguridad y otros miembros del personal universitario reciben formación específica de prevención de riesgos para actuaciones en caso de emergencia, protocolos de intervención en laboratorios, etc. ●

Texto: Gemma G. Juanes.
Fotos: Universidad de Cantabria

*Servicio dependiente del Vicerrectorado de Campus, Servicios y Sostenibilidad.

Simulacro de Incendio en la instalación universitaria.

FRANCISCO JAVIER RODRÍGUEZ DE LAS HERAS. DIRECTOR DE INFRAESTRUCTURAS.
UNIVERSIDAD NEBRIJA

«La **seguridad** en una universidad debe abordarse de manera **integral**»

—¿Podría explicarnos el origen de la institución universitaria, así como el número de alumnos, empleados, carreras, etc., que se imparten actualmente?

—La Universidad Nebrija tiene su origen en el Centro de Estudios Hispánicos, que abre sus puertas en julio de 1985 con la vocación de difundir el español y nuestra cultura entre los estudiantes extranjeros, y mejorar la formación y metodología de los profesionales de la enseñanza del español. Este proyecto, impulsado por Belén Moreno de los Ríos y Manuel Villa-Cellino, sufre un rápido y constante desarrollo. Ese mismo año se crea el Centro de Estudios Antonio de Nebrija, y en 1988 la Fundación Antonio de Nebrija, y se ponen en marcha distintos programas de máster y actividades docentes y de investigación en áreas de Ciencias Sociales, Informática, Lenguas Modernas, Economía, Derecho y Ciencias Empresariales. En 1992 se presentó la memoria para el Reconocimiento de la Universidad por el Ministerio de Educación y en mayo de 1995 queda finalmente reconocida la Universidad Nebrija, tal y como hoy la conocemos. En 2016, se ha celebrado por tanto su 20º aniversario.

Actualmente la Universidad tiene implantadas las siguientes Facultades y Escuelas:

- Facultad de Ciencias Sociales, con titulaciones de ADE, Derecho, Turismo y Relaciones Internacionales.
- Facultad de Ciencias de la Comunicación, con titulaciones de Periodismo, Publicidad y Marketing.
- Facultad de Artes y Letras, con titulaciones de Educación Infantil, Artes, Escénicas, Bellas Artes y Diseño de Interiores.
- Escuela Politécnica Superior de Ingeniería, con titulaciones de Ingeniera Industrial, Mecánica, Arquitectura e Ingeniería del Automóvil.
- Ciencias de la Salud, con titulaciones de Enfermería y Fisioterapia.

A eso hay que añadir un gran número de máster de postgrado, y los cursos de español del CEHI.

La actividad se desarrolla en tres Campus distintos:

- La Berzosa, en Hoyo de Manzanares.
- Dehesa de la Villa, en la calle Pirineos 55, de Madrid, y Princesa, en la calle Santa Cruz de Marcenado 27, de Madrid.

Además está el centro asociado de San Rafael en la calle Serrano, donde se imparten los estudios de Ciencias de la Salud.

El curso pasado se han superado los 4.000 alumnos matriculados, con una plantilla de más de 300 personas y más de 200 profesores asociados.

—¿Cuál es la estructura e infraestructura actual del área/departamento de Seguridad de la Universidad Nebrija?

—La seguridad general de la Universidad depende en su totalidad del departamento de Infraestructuras, que después tiene distintos responsables para cada uno de los problemas a afrontar.

Podríamos también hablar de ciberseguridad, pero eso es competencia del departamento de Sistemas.

—¿Cuáles son las funciones concretas que lleva a cabo?

—El departamento de Infraestructuras se ocupa de obras, organización de espacios, limpieza, mantenimiento, recepción, transporte, eventos y servicios generales, y mi función se resume en conseguir que todos los días los Campus abran sus puertas en buen estado de funcionamiento, y que a lo largo del día, alumnos, profesores y personal puedan desarrollar su actividad en las mejores condiciones posibles de operatividad, confort, y seguridad.

Centrándonos en la seguridad, creo que sólo puede ser afrontada como un todo, de una forma integral. Hay que velar por todos sus aspectos: Seguridad laboral, seguridad de uso, seguridad en el transporte, seguridad ante un siniestro y seguridad al robo.

—¿Podría explicarnos las medidas y medios de seguridad con que cuenta la Universidad?

—La mejor medida de seguridad general es la constante revisión de la implantación y el cumplimiento de la normativa en lo que hace referencia a seguridad laboral, uso y transporte. Así mismo lo es en cuanto a un incendio, mediante la existencia de Planes de Emergencia y las dotaciones necesarias de Extintores, BIE, y detección de incendios.

En cuanto al robo, no consideramos que tengamos un nivel de riesgo elevado, pero evidentemente tomamos las mínimas medidas razonables. Alarmas y cámaras de seguridad para la noche, cámaras de seguridad para el día y en el caso de Princesa, tornos y cerraduras con tarjetas inteligentes que permiten un control del acceso y la circulación por el Campus

—¿Cuáles son los riesgos más habituales a los que tiene que hacer frente el área de Seguridad de la Universidad Nebrija?

—Hay que decir que afortunadamente las incidencias en seguridad son bajas.

Las más habituales son pequeños robos a estudiantes, y cambiando completamente de plano, a los que más tiempo se les dedica es a los derivados de los trabajos de mantenimiento y/o obras. Finalmente son estos trabajos los que con diferencia más riesgos conllevan, por el uso de maquinaria y por la realización de trabajos en altura.

—¿Cuáles considera que son las claves para una seguridad satisfactoria en instalaciones como las de la Universidad Nebrija?

—Como ya he comentado anteriormente, la forma de abordar la seguridad tiene que ser integral.

Las claves para un buen funcionamiento de la seguridad es el estudio a conciencia de los edificios y de sus flujos de funcionamiento, y a partir de ahí extraer todos los riesgos que se generan, sean del tipo que sean, para ir dándoles solución desde los distintas áreas involucradas.

—¿Cree que los alumnos, trabajadores,... valoran las medidas de seguridad implantadas en la Universidad o se trata de un hecho que pasa desapercibido?

—Pues creo que las dos cosas. Pasan desapercibidas y por eso finalmente las valoran. Cuando día tras día no se producen incidencias en la Universidad, la seguridad pasa desapercibida, que es lo mejor que puede ocurrir. Pero si finalmente uno pregunta al usuario si se siente seguro en la Universidad, estoy seguro de que su respuesta será afirmativa, lo que significa que la valora.

—¿Qué papel cree que han jugado las nuevas tecnologías a la hora de mejorar la seguridad en instalaciones universitarias?

—La tecnología siempre mejora nuestra vida. Alarmas, detecciones, controles de acceso… son una mejora constante.

—¿Reciben algún tipo de formación en temas de prevención de riesgos laborales y seguridad los trabajadores de la universidad?

Naturalmente. Todos los empleados reciben una formación genérica, y luego de forma mucho más concreta los empleados de mantenimiento. ●

Fotos: Universidad Nebrija

FERNANDO PIRES. VP SALES MANAGER AND MARKETING. MORSE WATCHMANS

Ventajas de la **gestión de llaves en** centros educativos

La gestión de la seguridad puede ser particularmente compleja para las universidades y otras instalaciones educativas, que deben proporcionar un acceso conveniente y garantizar la seguridad de los estudiantes, el personal y los visitantes. Las recientes tragedias han aumentado el conocimiento de esta necesidad y han puesto en examen todos los aspectos de la protección y la seguridad en la educación. Los extensos sistemas heredados en forma de claves físicas tienden a ser objeto de un mayor escrutinio mientras la administración busca maneras de mejorar la seguridad y protección, al tiempo que maximiza los presupuestos.

Desde un punto de vista de costos, así como del tiempo, tiene sentido para las escuelas encontrar maneras de seguir utilizando llaves, mientras aumenta el nivel de seguridad que ofrecen. La seguridad y el rastreo de las llaves físicas mediante un sistema de gestión de llaves no sólo ayuda a que el campus sea más seguro para los estudiantes, el personal y los visitantes, sino que también ahorra costos y protege contra la pérdida.

Los sistemas de control de llaves están diseñados para almacenar y registrar el historial de acceso de cada llave, incluyendo el usuario, la fecha y la hora de la devolución. Así se eliminan las cajas de bloqueo obsoletas, los registros manuales poco fiables y las etiquetas de identificación de llaves desordenadas, todas las cuales pueden disminuir potencialmente la seguridad del campus. Con un sistema automatizado de control de llaves, cuando un usuario autorizado necesita acceder a una clave, simplemente ingresa su código PIN pre-registrado o escanea su tarjeta o huella digital para desbloquear el gabinete a prueba de manipulaciones.

Las llaves almacenadas están conectadas a un mecanismo de bloqueo con un microchip que contiene un número de serie único, que es leído por el sistema para identificar qué llave está siendo retirada o devuelta. Las llaves para áreas específicas pueden agruparse en llaveros de código de colores, y un rastro de auditoría puede asegurar que

la última persona que saque las llaves pueda ser identificada. Las alertas basadas en software pueden notificar a los administradores cada vez que una llave no se devuelva al gabinete, y proporcionar información sobre quién tiene alguna llave en un momento dado.

Además de almacenar y rastrear las llaves, los sistemas también pueden configurarse con armarios para almacenar con seguridad artículos más pequeños a los que se debe controlar el acceso. Esto puede incluir armas de fuego de los agentes de seguridad, radios, teléfonos celulares, ordenadores portátiles y otros artículos que son utilizados por diferente personal durante el transcurso de un día determinado.

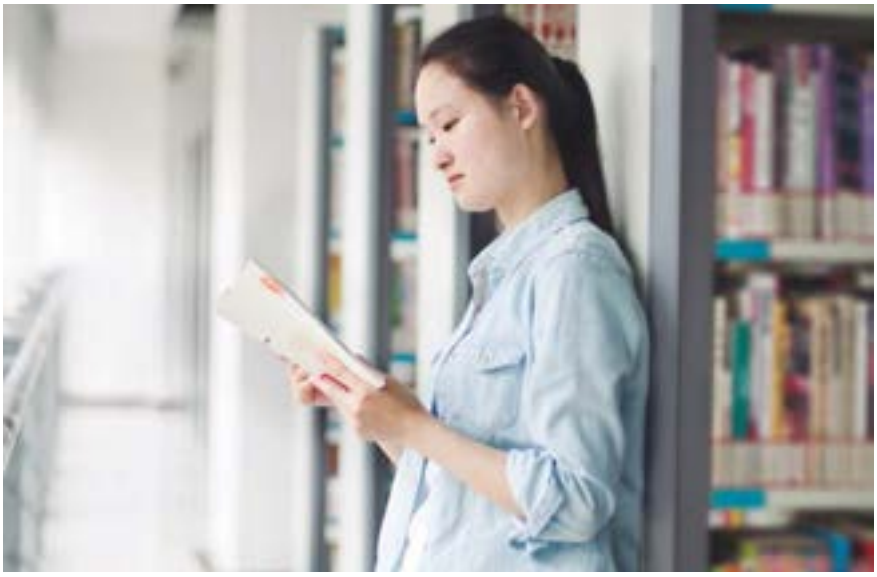
Si son robados o extraviados, estos elementos podrían causar una brecha de seguridad potencial. Además, a medida que los sistemas de control de acceso continúan proliferando, los propios dispositivos de acceso, tales como tarjetas magnéticas o dispositivos de proximidad, necesitan ser protegidos de la misma manera que las llaves físicas. Los sistemas más avanzados también acomodan estos dispositivos con módulos diseñados específicamente que se pueden utilizar en cualquier combinación con los módulos estándar de la llave o del armario.

La integración del sistema y el control centralizado es otra forma de mejorar el valor de un sistema de gestión de llaves. Los administradores pueden acceder, programar y supervisar el sistema a través de una red desde cualquier lugar. Esta conveniencia permite a los administradores de instalaciones acceder a informes, cambiar usuarios, establecer niveles de permisos para cada código de usuario, monitorear datos o configurar los sistemas desde prácticamente cualquier ubicación. Es un ahorro de tiempo tremendo, así como un refuerzo a las medidas de seguridad en todos los ámbitos, ya que las personas pueden ser eliminadas del sistema rápida y fácilmente.

> «La integración del sistema y el control centralizado es otra forma de mejorar el valor de un sistema de gestión de llaves»

En última instancia, el objetivo de un sistema de gestión de llaves es el mismo que para cualquier otra solución de seguridad: hacer que el campus sea un lugar más seguro para estudiantes, personal y visitantes. Los sistemas de gestión de llaves son una solución altamente práctica y rentable que alcanza este objetivo en un entorno educativo. ●

Fotos: Morse Watchmans/Freepik



Contactos de empresas, p. 7.

BORJA GARCÍA-ALBI GIL DE BIEDMA. VICEPRESIDENTE PARA IBERIA Y LATINOAMÉRICA DE RISCO GROUP

Sistemas centralizados, claves para la seguridad en **centros universitarios**

LOS centros universitarios son edificios públicos en los que la afluencia de gente es continua y diaria por lo que la seguridad es muy importante. Los campus suelen estar compuestos de varios edificios por lo que el tema de la seguridad es algo más complejo que en otro tipo de inmuebles, pero no por ello hay que dejarla de lado.

Los sistemas de seguridad en los centros universitarios deben garantizar la protección de los estudiantes, empleados y profesores, además de salvaguardar las instalaciones y todos los materiales que en ellos se encuentran, y que en ocasiones son objeto de actos vandálicos.

Debido a la magnitud, escalas y desafíos que la protección de un campus de universidad conlleva es esencial que se instale un sistema que integre control y gestión, control de accesos, CCTV, intrusión, y todo ello adecuado al ambiente propio de un campus para que sea lo más discreto posible.

Características de la solución para la seguridad de un centro universitario

Ya hemos hablado de la dificultad de integrar un sistema de seguridad en centros universitarios debido a los distintos edificios de los que está formado. Por esta característica, algo importante a tener en cuenta a la hora de elegir un sistema para implementar en los centros universitarios es que los distintos dispositivos que se instalen en el campus se puedan integrar en una plataforma, que permita un control y vigilancia centralizada a través de todo el espacio, mediante una interfaz con mapas sinópticos intuitivos en tiempo real.

Otra característica que debe tener la solución que se vaya a integrar en el campus es que desde su plataforma de gestión de seguridad permita a la persona responsable ver y verificar todas las funciones del sistema, generar informes de sucesos, inhibir o anular los detectores para evitar las falsas alarmas y controlar autorizaciones.

Además, el sistema

que se instale tiene que tener la capacidad de identificar y navegar por los detectores que se hayan disparado en el momento, así como localizar rápidamente las puertas y ventanas por las que se está accediendo al edificio, para evitar así cualquier tipo de acto vandálico, y en caso de que ocurriera poderlo solventar cuanto antes.

Por último, algo indispensable es que el sistema sea flexible, es decir, que se adapte a las necesidades de cada centro universitario. Cada campus es distinto, tiene características diferentes y pueden ser modificados en extensión. Por eso veo necesario que el sistema de seguridad se pueda adecuar al centro y pueda ampliarse en caso de que haya modificaciones en las instalaciones y se necesite aumentar la extensión que hay que proteger.

En definitiva, si tenemos en cuenta todo lo mencionado y añadimos que tenga una fácil utilización y que sea discreto, obtendremos ese sistema de seguridad ideal para los centros universitarios, que hará que empleados, estudiantes y profesores se sientan más seguros en la universidad. ●

«Es indispensable que el sistema de seguridad sea flexible, es decir, que se adapte a las necesidades del centro»

Fotos: *Risco Group*

Contactos de empresas, p. 7.

ANTONIO TORTOSA. VICEPRESIDENTE. TECNIFUEGO-AESPI

Universidad: subir nota en Protección contra Incendios

LAS Universidades Públicas y Privadas deben cumplir en materia de seguridad contra incendios el Código Técnico de la Edificación, cuyo ámbito de aplicación se recoge en el denominado uso Docente: Edificio, establecimiento o zona destinada a docencia, en cualquiera de sus niveles: escuelas infantiles, centros de enseñanza primaria, secundaria, universitaria o formación profesional. Las zonas de un establecimiento de Uso Docente destinadas a actividades subsidiarias de la principal, como cafeterías, comedores, salones de actos, administración, residencia, etc., deben cumplir las condiciones relativas a su uso.

Requisitos de Protección Pasiva contra Incendios:

Las exigencias básicas para la protección pasiva de un edificio docente quedan contempladas en el CTE:

Exigencia básica SI 1: Propagación interior, sobre división en sectores de incendio y sus características de Resistencia y Reacción al Fuego. Exigencia básica SI 2: Propagación exterior, que implica poner medios para evitar la propagación del fuego tanto por fachada como por cubierta. Exigencia básica SI 3: Evacuación de ocupantes, es decir, medios de evacuación y control de humos.

Y exigencia básica SI 6: Resistencia estructural al incendio, que recoge que

la estructura será diseñada de forma adecuada y bien protegida con los medios adecuados.

Para cumplir estas exigencias, se facilitan unos documentos:

•Documento SI 1, que hace mención de sistemas compartimentadores, sistemas de sellado de paso de huecos, conductos de ventilación, etc.

•Documento SI 2, con mención a las franjas resistentes al fuego.

•Documento SI 3, con las características de los pasillos y escaleras de evacuación, así como de los medios de control de humos.

•Y Documento SI 6, donde se trata todo lo relacionado con la protección estructural, tanto si es metálica como de otros materiales, y que se complemente en los Anejos. **(Tabla 1)**

Deficiencias

Según un estudio, publicado por la Fundación Eroski, las Universidades (sobre todo las construidas hace años) presentan deficiencias de seguridad contra incendios relacionados con planes de emergencia y sistemas de seguridad. Las principales asignaturas pendientes de las Universidades son la inexistencia de sistemas de detección de incendios, la falta de protocolos escritos de actuación conocidos por los alumnos para saber cómo actuar en caso de emergencia y el escaso hábito de realización de simulacros de evacuación del centro por una emergencia.

Algunas de las faltas más impor-

PROTECCIÓN ACTIVA: INSTALACIONES CONTRA INCENDIOS OBLIGATORIAS

Tabla 1.1. Dotación de instalaciones de protección contra incendios

Uso previsto del edificio o establecimiento / Instalación	Condiciones
En general	
Extintores portátiles	Uno de eficacia 21A -113B: - Cada 15 m de recorrido en cada planta, como máximo, desde todo *origen de evacuación*. - En las zonas de riesgo especial conforme al capítulo 2 de la Sección 1 [(i)] de este DB.
Bocas de incendio	En zonas de riesgo especial alto, conforme al capítulo 2 de la Sección SI1, en las que el riesgo se deba principalmente a materias combustibles sólidas [(ii)]
Ascensor de emergencia	En las plantas cuya *altura de evacuación* exceda de 50 m. [(iii)]
Hidrantes exteriores	Si la *altura de evacuación* descendente exceda de 28 m o si la ascendente excede 6 m, así como en establecimientos de densidad de ocupación mayor que 1 persona cada 5 m^2 y cuya superficie construida está comprendida entre 2.000 y 10.000 m^2. Al menos un hidrante hasta 10.000 m^2 de superficie construida y uno más por cada 10.000 m^2 adicionales o fracción. [(iv)]
Instalación automática de extinción	Salvo otra indicación en relación con el uso, en todo edificio cuya *altura de evacuación* exceda de 80 m. En cocinas en las que la potencia instalada exceda de 20 kW en uso *Hospitalario* o *Residencial Público* o de 50 kW en cualquier otro uso [(v)] En centros de transformación cuyos aparatos tengan aislamiento dieléctrico con punto de inflamación menor que 300 ºC y potencia instalada mayor que 1 000 kVA en cada aparato o mayor que 4 000 kVA en el conjunto de los aparatos. Si el centro está integrado en un edificio de uso *Pública Concurrencia* y tiene acceso desde el interior del edificio, dichas potencias son 630 kVA y 2 520 kVA respectivamente.
Docente	
Bocas de incendio	Si la superficie construida excede de 2.000 m^2.
Columna seca	Si la *altura de evacuación* excede de 24 m.
Sistema de alarma	Si la superficie construida excede de 1.000 m^2.
Sistema de detección de incendio	Si la superficie construida excede de 2.000 m^2, detectores en zonas de riesgo alto conforme al capítulo 2 de la Sección 1 de este DB. Si excede de 5.000 m^2, en todo el edificio.
Hidrantes exteriores	Uno si la superficie total construida está comprendida entre 5.000 y 10.000 m^2. Uno más por cada 10.000 m^2 adicionales o fracción.

> «Las universidades públicas y privadas deben cumplir en materia de seguridad contra incendios con el Código Técnico de la Edificación»

tantes detectadas son las salidas de las aulas, que para facilitar las evacuaciones no se deben encontrar unas enfrente de las otras; las tomas de agua para casos de incendio o hidrantes y los indicadores de dirección de las salidas de emergencia en los recintos cerrados; la falta de mantenimiento de los extintores; la inexistencia de sistemas de detección y rociadores automáticos.

La debida protección contra incendios en los centros de estudio debe revisarse y adecuarse a las nuevas tecnologías existentes. Es conveniente que se solicite un informe a una empresa especializada en la materia que adecuará las medidas a la legislación vigente, como mínimo.

Las empresas de protección contra incendios, que integran TECNIFUEGO-AESPI, pueden prestar su servicio a las Universidades para la revisión y adecuación de las instalaciones de seguridad contra incendios. Es importante que los gestores de este tipo de centros, los alumnos, los profesores y la sociedad en general sepan que existen suficientes avances tecnológicos en los equipos y sistemas de protección contra incendios como para prevenir, detectar y extinguir un incendio en cualquier tipo de ambiente y edificio. ●

Tabla 1.1 Ampliación de Información

(i) Un extintor en el exterior del local o de la zona y próximo a la puerta de acceso, el cual podrá servir simultáneamente a varios locales o zonas. En el interior del local o de la zona se instalarán además los extintores necesarios para que el recorrido real hasta alguno de ellos, incluido el situado en el exterior, no sea mayor que 15 m en locales de riesgo especial medio o bajo, o que 10 m en locales o zonas de riesgo especial alto.

(ii) Los equipos serán de tipo 45 mm, excepto en edificios de uso Residencial Vivienda, en lo que serán de tipo 25 mm.

(iii) Sus características serán las siguientes:

– Tendrá como mínimo una capacidad de carga de 630 kg, una superficie de cabina de 1,40 m², una anchura de paso de 0,80 m y una velocidad tal que permita realizar todo su recorrido en menos de 60s.

– En uso Hospitalario, las dimensiones de la planta de la cabina serán 1,20 m x 2,10 m, como mínimo.

– En la planta de acceso al edificio se dispondrá un pulsador junto a los mandos del ascensor, bajo una tapa de vidrio, con la inscripción «Uso Exclusivo Bomberos». La activación del pulsador debe provocar el envío del ascensor a la planta de acceso y permitir su maniobra exclusivamente desde la cabina.

– En caso de fallo del abastecimiento normal, la alimentación eléctrica al ascensor pasará a realizarse de forma automática desde una fuente propia de energía que disponga de una autonomía de 1 h como mínimo.

(iv) Para el cómputo de la dotación que se establece se pueden considerar los hidrantes que se encuentran en la vía pública a menos de 100 de la fachada accesible del edificio.

(vi) Para la determinación de la potencia instalada sólo se considerarán los aparatos destinados a la preparación de alimentos Las freidoras y las sartenes basculantes se computarán a razón de 1 kW por cada litro de capacidad, independientemente de la potencia que tengan. La eficacia del sistema debe quedar asegurada teniendo en cuenta la actuación del sistema de extracción de humos.

Fotos: *Tecnifuego-Aespi / shutterstock*

FUJIFILM
Value from Innovation

Una nueva dimensión de la Seguridad:

4K

Primeras lentes Vari Focales 4K de Fujinon

kremer kommunikation

Day Night

Nuevo DV2.2x4.1SR4A-SA2L de Fujifilm
Rendimiento óptico avanzado para capturar imágenes de seguridad en alta resolución 4K. Detalles más finos durante el día y la noche gracias a la tecnología Día/Noche incorporada. Escanea para más información o visita www.fujifilm.eu/fujinon
Fujinon. Para ver más. Para saber más.

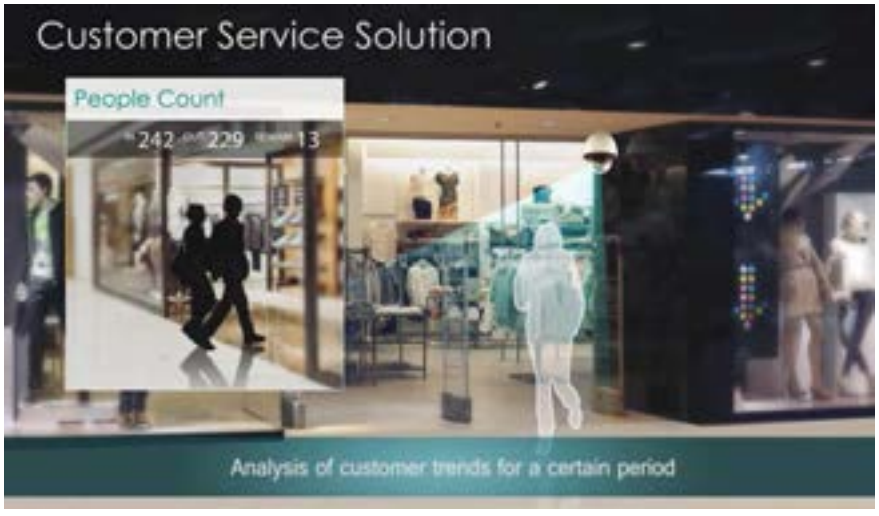
FUJINON

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

Análisis de Vídeo, un mundo de **nuevas aplicaciones**

Los responsables de seguridad de todo el mundo confían desde hace muchos años en las cámaras de videovigilancia como una herramienta eficaz para ayudar a detectar actividades delictivas y mantener la seguridad de las personas. El desarrollo de cámaras con mayores resoluciones de imagen, como Full HD o la ultra-alta definición 4K, ha aumentado la contribución de la videovigilancia a la protección de personas, propiedades y bienes. Con la reciente introducción de los más avanzados chipsets (DSP) de plataforma abierta, las cámaras ahora pueden integrar procesos de análisis específicos que brindan beneficios reales adicionales a los usuarios finales.

La estrategia que están aplicando algunos fabricantes líderes del mercado, como es el caso de nuestra compañía, consiste en suministrar cámaras con las aplicaciones de análisis ya integradas, lo que permite disfrutar de estos beneficios desde que la cámara se instala. El objetivo de ofrecer aplicaciones ya integradas en las cámaras, previamente probadas y evaluadas por nuestro equipo técnico, es ahorrar a los instaladores, integradores de sistemas y usuarios el tiempo y esfuerzo que supone tener que buscar aplicaciones disponibles de entre una lista que crece a un ritmo vertiginoso.

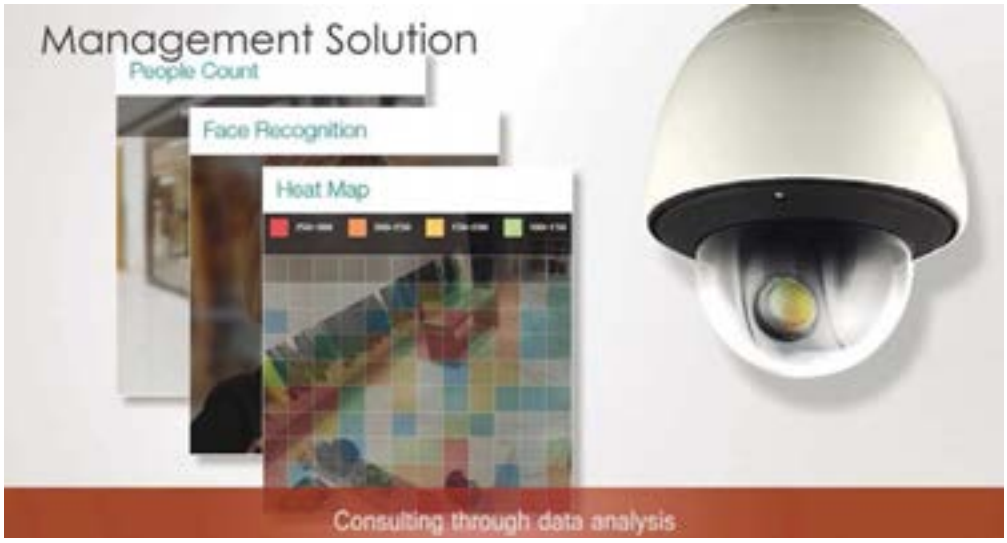


Productividad en el sector de comercio minorista

El sector de comercio minorista, en particular, se puede beneficiar enormemente de los datos que las soluciones de análisis pueden proporcionar. Comprender el comportamiento de los clientes nunca ha sido tan importante, ahora que los comerciantes minoristas de las calles principales de una ciudad afrontan una feroz competencia con las alternativas de comercio electrónico. Los comerciantes minoristas pueden aprovechar las ventajas del análisis de vídeo para monitorizar y dimensionar el impacto que las promociones por Internet y otras acciones de marketing tienen sobre el número de personas que acuden a sus tiendas.

La disponibilidad de cámaras asequibles, fáciles de configurar y de utilizar, equipadas con software de análisis de vídeo, ha creado la oportunidad de

que los comerciantes minoristas reúnan datos fiables y verificables, que ayuden a identificar por qué una determinada tienda da mejores resultados que las demás. Crear procesos más eficientes, aumentar la satisfacción del cliente minimizando los retrasos en las cajas de pago, identificar las horas y lugares ideales para realizar promociones de productos, son solo unos ejemplos de los objetivos que pueden lograrse con muy poco esfuerzo, gracias a la opción de conteo de personas incluida en el análisis de vídeo.



Cámaras con mapas de calor

Una cámara con mapas de calor ofrece información precisa y en tiempo real sobre el comportamiento de los clientes en el interior de las tiendas. Muestra puntos calientes dentro del establecimiento para indicar los patrones de compra de los clientes y el tiempo que permanecen en la tienda. La prestación de grabación de vídeo a cámara rápida ofrece informaciones de gran valor a la hora de tomar decisiones como, por ejemplo, dónde colocar ciertos productos, al poder identificar aquellas zonas de la tienda que pueden presentar poca actividad.

Conteo de personas

Las cámaras con conteo bidireccional de personas ofrecen a los comerciantes minoristas la posibilidad de dimensionar la eficiencia de la tienda, comparando la afluencia de clientes y las ventas reales. También se identifican los días, horas y temporadas de más trabajo, lo que ayuda a gestionar picos y valles en el flujo de clientes en las líneas de caja.

Cámaras Ojo de pez de 360 grados

Una sola cámara de 360 grados suele ser suficiente para cubrir de forma eficaz y asequible toda un área que, de otro modo, requeriría un gran número de cámaras estándar. Por este motivo, las cámaras de 360 grados se especifican cada vez más en proyectos donde es necesario supervisar la actividad de forma ininterrumpida como en bancos, oficinas, comercios minoristas y almacenes. Las ventajas de las cámaras de 360 grados son aún mayores cuando están equipadas con análisis de mapas de calor y conteo de personas, permitiendo la monitorización de clientes durante toda la jornada.

Desarrollos futuros

Durante los próximos meses es probable que aparezcan muchos más tipos de aplicaciones de análisis innovadores como, por ejemplo, la recién presentada solución de control de acceso para vehículos. Aprovechamos las ventajas de la tecnología de cámaras de plataforma abierta y de la última generación de software de reconocimiento automático de matrículas, permitiendo que los usuarios puedan registrar, supervisar y controlar con precisión todos los vehículos que entran en un área las 24 horas del día, los 7 días de la semana, independientemente de las condiciones lumínicas o medioambientales. La cámara Wisenet Access –que se suministra con el software preinstalado en las cámaras–, es fácil de instalar y genera notificaciones de evento cuando se reconoce la matrícula de un vehículo no autorizado. Además, pueden configurarse notificaciones para que se activen distintas operaciones de control de accesos como la apertura y el cierre de una barrera y el envío de informes de actividad e imágenes por correo electrónico o FTP.

Se puede predecir con seguridad que dentro de un año aproximadamente, podremos mirar hacia atrás a fin de sorprendernos con la diversidad de nuevas aplicaciones que han aparecido. Esta es una situación que beneficia a todas las partes involucradas en la cadena de suministro de videovigilancia. Habrán oportunidades de generar nuevos ingresos para fabricantes, integradores de sistemas e instaladores al dar a los usuarios finales un valor añadido y un gran retorno de la inversión en sistemas de videovigilancia. ●

Fotos: Hanwha Techwin

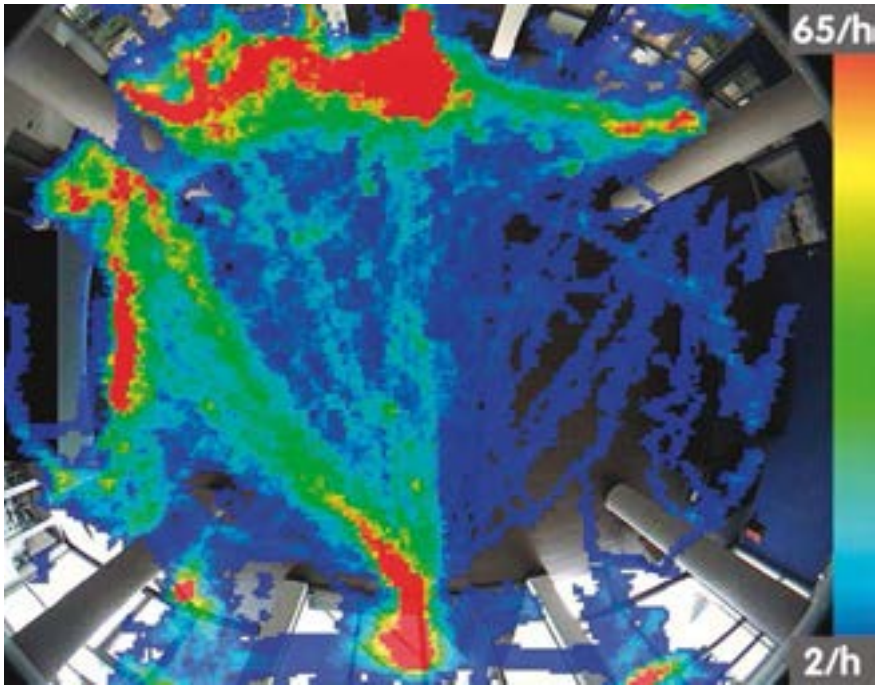
Contactos de empresas, p. 7.

ALFREDO GUTIÉRREZ. BUSINESS DEVELOPMENT MANAGER PARA IBERIA DE MOBOTIX AG

Sistemas de análisis de vídeo inteligente para todo tipo de negocios

Hoy día, en cualquier negocio, independientemente de su tamaño o actividad, se ha hecho fundamental la instalación de un buen sistema de videovigilancia. No nos referimos solamente al establecimiento de una serie de cámaras que registren la actividad ocurrida en un momento dado. Sino a una herramienta que tenga la capacidad de analizar de forma inteligente, todos y cada uno de los movimientos que se realicen en el lugar analizado.

YA sea para proteger una zona determinada, para obtener información importante destinada a optimizar procesos o para realizar estudios de marketing, el software inteligente de vídeo se ha convertido en una tecnología esencial tanto para el sector público como para el privado.

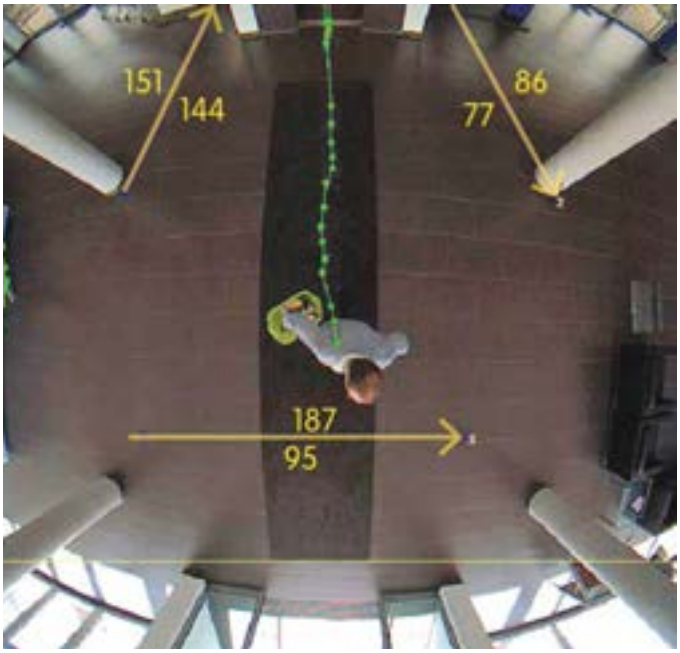


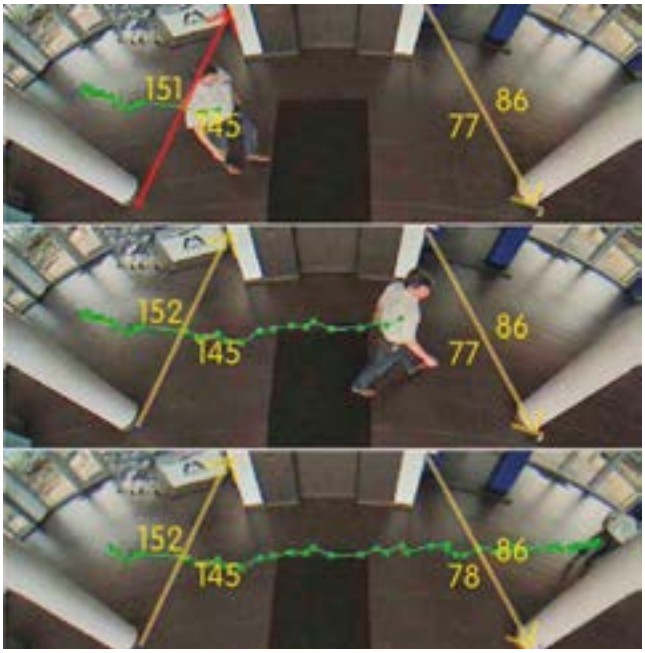
Gracias a que la tecnología de vanguardia permite agregar valor añadido a las técnicas de videovigilancia tradicional, a través de unos parámetros establecidos como pueden ser la velocidad o la dirección, se puede conseguir una serie de ventajas adaptables a la realidad de cada negocio.

¿Qué beneficios obtenemos con un sistema de análisis de vídeo?

Con un mercado potencial muy importante, al ser una herramienta válida tanto para pequeños comercios como para establecimientos públicos, es capaz de detectar movimiento e ignorar todo tipo de interferencias, a la vez que proporciona una gestión de alarma fiable y avisa al personal de seguridad en caso de algún tipo de intrusión.

En el caso, por ejemplo, de un comercio de moda, este tipo de sistemas nos permitiría conocer qué estanterías atraen más al público, delante de qué productos se detiene el mayor número de clientes, o cuáles son las prendas más probadas por los consumidores. Esto es gracias a un mapa de calor, un diagrama de movimiento de un área determinada previamente, con el que





podemos registrar y analizar con fiabilidad movimientos de personas u objetos en la imagen en vivo.

Además, si hablamos de tecnología de medición térmica, se pueden generar alarmas automáticas definidas por límites o rangos de temperaturas elevados, detectando fuentes de calor o posibles incendios.

Otro de los beneficios que podemos obtener con este sistema es la posibilidad de contabilizar el número de personas que se encuentra en una zona determinada. Por ejemplo, en lugares en los que la afluencia de visitantes es muy elevada, como puede ser un centro comercial, espacios en los que se registraron más de 1.900 millones de visitas en España durante el pasado 2015, se pueden mostrar estadísticas sobre los consumidores y así optimizar, entre otros, la planificación de marketing y personal.

Son sistemas de videovigilancia automática que, al analizar las imágenes en tiempo real y en función de una serie de criterios de riesgo, advierten en caso de producirse cualquier tipo de altercado, reduciendo, además, las falsas alarmas causadas por animales, árboles, etc.

No obstante, es importante señalar que, para que estas herramientas sean lo más eficiente posible, deben ser fáciles de usar, de alto rendimiento y sin límites. Además, debe permitir a los usuarios gestionar un gran número de cámaras clasificando y estructurando los dispositivos en grupos y en vistas con distintas disposiciones.

En definitiva, el uso de tecnología inteligente resulta primordial para todo tipo de negocios dedicados a cualquier sector, ya sean grandes o pequeños, públicos o privados. Ya que además de sus funciones básicas de videovigilancia nos pueden proporcionar un plus como es la información acerca del número de personas que se concentra en un espacio, avisar con precisión en caso de ocurrir alguna contrariedad y ayudar en aspectos relacionados al análisis de comportamiento. Características enfocadas a mejorar los servicios de las empresas y, ante todo, a reducir cualquier tipo de peligro o alarma, aumentando la seguridad del establecimiento. ●

> «El software inteligente de vídeo se ha convertido en una tecnología esencial tanto para el sector público como para el privado»

Fotos: Mobotix

Contactos de empresas, p. 7.

ALBERTO ALONSO. BUSINESS DEVELOPMENT MANAGER IBERIA. AXIS COMMUNICATIONS

Sistemas **inteligentes de vídeo**

Con la expansión en el uso de las cámaras de videovigilancia, se hace patente una necesidad: los sistemas deben ser proactivos en la detección de incidentes, de otro modo la observación directa de las mismas es poco eficiente para prevenir actos no deseados y para responder a ellos de manera eficaz.

PARA ello contamos con algunas alternativas. La primera en orden cronológico es la «integración» o interconexión de los subsistemas de seguridad que detectan o generan las incidencias con el subsistema de vídeo. Esta opción, se apoyaba (y aún se utiliza) en la capacidad de los elementos de detección de intrusión, incendio y control de accesos para enviar alertas al sistema de vídeo en caso de un evento relevante. Ya sabemos que esta aproximación tiene importantes limitaciones. La más evidente es la propia integración, a menudo realizada con cableado de salida y entradas de alarma en los subsistemas con la dificultad y el coste generados. Otra es la propia sincronización y sintonía de los diferentes sistemas, esto es, que las cámaras de verificación se encuentren exactamente en los lugares de detección, que su cobertura permita realmente una buena verificación, que sus capacidades de ofrecer detalles faciliten esa verificación, etc. Vemos que no siempre resulta ésta la mejor de las opciones, más aún cuando a fin de cuentas precisa de una ingente inversión en diferentes subsistemas, dispositivos, cableado y sinergias no siempre alcanzables.

La otra alternativa es convertir al propio sistema de vídeo en el elemento iniciador de la detección y control. Para ello, naturalmente, hay que disponer de herramientas que analicen la escena capturada por la cámara, y de acuerdo a criterios establecidos indiquen cuándo se está produciendo la circunstancia de interés y así alertar al operador para completar los protocolos de respuesta, o bien simplemente proceder a su registro en la grabación de vídeo. Son las llamadas analíticas, o aplicaciones de análisis de contenidos.

En los primeros años de la década de los 2000, ya se produjo un fuerte despliegue de estas analíticas. Parecía que finalmente el sistema de vídeo había alcanzado la madurez como para constituirse en el principal elemento de la vigilancia y seguridad física. Sin embargo, pronto comprobamos que ni las citadas analíticas tenían el nivel de fiabilidad, estabilidad y adaptabilidad necesarios para ofrecer una solución de garantías, ni seguramente las imágenes generadas por aquellas cámaras analógicas y de baja resolución (hoy las consideramos de baja resolución, no entonces) tenían la información adecuada para que el análisis de contenidos tuviese más éxito. Fue la llamada «burbuja de las analíticas». El efecto en el mercado se tradujo en una desconfianza generalizada en estas tecnologías y el retorno a soluciones más clásicas, toda vez que además los precios de mercado de esas aplicaciones «inteligentes» eran realmente desorbitados si los contrastamos con su baja eficiencia.

Sin embargo la tecnología evoluciona con velocidad; hoy las cámaras suministran imágenes de gran resolución y se adaptan mejor a las cambiantes condiciones lumínicas ambientales. Por otro lado, los procesadores disponibles para ejecutar las analíticas han aumentado exponencialmente su capacidad y los algoritmos y técnicas matemáticas para la discriminación de lo que sucede en la escena se han vuelto mucho más eficaces y fiables. Vivimos pues una nueva (y parece que definitiva) expansión de la utilización de las analíticas, que propicia aún más la utilización masiva de las cámaras de vídeo vigilancia.

Este nuevo advenimiento del llamado «vídeo inteligente», como en casos similares, arrastra consigo una no desdeñable parte de confusión y desinformación. ¿Hasta qué punto son fiables y eficientes las analíticas disponibles? ¿Son todas iguales? ¿Es éste el último paso de la vídeo vigilancia? Son todas ellas cuestiones que suscitan respuestas muy diversas según el profesional de la segu-

ridad física que las responda. Este artículo no es sino una personal reflexión de uno de esos profesionales, digamos una aportación para intentar desenmarañar los conceptos que masivamente se manejan en las campañas publicitarias, promociones, ferias, exposiciones, e incluso sesudas conferencias y congresos.

Las analíticas de vídeo que se ofrecen hoy día pueden englobarse de modo general en tres grupos de diverso perfil:

En primer lugar, por ser el más conocido, difundido, utilizado y variado, nos referiremos a las analíticas de objetos y su movimiento en la escena. Por describirlas de modo simple, estas analíticas identifican objetos (formas y colores), y miden sus trayectorias y velocidades dentro de la escena. Son las que subyacen en los vídeo sensores, detectores de perímetro, vallas virtuales, merodeo, objetos abandonados, movimiento de vehículos, de multitudes, etc. En esencia son realmente eficaces toda vez que son las analíticas más maduras, con más tiempo de desarrollo y que son más fácilmente aplicables. ¿Son fiables? Pues no todas ni en todas las situaciones. En cuanto al grado de usabilidad de estas analíticas, debemos atender a la criticidad de la situación a controlar. Es decir, si pretendemos que nos alerten sobre posibles incidentes relevantes para su posterior verificación, vamos bien encaminados aunque tendremos que aceptar una cierta tasa de falsas alarmas. Si las usamos para optimizar nuestras grabaciones filtrando horas de contenido irrelevante, estamos en el buen uso, si aprovechamos estas herramientas para efectuar búsquedas de secuencias de vídeo de interés podemos ahorrar mucho tiempo, pero si queremos automatizar decisiones críticas como detener un tren, o poner en marcha un costoso protocolo de respuesta con movilización de recursos, seguramente nuestros deseos han ido más allá de la realidad que nos ocupa. Hay demasiados factores ambientales que afectan al contenido de las imágenes (perspectiva, luces, sombras, lluvia, reflejos, objetos confusos, situaciones de difícil identificación, etc.) como para estimar que nuestra analítica será infalible al 100%. Hay que resaltar algo que es aplicable a cualquier analítica, y aunque ya mencionado conviene recordar: las analíticas trabajan con la información contenida en la imagen que suministra (captura) la cámara, por lo tanto su rendimiento estará fuertemente sujeto a la calidad de esa imagen. Es decir, la mejor de las analíticas no arreglará el problema de unas imágenes con calidad deficiente. Así pues es importante que la analítica tenga recursos para compensar la perspectiva, incluso en las más avanzadas triangular varias cámaras para obtener datos más precisos, que suprima el ruido de fondo en la escena, que filtre las situaciones transitorias producidas por reflejos y otros factores de influencia, y en definitiva tenga en cuenta cuantos más elementos de evaluación. Pero también es muy importante que la cámara suministre imágenes con poco ruido debido a la baja iluminación, alto contraste, colores reales, adaptación a situaciones cambiantes de luz, compensación de posibles vibraciones de la propia cámara debidas a viento o paso de vehículos pesados y un flujo de vídeo estable sin saltos o parpadeos. Con todo ello encontraremos una amplia gama de soluciones que incrementarán su complejidad a la par que su coste y que deberán ser seleccionadas de acuerdo a las necesidades y criticidad de la aplicación. Ya vemos que es importante definir las expectativas que tenemos respecto al rendimiento de la analítica para no encontrarnos con inversiones frustrantes. El ejemplo de las analíticas usadas en el mundo del comercio, casi todas del grupo que estamos comentando, ilustra bien cómo una expectativa de rendimiento «suficiente» para el uso (normalmente estadístico) que se pretende permite una explotación muy interesante de estas nuevas tecnologías.

El segundo grupo de analíticas es más específico y con una rango de aplicación más determinado. Se trata de aquellas que se orientan a la lectura de caracteres alfanuméricos y/o gráficos tales como las matrículas de vehículos, placas de señalización, códigos de barras, códigos QR, etc. Su desarrollo ha sido grande en los últimos años y gracias a la mejora en la resolución y las prestaciones de las cámaras y la evolución en los procesadores y algoritmos su rendimiento es hoy día muy aceptable. De nuevo existen muchos factores ambientales que pueden reducir ese rendimiento, como el ángulo de visión, la distancia, la iluminación, los

reflejos y las vibraciones de la cámara. Aquí debemos especificar la diferencia entre la pura captura y reconocimiento de los caracteres y el proceso de identificar el texto, clasificarlo e interpretar su contenido de modo eficiente para proceder a la gestión posterior de acuerdo con ese contenido. Las diferencias entre analíticas de diversa complejidad vienen reflejadas en la velocidad de lectura e interpretación de los datos, que se traduce en la máxima velocidad de los vehículos y la frecuencia máxima entre uno y otro. También en la tolerancia a ángulos mayores de captura de la matrícula, la capacidad para solventar matrículas defectuosas o sucias, la eficiencia en distinguir caracteres similares y el rango de diferentes tipos de matrículas e incluso caracteres que son capaces de proporcionar. De nuevo la importancia de una buena cámara, adecuada para el tipo de lectura pretendido (control de acceso, circulación urbana, alta velocidad de vehículos, etc.) y para las condiciones ambientales (luz, distancia, ubicación física, vibraciones previsibles, contraluces o reflejos, etc.) será vital para un rendimiento óptimo. Al igual que en el caso anterior, la combinación perfecta entre dispositivo de captura (cámara) y la analítica de prestaciones profesionales permitirá una operación satisfactoria, dado que en muchos casos la tolerancia a errores es muy baja puesto que hablamos de dar acceso a zonas restringidas o identificar inequívocamente un vehículo.

El último grupo es el de las analíticas basadas en características biológicas, o también llamadas biométricas. Quizás las que despiertan más interés son las de reconocimiento facial. La posibilidad de que una máquina reconozca a una persona a semejanza de cómo lo puede hacer el ser humano, nos transporta en cierto modo a la cibernética y los androides. Son muchas las posibles aplicaciones de estas analíticas, pero sin duda la más extendida es la del control de accesos. Seguramente porque con el nivel de desarrollo de hoy esa es la aplicación que con mayor facilidad y fiabilidad puede ser usada, dado que la posición de la cara y las condiciones lumínicas pueden ser controladas para ayudar a la analítica, y por otro lado comparar esa cara con una muestra igualmente obtenida de modo dirigido, con la calidad y posición idónea, lo más parecido al reconocimiento que se hará posteriormente. Otra vez estamos ante muy diferentes niveles de complejidad, encontrando desde analíticas sencillas que se ejecutan en teléfonos móviles hasta otras extremadamente complejas usadas por autoridades policiales en entornos críticos y que requieren recursos de hardware de altas prestaciones. Podemos imaginar los múltiples factores que afectarán al rendimiento de estas analíticas tanto desde el punto de vista ambiental (luz, ángulo de captura, sombras, distancia, etc.) como desde la perspectiva de las diferencias con la muestra original, toda vez que el rostro, al pertenecer a un ser vivo, altera su apariencia de modo sustancial, no solo con el paso del tiempo, sino por el uso de gafas o lentillas, barba, diferente color de pelo y peinado, tono de la piel y otras alteraciones temporales o permanentes (heridas, cicatrices, manchas cutáneas, etc). La mayor parte de estas analíticas efectúan mediciones de distancias entre puntos de la cara, proporciones, y otros factores físicos para componer un único conjunto de parámetros que permita determinar si se trata de la misma persona que la muestra original. Normalmente se puede ajustar el rango de tolerancia para aceptar alguna desviación de la muestra mientras que la mayoría de los parámetros coincidan. Los algoritmos utilizados pueden ser tan complejos que se precisa una potencia de computación realmente avanzada. Además, la velocidad de respuesta puede ser crítica, en cuyo caso esa necesidad de potencia de proceso se torna aún mayor con lo que los costes se incrementan, así como la necesidad de ubicar físicamente grandes máquinas de proceso. Si bien algunas analíticas en la vanguardia de esta tecnología son capaces de identificar varias caras simultáneamente, lo más usual es que sólo se identifique una en cada operación y que ello requiera algunos segundos para efectuarse. Eso, como comentamos reduce su uso a controles de acceso o identificaciones en lugares de tránsito reducido. La posibilidad de colocar una cámara en un lugar público y con multitud de individuos circulando libremente y poder detectar sospechosos o personas dentro de una lista dada es a día de hoy bastante limitada. No obstante, controlando las condiciones ambientales, con las cámaras adecuadas ubicadas de forma idónea y con analíticas del más alto nivel se pueden conseguir resultados muy aceptables, pero aún los costes pueden representar una gran barrera. Como

Axis Solution Conference 2017

Unidos Creamos Soluciones

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

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

II Edición Axis Solution Conference. **Regístrese antes del 1 de marzo para descubrir un mundo de soluciones sectoriales.**

Siga el evento en Twitter: #AxisSolution2017
Puede registrarse en:
www.axissolution2017.es
**Axis Communications se reserva el derecho de admisión.*

AXIS COMMUNICATIONS

VAXTOR SYSTEMS · milestone · TechnoAware TECHNOLOGIES FOR AMBIENT INTELLIGENCE

Citilog · ngaro · herta · PACOM · COGNIMATICS · crambo

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

ADI GLOBAL DISTRIBUTION · ANIXTER · Ciid · INGRAM MICRO · TechData

en el caso del primer grupo de analíticas si limitamos la expectativa a obtener datos estadísticos aceptando ciertos niveles de error, el uso para marketing en los comercios puede ser muy aceptable, especialmente si más que identificar sólo se pretende determinar el sexo, edad y tal vez raza de los clientes que visitan un local.

Quizás una de las discusiones interesante hoy día, es acerca de la alternativa de ejecutar la analítica en un servidor dedicado, en un equipamiento de grabación o gestión de vídeo, o embebida en la propia cámara ya que algunas cámaras IP tienen esa capacidad. La respuesta seguramente no es única y vendrá condicionada sobre todo por las limitaciones que en potencia de proceso tengan las cámaras en relación con las necesidades que presenten las analíticas. Así, por ejemplo, las analíticas más complejas de reconocimiento facial están aún lejos de poder ser ejecutadas en la propia cámara. Sin embargo otras como el reconocimiento de matrículas, la detección de movimiento, el control perimetral entre otras muchas, son cada día más comunes como analítica a bordo de la cámara. Las ventajas que aporta esta arquitectura sobre la más tradicional que utiliza un servidor son múltiples. En primer lugar la escalabilidad, ya que cada cámara realiza su proceso por lo que en principio el número de cámaras del sistema no tendrá límite y se puede aplicar para un solo dispositivo, mientras que con un servidor habrá un límite de cámaras que el servidor puede procesar, además de un costoso hardware adicional desde la primera cámara. Otra ventaja es la de evitar un enorme tráfico de datos en la red en forma de flujo de vídeo que cada cámara tendría que enviar al servidor para ser procesados. Es cierto que las cámaras suelen estar enviando constantemente vídeo para ser grabado, pero tal vez no sea necesario si no hay nada relevante que grabar. Por otro lado, el flujo de vídeo para grabación no tiene que ser necesariamente igual al que se precisa para la analítica, por lo que se incrementa el tráfico y/o el proceso y en los casos de estadísticas o lectura de matrículas, lo realmente relevante es el dato obtenido, más que el vídeo completo que puede resultar muy pesado para su transmisión, permitiendo así gestión remota o la utilización de soluciones en la nube. Otra importante diferencia es la flexibilidad que esta arquitectura otorga al sistema, pudiendo usar muy diversas analíticas en las múltiples cámaras de un sistema, no necesariamente del mismo proveedor. Esto es, no siempre el mismo proveedor dispondrá de la analítica óptima para cada aplicación, y si pensamos en varios proveedores entonces el número de servidores de proceso irá creciendo. Con las analíticas a bordo de las cámaras la libertad de selección es mayor para cada dispositivo individualmente, sin incremento del hardware. Esta flexibilidad permitirá también en un futuro actualizar algunas de las analíticas con nuevas versiones o con otras analíticas de diferente proveedor si es que aportan mejoras interesantes, sin tener que replantear todo el conjunto de analíticas que un único servidor puede estar albergando.

Y finalmente, no es de menor importancia la facilidad para probar las analíticas (o comparar varias de ellas) que se nos ofrece con la simple acción de solicitar una versión de evaluación, cargarla en la cámara correspondiente y sin más inversión en hardware o instalación realizar las pruebas para efectuar una correcta selección y asegurar la inversión a realizar.

Respecto a si estamos ante el último paso en la inteligencia de los sistemas de vídeo, mi consideración es que más bien al contrario nos encontramos en los albores de una tecnología que empezando por estas citadas analíticas aplicadas a cada flujo de video deberá pronto empezar a orientarse hacia una inteligencia que combine contenidos de diferentes fuentes de vídeo para aportar más información, realizar análisis más precisos y contribuir de manera activa a facilitar las tareas del operador de video. Esa será otra generación de sistemas inteligentes de vídeo. ●

*Fotos: **Axis Communications***

Contactos de empresas, p. 7.

PROVISION ISR®

Now you can see!

Tecnología exclusiva a precios competitivos! Disfrute lo mejor de ambos mundos en una sola marca

CONTACTE CON NOSOTROS EN

facturacion@grupoquantum.es

grupoquantum

Nuevo y exclusivo para España

ANDREAS WOLF. PRODUCT MANAGER INTELLIGENT VIDEO SURVEILLANCE. DALLMEIER

«La tecnología de **sensores multifocal** y **cámaras térmicas** es la combinación ideal»

Cuando se trata de la protección del exterior y la protección perimetral/del perímetro de instalaciones sensibles, se emplean en la mayoría de los casos cámaras térmicas. Proporcionan una alta tasa de detección de intrusos no autorizados, pero desgraciadamente ninguna verificación visual de las alarmas. La combinación de cámaras térmicas y tecnología de sensores multifocal hace surgir ahora posibilidades completamente nuevas para el análisis, seguimiento de objeto y reconocimiento de personas en el perímetro. Andreas Wolf, Product Manager Intelligent Video Surveillance de Dallmeier, habla para Cuadernos de Seguridad sobre está combinación ideal de tecnologías.

POR qué es más apta la tecnología de sensores multifocal para la protección perimetral que las cámaras HD o megapíxeles convencionales?

—En la protección perimetral se manejan generalmente distancias muy largas. La tecnología de sensores multifocal (MFS) es una tecnología de cámara que es apta especialmente para la vigilancia y protección de áreas más grandes y distancias largas. Con una distribución sofisticada, este patentado sistema es capaz de proporcionar vigilancia de toda el área en cuestión con una resolución de imagen constante, gran dinámica y profundidad de campo continua, desde un único lugar, esto no lo lograrían cámaras convencionales de un solo sensor y la resolución sería demasiado baja.

En el caso de que se quisiera obtener una resolución tan alta, se debería emplear un número incomparablemente mayor de cámaras de un solo sensor. Además de los gastos que originarían postes, cableado, etc. adicionales, aún habría otro problema: el tiempo y trabajo necesarios para la configuración manual de cada punto de instalación de cámara serían considerables. En esto, también se debería tener en cuenta que la vigilancia perimetral siempre requiere el trabajo con modelos 3D para poder clasificar objetos de manera razonable. La calidad de análisis naturalmente depende de que la cámara y el análisis hayan sido configurados correctamente. Si un gran número de cámaras ha de configurarse manualmente y el proceso no se lleva a cabo como es debido, el análisis no puede funcionar de forma fiable. Con la tecnología de sensores multifocal, la configuración se realiza automáticamente porque el sistema de sensores multifocal integra 3D. De este modo, el problema de seguridad de la configuración manual se elimina.

Otro aspecto que logramos sólo en combinación con la tecnología MFS es la observación de la zona de prealarma.

—¿Qué quiere decir exactamente con observación de la zona de prealarma?

—En caso de alarma es necesario que el personal de vigilancia actúe rápidamente y con un objetivo concreto. Particularmente en la protección perimetral es razonable seguir observando la escena para conocer los movimientos del objeto detectado. En instalaciones perimetrales estándares, sin embargo, el campo de observación está limitado exclusivamente a la zona de detección, es decir, las cámaras tienen un ángulo de apertura estrecho y sólo un campo de visión pequeño. Así, no es posible

ver lo que está ocurriendo en la zona de prealarma. Con la tecnología multifocal son abarcables grandes distancias en las que un objeto y su paradero pueden ser detectados con certeza. Tras una alarma, un objeto puede ser visualizado automáticamente en varias vistas y observado de manera óptima. De este modo, también es posible averiguar de dónde viene o adónde se mueve y así no se lo pierde de vista enseguida. La alta resolución provista por el patentado concepto de sensores de la tecnología MFS permite una detección continua de una persona.

En una palabra, el sistema de sensores multifocal en la valla reúne tres sistemas en uno: la detección clásica de intrusión en el perímetro, el análisis y observación de objetos mucho más allá de la zona de detección mediante el campo de visión más grande y, finalmente, la detección e identificación de personas mediante su alta resolución.

Además, se debe añadir la alta disponibilidad y fiabilidad del análisis de vídeo mediante la combinación de tecnología de sensores multifocal con cámaras térmicas. En el fondo, ¡este nuevo concepto de protección perimetral inicia un cambio de paradigmas en la valla!

—¿Por qué se emplean en la protección perimetral muchas veces cámaras térmicas?

—Los sistemas térmicos ofrecen la base para una muy alta tasa de detección con una muy baja tasa de falsas alarmas. Porque los análisis en el rango de longitudes de onda visibles son vulnerables a notablemente más influencias potenciales de perturbación como sombras, árboles o arbustos, y llegan a sus límites cuando condiciones ambientales como la lluvia, nieve o una tormenta de arena, o algo tan banal como las propias

instalaciones del alumbrado, ya no permiten detectar ningún objeto.

No obstante, la tecnología térmica también se ve impotente cuando ya no existe contraste entre los objetos y su entorno debido a las condiciones térmicas. Y el uso de las cámaras térmicas conlleva otra desventaja crucial: no hay ninguna imagen en color de alta resolución del escenario, es decir, al margen de la simple constatación de la alarma no hay ninguna posibilidad de reconocer a intrusos y mucho menos identificarlos.

—Entonces, ¿de ahí, la combinación con cámaras multisensores?

—El uso conjunto de sistemas MFS con cámaras térmicas ofrece una combinación ideal para la vigilancia perimetral activa. El enlace de ambas tecnologías tiene el objetivo de compensar los puntos débiles de una tecnología con la otra.

El análisis de vídeo es efectuado primordialmente con el vídeo térmico que es menos susceptible a interferencias. Si la tecnología térmica alcanza sus límites debido a las condiciones ambientales climáticas y térmicas, el sistema conmuta automáticamente a análisis en el rango de longitudes de onda visibles. Sólo cuando se combinaron la tecnología de sensores multifocal y la tecnología térmica fue posible la disponibilidad prácticamente total del análisis de vídeo.

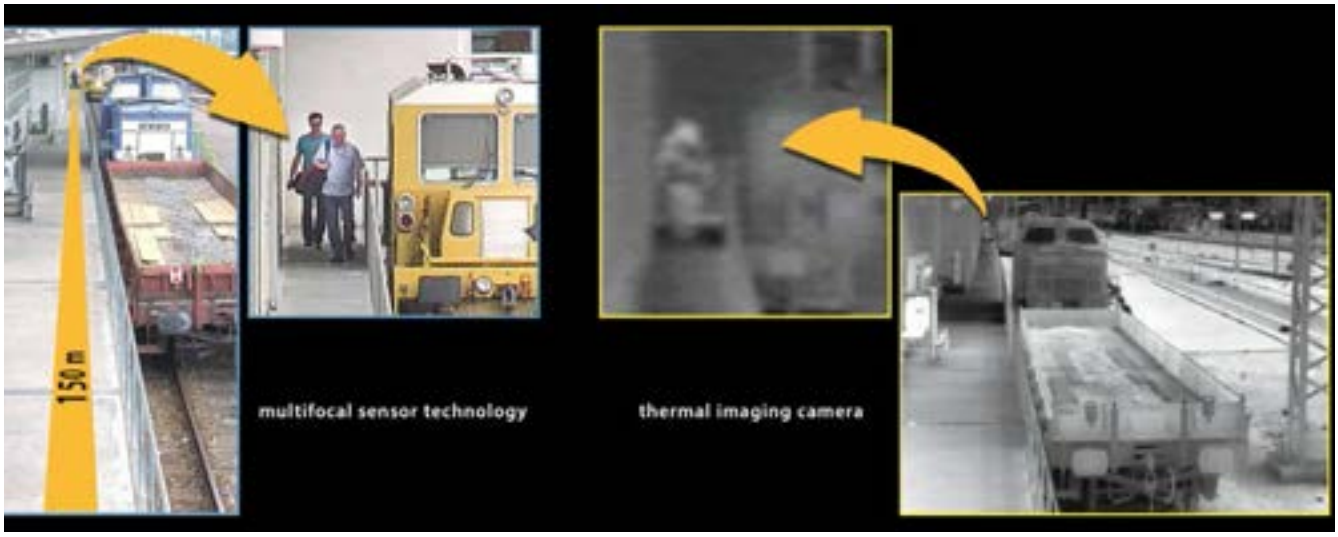
—¿Cuándo exactamente llegan las cámaras térmicas a sus límites?

—Los sensores térmicos miden la radiación térmica de un objeto y la convierten en una imagen en escala de grises. Para que un vídeo térmico sea analizable es decisivo el contraste entre objeto y fondo. Este contraste depende de la diferencia de temperatura absoluta en la imagen, así como de la temperatura relativa entre el entorno inmediato y el objeto. A efectos del análisis de vídeo, los sensores térmicos alcanzan sus límites cuando la temperatura del entorno inmediato es prácticamente idéntica a la del objeto y la diferencia de temperatura absoluta es muy alta, de modo que están disponibles pocos valores grises por grado de diferencia de temperatura. Entonces, la imagen en escala de grises resultante ofrece ningún o muy poco contraste entre el objeto y su entorno, lo que significa que el objeto no es visible y, por tanto, tampoco analizable.

Una gran diferencia de temperatura absoluta y una baja temperatura relativa entre objeto y entorno inmediato se dan particularmente de forma frecuente en ambientes industriales y meses de verano cálidos entre las últimas horas de la tarde y las primeras de la mañana. Los solados, calles y fachadas almacenan el calor tan intensamente que personas en o delante de ellas desaparecen.

—¿Es entonces cuándo se emplea la tecnología MFS?

—Correcto. Un así llamado módulo «Quality of Video» comprueba permanentemente la calidad del contenido de vídeo en cuanto a su analizabilidad mediante procedimientos de análisis de vídeo. Este módulo capta diferentes valores de medición en el vídeo y los utiliza para calcular medidas de nitidez,



relaciones de contraste y características de visibilidad, entre otras, así como en caso de sensores térmicos también los rangos de temperatura medidos. Si la tecnología térmica a efectos del análisis de vídeo llega a sus límites, el sistema emplea los vídeos de la tecnología MFS para el análisis. La conmutación se efectúa automáticamente pero se avisa mediante un evento.

«La combinación de cámaras térmicas y tecnología de sensores multifocal hacen surgir ahora posibilidades nuevas para el análisis»

—¿Los vídeos de los sistemas MFS sólo se utilizan para el análisis?

—No, los flujos de vídeo de los sistemas MFS son grabados simultáneamente con la máxima resolución, o de manera permanente o controlada por eventos. En caso de un incidente se muestra automáticamente la mejor resolución para la verificación visual del evento.

—¿En qué tecnología de grabación y análisis se basa?

—En un software de servidor de análisis. Se trata de una instalación de sistema completa, que incorpora tanto las amplias funciones de grabación como las de análisis de vídeo de alto rendimiento. Estas aplicaciones de análisis de vídeo están ya preinstaladas y sirven, por ejemplo, para la detección de intrusión, recuento de personas o recuento de objetos. Dependiendo de los requerimientos de los algoritmos de procesamiento de imagen, los análisis de vídeo trabajan con un rendimiento de hasta 25 ips y una resolución de hasta 16 MP.

El software de servidor de análisis se basa en un sistema de análisis de vídeo de alto rendimiento y autodidacta, que proporciona excelentes resultados de análisis, mediante los más modernos algoritmos de evaluación de imágenes y la adaptación permanente de los parámetros del sistema a las condiciones ambientales actuales. La aplicación de análisis para la vigilancia automatizada de instalaciones interiores y exteriores es capaz de avisar del acceso no autorizado a zonas determinables libremente. La aplicación detecta si un objeto está acercándose a una instalación, de qué dirección viene y cuánto tiempo permanece en un área. El análisis contiene módulos y mecanismos especiales para eliminar la oscilación de cámaras, sombras, reflexiones por sol y focos, reduciendo así las falsas alarmas al mínimo.

—¿Se tendrían que renovar por completo los sistemas existentes para implementar este concepto perimetral?

—Todos los sistemas de que hemos estado hablando trabajan con interfaces abiertas, de modo que es totalmente posible integrar la solución MFS en un sistema existente con cámaras térmicas. En este caso, también sería posible proceder paso a paso, protegiendo primero los puntos neurálgicos importantes como calles de acceso y puertas con la tecnología multifocal. Asesoramos a los clientes en este aspecto y elaboramos conceptos de migración personalizados porque ¡en cualquier análisis de vídeo siempre es fundamental una buena planificación! ●

Fotos: Dallmeier

Contactos de empresas, p. 7.

El nuevo estándard en alta resolución analógica

HDCVI 4MP

Dobla 1080P y pásate a 4MP sin complicaciones

Cámaras serie HAC-2401 y grabadores serie HCVR7000-4M

INTEGRADO CON CRA

SERVIDORES DDNS Y P2P PROPIOS

Tel. 902 502 035 - iptecno@iptecno.com - www.iptecno.com

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

IPTECNO BARCELONA - C. Besós, Nº 12 - Pol. Ind. Can Buscarons de Baix - 08170 Montornès (BCN)

iPTECNO

DISTRIBUIDOR OFICIAL DAHUA ESPAÑA

DIEZ AÑOS FORTALECIENDO LA CIBERSEGURIDAD NACIONAL

Más de 1.400 profesionales, en las X Jornadas **CCN-CERT**

Con la asistencia de más de 1.400 personas y el apoyo de las principales empresas del sector de la ciberseguridad, se clausuraron las X Jornadas CCN-CERT, organizadas por el Centro Criptológico Nacional (CCN), organismo adscrito al Centro Nacional de Inteligencia (CNI). Bajo el lema «Diez años fortaleciendo la ciberseguridad nacional», el evento fue inaugurado por el secretario de Estado director del CNI, Félix Sanz Roldán, quien felicitó al CCN por el éxito de convocatoria y, sobre todo, por el «camino inimaginable» recorrido en este tiempo por su Equipo de Respuesta a Incidentes.

DIEZ años en los que ha sido preciso renovarse todos los días y en los que se han gestionado más de 66.000 ciberincidentes de forma rápida y eficiente, constituyendo el baluarte para la defensa del ciberespacio español.

De cara al futuro, tal y como aseguró Sanz Roldán, «vamos a seguir trabajando con tres grandes líneas de acción: detección de intrusiones, creación de tecnologías y formación de personas». Una actividad, prosiguió el secretario de Estado director, en donde «necesitamos el esfuerzo de todos para crear un buen sistema de protección nacional en el ciberespacio».

Las X Jornadas CCN-CERT, que han batido todos los récord de participación hasta la fecha, han contado con un inmejorable plantel de ponentes, que hablaron de aspectos de ciberespionaje, Amenazas Persistentes Avanzadas (APT), nuevas herramientas y tecnología y Esquema Nacional de Seguridad (ENS) y cumplimiento normativo. Ponencias tan llamativas como «En ocasiones mi móvil oye voces», «Votando entre tiburones», o «Poltergeist en tu edificio» son algunas de las ofrecidas en una agenda en donde el propio CCN-CERT, como centro de alerta y respuesta nacional, ofreció una visión general de la situación de la ciberseguridad en nuestro país y de los principales incidentes gestionados durante este año por su equipo.

Clausuró el evento el embajador en Misión Especial para la Ciberseguridad del Ministerio de Asuntos Exteriores y de Cooperación, Ricardo Mor, y el subdirector general del CCN, Luis Jiménez.

Apoyo del sector de la ciberseguridad

Treinta y dos empresas y ocho entidades muy representativas del sector de la ciberseguridad han mostrado su apoyo y colaboración a esta iniciativa en su décimo aniversario. ●

Fotos: CCN-CERT

EL EVENTO NACIONAL DE LA CIBERSEGURIDAD CONTÓ CON CASI 20.000 VISITANTES ENTRE PÚBLICO ASISTENTE Y ONLINE

CyberCamp vuelve a batir récord de asistentes

CyberCamp 2016, el gran evento de ciberseguridad orientado a jóvenes talentos y familias y organizado por el Instituto Nacional de Ciberseguridad (INCIBE) en León, superó todas las expectativas y volvió a batir récord de participación en su tercera edición.

MÁS de 12.000 personas, entre ellas, unos 4.500 niños, visitaron este evento que pretende captar talento en ciberseguridad, ahondar en las últimas novedades del sector, proyectar carreras profesionales en el ámbito de la ciberseguridad e inculcar en las familias el uso seguro y responsable de internet. A estas cifras hay que añadir las casi 7.000 personas que siguieron CyberCamp online a través de video estreaming y las que visitaron la carpa, puesto que las actividades para menores continuaron durante todo la jornada.

En materia de empleo, las empresas participantes en el Foro de Empleo y Talento en Ciberseguridad ofertaron 2.272 vacantes para expertos en ciberseguridad y se recibieron 657 currículums para recibir asesoramiento personalizado de los coaching corner.

En la clausura, el director general de INCIBE, Alberto Hernández, calificó como muy positivo este balance provisional e indicó que iniciativas como ésta están contribuyendo de forma determinante a acercar la ciberseguridad a todos los ciudadanos.

Durante cuatro días, León se convirtió en la capital de la ciberseguridad al albergar este gran evento que contó con más de 70 actividades técnicas y lúdicas que se desarrollaron en el Auditorio Ciudad de León y en una carpa de 3.500 metros cuadrados instalada frente a dicho edificio. Expertos de reconocido prestigio a nivel nacional e internacional participaron como ponentes ofreciendo conferencias, keynotes y talleres en los que analizaron el presente y el futuro de la ciberseguridad desde diferentes ámbitos.

En el acto, se hizo entrega de los premios a los ganadores de las diferentes competencias técnicas que se desarrollaron en el marco de CyberCamp, como son el hackathon, el torneo de desarrollo seguro de software y el CTF (Capture the flag) individual, además de los retos breves.

Los 10 mejores clasificados en la competición de retos para jóvenes hackers formarán la selección española de hackers que nos representará en el campeonato europeo 2017 que se celebrará en España, donde defenderán el título conseguido este año en Dusseldorf.

Fotos: INCIBE

PWC: ENCUESTA MUNDIAL SOBRE EL ESTADO DE LA SEGURIDAD DE LA INFORMACIÓN

Las **empresas españolas** pierden 1,4 millones de dólares al año por **ciberataques**

La digitalización de los negocios impulsa el crecimiento de presupuestos en ciberseguridad de las empresas

La digitalización de los negocios está impulsando la inversión en ciberseguridad de las empresas en España y en el mundo. La Encuesta Mundial sobre el Estado de la Seguridad de la Información –que cada año elabora PwC, a partir de entrevistas a más de 10.000 directivos y responsables de IT (411 españoles) de 133 países–, refleja que, desde 2012, el presupuesto medio que las empresas dedican a ciberseguridad en el mundo casi se ha duplicado, pasando de 2,8 a 5,1 millones de dólares.

EN España, la inversión de las compañías en seguridad de la información ha seguido una evolución parecida –ha pasado de 3,1 a 3,9 millones de dólares de media– aunque algo más moderada. Pero, ¿qué causas están haciendo que las empresas inviertan cada vez más en ciberseguridad? El documento revela que el factor impulsor de la inversión en ciberseguridad en todo el mundo está siendo el profundo proceso de digitalización por el que, en los últimos años, están pasando los negocios, en general, y las empresas en particular. Así lo asegura el 59% de los directivos y responsables de IT de todo el mundo entrevistados en el informe, y el 62,9% de los pertenecientes a compañías españolas. «La inversión en seguridad ya no es percibida por las empresas como un aspecto exclusivamente defensivo sino como una forma de facilitar e impulsar el crecimiento de la compañía», explica Elena Maestre, socia responsable de Riesgos Tecnológicos en PwC.

De hecho, el fuerte incremento de los presupuestos en ciberseguridad está dando sus frutos y, en el último año, las empresas tanto a nivel global como en España están viendo cómo los incidentes de seguridad se han reducido porque las compañías están, ahora, mejor preparadas y protegidas. Si entre 2012 y 2015 el número de incidentes de seguridad que, de media y al año, sufrían las compañías en todo el mundo aumentó significativamente –de 3 a 6,8–, en la actualidad esta cifra ha caído hasta los 5,1 ataques/año. Un fenómeno similar ha sucedido en las empresas españolas. Entre 2012 y 2015, el número de ataques cibernéticos que sufrían nuestras compañías, de media, creció de 2,7 a 4,6. Actualmente, ha caído sensiblemente hasta 2,8 incidentes/año.

Para Javier Urtiaga, socio responsable de Ciberseguridad en PwC, «en la medida que cada vez más productos y servicios están conectados a Internet, los riesgos y las necesidades en materia de

ciberseguridad de las empresas aumentan. A esto se une, además, que los consumidores son cada vez más exigentes sobre la privacidad de sus datos y que la cantidad de información que las compañías tienen de ellos es cada vez mayor».

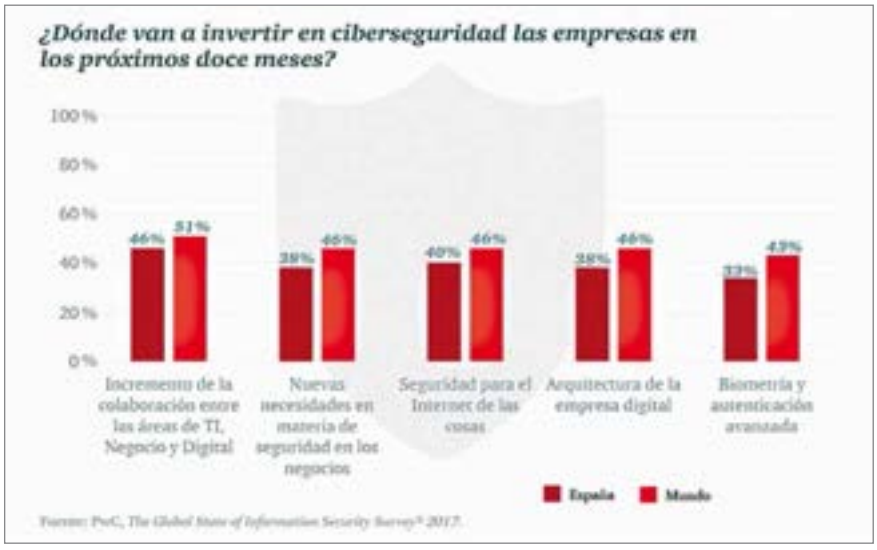
Tendencias en materia de ciberseguridad

El estudio recoge, además, cuáles son las cinco principales tendencias en materia de ciberseguridad que se están imponiendo entre las empresas en España y en el mundo. Y son las siguientes.

–El cloud se generaliza y ya no es una opción. Cada vez más compañías utilizan la nube para almacenar toda o parte de sus infraestructuras tecnológicas y de seguridad. El 63% de los 10.000 directivos entrevistados asegura tener en la nube las plataformas que sustentan sus funciones de IT; el 36% sus operaciones; el 34% las de servicio al cliente, el 34% las de marketing y ventas, y el 32% las funciones financieras. En España, esta práctica es muy similar.

–Gestionar la ciberseguridad, sí pero con apoyo externo. La gestión de la seguridad de los sistemas y tecnologías de las empresas es una cuestión tan compleja que estas se apoyan, mayoritariamente, en empresas externas expertas, según reconoce el 62% del total de entrevistados en el informe –el 67% de los españoles–. Aquellos servicios de seguridad relacionados con la autenticación (71%), la protección de datos (66%), y la identidad y el access management (63,7%) son los tres que más apoyo externo demandan.

–El data analytics, un arma potente para adelantarse a las amenazas. A la hora de anticiparse en la detección de amenazas y ataques, los sistemas de análisis de datos avanzados y en tiempo real están ganando peso entre las empresas. Así lo asegura el 51% de los encuestados a nivel global –y el 37% de los españoles–. Hacerlo, no obstante, supone un desafío muy importante para las empresas por la gran cantidad de datos que debe almacenar y procesar, así como por el uso de sofisticados algoritmos y por la escasez de los perfiles profesionales adecuados.



–Los sistemas avanzados de autentificación, al alza. En materia de autentificación, las compañías de todos los sectores se están inclinando por la utilización de tecnologías avanzadas que no solo hagan el proceso más fácil para los usuarios sino también más seguros como, por ejemplo, a la hora de autorizar transacciones. Algo que, en el pasado parecía ser una cuestión que solo preocupaba al sector público o al sector financiero y que, ahora, se ha generalizado. El 57% de los entrevistados en el estudio a nivel global ya usa algún tipo de tecnología biométrica (huellas, rasgos faciales, escaneo de retina…) para los procesos de autentificación –el 60% en España–.

–El software open-source también se impone. La adopción de software open-source –o de código abierto– es uno de los grandes cambios que está experimentando las áreas de IT de las empresas. Más de la mitad de los directivos y responsables de IT en todo el mundo –el 53%– utilizan software de código abierto y, de ellos, el 49% asegura que ha mejorado sus programas de seguridad. En España estos porcentajes son del 51% y el 50%, respectivamente.

A pesar de que los ataques e incidentes de seguridad entre las empresas de todo el mundo se han reducido en los últimos años, estos siguen siendo una amenaza importante para las empresas. Según el informe, las compañías de todo el mundo pierden al año, de media, 2,3 millones de dólares como consecuencia de ciberataques o incidentes de seguridad. En España, esta cifra asciende a 1,4 millones de dólares. Según las empresas españolas entrevistadas, desde el punto de vista del negocio, los principales incidentes que sufren son el robo de información estratégica, como pueden ser planes estratégicos, documentos relacionados con fusiones y adquisiciones y de carácter financiero, seguida de la captura de emails. Entre los incidentes de seguridad que, en los últimos doce meses, se están empezando a producir con más frecuencias, se encuentran el uso de programas informáticos que infectan y bloquean los archivos y sistemas de las empresas y piden una compensación económica, a cambio para liberarlos –los llamados ransomware programs–.

Fotos: PWC

«EL PRÓXIMO NIVEL-8 PREDICCIONES DE SEGURIDAD PARA 2017», INFORME TREND MICRO

El Internet de las Cosas, principal blanco de ataques cibernéticos en 2017

Los ataques se ampliarán y se diferenciarán para atacar nuevas superficies vulnerables

Trend Micro ha publicado su informe anual de predicciones de seguridad para 2017, «El Próximo Nivel - 8 Predicciones de Seguridad para 2017». Según este estudio, 2017 traerá consigo una mayor amplitud y profundidad de los ataques, con agentes de amenazas maliciosas que diferenciarán sus tácticas para capitalizar el cambiante panorama tecnológico.

La industria de la ciberseguridad entrará en un nuevo territorio el próximo año, después de que el panorama de amenazas de 2016 abriera las puertas para que los criminales exploraran una gama más amplia de ataques y de superficies de ataque», explica Raimund Genes, director de Tecnología de Trend Micro. «Prevemos que la Regulación General de Protección de Datos (GDPR) va a provocar cambios radicales en la gestión de datos para todas las compañías, generando nuevos métodos de ataque que amenazarán a las corporaciones de todo el mundo, expandiendo tácticas más numerosas de ransomware que afectarán cada vez a más dispositivos, y permitiendo que la propaganda cibernética influya directamente en la opinión pública».

En 2016, se ha detectado un gran aumento en las vulnerabilidades de Apple®, con 50 notificaciones, junto con 135 fallos revelados en Adobe y 76 en Microsoft. Este aparente cambio en los exploits contra el software vulnerable continuará en 2017, mientras Microsoft continúa mejorando, Apple sigue siendo visto como el sistema operativo más destacado.

Ataques dirigidos

El Internet de las Cosas (IoT) y el Internet Industrial de las Cosas (IIoT) jugarán un papel más impor-

tante en los ataques dirigidos en 2017, convirtiéndose en ejes sustanciales de estos ataques, ya que aprovecharán la creciente aceptación de los dispositivos conectados mediante la explotación de vulnerabilidades y sistemas no seguros para alterar e interrumpir los procesos de negocio, como ya se vio en Mirai.

El creciente uso de dispositivos móviles para monitorizar los sistemas de control en entornos industriales y de fabricación conllevará que haya que hacer frente a un gran número de vulnerabilidades encontradas en estos sistemas que amenazarán a las organizaciones.

El Compromiso del Correo Electrónico Corporativo (BEC, por sus siglas en inglés) y el Compromiso de los Procesos de Negocio (BPC, por sus siglas en inglés) continuarán creciendo como una forma rentable y relativamente simple de extorsión corporativa. Un ataque BEC puede generar hasta 140.000 dólares si se consigue que un empleado inocente transfiera esta cantidad a la cuenta del criminal. Por otro lado, la violación de los sistemas de transacciones financieras, aunque requiere más trabajo, podría resultar en unas ganancias mucho mayores – alcanzando hasta 81 millones de dólares.

> «El Internet de las Cosas (IoT) y el Internet Industrial de las Cosas (IIoT) jugarán un papel más importante en los ataques dirigidos en 2017»

«Continuamos observando cómo los ciberdelincuentes van evolucionando a media que cambia el panorama tecnológico», subraya Ed Cabrera, jefe de Ciberseguridad de Trend Micro.

«Si bien en 2016 vimos un aumento exponencial de nuevos ransomware, este crecimiento ya no se mantendrá, pues no es sostenible; por lo que los atacantes encontrarán nuevas formas de utilizar las familias de malware existentes. Del mismo modo, los cambios en el IoT abrirán nuevas puertas a otras superficies de ataque adicionales, en tanto que los cambios en el software impulsarán a los criminales hacia la búsqueda de nuevas vulnerabilidades».

Fotos: **Freepik**

Contactos de empresas, p. 7.

VideoXpert™ The Gateway to Performance

La Experiencia marca la Diferencia

Conéctese a la flexibilidad de VideoXpert™

Históricamente, los sistemas de gestión de video son complejos por naturaleza – una complejidad que con frecuencia supera la experiencia del usuario y resulta en un complejo aprendizaje y una pérdida de foco.

VideoXpert™ marca la diferencia

Su diseño intuitivo y su sencillo manejo permiten mostrar sin esfuerzo lo que se necesita y cuando se necesita. Esto permite a los profesionales de la seguridad tomar decisiones rápidas y eficaces que ayudarán a su negocio.

Gracias a su potente capacidad de integración, con VideoXpert puede hacer uso de la experiencia de terceros proveedores para personalizar sus funcionalidades y lograr la máxima flexibilidad.

Experimente el fácil manejo, fiabilidad y rendimiento que Usted necesita.

Principales Características

- Experiencia de usuario inigualable
- Diseño intuitivo
- Arquitectura integrable con terceros mediante plug-ins
- Escalable modularmente
- Implementación como solución software o mediante Hardware Pelco
- Migración sencilla para usuarios actuales de Pelco

PELCO

by Schneider Electric

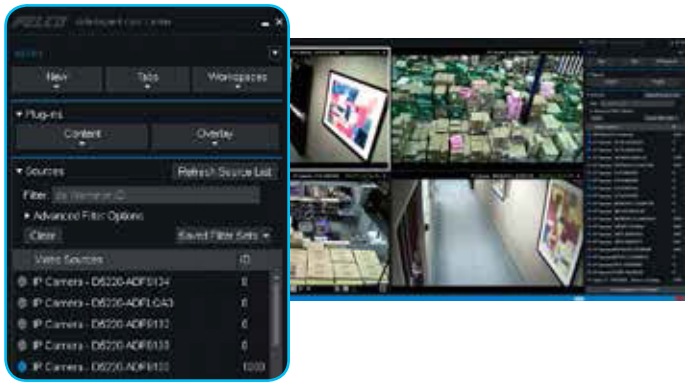
Choose with Confidence.

Interfaz de Usuario Única

- Con elementos “arrastrables”, para organizar su espacio de trabajo sobre la marcha
- Organización mediante etiquetas
- Interfaz con aspecto similar al de un explorador, permite organizar sus espacios de trabajo en pestañas
- Espacio de trabajo extendido entre monitores independientes

Plug-ins de terceros fabricantes

- Visualización de video de Partners a través de la interfaz de usuario única de VideoXpertTM
- Lincado de datos críticos del negocio junto con el video
- Unificación de datos operacionales y de seguridad sobre el video del sistema
- Ampliación de funcionalidades a través de integración con partners



Gestión de Incidencias

- Modo de investigación para localizar y organizar video rápidamente
- Reproducción síncrona de video para capturar la misma escena desde múltiples ángulos
- Organización en listas de reproducción para crear una investigación completa
- Exportación o almacenamiento de las listas de reproducción para referencia futura

Sincronización de Video

- Añadir dinámicamente nuevas cámaras a grupos que ya están sincronizados
- Ubicación conveniente de controles de reproducción
- Conmutación entre video en vivo y reproducción de video grabado mientras se mantiene la operación síncrona

Fiabilidad Absoluta

- Redundancia con hardware dedicado
- Escalabilidad modular y con capacidad de failover
- Arquitectura distribuida para evitar puntos únicos de fallo
- Capacidad de decodificación de video maximizada, CPU dedicada por monitor
- Visualización de hasta 16 streams por monitor

Gestión de Video Centralizada

- Capacidad de agregar múltiples sistemas de gestión de video en una única interfaz con la utilidad VideoXpert
- Construcción y mantenimiento de sistema de gestión de video único para equipamiento distribuido y con recursos dispares a través de varias redes

Plan de Migración

- Migración de sistemas Endura® y Digital® Sentry actuales a VideoXpert
- Reutilización de hardware y de la infraestructura de gestión de video actual, mientras se adquieren nuevas funcionalidades y beneficios
- Se mantiene el hardware de almacenamiento (NSM y Digital Sentry), preservando el video almacenado existente y proporcionando acceso al mismo.

Contacte hoy mismo con el representante de ventas de su zona, o visite pelco.com para descargar las hojas de especificaciones.

C032615_GMA_US

CRISTIAN HERNÁNDEZ BERZOSA. JEFE DE PROYECTOS DEL DEPARTAMENTO DE INGENIERÍA, PROYECTOS Y GRANDES CUENTAS DE BY DEMES GROUP

«Los sistemas de análisis de vídeo son el **presente** y, sin duda, el **futuro**»

«Los sistemas de análisis de vídeo multiplican el retorno de la inversión en prácticamente cualquier instalación», así lo asegura Cristian Hernández Berzosa, jefe de Proyectos del Departamento de Ingeniería, Proyectos y Grandes Cuentas de By Demes Group, quien además explica durante la entrevista los ámbitos de aplicación más demandados por esta tecnología, o cómo un sistema de análisis de vídeo puede ayudar a mejorar la eficiencia del usuario/operador, entre otros aspectos.

CUÁL ha sido el mayor avance en los sistemas de análisis de vídeo en los últimos años?

—Los sistemas de análisis de vídeo han mejorado en diversos aspectos. Si tuviéramos que destacar uno probablemente sería la capacidad de analizar formatos en HD, lo cual supone romper muchas barreras que en baja resolución resultan imposibles. Hay que tener en cuenta que los sistemas de análisis de vídeo analizan vídeo, y cuanto más detalle tenga el vídeo, mayor capacidad de análisis se puede aplicar. El uso ya habitual de cámaras en HD está permitiendo que los sistemas de análisis de vídeo incorporen nuevas formas de procesamiento que redundan en mejores resultados, tanto en detección como en falsas alarmas.

—¿Qué ámbitos de aplicación son en la actualidad los más demandados por vuestros clientes?

—Nosotros percibimos cada vez más interés en soluciones de lectura de matrículas, protección perimetral y conteo. La lectura de matrículas puede parecer un clásico, todos estamos acostumbrados a verla en parkings públicos, pero el hecho de que cada vez sea más asequible, permite multiplicar su campo de aplicación para ámbitos privados, protección de ciudades, control de tráfico en centros urbanos, etc. El análisis de vídeo ya ha conseguido implantarse como solución para proteger grandes perímetros. En los últimos cinco años hemos visto cómo la calidad de los algoritmos no ha parado de mejorar, mientras que los precios han bajado de forma muy importante. Para los sistemas de conteo basados en imagen, la llegada de cámaras analógicas de alta definición puede suponer un gran crecimiento. Y no requiere nueva instalación, el coste de la cámara es asequible y los sistemas son fáciles de usar.

—¿Qué importancia tiene la elección de una buena analítica de vídeo en un sistema CCTV?

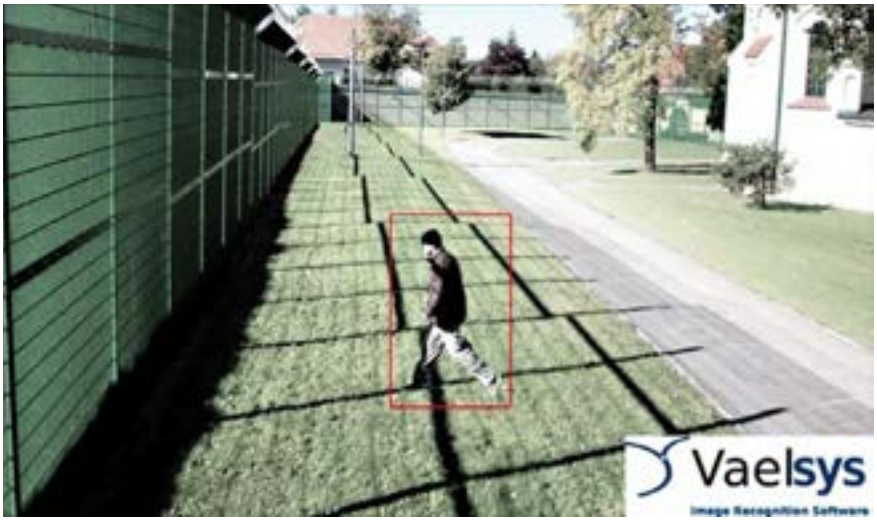
—Los sistemas de análisis de vídeo multiplican el retorno de inversión en prácticamente cualquier instalación. ¿De qué sirve grabar miles de horas de vídeo si no las ve nadie? Los sistemas de análisis de vídeo son el presente y, sin duda, el futuro. Elegir un buen sistema puede tener distintas consecuencias, en algunos casos críticas. Un buen sistema de análisis de vídeo no solamente tiene buenos algoritmos de procesado, también tiene que ser flexible y debe poder trabajar con otros sistemas. Hay muchas soluciones en el mercado incapaces de integrarse con soluciones de terceros. ¿De qué sirve un sistema de detección perimetral si no puede enviar alarmas a nadie? Creemos que a la hora de elegir una solución de análisis de vídeo hay que tener en cuenta la tasa combinada de detección y alarmas no deseadas, la capacidad de integración y la facilidad de configuración. Un sistema puede ser fantástico, pero si está mal configurado lo más probable es que no funcione. Finalmente, hay que tener en cuenta que un buen sistema de análisis de vídeo a la larga suele ser mucho más económico que uno malo, una vez sumemos el tiempo de puesta en marcha, mantenimiento, supervisión y atención a averías.

—¿Cómo un sistema de análisis de vídeo puede ayudar a mejorar la eficiencia del usuario/operador?

—Los sistemas de análisis de vídeo suponen una mejora total en la eficiencia de un operador de CRA o de un centro de control. Partimos de la base que un sistema de análisis de vídeo puede trabajar de la misma forma durante 24 horas, 7 días a la semana, cosa que para un ser humano es imposible. La eficiencia aumenta al menos en un orden de magnitud, en muchos casos incluso dos. El problema es que muchas veces se comparan los sistemas de análisis de vídeo con detectores de presencia de interior, y en esa comparativa el número de falsos positivos del análisis de vídeo puede parecer elevado. Pero el análisis frío de los datos es claro, un operador puede supervisar varios cientos de cámaras conectadas a una buena solución de análisis de vídeo. Ese mismo operador difícilmente podría supervisar medio centenar de cámaras sin análisis. ¿Qué es más eficiente, las rondas de vídeo secuenciales en las que solamente detectamos a un intruso si tenemos suerte, o las rondas de vídeo inteligentes en las que supervisamos sólo vídeo que previamente una máquina ha filtrado? Calcule el tiempo de vídeo donde no pasa nada en las rondas de vigilancia, ¿acaso no es mayor que el utilizado en supervisar una instalación con análisis de vídeo? El aumento en la eficiencia es innegable.

—¿Son todos los sistemas de análisis de vídeo iguales?

—En absoluto. A la hora de elegir un sistema de análisis de vídeo hay que responder varias preguntas. Por ejemplo, si hablamos de protección perimetral deberíamos preguntarnos si el sistema puede enviar alarmas a la CRA. Si vamos a poder configurarlo de forma remota. Si es capaz de analizar en alta resolución y cuántos canales. Si tiene capacidad para ampliarse. Es importante conocer el proceso de configuración, a qué grado de detalle nos permite acceder y qué fiabilidad tiene la detección. Muchas veces nos preocupamos por las falsas alarmas y nos olvidamos que lo realmente



importante en un sistema de protección perimetral es que detecte al intruso. Cuando ves instalaciones con cámaras a más de 50 metros con analíticas a baja resolución, hay que preguntarse si realmente esa solución es capaz de detectar algo. Para otras analíticas, como lectura de matrículas, tenemos que saber con qué cámaras es compatible, si puede detectar vehículos circulando a alta velocidad, qué tolerancia tiene a matrículas giradas y de nuevo qué capacidad de integración con otras soluciones ofrece.

—¿En qué debemos fijarnos a la hora de elegir un sistema de análisis de vídeo?

—A día de hoy creemos que lo más importante a la hora de elegir un sistema de análisis de vídeo es la flexibilidad para integrarse de manera rápida y sencilla con sistemas de terceros, ya sean cámaras, grabadores, VMS o sistemas Scada, entre otros. También hay que tener en cuenta que estos sistemas sean capaces de trabajar en un mismo hardware las diferentes analíticas del mercado para poder aumentar las prestaciones del sistema de CCTV.

—¿Cuál es el mejor sistema de análisis de vídeo que se puede ofrecer a un instalador?

—Desgraciadamente no hay un sistema de análisis de vídeo que sirva para cualquier escenario, por eso es importante que el instalador confíe en un proveedor con experiencia que pueda ofrecerle la solución adecuada para cada caso, y que le ayude a definir los materiales en el proceso de preventa de la instalación. El éxito del buen funcionamiento del sistema de análisis de vídeo, ya sea análisis perimetral, análisis en HD, LPR o conteo, depende en gran medida del diseño del proyecto previo.

Nuestro departamento especializado en este tipo de soluciones cuenta con una experiencia de más de cinco años en el diseño de proyectos de análisis de vídeo, sumado a que Vaelsys, el fabricante de estos sistemas, tiene una experiencia de más de 10 años en el desarrollo de aplicaciones de vídeo. El número de proyectos ejecutados con éxito ha ido aumentando de manera exponencial desde que adquirimos la exclusividad en 2013, generando un grado de satisfacción muy alto entre nuestros clientes, lo cual nos dota de una posición destacada en el sector.

—¿Podría explicar brevemente su más reciente caso de éxito de análisis de vídeo?

—Uno de nuestros últimos casos de éxito ha sido el del Centro de Tratamiento de Resinas de Almazán, donde apostamos por la tecnología analógica HD y un sistema de análisis de vídeo en HD. Esta combinación permite que el usuario final disfrute de grabaciones en 1080p y al sistema de análisis de vídeo poder detectar cualquier intrusión con total seguridad a 100 metros, con una tasa de falsos positivos muy cercana a cero. Algo impensable para sistemas de análisis a baja resolución con cámaras visibles. ●

Fotos: By Demes Group

Centro de Tratamiento de Resinas de Almazán.

Contactos de empresas, p. 7.

Sistemas de Detección de Incendios

detnov

Nuestra tecnología, su tranquilidad

Diseñado y fabricado en España

detnov.com

ANA MARZO. SOCIA WHITAN LAW TECH

Reglamento General de Protección de Datos: mayor regulación, menor seguridad jurídica

Tiempo atrás, en el año 1992, nuestra primera norma sobre protección de datos de carácter personal, concretamente la llamada LORTAD (Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, vigente hasta la entrada en vigor de la LOPD, el 14 de enero de 2000) auguraba el inevitable y rápido desfase que las normas de derecho positivo, y en particular las de protección de datos, ofrecían respecto de las transformaciones sociales, cuya evolución tecnológica es especialmente dinámica, concluyendo la necesidad de múltiples modificaciones, al socaire de las distintas innovaciones tecnológicas, de las sucesivas y diferentes aplicaciones o de la ampliación de los campos de utilización de la tecnología.

Y ADEMÁS hacía hincapié en el hecho de que, ello hacía aconsejable, a la hora de normar estos campos, acudir a mecanismos jurídicos dotados de menor nivel de vinculación, susceptibles de una elaboración o modificación más rápida de lo habitual y caracterizados porque es la voluntaria aceptación de sus destinatarios la que les otorga eficacia normativa. Como ejemplo de ello, la exposición de motivos nos indicaba dos caminos que evitaban los inconvenientes derivados de la especial rigidez de la Ley Orgánica que, por su propia naturaleza, es inidónea para un acentuado casuísmo: las normas de autorregulación y las recomendaciones de la Agencia Española de Protección de Datos, que evitan.

De aquellos tiempos a estos, ¿en qué han cambiado las cosas? Quizás la respuesta dependa del punto de vista desde el que se quiera mirar.

De las 81 denuncias en total recibidas por la AEPD en el primer año de vida de la norma (1993) a las 10.074 denuncias recibidas en 2014 u 8.489 recibidas en el año 2015. De los 5.751.685,84€ euros (entonces 957 millones de pesetas) impuestos en multas en el año 1997, a los 13.712.621 euros impuestos en sanciones durante el ejercicio de 2015 o los 22.339.440 euros durante el ejercicio de 2013. De la función de la AEPD como órgano. De las funciones atribuidas por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) al Plan Estratégico 2015-2019 del citado organismo para consolidar su eficiencia, participación y colaboración con los afectados o titulares de los datos y los responsables. De la LOPD al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD).

Armonizar la protección de derechos y libertades fundamentales

Según nos explica el legislador europeo, el RGPD trata de armonizar la protección de los derechos y las libertades fundamentales de las personas físicas en relación con las actividades de tratamiento de datos de carácter personal, y de garantizar la libre circulación de estos datos entre los Estados miembros, y trae causa de los nuevos retos planteados para la protección de datos, por la rápida evolución tecnológica y la globalización.

En este sentido, según los considerandos del RGPD, las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial, y los avances requieren un marco más sólido y coherente para la protección de datos en la Unión Europea con diversos fines: eliminar las diferencias en la transposición de la normativa euro-

pea (que nos trajo la Directiva 95/46/CE), proporcionar a las personas físicas el control de sus propios datos personales, establecer un marco de confianza para el desarrollo de la economía digital del mercado interior y reforzar la seguridad jurídica.

La pregunta que nos deberíamos hacer es sí realmente con el RGPD los objetivos pretendidos serán pura ficción o serán una realidad alguna vez, en algún momento.

Cierto es que la norma comunitaria es de efecto directo y no requiere transposición al derecho interno (ni de otras normas interpretativas) pero, también lo es, el hecho de que esta norma no desplaza a la LOPD en las materias no reguladas y, aunque deroga a nuestra vigente Ley Orgánica en aquello que se regula sobre la misma materia, también plantea previsiones específicas para que los estados miembros desarrollen su propia normativa sectorial, en la medida en que el RGPD contemple habilitaciones expresas de aplicación o desarrollo a los estados miembros.

Y aún más, el propio RGPD en su considerando 10 establece que, junto con la normativa general y horizontal sobre protección de datos, los Estados miembros cuentan con distintas normas sectoriales específicas en ámbitos que precisan disposiciones más específicas y el RGPD reconoce también un margen de maniobra para que los Estados miembros especifiquen sus normas, inclusive para el tratamiento de categorías especiales de datos personales («datos sensibles»). Por lo que, en este sentido, el Reglamento no excluye el Derecho de los Estados miembros que determina las circunstancias relativas a situaciones específicas de tratamiento.

Veamos en todo caso en aquellas cuestiones que parece que los Estados miembros sí se pondrán de acuerdo con el RGPD.

Parece que Europa se ha puesto de


Rawpixel.com/Shutterstock.

acuerdo en que las infracciones de las disposiciones del RGPG se sancionarán, según el artículo infringido, con multas administrativas entre los 10.000.000 y 20.000.000 euros como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % o al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

Poderes de las autoridades de control de cada país

También parece que hay acuerdo en los poderes que tendrán las autoridades de control de cada país (en España la AEPD), principalmente en la disposición de todos los poderes de investigación, correctivos, de autorización y consultivos que se indican en el artículo 58 del RGPD, y entre ellos, obtener del responsable y del encargado del tratamiento el acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus funciones.

> «Según los considerandos del RGPD, las personas físicas difunden un volumen cada vez mayor de información a escala mundial»

Igualmente hay consenso en que el desempeño de las funciones de cada autoridad de control será gratuito para el interesado y, en su caso, para el delegado de protección de datos, permitiendo el cobro de una «tasa razonable basada en los costes administrativos» (o incluso negar una actuación respecto de cualquier solicitud) cuando las soli-

Mathias Rosenthel/Shutterstock

citudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo.

rantías del burocrático y lento proceso legislativo del Parlamento y del Consejo europeos). De hecho, en el caso en

> «Seamos optimistas y esperemos que con el RGPD se contribuya a la plena realización de un espacio de libertad, seguridad y justicia que lleve al progreso económico y social»

Y finalmente es destacable el acuerdo en la creación de un Comité Europeo de Protección de Datos (Comité), como organismo de la Unión, con su propia personalidad jurídica, compuesto por el director de una autoridad de control de cada Estado miembro y por el Supervisor Europeo de Protección de Datos o sus representantes respectivos, con una serie de funciones supervisoras, asesoras y «pseudo legislativas» consistentes en la emisión de directrices, recomendaciones y buenas prácticas, que seguramente acabarán siendo verdaderas normas vinculantes para los Estados miembros (eso sí, sin las garantías del burocrático y lento proceso legislativo del Parlamento y del Consejo europeos). De hecho, en el caso en que una decisión de una autoridad de control europea por la que se ejecuta una decisión del Comité se impugnase ante un tribunal nacional cuestionando su validez, dicho tribunal nacional no será competente para declarar inválida la decisión del Comité, sino que, si la considera inválida, tendrá que remitir la cuestión de la validez al Tribunal de Justicia de conformidad con el artículo 267 del Tratado de Funcionamiento de la Unión Europea (TFUE).

Algunos escépticos (entre los que me incluyo) no vemos con tanta benevolencia el RGPD ni pensamos que con esta norma se alcancen los pretendidos objetivos de seguridad jurídica y marco de confianza, máxime cuando muchas de las obligaciones que se recogen (especialmente en materia de transferencias internacionales) reiteran lo establecido en la actual Directiva y conjunto de Decisiones Europeas, que el Tribunal de Justicia de la Unión Europea ya ha puesto en tela de juicio en cuanto a las garantías para los ciudadanos se refiere.

Tampoco parece que con la nueva norma se eviten aquellos «augurados inconvenientes derivados de la especial rigidez de las leyes» que ya indicaba nuestra LORTAD en el año 1992, si tenemos en cuenta el yugo que supondrá para los responsables y los encargados del tratamiento el tan nombrado principio de «accountability», traducido al castellano como «responsabilidad proactiva», y que supone la capacidad del responsable y encargado del tratamiento no sólo de cumplir la norma, sino también de demostrarlo.

El objetivo que desde luego parece que sí ha conseguido Europa, es el de disponer de una norma que con la misión de garantizar a los ciudadanos el derecho fundamental a la protección de sus datos personales, ha otorgado a las autoridades de control (órganos administrativos) de todos los Estados miembros, un poder sino igual, similar al que tienen los órganos de competencia, para regular cualquier sector de actividad empresarial que lleve a cabo el tratamiento de datos y para imponer unas multas administrativas correctivas y disuasorias, que en nada envidian a las de los órganos administrativos de defensa de la competencia.

En todo caso, seamos optimistas y como dice el Reglamento en su considerando segundo, esperemos que con el RGPD se contribuya también a la plena realización de un espacio de libertad, seguridad y justicia que lleve al progreso económico y social. ●

LA SMART TOWER, ALTERNATIVA TECNOLÓGICA A LOS VIGILANTES

Es portátil, apta para cualquier terreno y ante cualquier circunstancia, se puede elevar hasta los siete metros de altura, graba 24 horas incluso con infrarrojos, cuenta con múltiples sensores, tiene la capacidad de mandar imágenes en tiempo real y hasta cuenta con altavoces para poder interactuar con cualquier intruso. Así son las nuevas torres de vigilancia Smart Towers. Lo último en vigilancia de espacios exteriores que va a implantarse en el mercado español y que será una alternativa a los vigilantes de toda la vida.

Desde que salieron al mercado en el Reino Unido, hace ya 10 años, su uso no ha parado de crecer, sobre todo en espacios en proceso de construcción, infraestructuras, instalaciones aisladas, mantenimiento de autopistas y, por supuesto organización de eventos. Hablamos con Oscar Aragón, Managing director del Grupo VPS, empresa de referencia en la gestión de este tipo de servicios. "Se trata de una de las mejores soluciones en cuanto a seguridad exterior que existe hoy en día.

LAS SMART TOWER HAN LLEGADO CON FUERZA Y LO HAN HECHO PARA QUEDARSE, PARA CONVERTIRSE EN LA MEJOR ALTERNATIVA EN SEGURIDAD.

Las Smart Towers son versátiles, fiables, con un alto carácter tecnológico y proporciona un ahorro de costes con respecto al uso de vigilantes superior a un 25 por ciento." Asegura.

Grupo VPS, es la empresa que se ocupa de la gestión de forma integral de este tipo de servicio, desde el diseño, la fabricación o la instalación, hasta la video vigilancia. Según Aragón "cada vez más la empresas confían en nosotros y en este tipo de soluciones. Consiguen una gran efectividad y un gran ahorro. Una Smart Tower es fácilmente instalable y es efectiva ante cualquier entorno por muy adverso que este sea, ya sea en cuanto a climatología o a la ausencia total de electricidad o cobertura telefónica. Además, el hecho de que se ofrezca en alquiler cubre un nicho necesario, que es el de la necesidad temporal de seguridad", concluye Oscar Aragón.

Más información en:

www.vpsitex.es
spain@vpsitex.es

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Objetivos de la AEPD para 2017

El Reglamento Europeo de Protección de Datos y la concienciación entre ciudadanos y entidades centrarán las actuaciones de la Agencia en 2017

La Agencia Española de Protección de Datos (AEPD) presentó el balance del primer año de su Plan Estratégico 2015-2019, un documento que recoge más de 110 medidas enfocadas a consolidar un organismo eficiente y participativo que permita tanto salvaguardar el derecho fundamental de los ciudadanos como colaborar con aquellas entidades que tratan datos.

DURANTE la presentación de las líneas estratégicas, diferentes miembros de la institución realizaron un repaso por las acciones más significativas puestas en marcha en 2016 y los retos más relevantes que debe afrontar la Agencia en 2017, destacando que la prevención y la concienciación son elementos imprescindibles para difundir y asentar una cultura de protección de datos, que permita tanto que los ciudadanos sean más conscientes de cómo ejercer sus derechos como que aquellos que tratan datos aborden el fomento de la privacidad como una ventaja competitiva.

En cuanto al estado de ejecución del Plan Estratégico, la Agencia ha iniciado durante el periodo 2015-2016 la totalidad de las 76 actuaciones previstas. Del conjunto de iniciativas realizadas en 2016 hay que destacar la publicación de siete guías sobre diversas materias; las actuaciones realizadas para sensibilizar a los menores sobre la importancia de proteger su información personal en internet; la actualización de contenidos prácticos de diversa temática para orientar al ciudadano en temas como el ejercicio del derecho al olvido o cómo solicitar la eliminación de fotos y vídeos publicados en internet; o la optimización de los recursos de la Agencia, entre otros.

La AEPD, que resolvió en 2015 cerca de 11.000 denuncias y más de 2.100 reclamaciones, se enfrenta en paralelo a un reto de gran envergadura en 2017: sentar las bases para que tanto las entidades como los profesionales de la privacidad puedan adaptarse de forma paulatina al nuevo Reglamento Europeo de Protección de Datos, que será de aplicación directa en mayo de 2018. En este sentido, la Agencia contempla prestar especial atención a las pymes, que constituyen el 99% del tejido empresarial español, para facilitarles herramientas y orientaciones que les permitan cumplir con la nueva legislación. Todo ello sin dejar de lado otros bloques relevantes como el lanzamiento de nuevas herramientas de prevención y concienciación para los ciudadanos, y el análisis pormenorizado de nuevas tecnologías que puedan tener un gran impacto sobre la privacidad.

El Plan Estratégico de la Agencia ha sido proyectado como un documento que permite la incorporación y el desarrollo de nuevas iniciativas, el enriquecimiento de las ya existentes y la adaptación de las existentes en función del diagnóstico realizado. La AEPD mantiene abierto un Buzón de Sugerencias en su página web para que ciudadanos, responsables de tratamiento, expertos en protección de datos y organizaciones públicas y privadas puedan realizar sus sugerencias y aportaciones.

Fotos: Shutterstock

INFORME DE LA FUNDACIÓN ESYS

El Reglamento General de Protección de Datos de la UE: una perspectiva empresarial

El Reglamento Europeo de Protección de Datos es el mayor hito legislativo en materia de privacidad y protección de datos en Europa en los últimos 20 años, y su aplicación, que será de obligado cumplimiento desde el 25 de mayo de 2018, hace necesario que el legislador español y la Autoridad Nacional de Control actúen cuanto antes para ofrecer a las empresas un marco claro sobre cómo aplicar la nueva normativa comunitaria. Esta es una de las principales conclusiones del estudio «El Reglamento General de Protección de Datos de la UE: una perspectiva empresarial» elaborado por la Fundación Empresa, Seguridad y Sociedad (ESYS).

EL estudio, presentado por el presidente de la Fundación ESYS, Javier Gómez-Navarro, recuerda que, aunque el nuevo Reglamento entró en vigor el 25 de mayo de 2016, las autoridades comunitarias han concedido un periodo transitorio de dos años para que las empresas tengan tiempo de adaptarse a la nueva norma. El informe destaca que el Reglamento «no regula de manera completa y exhaustiva todas y cada una de las materias», y plantea «dudas interpretativas» e «incertidumbre sobre la compatibilidad con la normativa actualmente vigente en España» (Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD) y el Real Decreto 1720/2007, de 21 de diciembre, que regula su desarrollo reglamentario).

Por este motivo, la Fundación ESYS considera que las autoridades españolas deberían despejar cualquier incertidumbre antes del 25 de mayo de 2018 y en todo caso «a la mayor brevedad para evitar la inseguridad jurídica» tras consultar a los distintos interesados, especialmente empresas y organizaciones de consumidores.

Cultura de la protección de datos

El Reglamento busca crear una verdadera cultura de la protección de datos a nivel europeo, eleva la responsabilidad de las empresas en su tratamiento y la capacidad de control de los ciudadanos sobre sus propios datos personales. Así, surgen nuevos derechos como el derecho al olvido o el derecho a la portabilidad de los datos, se añaden nuevas categorías especiales de datos personales (como los datos genéticos o biométricos), y se establece un régimen sancionador con multas que pueden alcanzar hasta los 20 millones de euros o el 4% del volumen de negocio anual de la empresa infractora.

Sin embargo, según el estudio, el Reglamento deja «muchas materias pendientes de desarrollo y concreción» y recurre a «abundantes conceptos jurídicos indeterminados». Así, no regula de forma específica ficheros que no requieren el consentimiento de los interesados como los ficheros sobre solvencia patrimonial y crédito, los ficheros con fines de publicidad y prospección comercial y las denominadas «Listas Robinson» (listas de ciudadanos que han solicitado expresamente no recibir publicidad no deseada).

El estudio apunta también que se echa de menos «una regulación específica de fenómenos como el Big Data o el Internet de las Cosas» para dar una mayor seguridad jurídica a las empresas en el tratamiento de datos personales en esos entornos.

Además, recomienda que la Agencia Española de Protección de Datos (AEPD) publique una lista con los tratamientos de datos que requerirán de la nueva evaluación de impacto (PIA), y clarifique en qué casos se debe informar a los afectados cuando se haya producido una violación de seguridad de los datos personales que suponga un alto riesgo para sus derechos y libertades. ●

BALANCE DE SEGURIDAD VIAL 2016

Los accidentes de tráfico se cobran la vida de 1.160 personas en 2016

El director general de Tráfico, Gregorio Serrano, presentó el balance de siniestralidad vial de 2016. Durante el pasado año se produjeron 1.038 accidentes mortales en vías interurbanas en los que fallecieron 1.160 personas y otras 5.067 necesitaron hospitalización como consecuencia de las heridas sufridas. Estas cifras suponen aumentos del 1,4% (+15) en accidentes mortales; 2,6% (+29) en el número de fallecidos y 4,3 % (+209) en heridos hospitalizados.

SEGÚN el director general de Tráfico «no son los datos que hubiésemos querido comunicar hoy, porque son muchas las vidas y familias rotas, así que más que nunca, tenemos que trabajar todos juntos para reducir esta lacra que como sociedad moderna que somos no podemos permitirnos. Hay que revisar y adaptar, tras una primera evaluación, la estrategia de seguridad vial y crear un plan de choque que nos permita volver a la tendencia de disminución de accidentes que veníamos observando en los últimos años».

Todas las cifras contenidas en esta información son provisionales y se refieren únicamente a los accidentes mortales ocurridos en vías interurbanas y víctimas tomadas hasta las 24 horas de producirse el accidente. Las cifras definitivas ya consolidadas, que incluirán las victimas a 30 días de accidentes ocurridos en vías urbanas e interurbanas estarán disponibles en los próximos meses, gracias a las mejoras sustanciales conseguidas en los sistemas de información de la siniestralidad, con cruce con el fichero del INE de fallecidos en 2016.

La cifra de fallecidos sigue por debajo de los registrados en 1960, primer año en el que se tienen estadísticas, cuando hubo 1.300 muertos, con un escenario de movilidad absolutamente distinto (en 1960 había un millón de vehículos y en 2016 el parque automovilístico sobrepasa los 32 millones).

Evolución del número de fallecidos en vías interurbanas (24 horas) 1960 – 2016

Con estos datos, la accidentalidad en carretera se mantiene en el promedio diario de víctimas mortales, que ha pasado de los 11,6 muertos diarios en carretera en 2.000 a los 3,2 fallecidos diarios en 2016.

Dentro del ámbito europeo, España presenta una tasa de 36 muertos por millón de habitantes, muy por debajo de la tasa de mortalidad media de la UE que se encuentra en 52 (con los últimos datos disponibles de 2014-2015). Lo que sitúa a España como uno de los países del mundo con mejores niveles de seguridad vial.

A destacar

En la siniestralidad de 2016 destacan las siguientes circunstancias:

Movilidad: Se ha constatado un aumento de 18,6 millones de viaje de largo recorrido por carretera, lo que supone un 5% más. En total se han registrado 392 millones de desplazamientos de largo recorrido en 2016, lo que representa un incremento acumulado del 10% en los tres últimos años.

Desde 2014, han aumentado los movimientos en 37,8 millones.

Mayor envejecimiento del parque. En 2016 se ha producido un aumento de la antigüedad media de los vehículos implicados en accidentes mortales. Los turismos en que viajaban los fallecidos tienen una edad media de 13,6 años; 11,1 las furgonetas y 9,5 las motos.

Más infracciones por consumo de drogas ilegales. En 2016 la DGT, a través de la ATGC, ha realizado hasta noviembre un total de 60.942 pruebas, resultando positivas 23.822 (39%)

Respecto del alcohol, los agentes de la ATGC han realizado en total 4,6 millones de pruebas, resultando positivas 68.852, el 1,5%.

De ellas 4.024.101 preventivas, resultando positivas 59.526 (1,5%); 113.396 pruebas a conductores involucrados en accidentes con 5.045 positivos (4,5%) y otras 554.593 pruebas a conductores infractores con 4.281 positivos (0,8%).

Uso elementos de seguridad: Persiste un reducido número de usuarios que continúa sin utilizar los elementos

de seguridad. En 2016, 161 fallecidos no hacían uso de los dispositivos de seguridad (cinturón o casco) en el momento del accidente.

Características de la siniestralidad 2015

Por sexos: Se sigue observando un mayor porcentaje de fallecidos de sexo masculino. La proporción de varones sobre el total ha sido del 79%, porcentaje que se mantiene respecto a 2015.

Por edades: En cuanto a los grupos de edad, el mayor porcentaje de fallecidos se sitúa en el grupo de edad de 45 a 54 años con 225 muertos, un 19% del total y en el de 35 a 44 años, con 216 fallecidos, también un 19% del total. El siguiente grupo de edad con mayor número de fallecidos es el de 25 a 34 años con 165 fallecidos, un 14% del total.

Los niños fallecidos (hasta 14 años) han sido 19, el 2% del total. Los mayores de 65 años, con 240 fallecidos han supuesto el 21% del total.

Por Comunidades Autónomas: Registran incrementos la Comunidad Valenciana (+19) Galicia (+15), Andalucía (+14), Castilla la Mancha (+11), Baleares (+9), Murcia (+8), Asturias (+7), La Rioja (+6) Extremadura (+3) y Aragón (+1).

Registran descensos Cataluña (-23), Castilla-León (-20), Cantabria (-7), Madrid (-6), País Vasco (-5), Navarra (-2) y Canarias (-1).

Por tipo de vía: Las carreteras convencionales siguen siendo las vías donde fallece el mayor número de personas (75%), aunque se registra una mejora con un 3% menos que el año anterior.

Por tipo de accidente: En las vías de gran capacidad el 47% de los fallecidos en 2016 se han producido en accidentes que fueron salidas de la vía, el 20% en accidentes con colisión trasera y múltiple y el 17% en atropellos a peatones. En las carreteras convencionales el 41% de los fallecidos se debió a accidentes en los que el vehículo se salió de la vía, mientras que un 25% se debió a colisiones frontales.

Por tipo de usuario: Los fallecidos por tipo de usuario presentan diferentes comportamientos. Aumentan los fallecidos en turismo, camión de menos de 3.500 kg, autobús y peatones

Disminuyen también los usuarios de bicicleta fallecidos, situándose en 33, 10 menos que en 2015.

Se reducen los fallecidos en motocicleta y en ciclomotor. En 2016 fallecieron 214 usuarios de moto, 10 menos que en 2015 y 21 de ciclomotor, 6 menos que el año anterior.

Los fallecidos en turismo (604) aumentan un 6% respecto al año anterior (34 fallecidos más).

Aumentan en 16 los fallecidos en autobús, 18 en 2016 respecto a los 2 de 2015.

Los peatones fallecidos aumentan en 5. De 113 en 2015 a 118 en 2016.

Uso de accesorios de seguridad: El 22% de los conductores y pasajeros fallecidos en turismos y furgonetas en 2016 no llevaban puesto el cinturón de seguridad. Aumenta en 3 el número de fallecidos que no hacían uso de dicho dispositivo de seguridad en turismos, llegando hasta 129. De los 214 fallecidos en motocicleta, 4 no utilizaban casco en el momento del accidente. En el caso de los 21 fallecidos en ciclomotor, 1 solo no hacía tampoco uso de dicho dispositivo. Entre los ciclistas, de los 33 fallecidos, 6 no utilizaban casco, pese a ser obligatorio en vías interurbanas.

Unidad de Coordinación de Víctimas de Accidentes de Tráfico: UVAT

La DGT tiene en funcionamiento las Unidades de Víctimas de Accidentes de Tráfico creadas en cada una de las jefaturas provinciales de Tráfico de toda España con el objetivo de coordinar una red integral de ámbito nacional, de información y atención a las víctimas de accidentes de tráfico, facilitando el acceso de las víctimas a los recursos existentes, velar por sus derechos y promover la participación de las instituciones y las administraciones locales, autonómicas y nacionales.

Esta Unidad, desde su creación, ha atendido a más de 70.000 víctimas de accidentes y ha realizado numerosas acciones formativas e informativas con Cuerpos y Fuerzas de Seguridad del Estado, policías locales y autonómicas y profesionales del ámbito sanitario, social. ●

Fotos: DGT

INFORME «RETOS Y PERSPECTIVAS DEL COMERCIO ESPAÑOL PARA 2017», DE CHECKPOINT SYSTEMS

Cataluña, Madrid y Andalucía, las comunidades con más **hurtos en comercios**

Cataluña es, con diferencia, la comunidad autónoma con más incidencia del hurto en establecimientos comerciales, seguida de Madrid y Andalucía. Sin embargo, el número de sustracciones en el conjunto de España se redujo un 3,82% en 2015. Así lo concluye el informe «Retos y perspectivas del comercio español para 2017» realizado por Checkpoint Systems, empresa especializada en soluciones para la disponibilidad de la mercancía en el sector minorista, a partir de datos del Ministerio del Interior y de los principales cuerpos de seguridad españoles.

LAS fuerzas policiales registraron 236.504 hechos de hurto en comercios minoristas en 2015. La mayoría se concentraron en Cataluña (59.952), Madrid (49.280), Andalucía (32.770) y la Comunidad Valenciana (24.220), coincidiendo con el mayor número de población y la mayor afluencia de turistas en las tiendas. En cambio, La Rioja (1.148), Cantabria (1.922) y Extremadura (2.142), además de Ceuta y Melilla, fueron las zonas menos afectadas por esta problemática.

La tendencia a la baja en la cantidad de faltas y delitos de hurto registrados en las tiendas se reflejó con claridad en Navarra (-17,65%), Cataluña (-10,98%) y Extremadura (-10,97%). En cambio, Ceuta (+18,3%), La Rioja (+17,5%) y Murcia (+12,24%) experimentaron una evolución al alza.

«Aunque en España disminuya el número de casos de hurto en establecimientos comerciales, el valor de la pérdida desconocida es similar a la de los últimos años», matiza David Pérez del Pino, director general de Checkpoint Systems en España y Portugal. «La época más difícil para prevenir el hurto es la de Navidad, porque hay más afluencia de clientes y porque se exponen más productos, de mayor valor y más codiciados por los hurtadores», alerta.

En este sentido, el Estudio sobre la Pérdida en el Sector Minorista en la Campaña de Navidad 2016 elaborado por el analista Ernie Deyle con el patrocinio de Checkpoint Systems sitúa en un 16% el aumento de la pérdida desconocida desde octubre hasta noviembre. Esta espada de Damocles puede afectar el balance final de la Navidad para los comerciantes, pese a que las ventas previstas para este final de año aumenten un 39% respecto al resto de 2016.

La prevención del hurto es una de las seis problemáticas que ha detectado Checkpoint Systems en el estudio «Retos y perspectivas del comercio español para 2017» que acaba de hacer público basándose en análisis de consultoras como Nielsen o EY, así como en instituciones públicas españolas y en la propia información facilitada por los retailers con los que trabaja.

Retos

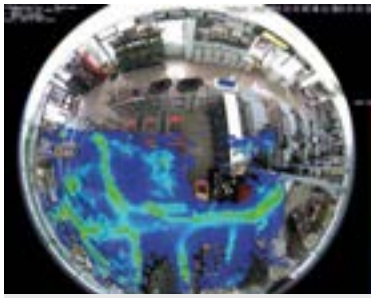
Los otros retos que analiza el informe son la reducción de la merma en productos frescos, la protección en origen, la gestión de datos inteligentes, los servicios de compra omnicanal y la mejora de la experiencia de compra de acuerdo con los hábitos del consumidor actual.

En cuanto al primero de los retos, el informe destaca que los productos frescos representan casi la mitad del gasto total en alimentación de los hogares españoles. De acuerdo con el estudio «La pérdida en la Gran Distribución en España 2016» de AECOC y EY, la pérdida desconocida de productos frescos equivale al 1,73% sobre las ventas de su categoría, y uno de los principales motivos es la falta de control sobre las fechas de caducidad y de consumo preferente, además de otros problemas logísticos. ●

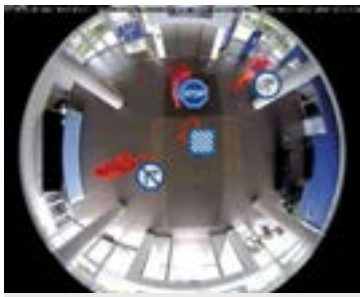
MxAnalytics

Análisis de Vídeo y Detección de Comportamiento

Diseñado para Retail • Sin Infraestructura Adicional • Integrado en la cámara



Mapa de Calor con Hot Spots



Estadísticas de personas u objetos

Múltiples eventos de comportamiento

Las cámaras hemisféricas de MOBOTIX son completamente adecuadas para supervisar tiendas y otros entornos de venta. En el 2012, MOBOTIX incorporó un paquete de análisis dentro de la cámara que permite generar mapas de calor y contar objetos en pasillos definidos por el usuario con informes automáticos.

MOBOTIX AG • Kaiserstrasse • D-67722 Langmeil • Tél. : +49 6302 9816-103 • Fax : +49 6302 9816-190 • sales@mobotix.com • www.mobotix.com

MOBOTIX

CLOUD COMMUNITY EUROPE REPRESENTA LA REVOLUCIÓN DE LA TRANSFORMACIÓN DIGITAL QUE SUPONE LA APLICACIÓN DE LA TECNOLOGÍA CLOUD

EuroCloud evoluciona y ahora es Cloud Community Europe

La asociación europea celebrará Expocloud los días 17 y 18 de octubre en el Círculo de Bellas Artes de Madrid

Cloud Community Europe, Asociación Europea de Empresas que ofrecen sus productos y servicios en tecnología Cloud Computing, con el objetivo de difundir e impulsar en el mercado los beneficios de su utilización y la competitividad que supone la aplicación de estas tecnologías en cualquier tipo de negocio, presentó el pasado 17 de enero en la Asociación de la Prensa de Madrid la Memoria de Actividades realizadas durante 2016 y el avance de su ambicioso Plan Estratégico para este año. El acto contó con la presencia de Francisco J. González Gosálbez, presidente de la asociación.

RESPECTO a la Memoria de Actividades de la asociación durante 2016, Francisco González, junto a Ignacio Carrasco, secretario General de la asociación, hicieron un balance positivo.

A nivel europeo, el capítulo español ha tomado un papel de gran relevancia dentro de Europa con la evolución de la marca EuroCloud a Cloud Community Europe, fruto de la revolución que supone la trasformación digital de la aplicación de la tecnología Cloud en velocidad, deslocación y tratamiento de la información a todos los niveles.

A nivel nacional, caben destacar los encuentros entre asociados y profesionales de «Cloud Profesional» con motivo de las reuniones llevadas a cabo por las Comisiones de Trabajo, principalmente: Seguridad, Big Data, Compliance e IoT Internet of Things. La creación de ofertas propias y específicas para cubrir las necesidades de las empresas en los ámbitos de Seguros, Formación, Certificación –principalmente StarAudit y IoTrust– Subvenciones y Ayudas. Estas últimas junto con SETSI, RED.ES, INCIBE, Ministerio del Interior, Ministerio de Administraciones Públicas y Ministerio de Justicia y AEPD.

Organización de eventos

En cuanto a la organización de eventos, destacaron: ExpoCloud 2016, que consigue dar un salto cualitativo en una feria de «cloud» para «clouders» con más de millar y medio de visitantes, 22

fusión de las ventajas de la Nube y la Transformación Digital con eventos dirigidos a empresas y emprendedores; con el fin de divulgar el conocimiento del Cloud Computing y sus tecnologías relacionadas: Virtualización, Big Data, Movilidad y Seguridad, entre otros.

expositores y más de 50 panelistas y conferenciantes; la última edición de los Awards EuroCloud nacional con el resultado de tres finalistas europeos. Y la celebración de Cloud4 en Madrid, dentro de la Semana del Cloud promovida por EOI, HOLA CLOUD y EuroCloud España.

La asociación también ha destacado la iniciativa del estudio de mercado del Cloud Computing, junto a IDC, que permitirá identificar las necesidades del mercado, visualizar el posicionamiento de los principales competidores y mostrar las estrategias de venta para maximizar el crecimiento.

En cuanto al Plan Estratégico concebido para a medio y largo plazo, la asociación espera continuar con la difusión de las ventajas de la Nube y la Transformación Digital con eventos dirigidos a empresas y emprendedores; con el fin de divulgar el conocimiento del Cloud Computing y sus tecnologías relacionadas: Virtualización, Big Data, Movilidad y Seguridad, entre otros.

> «Durante el encuentro se presentó un avance de un estudio de mercado del Cloud Computing»

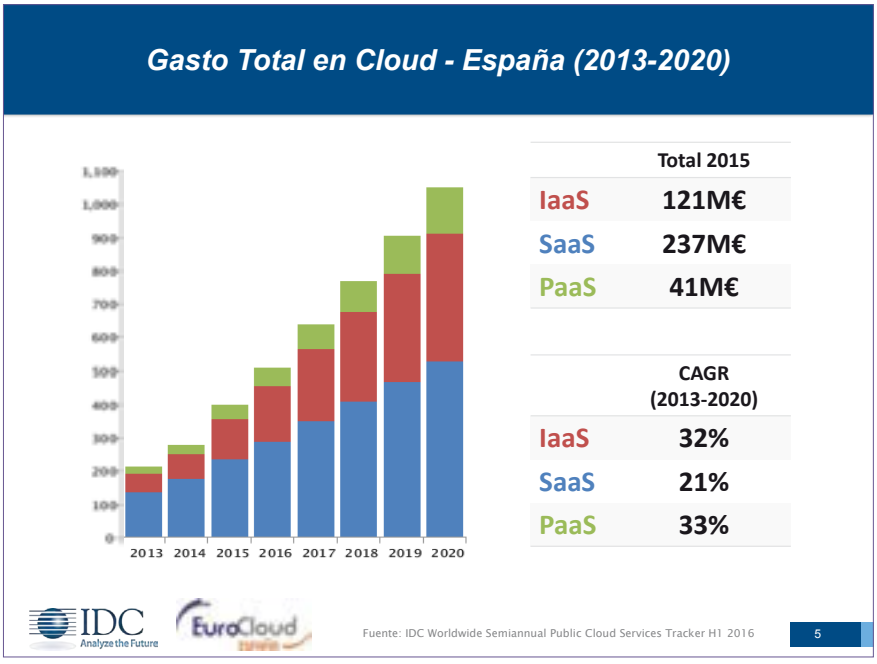
Adicionalmente y para este año, la asociación tiene presente la celebración de ExpoCloud, los días 17 y 18 de octubre en el Círculo de Bellas Artes de Madrid; la celebración del Congreso Europeo Community Europe Madrid Forum, en el mes de octubre, Cloud-4Verticals, dirigidos a sectores verticales –defensa, banca, sanidad etc.–, y CloudInBreakfast, estos últimos en formato desayuno de trabajo con el fin de difundir las propiedades del Cloud en Madrid y Barcelona; y una nueva edición de los Premios Awards.

Nuevos convenios con entidades

La Asociación también ha informado de nuevos convenios con entidades empresariales, profesionales y con la AAPP, el desarrollo del colectivo «Cloud Profesional» y de una Bolsa de Trabajo, asesorías tecnológicas de migración al «Cloud», programas de internacionalización de empresas, soporte para las pequeñas empresas, «starts-up» y «spin-off» en comunicación y marketing, y cursos de formación en colaboración con Universidades, Escuelas de Negocio y Centros de Formación tanto «on-line» o presenciales, «in-house» o en aulas homologadas.

Dentro de las actividades previstas, la asociación continuará potenciando las acciones de formación para la obtención de la certificación europea StarAudit, un referente en la industria, avalada e impulsada por la Unión Europea, que pretende estandarizar y aportar una mayor confianza a los usuarios dentro del espacio común Europeo, a la hora de elegir proveedor y contratar los servicios Cloud.

Con el convencimiento de que la estrategia marcada para los próximos años garantiza a sus asociados el compromiso de promocionar el conocimiento y la confianza de la tecnología Cloud, EuroCloud España, ahora Cloud Community Europe, dio por clausurada la jornada. ●



Texto y Fotos: Cloud Community Europe/Redacción

EL EVENTO TUVO LUGAR EL PASADO 20 DE DICIEMBRE EN MADRID

Cepreven celebra su 41 Encuentro Anual

Más de un centenar de profesionales participaron en el evento

CEPREVEN celebró el pasado 20 de diciembre su 41 Encuentro Anual. Los actos comenzaron con la reunión del Consejo de Administración de Servicios Técnicos Cepretec y el Consejo de Dirección de la Asociación de Investigación para la Seguridad de Vidas y Bienes, en los que se presentaron los cierres del ejercicio económico, y los presupuestos y las líneas de acción para 2017, todos ellos aprobados por sus órganos de gobierno.

MÁS de un centenar de profesionales del sector asegurador y reasegurador, de la pericia, de los fabricantes e instaladores en el campo de la seguridad y fundamentalmente del mundo de la prevención, así como de otros ámbitos profesionales afines, participaron en esta celebración. Durante el cóctel celebrado al efecto, el presidente de CEPREVEN, Ignacio Eyries, destacó que «2016 ha sido un año muy bueno para nuestra organización, pues es un ejercicio que ha supuesto la consolidación de nuestro modelo de empresa, que nos ha permitido obtener suficientes recursos para cumplir con nuestra misión más ampliamente. Es un año que, sin duda, nos deja con muy buenas perspectivas para los próximos ejercicios», concluyó.

Aumento de la Prevención

Por su parte, el director general de CEPREVEN, Jon Michelena, trasladó el agradecimiento a todos los colaboradores y adelantó que «en 2017 queremos hacer más cosas para que la Prevención siga aumentando en la sociedad». Finalizó poniendo de manifiesto el excelente trabajo del equipo de personas que componen su organización, «que nunca escatiman horas de esfuerzo para cumplir con nuestros fines». ●

Ignacio Eyres, presidente de CEPREVEN, y Jon Michelena, director general de CEPREVEN (de dcha. a izq.)

EL ENCUENTRO SE CELEBRA ENTRE EL 14 Y 16 DE MARZO

HOMSEC 2017 con un Pabellón de China entre sus nuevos expositores

El Salón Internacional de Tecnologías de Seguridad Nacional –HOMSEC 2017– acogerá en su ya sexta edición entre sus nuevos expositores un Pabellón de China en el que empresas del sector procedentes del país asiático podrán exponer sus productos y soluciones a la par que participar de las diversas actividades de networking ofertadas en el evento.

HOMSEC 2017, organizado por el Grupo ATENEA, abrirá sus puertas en Madrid entre el 14 y 16 de marzo en el pabellón 12 de IFEMA, con una firme apuesta por el crecimiento internacional para promocionar la industria de Seguridad Nacional de España a todos los niveles, así como acoger las propuestas tecnológicas procedentes del resto del mundo.

Plataforma de promoción

HOMSEC 2017 se constituye en una excelente plataforma de promoción ante los «decision makers» de la Administración española, así como ante los mercados con mayor demanda de tecnologías de primer nivel gracias a la presencia de más de 30 delegaciones oficiales.

«Las cifras de crecimiento en relación a visitantes, número de delegaciones e impacto de HOMSEC en cuanto a visibilidad de la industria de Seguridad Nacional española de los últimos años nos avalan, pero no nos conformamos, queremos seguir creciendo en los servicios que ofrecemos en nuestro Salón a este sector, tractor de la I+D y absolutamente fundamental para el crecimiento económico de nuestro país», ha manifestado José Luis Cortina, presidente del Grupo ATENEA.

«Tenemos un mercado consolidado y bien posicionado para la exportación y la internacionalización, con destacados ejemplos de éxito, a la par que contamos con empresas jóvenes, grupos de investigación en universidades, abundante talento que ha de darse a conocer, interactuar con el talento de otros países y para ello trabajamos en un HOMSEC que apuntale su proyección y genere oportunidades de negocio», ha afirmado el presidente.

fotos: *HOMSEC*

José Manuel Leceta, nuevo director general de Red.es

El Consejo de Administración de Red.es ha nombrado a José Manuel Leceta nuevo director general de esta entidad pública del Ministerio de Energía, Turismo y Agenda Digital, en sustitución de Daniel Noguera.

El nuevo director general de Red.es, ingeniero de Telecomunicaciones y tiene diplomas en Dirección Estratégica, Economía de Redes, Estudios Internacionales y Gestión de la Innovación. Fue también alumno y profesor de la Universidad Internacional del Espacio (ISU) y se declara un firme defensor del poder de la educación y la experimentación para transformar la sociedad. Es, asimismo, experto en políticas y estrategias internacionales de innovación y emprendimiento.

Comenzó su carrera en la industria espacial en 1987, primero en España y luego en Finlandia, Francia y Japón, y se unió al Centro para el Desarrollo Tecnológico Industrial (CDTI) en 1992, como miembro de la delegación española ante la Agencia Espacial Europea (ESA). En 1996 fue nombrado jefe del Departamento de Tecnologías y Aplicaciones en el CDTI, y entre 2000 y 2002 fue presidente del Consejo Director del Programa de Lanzadores Ariane y vicepresidente del Consejo de Programas de Telecomunicaciones por Satélite de la ESA. Entre 2004 y 2010 fue director internacional del CDTI, miembro activo de CREST-ERAC y representante de alto nivel en Eureka y TAFTIE (la Red Europea de Agencias Nacionales de Innovación). En estos últimos años ha ejercido como director del Instituto Europeo de Innovación y Tecnología (EIT), con sede en Budapest. En 2011 lideró y estructuró las relaciones del Instituto con las primeras «Comunidades de Innovación y Conocimiento» (KICs), logrando su reconocimiento como nuevos actores en el panorama europeo. Desde el verano de 2014 ha sido también profesor visitante en el Centro Robert Schuman de Estudios Avanzados del Instituto Universitario Europeo (EUI) de Florencia, donde ha estudiado la evolución de las políticas europeas de innovación.

Synology redefine el concepto de almacenamiento en red NAS para hacer las pymes más competitivas

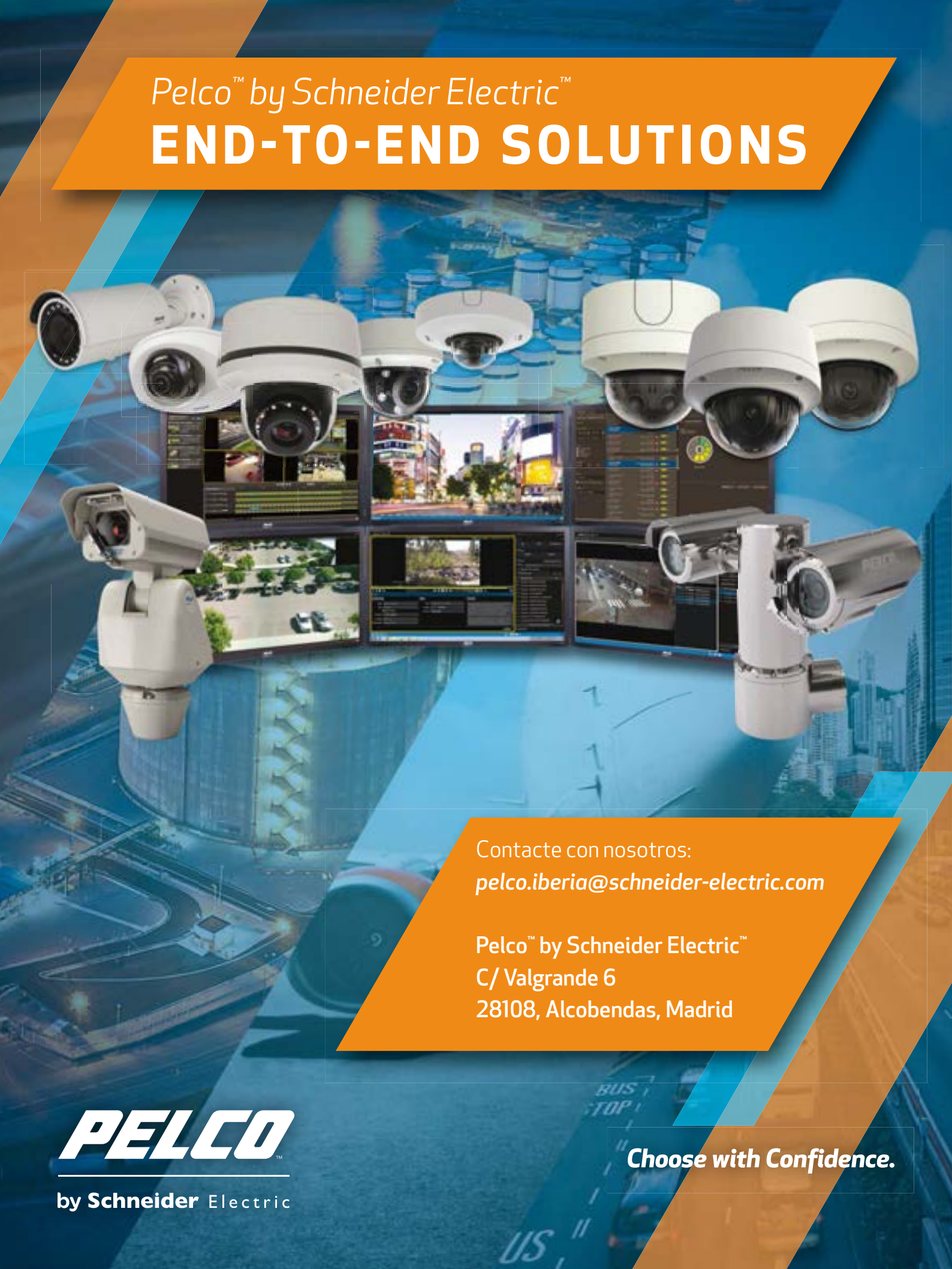
Consciente de la evolución que está experimentando el mercado del almacenamiento y de la tecnología cloud, Synology ha dado un paso más en su estrategia de innovación orientada a dar servicio a las demandas de las pequeñas y medianas empresas, ya que las pymes constituyen casi la mitad de los usuarios de la compañía con sede central en Taiwan. Así, ha anunciado la redefinición del término de almacenamiento en red NAS (Network-Attached Storage) hacia el concepto «Networking, Application and Storage».

Esta nueva estrategia, presentada en el evento anual Synology 2017, supone la introducción de soluciones que la compañía califica de «revolucionarias», diseñadas para cubrir diferentes niveles de necesidades, incluyendo servicio híbrido de recuperación de desastres en la nube, nuevo almacenamiento All-flash, suite de colaboración completa en nube privada, protocolo de transferencia de archivos de Internet de nueva generación, un nuevo router, y la adaptación de su aplicación de acceso remoto para trabajar desde el móvil. «Synology 2017 es nuestro evento más importante del año, donde tenemos la oportunidad de hablar con nuestros usuarios en primera persona, y recoger sus impresiones, que son muy valiosas para el desarrollo del valor añadido en nuestras soluciones y la creación de una experiencia de primer nivel especial para ellos», afirmó Rosiel Lee, directora general de Synology Francia y Sur de Europa, durante la presentación a los medios que tuvo lugar en Madrid.

«Buscamos aprovechar nuestra fuerza en el desarrollo de software para hacer a las pymes más competitivas, porque creemos en el concepto 'software -defined'. Creemos que, al hacerlo, ayudamos al mercado español a convertirse en un destino más atractivo para las empresas internacionales a la hora de hacer negocios» señaló Lee. En el acto también estuvieron Marcos de Santiago, director de Gestión de Productos para Francia y sur de Europa, y Manuel Jordán, product manager para España, Portugal y Grecia.

Pelco™ by Schneider Electric™

END-TO-END SOLUTIONS



Contacte con nosotros:
pelco.iberia@schneider-electric.com

Pelco™ by Schneider Electric™
C/ Valgrande 6
28108, Alcobendas, Madrid

PELCO™
by Schneider Electric

Choose with Confidence.

Tecnifuego-Aespi premio I+D+i en Seguridad en S²R European Forum

TECNIFUEGO-AESPI «in memoriam de D. Xavier Grau» recibió el Premio S2R 2016 a la I+D+i en Seguridad en el Congreso S2R Fórum, que ha tenido lugar del 26 al 28 de octubre en el Palacio Euskalduna de Bilbao. El premio fue recogido por Carlos Luján, que agradeció en nombre de la Asociación el distintivo y subrayó la importancia del I+D+i para crear soluciones que favorezcan la seguridad contra incendios.

En el Congreso, Xavier Grau (q.e.p.d.) presidía la sesión de Tecnologías de Seguridad contra Incendios, por ello la organización ha dedicado este apartado a su memoria.

Durante el acto, y en la sesión destinada a la seguridad contra incendios, Francisco Herranz, director Técnico de TECNIFUEGO-AESPI recordó la figura de Xavier Grau, que trabajó durante más de 35 años en el desarrollo del sector y de las actividades asociativas, participando desde los inicios en la configuración de la Asociación.

Además, Herranz introdujo el momento actual del sector y todas las iniciativas y actividades de la Asociación, como la representación ante las Administraciones y los Organismos, tanto nacionales como europeos, participación en los procesos normativos y reglamentarios, y presencia en ferias, apoyando los procesos de exportación, etcétera. Finalmente, el ponente destacó los objetivos del sector de seguridad contra incendios ante los nuevos retos que se plantean.

UGT solicita adelantar la edad de jubilación a los vigilantes, escoltas y guardas rurales

La Unión General de Trabajadores ha anunciado – en el Consejo General del Instituto Nacional de la Seguridad Social- el inicio del procedimiento para establecer coeficientes reductores que rebajen la edad de jubilación para el colectivo profesional de Vigilantes de Seguridad, Guardias Rurales –con sus especialidades- y Escoltas, todos ellos encuadrados en el Sindicato de Seguridad Privada de la Federación de Servicios, Movilidad y Consumo de UGT (FeSMC-UGT). Desde FeSMC-UGT pedimos la implicación en este proyecto a las patronales del sector y al Ministerio del Interior.

El sindicato entiende que estos profesionales están comprendidos dentro de lo dispuesto en el Real Decreto 1698/2011, por el que se regula el régimen jurídico y el procedimiento general para establecer coeficientes reductores y anticipar la edad de jubilación en el sistema de la Seguridad Social.

Desde el sector de Limpieza y Seguridad de la FeSMC-UGT se considera que es hora de valorar el trabajo de este colectivo, ya que cada día en mayor medida estos trabajadores vienen asumiendo funciones que en el pasado eran exclusivas de la seguridad pública: vigilancia de aeropuertos, puertos, transporte ferroviario, estaciones de metro, espectáculos públicos, recintos carcelarios, etc.

Además, en la actualidad –y en muchos de estos puestos de trabajo se comparten funciones con agentes de la seguridad pública, trabajadores que sí tienen reconocidos el pase a una segunda actividad al llegar a una determinada edad.

Otro factor que hay que tener en cuenta es el preocupante envejecimiento de las plantillas que tiene repercusión en la calidad del servicio, en la operativa de las empresas, en la imagen del sector y, por supuesto, en las capacidades de los trabajadores.

safire

IP CÁMARAS

ADVANCE SERIES

- Mayor Resolución 2Mp & 4 Mp
- WDR Real (120 dB)
- H.264/H.264+
- Audio, Alarmas, PoE, Slot SD
- Video Content Analytics

ONVIF

Distribuidores oficiales:

www.jmsystems.es

Avantech Electronics
www.avantech.info

VISIOTECH
www.visiotech.es

SAFIRE
www.safirecctv.com
info@safirecctv.com

Ingram Micro distribuye las soluciones de DynaScan para España y Portugal

INGRAM Micro España a través de su división Pro AV – división especializada para el mercado audiovisual – ha anunciado un acuerdo de distribución con DynaScan Technology, convirtiéndose en el mayorista oficial para la región de Iberia (España y Portugal) con un fuerte desarrollo en el foco de soluciones profesionales de alta luminosidad. Ingram Micro ha sido seleccionado por sus capacidades para promover el crecimiento de la compañía de productos profesionales de LCD en el mercado español. Ingram Micro distribuirá la línea de soluciones videowall y de alta luminosidad «DS²» deDynaScan.

Ingram Micro es uno de los distribuidores de tecnología más grandes del mundo, liderando el mercado de tecnología al traer los últimos productos y servicios al mercado y encontrar nuevas maneras de aportar valor a sus clientes. Alejandro Rincón, Pro AV Business Manager, señala: «Estamos muy entusiasmados llegando a este acuerdo para trabajar con DynaScan Technology como uno de nuestros socios dentro del portfolio de la división de Pro AV.

Con las innovadoras soluciones de alta luminosidad de DynaScan hemos completado nuestra cartera de Digital Signage, y estamos tomando un nuevo camino para ser un proveedor de servicios completo para nuestros socios del canal».

El presidente de DynaScan, Alan Kauffman, señala que la asociación con Ingram Micro ayudará a impulsar el crecimiento de la compañía en la región de Iberia. «Creemos que las pantallas LCD profesionales de DynaScan son un excelente ajuste para la oferta de productos de Ingram Micro y confiamos en que podrán promover con éxito la marca DynaScan en la región».

Casmar presenta las soluciones Smart Home de Risco en ciudades españolas

Casmar, especialista en soluciones de seguridad electrónica, y Risco Group, especialista global en soluciones integradas de seguridad, han presentado sus soluciones Smart Home de Risco por diversas ciudades españolas.

El tour de presentaciones comenzó el pasado 26 de octubre en Madrid y finalizó el 29 de noviembre en San Sebastián, pasando por Barcelona, Las Palmas y Tenerife. En estas jornadas, Risco Group, ha mostrado junto a Casmar las distintas soluciones que ofrece Smart Home, un sistema integral de automatización del hogar basado en la nube de Risco Group que integra también seguridad y vídeo en la misma plataforma.

Smart Home está basado en dispositivos Z-Wave y ofrece nuevos modelos de negocio a las empresas instaladoras y CRAs, a la vez que aporta a los usuarios nuevas funcionalidades como: control de acceso remoto, control energético o gestión de automatismos.

Estas nuevas funcionalidades se pueden utilizar de forma autónoma al sistema de seguridad o pueden ser integradas en las plataformas de seguridad Agility, LightSYS y ProSYS Plus de RISCO Group. De esta manera, se obtienen mayores ventajas y prestaciones, ya que se añaden al sistema de seguridad, las cámaras IP y los dispositivos Smart Home. Otra novedad presentada ha sido el lanzamiento del nuevo sistema de seguridad ProSYS Plus de Grado 3, el cual permite acometer de forma flexible y escalable, gracias a sus prestaciones y sistema de licenciamiento, grandes instalaciones comerciales, industriales o simplemente instalaciones que requieran sistemas certificados EN50131 Grado 3.

«Las soluciones Cloud de Risco en general, y las soluciones Smart Home en particular, han tenido una gran aceptación entre los asistentes al Tour, tanto por el beneficio que les aportan estos nuevos modelos de negocio, como por las ventajas que pueden ofrecer a sus clientes en términos de gestión y uso de los sistemas», comenta Alejandro Ramón, director comercial de Casmar.

Axis distribuye las nuevas cámaras de red de Canon en EMEA y Norteamérica

En el marco del acuerdo de colaboración en marketing y ventas sellado recientemente entre Axis Communications y Canon, Axis ha incorporado recientemente siete nuevos modelos de la gama de cámaras de red Canon a su oferta para los clientes de EMEA y Norteamérica.

La VB-S30VE es uno de los nuevos productos de Canon disponibles en el primer trimestre de 2017 a través de los canales de distribución de Axis en EMEA y Norteamérica.

Desde el 1 de septiembre en EMEA y el 1 de octubre en Norteamérica, Axis Communications ha asumido la gestión del marketing y las ventas de toda la oferta de productos de vídeo en red de Canon en estas regiones.

Dentro de este nuevo marco de colaboración, Axis complementa hoy su catálogo de soluciones de seguridad en el sector con la incorporación de siete nuevas cámaras de red Canon. Entre ellas, encontramos la VB-S30VE, una cámara minidomo PTZ compacta para exteriores, y la VB-H761LVE, una cámara de caja fija para exteriores con zoom de 20 aumentos e iluminación infrarroja. La mayor parte de los nuevos modelos están pensados para la vigilancia en exteriores y todos pueden funcionar en resolución HDTV a 1080p a la máxima velocidad de fotogramas.

Las nuevas cámaras estarán disponibles en el primer trimestre de 2017 a través de los canales de distribución de Axis en EMEA y Norteamérica. En el mercado japonés y en el resto de la región Asia-Pacífico, los productos Canon estarán disponibles a través de los canales de distribución existentes de Canon.

La Ertzaintza lanza una app para mejorar la atención al ciudadano

La Ertzaintza y el Departamento de Seguridad del Gobierno Vasco han implementado una aplicación para dispositivos móviles para que el ciudadano pueda contactar con la Ertzaintza: APP ERTZAINTZA.

Se trata de una app que puede ser descargada en cualquiera de los stores de los diferentes sistemas operativos (Android, iOS y Blackberry), y que permite contactar de manera directa con la Ertzaintza; tanto por teléfono (línea 900 gratuita) y SMS, como por mensajería instantánea Whatsapp, email o de forma anónima. También dispone de una opción para contactar con SOS Deiak (112) en caso de emergencia.

«Dado que hoy en día el uso de los smartphones está totalmente extendido entre nosotros, nos parece adecuado disponer de la APP ERTZAINTZA tanto en organismos oficiales como en comunidades vecinales y diferentes asociaciones», afirma la policía vasca en una nota.

«Les animamos a hacer uso de esta vía de contacto con la Ertzaintza para cualquier problema que pudieran tener o para cualquier información relativa al Departamento de Seguridad que pudieran necesitar o que quisieran aportar», prosigue el comunicado.

El servicio está atendido las 24 horas del día, los 7 días de la semana.

Los enlaces para poder descargar la app son los siguientes:

-Android https://play.google.com/store/apps/details?id=com.gvdi.b70.ertzaintza

-iOS https://appsto.re/es/5nAXdb.i

-Blackberry http://appworld.blackberry.com/webstore/content/59998130

El cibercrimen supera en preocupación al crimen físico, según Sophos

SOPHOS, empresa especializada en seguridad para protección de redes y endpoints, ha anunciado los resultados de una encuesta reciente donde se ha preguntado a los consumidores por sus conocimientos sobre phishing, ransomware, malware, spyware, ataques y otras ciberamenazas. Significativamente, la encuesta revela que los consumidores están más preocupados por el cibercrimen que por la delincuencia física mundial.

De los encuestados, al 63% les preocupan las pérdidas económicas debido a una violación de los sistemas, el 61% se muestra preocupado de que los cibercriminales se apoderen de su ordenador para enviar campañas de spam y malware a sus contactos y a otras personas inocentes, y al 58% les preocupa que los ciberdelincuentes inutilicen sus equipos. En contraste, a un 46% les preocupa que les roben, agredan físicamente o entren en su coche, al 52% les preocupa que su casa sea robada y el 56% de los encuestados se muestra preocupado por el terrorismo. El estudio, encuestó a 1.250 consumidores en Estados Unidos, Reino Unido, Alemania, Austria y Suiza. A pesar de la preocupación general mostrada por la ciberdelincuencia entre los consumidores encuestados,

LSB: Se endurecen los controles a empresas en relación a las horas realizadas por sus trabajadores

La Instrucción 3/2016, de la Dirección General de la Inspección de Trabajo, especifica la intensificación en las tareas de control sobre las horas realizadas por los trabajadores de las diferentes empresas, y en especial sobre las catalogadas como horas extras.

El empresario debe saber que tiene la obligación legal de implantar un sistema para el control horario de sus trabajadores, y que de no hacerlo se expone a las posibles sanciones derivadas de una inspección.

El sistema o modelo será elegido libremente por la empresa dado que la ley nada dice sobre este particular, no obstante debe ser un sistema de registro que garantice la fiabilidad y la invariabilidad de los datos.

El registro de la jornada deberá ser diario e incluir el horario concreto de entrada y salida respecto de cada trabajador.

Esta nueva normativa está provocando un incremento en la venta de sistemas para realizar dicho control horario (hardware y software), que es interesante sea aprovechado por el distribuidor/ instalador del sector.

La tendencia es el uso de equipos de identificación por patrón biométrico (huella dactilar fundamentalmente).

Pero el hincapié se debe realizar sobre el software que gestiona el equipo. Normalmente el fabricante regala uno el cual no responde muchas veces a las necesidades de la empresa. El software aloja una base de datos donde se van volcando los fichajes de entrada/ salida que van realizando los trabajadores. A partir de esa información, el software permite generar diferentes informes, entre ellos importante verificar que alguno cumpla con lo requerido en las posibles inspecciones.

la concienciación sobre el phishing y el ransomware sigue siendo relativamente baja. El 47%, casi la mitad, no están familiarizados con el phishing o lo perciben como una amenaza baja, lo cual es preocupante teniendo en cuenta que el phishing es el método de ataque número uno utilizado para obtener acceso a la información personal. Más del 30% de los encuestados consideran que están extremadamente desprotegidos, se muestran inseguros de estar protegidos o ignoran completamente los ataques de phishing. El 31% de los encuestados dijeron que no están familiarizados con el ransomware o lo perciben como una amenaza menor.

El 55% de encuestados por Sophos dicen asesorar a otra persona (cónyuge, hijos, amigos, padres, y demás familiares y conocidos) sobre cómo mantener protegidos sus ordenadores contra el malware y los ataques cibercriminales. De estas personas que asesoran a terceros, un 14% no está realmente segura de haber llevado a cabo una copia de seguridad de forma correcta ni tampoco de ser capaces de poder recuperar los datos en caso de darse una brecha de seguridad en dichos ordenadores. El 18% de quienes asesoran a otros reconoce no estar seguro del todo de lo que hace, por lo que finalmente en total hasta un 32% de personas que confía su ciberseguridad a otros es potencialmente vulnerable a una violación de datos.

Además, el 11% de quienes asesoran sobre la ciberseguridad del ordenador de otros no están seguros de que esos equipos estén protegidos contra ciberdelincuentes y virus, mientras que un 14% de encuestados reconoce no tener ni idea de si realmente están o no protegiendo adecuadamente los ordenadores de otros. Esto significa que hasta un 25% de los ordenadores domésticos administrados por otras personas, según demuestra la encuesta de Sophos, son vulnerables a la ciberdelincuencia, incluyendo el phishing y el ransomware.

Segovia, Soria, Ávila y La Rioja, las provincias más seguras en España en 2016

Segovia ha sido la provincia más segura de España en 2016, según las incidencias registradas por clientes de Securitas Direct: apenas el 1,13% de ellos ha visto cómo su alarma avisaba de la presencia de un intruso. Le siguen muy de cerca Soria, Ávila y La Rioja.

En el extremo opuesto se encuentra Huelva, con un índice de incidencias en 2016 del 4,35%, lo que significa un riesgo de robo cuatro veces mayor que en Segovia, por ejemplo. Le siguen en este ranking de inseguridad Sevilla, Toledo y Jaén. En el octavo lugar se sitúa Barcelona y en una posición intermedia entre las 50 provincias españolas queda Madrid, en el puesto 22.

En lo que respecta a ciudades –el ranking se elabora entre las 50 localidades más pobladas de nuestro país–, curiosamente las tres más seguras pertenecen a la provincia de Madrid: lidera esta clasificación Boadilla del Monte –apenas un 1,06% de clientes con incidencia–, seguida de Arroyomolinos y de Majadahonda. Las más inseguras, por el contrario, son Huelva –4,66% de clientes han sufrido un robo o intento de robo–, Torrevieja y Sevilla, por ese orden.

Si nos ceñimos a las capitales de provincia, lideran el ranking de seguridad Granada (1,69%), Córdoba y Bilbao; en cuanto a las capitales más inseguras, aparte de Huelva y Sevilla, ya citadas, en tercer lugar se encuentra Tarragona.

El ranking se elabora en función del porcentaje de clientes de Securitas Direct a los que les ha saltado la alarma por una intrusión o intento de intrusión en su inmueble. En el gráfico se expone el ranking de las 15 provincias y ciudades más y menos seguras de España a lo largo de 2016.

Sergey Dzyuba / shutterstock

	Provincias más seguras	Provincias más inseguras	Ciudades más seguras	Ciudades más inseguras
1	Segovia	Huelva	Boadilla Del Monte	Huelva
2	Soria	Sevilla	Arroyomolinos	Torrevieja
3	Ávila	Toledo	Majadahonda	Sevilla
4	La Rioja	Jaén	Granada	Marbella
5	Albacete	Badajoz	Córdoba	Fuenlabrada
6	Palencia	Málaga	Bilbao	Sabadell
7	Huesca	Cádiz	Alcalá De Henares	Leganés
8	Lugo	Barcelona	Valencia	Gijón
9	Navarra	Almería	Málaga	Tarragona
10	Burgos	Cantabria	Vigo	Mataró
11	Valladolid	León	Zaragoza	Palma De Mallorca
12	Zaragoza	Asturias	Alicante	Alcorcón
13	Salamanca	Teruel	Las Rozas	Alcobendas
14	La Coruña	Las Palmas	Toledo	Sant Cugat Del Vallés
15	Vizcaya	Tenerife	Pozuelo De Alarcón	Badajoz

Axis Solution Conference: una experiencia diferente en un evento de fabricante

Durante muchos años desde Axis nos hemos preocupado de mantener una estrecha relación con nuestros socios de negocio, tanto distribuidores como integradores, sin olvidar a aquellas empresas que desarrollan tecnología (hardware o software), que permite a los productos Axis formar parte de soluciones más avanzadas y complejas. Para ello, disponemos en Axis de diferentes programas de colaboración, alguno de los cuales comenzó ya en el año 99 (Application Development Partner –ADP– Program) y celebrábamos una reunión anual para encontrarnos con todos ellos y comunicarles las novedades de la compañía y las líneas estratégicas de actuación para los años siguientes.

Sin embargo, hace un par de años percibimos que en la ecuación Axis + Socios = Soluciones faltaba un término esencial, el cliente final. Es cierto que habíamos invitado a algunos clientes relevantes en varias ediciones de nuestra reunión anual, pero los contenidos y formato nunca estuvieron orientados para ellos. En los últimos años, Axis Communications ha dedicado esfuerzos y recursos para progresar desde la posición de un fabricante de productos hacia la de un proveedor de soluciones. Las soluciones son, a diferencia de los productos, directamente asociables y aplicables a problemas reconocidos en los clientes finales, especializadas, diseñadas para entornos y situaciones particulares.

El siguiente reto era el formato de evento. Había que modificar el clásico formato de presentaciones sujetas a un programa en una jornada flexible en la que cada asistente encontrase la solución de su interés y pudiese obtener información detallada sobre la misma por parte de fabricantes y desarrolladores. Un evento que en la experiencia de cada visitante fuese «su» evento, en el que el tiempo dedicado y las soluciones encontradas parecieran dedicadas a cada uno de los clientes finales.

El resultado, el primer Axis Solution Conference celebrado en octubre de 2015, fue una exposición con un buen número de soluciones categorizadas por segmentos de mercado, junto a presentaciones de la compañía (los socios siguen siendo esenciales) y algunos testimonios directos de clientes finales que explicaron su experiencia en la implantación y explotación de las soluciones presentadas. Esto último tuvo una extraordinaria aceptación por parte de los clientes finales.

Ahora en la nueva edición del Axis Solution Conference –8 y 9 de marzo– vamos a profundizar con soluciones más únicas, socios más cercanos y presentes en el mercado español, con aplicaciones que aprovechan más y mejor las características de los productos Axis. También presentaremos más líneas de productos Axis incluyendo diferentes softwares, apps para hacer las cámaras más usables, línea económica Companion, productos de audio y de control de accesos, y aprovecharemos para mostrar algo de las compañías adquiridas por Axis como Cognimatics (analíticas de Retail) y Citilog (analíticas de tráfico). Desde Axis nos estamos esforzando en preparar un evento que, como en la edición anterior, cause impacto en los asistentes, pero sobre todo que resulte útil y provechoso para cualquiera de los perfiles que esperamos recibir: integradores, consultores, desarrolladores, autoridades y clientes finales.

Kaspersky: la protección de datos, prioridad de las empresas

La pérdida o la exposición de datos sensible es una de las peores consecuencias derivadas de un incidente de ciberseguridad. Sin embargo, cerca de la mitad (48%) de las compañías españolas son conscientes de que deberían estar mejor preparadas ante un ataque. Así lo destaca el Informe de Kaspersky Lab «Percepción de la Seguridad TI en las empresas: hacer frente a ataques inevitables», basado en la encuesta de riesgos de seguridad TI en las empresas 2016.

A pesar de la evidente amenaza de ciberataques, la encuesta revela puntos de vista diferentes en relación al estado de la protección y a los enfoques de mitigación, exponiendo las debilidades y vulnerabilidades ante las amenazas existentes y emergentes. A día de hoy, todas las compañías se enfrentan de alguna manera a ciberataques. De hecho, en los últimos 12 meses un 38% de las

empresas españolas ha experimentado una pérdida de datos como resultado de una brecha de seguridad. Asimismo, en cuanto a grandes empresas, una de cada cinco (19%) aseguró haber sufrido más de cuatro brechas de seguridad relacionadas con la pérdida de datos durante ese periodo.

ISMS Forum: Daniel García, nuevo director general

LA Asociación Española para el Fomento de la Seguridad de la Información, ISMS Forum Spain, ha nombrado a Daniel García Sánchez nuevo director general, tras ocupar durante los últimos cinco años el cargo de coordinador y responsable de Comunicación y Eventos de la Asociación.

Daniel García cuenta con amplia experiencia en el área de coordinación de proyectos, relaciones institucionales, gestión comercial, gestión de la comunicación interna y externa, así como en la organización de eventos. En los últimos cinco años ha desarrollado su carrera profesional en ISMS Forum como responsable de la planificación, el desarrollo y la ejecución de las actividades de la Asociación, entre las que destacan congresos nacionales e internacionales, estudios y cursos de formación, entre otros. Licenciado en Periodismo por la Universidad Rey Juan Carlos, Daniel García desarrolló su especialización en comunicación corporativa y actualmente es máster en gestión e investigación de la comunicación empresarial, y máster en economía aplicada a las ciencias sociales.

El conseller Jordi Janè preside el Día Català de la Seguretat Privada

El conseller de Interior, Jordi Jané, presidió el Día Català de la Seguretat Privada, donde se hizo la entrega de las menciones de la Seguridad Privada de Cataluña, que en esta ocasión cumplió su quinta edición.

El conseller explicó que el sector de la seguridad privada debe tener unos principios de preeminencia, con una subordinación, pero a la vez un esfuerzo constante de colaboración coordinación y complementación «en el ámbito de la seguridad nunca sobra nadie» dijo.

Janè avanzó que se está actualizando el código de buenas prácticas para reafirmar la imagen de proximidad y de complicidad de la seguridad privada, principios éticos que deben regir en el sector. «El principio de trato digno y ejemplar ante la ciudadanía el sector ya lo hace, pero nos debe ayudar a que si alguien no lo cumple sea rechazado», insistió.

El director de Administración de Seguridad, Jordi Jardí, alabó las grandes cualidades humanas de los agentes de seguridad privada y destacó su empatía, generosidad y humildad. «Se puede ser buen profesional, pero para ser excelentes debe tener implicación, sensibilidad y sobre todo ser buena persona», insistió.

El comisario jefe del cuerpo de Mossos, Josep Lluís Trapero, quiso destacar la importancia de este acto por tratarse de un reconocimiento público de la labor meritoria y de colaboración en pro de la seguridad.

Las menciones en el ámbito de la Seguridad Privada de Cataluña se crearon para reconocer la contribución del sector de la seguridad privada, en coordinación con la policía de la Generalidad y las policías locales, garantizar un sistema de seguridad de Cataluña más eficaz y eficiente. En definitiva, se quieren reconocer acciones meritorias, actuaciones humanitarias, trayectorias profesionales, excelencia en el cumplimiento de las funciones y, especialmente, la colaboración por parte del sector de la seguridad privada con el cuerpo de Mossos y las policías locales de Cataluña. En el acto se otorgaron un total de 54 menciones: 5 condecoraciones honoríficas, 40 distinciones honoríficas, 4 placas de honor, yy 5 diplomas.

Risco Group ha crecido un 17,22% en Iberia respecto a 2015

RISCO Group, empresa especializada en soluciones integradas de seguridad, ha incrementado su facturación anual en España y Portugal un 17,22% respecto al año 2015, y ha crecido un 180% desde 2012, año en el que comenzó a trabajar con soluciones en nube.

Risco Group es una compañía que lleva en Iberia desde finales de 2004. En 2012 apostó por hacer converger todas sus soluciones a la nube, lo que ha hecho que las ventas hayan ido creciendo de manera exponencial al adaptarse e incluso adelantarse a las necesidades del mercado.

«Estos resultados reflejan el buen momento que está viviendo la compañía, propiciado por el compromiso de RISCO Group para desarrollar y entregar productos innovadores», comenta Borja García-Albi, vicepresidente en Iberia y Latinoamérica en Risco Group.

En 2016 Risco Group sigue creciendo ya que ha tenido un incremento en sus ventas del 17,22% con respecto al año pasado, por lo que ha superado las expectativas de crecimiento anual con respecto al 2015, que tenían al comenzar el año.

«Este año ha sido importante para nosotros ya que hemos lanzado al mercado algunas novedades como la nueva central de Grado 3 ProSYS™ Plus de hasta 512 zonas integrada en la nube y nuestra nueva solución de Smart Home que nos ayudará a seguir creciendo este año», concluye García-Albi.

Mobotix y Advantech integran soluciones de vídeo para el sector transporte

MOBOTIX, fabricante mundial de sistemas en red de videovigilancia de cámaras megapíxel, y Advantech proporcionarán soluciones inteligentes integradas para la videovigilancia y aplicaciones en el sector del transporte. Advantech es un proveedor mundial de soluciones de automatización industrial e integrada, que se incorporarán en las cámaras Mobotix para aplicaciones de vídeo en servicios de transporte público, vehículos de servicios de emergencia y el transporte de mercancías.

Algunos ejemplos de aplicación son el recuento de pasajeros, la creación de mapas de calor y el control de multitudes. Se mostró en la feria InnoTrans 2016 en Berlín, el pasado 20 al 23 de septiembre en el stand de Advantech.

Sector del transporte y la logística

Advantech proporciona soluciones de automatización y sistemas integrados en el sector del transporte y la logística desde 1983. Se componen de ordenadores industriales certificados y sólidas pantallas. En respuesta a una creciente demanda de videovigilancia y aplicaciones, Advantech Europe ha iniciado una estratégica colaboración con Mobotix, fabricante de cámaras IP inteligentes de alta resolución y sistemas de gestión de vídeo (VMS). Ejemplos de aplicaciones que se benefician de esta colaboración: la vigilancia del transporte de personas y mercancías, el transporte de dinero y objetos de valor y los proveedores de servicios.

Grupo Quantum: nuevo delegado en Levante

GRUPO Quantum ha incorporado a Pablo Aparicio como nuevo delegado de Levante. Su gran experiencia en el sector de seguridad unido al amplio porfolio de grandes marcas que representa Grupo Quantum hace de Pablo un referente en el mercado de Seguridad en Levante.

@asLAN alcanza las 100 empresas asociadas

LA Asociación ha alcanzado uno de los objetivos estratégicos que la Junta Directiva había establecido hace unos años para conseguir incrementar la representatividad, y con ello el potencial de influencia y alcance tecnológico de las actividades realizadas.

Con esta base de 100 empresas asociadas, que incluye desde fabricantes líderes internacionales, hasta integradores especializados pasando por los principales centros de datos, proveedores de servicios, operadores de telecomunicaciones y mayoristas de valor añadido, la Asociación @asLAN considera que está en una excelente posición para divulgar en España las últimas innovaciones tecnológicas e impulsar el papel de las TIC y sus profesionales en el gran fenómeno de la Transformación Digital.

Ecosistema de socios tecnológicos

Markel Gruber, presidente de la Asociación, señala que «El cliente necesita rodearse de un ecosistema de socios tecnológicos que le acompañen en este proceso de Transformación. Ahora más que nunca la tecnología es un elemento clave en la generación de valor y ventajas competitivas para las empresas».

A un mes de ASLAN2017 (15 y 16 de Marzo), el Congreso anual, que se celebrará en el Palacio Municipal de Congresos de Madrid, girará en torno a tres polos de innovación tecnológica: 1. Network & IoT & DataCenter, 2. Cloud & Mobility & Collaboration, 3. Security & Analytics & Digital Identity.

INCIBE: Más de un centenar de asistentes en el «Venture Day»

Más de un centenar de inversores, emprendedores y profesionales de la ciberseguridad asistieron el pasado 17 de enero en Madrid a la jornada Venture Day, organizada por el Instituto Nacional de Ciberseguridad (INCIBE), organismo dependiente del Ministerio de Energía, Turismo y Agenda Digital, a través de la Secretaría de Estado de Sociedad de la Información y la Agenda Digital. La jornada sirvió como clausura del Certamen de Emprendimiento Incubadora Ciberemprende 2016, cuyo objetivo es la creación y aceleración de startups de ciberseguridad.

El director general de INCIBE, Alberto Hernández, que inauguró el encuentro, aseguró que «los programas de apoyo a emprendedores están teniendo una gran acogida, teniendo los proyectos seleccionados un elevado potencial para convertirse en líderes internacionales en su área», al tiempo que añadió que «la ciberseguridad se ha convertido en un área de inversión prioritaria en las empresas».

La ciberseguridad crece en España a un ritmo del 12%, «Es un sector altamente competitivo, lo que requiere de una aproximación y estrategia internacional, pero estamos muy bien situados debido al gran talento que existe en nuestro país y la orientación de la innovación a las necesidades específicas que demanda el mercado», explicó el máximo responsable de INCIBE.

En la jornada se presentaron los diez proyectos finalistas del Certamen de Emprendimiento 2016 Ciberemprende. El proyecto ganador ha sido Techvolucion, una solución que permite identificar modelos y patrones en el fraude con inteligencia artificial.

Coincidiendo con la celebración de esta jornada, se ha puesto en marcha el programa de aceleración en ciberseguridad para 2017, que abandera el Ministerio de Energía, Turismo y Agenda Digital, que tendrá un alcance de carácter internacional, bajo la denominación Cybersecurity Venture, organizado por INCIBE y que cuenta con la colaboración de los organismos citados anteriormente.

Los objetivos de este programa de aceleración en el que podrán participar empresas de reciente constitución o promotores a título individual con compromiso de constituir una empresa son incentivar el desarrollo de nuevas empresas de base tecnológica en el ámbito de la ciberseguridad y apoyar al talento emprendedor en la maduración de sus proyectos empresariales.

Contactos de empresas, p. 7

Dallmeier: cámara 4K Ultra HD

Con la nueva DDF5400HDV-DN, Dallmeier presenta una cámara 4K con resolución Ultra HD. Gracias a la resolución extremadamente alta, las cámaras de la serie Ultraline proporcionan imágenes aún más nítidas con aún más detalles.

La serie de cámaras DDF5400HD Ultraline ha sido desarrollada especialmente para aplicaciones que requieren imágenes de muy alta resolución en tiempo real. La cámara se ofrece con un objetivo integrado en una carcasa antivandálica tipo domo.

La alta resolución del sensor y el sofisticado procesamiento de imagen permiten imágenes en tiempo real con resolución UHD con una tasa de imágenes de hasta 25/30 ips (2160p/30) en una calidad excelente. Por ello, la cámara es idónea en condiciones que requieren la captación de los más finos detalles en tiempo real. La cámara está dotada con un sensor de luz ambiental y un filtro de corte IR removible, y puede conmutar automáticamente entre los modos día y noche. Además, es posible definir y adaptar en los ajustes de exposición diferentes preconfiguraciones para día y noche.

La cámara dispone de un objetivo varifocal megapíxel motorizado que está perfectamente adaptado al sensor de imagen. El ajuste de zoom, enfoque y diafragma se realiza cómodamente a través de un navegador web. No es necesario el ajuste manual del objetivo directamente en el lugar de montaje de la cámara.

El novedoso control de diafragma P-Iris proporciona un ajuste preciso y automático de la apertura óptima del diafragma. Con él, bajo casi todas las condiciones de luz, la cámara consigue una profundidad de campo notablemente mejor que con los objetivos DC-Autoiris convencionales.

La cámara está dotada de una memoria RAM que la función EdgeStorage utiliza para el almacenamiento del flujo de vídeo en caso de caída de red. Cuando la red está restablecida, la función SmartBackfill se encarga de la rápida transmisión de las imágenes grabadas al sistema de grabación SMAVIA.

Grupo IPTecno: servidor radar integrado en sistema de intrusión Mass Server IPtecno

Grupo IPTecno ha presentardo el servidor, exclusivo de IPTecno, Mass Server para la integración de radares Magos y cámaras PTZ asociados a sistemas de intrusión y Central Receptora de Alarmas.

Mass Server es un servidor de grado industrial de bajo mantenimiento, sin ventiladores, ideal para instalación en campo, que incluye el software servidor de radares Magos para conexión remota via webserver desde el cliente de monitorización e integación via IP de las cámaras domo o sistemas de posicionamiento PTZ, así como la nueva integración IPTecno para sistemas de intrusión y Central Receptora de Alarmas.

Con este desarrollo, los radares Magos, distribuidos en exclusiva por IPTecno, se convierten en el mejor sistema de detección perimetral exento de falsas alarmas para sistemas desatendidos. Son ideales para grandes instalaciones al aire libre como zonas portuarias, embalses, subestaciones eléctricas y de gas, campas de vehículos, instalaciones fotovoltaicas y todo tipo de instalaciones críticas donde el videoanálisis u otros sistemas de intrusión resultan en un foco de falsas alarmas.

Hanwha Techwin: nueva cámara ojo de pez 360 grados Samsung Wisenet P 4K

Con el lanzamiento de la cámara Samsung Wisenet 4K PNF-9010R, Hanwha Techwin declara su intención de establecer un nuevo estándar para las cámaras ojo de pez de 360 grados.

La cámara PNF-9010R 360 grados de 12 megapíxeles, con corrección esférica ojo de pez integrada, produce imágenes de una altísima calidad. Ofrece varios modos de visualización alternativos: vista panorámica sencilla, vista panorámica doble y modo cuadrante. Además, la cámara PNF-9010R tiene muchas otras prestaciones que hacen que este modelo destaque entre otros similares. Las más relevantes son:

Además de proporcionar una poderosa herramienta para disuadir las actividades delictivas, la cámara PNF-9010R permitirá a los usuarios obtener muchos más beneficios. En lugares de venta minorista, por ejemplo, el conteo de personas ofrece la oportunidad de dimensionar la eficiencia de la tienda comparando la afluencia de clientes con las ventas reales, ayudando además a identificar los días, horas y épocas de mayor afluencia para gestionar los picos y valles de flujo de clientes en las cajas. El mapa de calor proporciona información precisa sobre el comportamiento de los clientes en la tienda; muestra puntos calientes dentro del establecimiento para indicar los patrones de compra de los clientes y el tiempo que permanecen en la tienda.

Al igual que ocurre en todos los modelos de cámaras de la serie Wisenet P, la PNF-9010R cuenta con compresión H.265 y WiseStream, una tecnología complementaria de compresión que controla de forma dinámica la codificación, buscando el equilibrio entre calidad y compresión de acuerdo al movimiento en la imagen.

La eficiencia del ancho de banda se mejora hasta en un 75%, en comparación con la actual tecnología H.264, cuando se combina WiseStream con la compresión H.265.

Tyco anuncia soluciones para la protección del pequeño comercio

Según los datos del «Estudio sobre la experiencia de compra de los españoles», realizado por Tyco, empresa mundial en soluciones de seguridad y rendimiento para el retail, para los españoles es muy importante a la hora de comprar, la primera impresión que reciben de un comercio. El 61% cuando ve un escaparate llamativo y original decide entrar en la tienda. Por ello es importante que la instalación de medidas de seguridad no afecte a la apariencia y estética del establecimiento. El hurto afecta directamente a la rentabilidad y el crecimiento de los comercios, pero lo hace, aún más, cuando hablamos de la pequeña y mediana empresa. La pérdida desconocida supone de media una merma para el comercio del 1,33% de su facturación, según los datos del sector. Los sistemas antihurto ayudan a prevenir esta pérdida y al mismo tiempo contribuyen a aumentar las ventas de la tiendas, produciendo un valor añadido para el comercio.

Para hacer frente a estos problemas, Tyco ofrece protección antihurto con tecnología acustomagnética de alta gama, a un precio al alcance de todos los pequeños minoristas. El sistema antihurto Essentials es un sistema sencillo y fiable capaz de proteger cualquier tipo de producto, que permite el control del hurto a la vez que proporciona una experiencia agradable en el proceso de compra. La marca Sensormatic de Tyco garantiza la fiabilidad con más de 50 años de experiencia en el mercado con soluciones de protección electrónica de artículos (EAS). De esta manera se consigue que el empleado esté más centrado en la atención al cliente y no en vigilar a posibles hurtadores.

Mobotix: soluciones de radiometría térmica

Mobotix, fabricante mundial de sistemas en red de videovigilancia de cámaras megapíxel, ofrece su tecnología térmica más avanzada hasta la fecha, con el lanzamiento de la última serie de modelos de cámara de radiometría térmica (TR) de Mobotix (M15 y S15).

En procesos industriales de temperatura crítica, la radiometría térmica puede proporcionar una advertencia a tiempo para prevenir incidentes con efectos potencialmente catastróficos. Esto puede resultar crucial en la industria pesada y en los sectores mineros. También puede ser indispensable en la supervisión de máquinas en instalaciones industriales y centrales eléctricas, subestaciones y componentes de líneas eléctricas.

Utilizando ventanas de TR (radiometría térmica), o la imagen completa del sensor térmico de la cámara, es posible definir fácilmente hasta 20 activadores de temperatura para detectar posibles incendios o fuentes de calor peligrosos. También es posible calibrar los sensores térmicos a fin de evitar la interferencia de factores ambientales, como la reflexión o la temperatura del aire, lo que los hace más precisos que nunca.

El sensor térmico Mobotix mide rangos de temperatura de -40 °C a + 550 °C, con una resolución térmica de ±0,2 °C (50 mK). Si la temperatura es inferior o superior a los límites o rangos de temperatura predefinidos, se activa automáticamente una alarma. Entonces, se puede obtener una vista en vivo de la zona afectada. Las imágenes se pueden ver desde un centro de supervisión de alarmas, a través de un navegador web o mediante la aplicación de Mobotix, dependiendo de cómo se hayan instalado las cámaras. Esto facilita el inicio de una intervención y también permite una supervisión de las instalaciones remota y rentable.

Los sistemas de cámaras térmicas duales de Mobotix contienen un sensor térmico y un sensor de imagen estándar. Esta característica permite una superposición térmica sobre las imágenes regulares, lo que contribuye a localizar los puntos calientes en la imagen visual y prevenir daños mayores.

Las cámaras exteriores de Mobotix, como la M15 y la S15, también resultan ideales para ubicaciones exteriores.

Euroma: nuevo control horario C2 PRO

Euroma Telecom, como representante de la firma Anviz, ha presentado el nuevo control horario C2 PRO. La nueva gama de control horario ofrece una solución completa para una optimización de los recursos humanos.

El nuevo C2 Pro es un terminal para control horario de última generación, equipado con un altamente eficiente procesador Dual Core de 1 Ghz además de una memoria de 512 M DDR3, lo que permite un rápido análisis de las huellas y una comparación rápida de la base de datos interna en menos de 0,5 seg.

El equipo posee un monitor TFT color de 3,5" para una mejor visualización y un uso más cómodo. El dispositivo posee tres formas de identificación: Mediante teclado con la introducción de una contraseña, mediante tarjeta RFID o mediante el análisis biométrico de la huella dactilar, estas identificaciones pueden ser exigidas independientemente o podemos requerir a algunos usuarios, para una mayor seguridad combinar dos elementos: contraseña + huella, tarjeta + huella.

El sistema dispone de 1 salida de relé para apertura de puerta, haciendo que el dispositivo pueda además de realizar un control horario, realizar un control de acceso.

By Demes anuncia la nueva generación de productos Hyundai

Hyundai Corporation ha lanzado una amplia e innovadora gama de soluciones en sistemas de seguridad CCTV, a través de su distribuidor europeo exclusivo, By Demes Group, especialista en tecnologías de seguridad con sede en España y presente en múltiples países del mercado europeo.

En su larga trayectoria, Hyundai siempre ha trabajado para ofrecer las propuestas tecnológicas más avanzadas y satisfacer los requisitos más exigentes de todos los mercados en los que opera. Estos compromisos globales han ocasionado que la marca, tras una primera generación de cámaras y grabadores de seguridad, haya diseñado una nueva generación de productos más potentes y tecnológicamente superiores denominados Hyundai Nextgen.

Estos productos proporcionan la capacidad de adaptarse a cualquier tecnología disponible en el mercado actual, gracias a sus cámaras 4 en 1 (4 tecnologías: HDTVI, HDCVI, AHD, CVBS), a sus cámaras IP H.264+ y a sus grabadores ZVR 5 en 1 (5 tecnologías: IP, HDTVI, HDCVI, AHD, CVBS). En efecto, este concepto penta-híbrido será a partir de ahora un estándar en todos los grabadores ZVR de Hyundai, convirtiéndose en la solución perfecta para asegurar una plena compatibilidad entre sistemas analógicos HD, así como el Onvif ha sido para las cámaras IP.

Otra de las innovaciones de los equipos Nextgen diferenciales del mercado es la resolución 4K de las cámaras IP en codificación H.264+, para un ahorro de hasta el 70% del ancho de banda respecto al H.264 convencional, además de la nueva resolución de 3MP en sistemas HD-TVI o hasta 5MP en próximas versiones. Asimismo, las cámaras 4 en 1, con conmutación por dip-switch, ya incluyen en modo TVI hasta 3MP con un aumento de resolución que ofrece más detalles para una imagen más nítida.

También cabe destacar el nuevo software HYU-VMS para la gestión de hasta 256 dispositivos o más de 1.200 cámaras. La gama Hyundai también sigue ofreciendo las alarmas Smart4Home y la solución de videoporteros, intactas tras su buena acogida inicial, aunque con las mejoras pertinentes de las actualizaciones, las cuales añaden pequeñas funciones y mayor rendimiento al sistema.

Vivotek: nuevo domo antivandálico multi-sensor, El MS8392

Vivotek, proveedor mundial en vigilancia IP, ha presentado la nueva cámara tipo domo antivandálica MS8392-EV, para ampliar su línea de producto multi-sensor. Basándose en los logros de la cámara exterior MS8391-EV, la nueva cámara MS8392-EV ofrece una solución todo-en-uno, contando con cuatro sensores CMOS de 3 megapíxeles, vistas panorámicas de 180 grados y renovada con un nuevo diseño estético. En las áreas amplias que requieren cobertura detallada, tales como estacionamientos, centros comerciales, escuelas, parques y plazas, esta permite maximizar el campo de visión y reducir el número de cámaras necesarias, brindando un ahorro en tiempo de instalación y costos de mantenimiento.

Especialmente equipado con una función de alineación de vídeo, el MS8392-EV permite a los usuarios optimizar la calidad de la imagen de cada sensor y la experiencia de vistas panorámicas continuas naturales y óptimas. También está equipado con un filtro de corte IR removible y tecnología WDR mejorado para brindar protección día y noche y ampliar la visibilidad de la imagen en condiciones de iluminación de alto contraste.

Dahua: el nuevo software Back-end ANPR amplía la solución ANPR con más calidad y fiabilidad

Dahua Technology, fabricante y proveedor mundial de productos de videovigilancia con sede en Hangzhou, China, ha presentado el DHI-IVS-T7000-R-PRO, el software de back-end ANPR.

DHI-IVS-T7000-R-PRO proporciona un avanzado procesamiento digital de imágenes. Al ser instalado en un servidor específico, puede reconocer automáticamente el número de matrícula del vehículo e información relacionada usando la tecnología de seguimiento de posición de matrícula, y de segmentación y reconocimiento de caracteres.

Ventajas

En comparación con el sistema front-end ANPR, el servidor instalado en el DHI-IVS-T7000-R-PRO puede reconocer placas de matrícula de más de 100 países con mayor precisión y menor tiempo de procesamiento.

Aplicaciones

El software back-end ANPR ofrece una solución completa de ANPR cuando se instala en un servidor específico y se combina con el ITC de front-end de Dahua y el sistema de gestión DSS. Al recibir imágenes de las cámaras frontales, el DHI-IVS-T7000-R-PRO hace el reconocimiento y muestra el resultado del reconocimiento en el programa cliente del servidor DSS. La solución Dahua ANPR combina inteligencia, eficiencia y facilidad de uso en sistemas avanzados de videovigilancia, y proporciona un alto nivel de seguridad. Por lo tanto, es ideal para aplicaciones ANPR de alto volumen, así como para vigilancia de tráfico, aparcamiento y reconocimiento de placas de entrada y salida.

Aumento de la eficacia para el cliente

El mercado mundial de videovigilancia continúa avanzando hacia soluciones inteligentes y seguras. Además de la cámara integrada en la solución ANPR, Dahua ahora ofrece más opciones a los clientes con esta versión del DHI-IVS-T7000-R-PRO. Esta versión es particularmente especial para Dahua porque expande la escala y la eficacia de la solución ANPR a un nivel superior.

Características técnicas

- Software de reconocimiento de núcleo.
- Soporte para reconocer imagen 1080P.
- Los datos reconocidos de cada imagen incluyen:
  - Número de matrículas (hasta 3 en la misma imagen).
  - País, número de matrícula, fecha y hora, ID de la cámara.
  - Posición de la placa en la imagen.
- Soporte en más de 100 países.
- Alta fiabilidad de reconocimiento.

3M España: 3M Novect 1230 Fluid protege los tesoros del mundo

Los archivos y los museos albergan algunos de los documentos y las obras de arte más valiosos, delicados e irreemplazables. La protección de estos objetos supone una prioridad y, por esta razón, las instituciones disponen de sistemas avanzados anti-incendios. Sin embargo, el fuego no es el único riesgo, ya que la humedad puede convertirse en el mayor enemigo.

3M España apuesta por dos opciones finales: los HidroFluoroCarbonos (HFC), usados hace años como reemplazo a los halones, y 3M™ Novec™ 1230 Fire Protection Fluid, una solución innovadora de próxima generación.

El fluido Novec 1230 dota de numerosas ventajas, ya que es un agente limpio y seguro y no deja residuos, respondiendo a las necesidades de las aplicaciones más exigentes, como sucede en museos, bibliotecas y archivos.

Este agente sostenible de 3M, que ha sido diseñado para remplazar HFC e HidroCloroFluoroCarbonos (HCFC), se distingue por unas excelentes características ambientales, como un global warming potential (GWP) inferior a 1 y una permanencia en la atmósfera de menos de cinco días, y contribuye a minimizar las emisiones de CO_2 y cumplir los estándares de seguridad nacionales e internacionales.

Bosch lanza Video Management System 7.0

Bosch acaba de lanzar el software Bosch Video Management System 7.0 (Bosch VMS 7.0), que permitirá a los operarios de seguridad gestionar de manera eficiente los flujos de vídeo de alta resolución en su trabajo cotidiano.

El sector de las cámaras de vídeo está evolucionando a un ritmo muy rápido, y el volumen de datos de vídeo de alta resolución no para de crecer, por lo que gestionarlos y hacer un seguimiento de ellos supone todo un reto. En algunos lugares como las estaciones de metro y los aeropuertos, donde se necesitan muchas cámaras, la carga que se ejerce sobre la estación de trabajo es muy elevada. Y, si una estación de trabajo se sobrecarga, es muy probable que la aplicación del cliente sufra retardos.

Esto supone un enorme obstáculo para los operarios de seguridad que tienen que visualizar muchas cámaras a la vez para poder mantener una visión general completa e ininterrumpida de un lugar, como la terminal de un aeropuerto.

Ahora, con el nuevo software Bosch VMS 7.0, el usuario puede tener varias cámaras de ultra alta definición (UHD) abiertas sin que la aplicación se ralentice. Bosch VMS 7.0 emplea la tecnología de «streamlining», que se caracteriza por mostrar automáticamente la resolución óptima de vídeo en la pantalla. Si un operario necesita ver varias cámaras al mismo tiempo, Bosch VMS 7.0 usa automáticamente un flujo de resolución más baja. Y si es necesario ampliar imágenes mejoradas o verlas a pantalla completa, se selecciona un flujo de resolución más alto automáticamente. Esta función emplea las capacidades de múltiples flujos de las cámaras vídeo IP de Bosch y funciona en las estaciones de trabajo existentes.

Otra función nueva de Bosch VMS 7.0 es la comunicación cifrada entre las cámaras de Bosch y el sistema de gestión Video Management System.

Anatronic: cámara IP PoE IR 1080p para sistemas de videovigilancia

Planet Technology, empresa representada en España, Portugal y Chile por Anatronic, S.A., ha anunciado la disponibilidad de dos nuevas cámaras IP PoE IR con resoluciones Full HD 1080p a 30 frames por segundo (fps) para garantizar la identificación de personas y objetos en sistemas de videovigilancia. Los modelos ICA-3250 (tipo bala) e ICA-4250 (domo) incorporan sensor de imagen CMOS super low lux Sony Exmor de 1/2.8", lente de 3.6 mm con iris fijo e iluminadores infrarrojos (IR) con alcance de 25 y 20 metros, respectivamente.

Estas unidades con resolución de hasta 1920 x 1080 también destacan por compresión de vídeo H.264, alarma de detección de movimiento y facilidad de configuración mediante interfaz web.

Ambas cámaras con cubierta IP-66 (impermeable) han sido diseñadas para operar en entornos adversos (con temperatura entre -10 y +50 °C). Se pueden instalar en espacios públicos, como edificios, jardines, aparcamientos, galerías y mercados, estaciones de autobuses y ferrocarriles, aeropuertos y hospitales.

A la hora de adaptarse a los cambios constantes en las condiciones de iluminación durante el día y la noche, las unidades ICA-3250 e ICA-4250 se benefician de las prestaciones del sensor Sony de 0.01 lux y de los iluminadores IR para poder ofrecer vídeo a color cuando hay suficiente luz y en blanco y negro en situaciones de oscuridad. De esta forma, proporcionan imágenes nítidas las 24 horas del día.

Synology presenta DiskStation DS3617xs

Synology® Inc. ha lanzado al mercado DiskStation DS3617xs, un servidor NAS de 12 bahías escalable hasta 36 unidades de disco. Ofrece un alto rendimiento a más de 2.358 MB/s de lectura, y facilita un despliegue rápido para simplificar el trabajo a las empresas de mayor tamaño.

Equipado con una CPU de cuatro núcleos Intel Xeon-D de 2,2 GHz, que puede alcanzar los 2.7 GHz, el DS3617xs ofrece un rendimiento impresionante con más de 2.358 MB/s de lectura secuencial, y lectura de 406.760 IOPS en una configuración RAID 5 con Link Aggregation de 10GbE habilitado. DS3617xs viene con una ranura PCIe 3.0 que admite una tarjeta de interfaz de red (NIC) de alta velocidad.

«Hemos visto un fuerte interés y demanda de nuestros clientes en este modelo de NAS de escritorio, que ofrece un despliegue ágil y sencillo y con escalabilidad flexible», dijo Michael Wang, Product Manager de Synology Inc. «Hemos duplicado la capacidad de memoria RAM por defecto de DS3617xs a 16GB, para permitir una capacidad de actualización de hasta 48GB para que las empresas la utilicen».

El DS3617xs está diseñado para hacer frente al crecimiento futuro sin esfuerzo. Con dos unidades de expansión, Synology DX1215 conectadas, DS3617xs se puede escalar inmediatamente hasta 36 unidades. DS3617xs también proporciona soluciones de almacenamiento sin fisuras para entornos de virtualización como VMware, Citrix, Hyper-V y OpenStack.

DS3617xs funciona con DiskStation Manager (DSM), el sistema operativo más avanzado e intuitivo para dispositivos de almacenamiento conectados en red que ofrece una amplia gama de aplicaciones para mejorar la productividad en el trabajo. DSM ha obtenido la clasificación general más alta en la 10ª encuesta de los Premios de Calidad de TechTarget para sistemas NAS de rango medio, y recibió el premio PC Mag Business Choice durante cinco años consecutivos.

Avitom: cámaras IP-Nube inteligentes para hogares, tiendas y oficinas

Avitom, empresa especializada en el uso de la tecnología y la especialización en el asesoramiento, diseño, programación e integración de los diferentes sistemas de control, presenta la nueva gama de cámaras IP-Nube inteligentes que está especialmente indicada para integrarse en sistemas de seguridad y vigilar los bienes más valiosos: bebés, personas mayores y mascotas.

Disponibles en versiones para interiores y exteriores, estás cámaras «confort» se pueden instalar fácilmente en hogares, tiendas y oficinas. Al tratarse de unas soluciones plug-and-play, sólo se necesita descargar la aplicación (app) para comenzar a beneficiarse de las prestaciones de estos productos de alto rendimiento.

La imagen de la cámara se puede visionar a través de terminales inteligentes con muy diversas funciones como zoom digital y alarma en caso de movimiento o emergencia. Varios usuarios pueden ver la imagen de la misma cámara sin perder claridad. Las características comunes de los nuevos modelos incluyen alta resolución (hasta 1080P UHD), audio de dos vías para poder comunicarse con familiares, compañeros de trabajo o personal de seguridad, capacidad de visión nocturna (IR-Cut), conexión Smart Wi-Fi (sin necesidad de cable de red) y compatibilidad con los sistemas operativos Android, iOS y PC.

By Demes: PeepALL, la app revolucionaria que permitirá controlar las alarmas Paradox con las cámaras Dahua de forma combinada

By Demes Group lanza PeepAll, la primera aplicación que permitirá al usuario tener acceso a su sistema de alarma Paradox asociado a sus sistemas de videovigilancia Dahua para una verificación inmediata y eficaz.

En un país líder en el uso de smartphones y cuyo hábito ya es mayor que el de los ordenadores de sobremesa, son muchas las aplicaciones móviles que se han vuelto imprescindibles en la vida de sus ciudadanos. Un claro ejemplo son las app de control de sistemas de seguridad, pues permiten vigilar con un solo dedo y a distancia lo que sucede en los lugares más valiosos.

Son muchos los usuarios finales que ya disponen tanto de sistemas de alarma como de sistemas de videovigilancia en sus inmuebles, y que pueden gestionarlos mediante dos aplicaciones independientes para cada tipo de producto.

Pero By Demes Group, con ánimo de simplificar y mejorar la experiencia de los usuarios, ha desarrollado una única aplicación denominada PeepAll, a través de la cual el cliente final será capaz de gestionar tanto su sistema de alarma Paradox (EVO, SPECTRA SP y MAGELLAN) como sus sistemas de videovigilancia Dahua (IP y HDCVI). De hecho, al tratarse de una aplicación dinámica, próximamente se irán integrando otras marcas distribuidas por la compañía.

Entre sus funciones más notorias, PeepAll permite el armado y desarmado del sistema de alarma, alertando de ello al usuario mediante notificaciones push en tiempo real en su smartphone. También permite el control total del sistema de alarma (armado parcial del sistema, anulación de zonas, control de salidas programables, revisión del historial de eventos, etc.). Y lo más destacable, la aplicación notifica la alarma asociada con las cámaras o grabadores en tiempo real para su videoverificación. Después de un proceso de integración y desarrollo exhaustivo por los ingenieros de By Demes Group, PeepAll se presenta en el mercado como la única aplicación móvil de seguridad y vigilancia que integra varias marcas combinando por fin intrusión con CCTV. Se trata de la última y más ambiciosa app de la compañía que complementa el resto de aplicaciones profesionales lanzadas en los últimos años (CCTV EVO Plus, ASSS, HYU CMS, etc.) para liderar el mercado de la seguridad electrónica en Europa.

Honeywell: amplía su gama de cámaras IP y mejora las prestaciones del NVR Maxpro

Honeywell ha presentado nuevos productos de vídeo que ayudan a los profesionales de la seguridad a diseñar soluciones para edificios conectados. La compañía ha añadido nuevos modelos de cámaras IP a la ya conocida serie equIP, que ofrecen una excelente calidad de imagen incluso en condiciones de escasa iluminación. Asimismo, se ha lanzado la última versión (4.0) del NVR Maxpro, que permite almacenar y localizar vídeo archivado de manera más rápida, además de ofrecer un sistema completamente integrado que facilita la instalación.

Honeywell también ha presentado los nuevos domos de exterior de la serie HDZ PTZ antivandálicos, con IRs, que ofrecen una calidad de imagen superior para entornos de muy baja iluminación. Las cámaras equIP, los domos PTZ de la serie HDZ y los NVR Maxpro se integran perfectamente con los productos de Honeywell y también de otros fabricantes para crear una solución IP completa y totalmente integrada. La utilización del monitor de estado del NVR Maxpro permite comprobar más fácilmente el estado del sistema.

Además, las nuevas cámaras equIP se instalan más rápido gracias a la ayuda on-line y a la función de zoom motorizado.

Tesa: Smartair™ Pro Wireless Online: el control de acceso en tiempo real ahora a tu alcance

La seguridad en tiempo real ha sido uno de los mayores retos para los sistemas de control de accesos. Hasta ahora. El nuevo sistema SMARTair™ Pro Wireless Online te mantiene informado de todo lo que sucede en tu edificio –quién entra, dónde y cuándo– permitiéndote controlar el estado de seguridad de tu edificio en tiempo real. Es un sistema inalámbrico muy simple de instalar que proporciona un ahorro significativo de energía para los clientes. Un avanzado software de gestión permite al administrador controlar el sistema desde múltiples dispositivos, desde cualquier sitio y en cualquier momento.

La nueva solución de SMARTair™ es un sistema de control de accesos inteligente que funciona mediante una comunicación bidireccional, encriptada y segura que ofrece seguridad y comodidad para todos los usuarios de un edificio. Los dispositivos inalámbricos de SMARTair™ se comunican mediante tecnología de radiofrecuencia habilitada por Hubs de gestión TCP/IP, que posibilitan la comunicación entre el servidor central y cada una de las puertas a controlar. Con SMARTair™, los administradores del sistema pueden abrir las puertas desde cualquier lugar, configurar los permisos de acceso de los usuarios de forma remota o recibir registros de los dispositivos en cualquier momento.

Y esto solo es el principio. Smartair™ Pro Wireless Online ofrece una seguridad, un acceso y un uso inteligentes para cualquier edificio, ya sea pequeño, mediano o grande.

Este nuevo sistema inteligente de seguridad proporciona un registro del historial en tiempo real y desde cualquier lugar. Los gestores de la instalación pueden cambiar los permisos o los horarios de acceso al instante desde el ordenador o desde el acceso web, bloquear o desbloquear una puerta de forma remota a través de un clic, o recibir alertas en el email cuando las baterías de una puerta están cerca de agotarse, cuando hay un intento de intrusión o cuando alguien ha dejado una puerta abierta. La seguridad del edificio no se ve comprometida gracias a la encriptación de principio a fin entre el servidor, la puerta y los dispositivos inalámbricos, que funcionan incluso cuando se cae la red.

Lilin: nuevas cámaras IP HD con IR 2MP

La nueva cámara IP de 2 megapíxel ZR8022 está integrada en un nuevo chasis con una potente lente auto focus. Esta lente permite ajustar el zoom mediante los controles del explorador. Dos versiones disponibles; la versión ZR8022X20 (20X) con lente de 4.7-90mm y la versión ZR8022X10 (10X) con lente 5-50mm. estándar.

La ZR8022 incorpora Sense Up+, la tecnología exclusiva de Lilin que proporciona un vídeo increíble en condiciones de baja iluminación. Con un sensor de imagen inteligente, control AGC y reducción de ruido 3D.

Con la tecnología wide dynamic, la cámara captura las luces y las sombras simultáneamente eliminando la pixelación y el ruido. Combinado con la reducción de ruido 3D y la reproducción del tono adaptativo, el contraste de las imágenes con brillo/oscuridad se ven significativamente mejoradas.

IPTV: cámara IP tipo bala panorámica de 6Mpx

IPtv ha anunciado la disponibilidad de una cámara IP tipo-bala panorámica de 6 Mpx de Secubest, que está especialmente indicada para su uso en sistemas de vigilancia digitales.

El modelo NBM2-H6, que es compatible con las soluciones de gestión de vídeo de Network Optix, se distingue por necesitar una sola licencia para beneficiarse de sus prestaciones en proyectos de videovigilancia.

La nueva cámara panorámica cuenta con tres sensores CMOS de 2 M (resolución de 1920 x 1080) y una lente fija de 4.3 mm que proporcionan un campo de visión (FOV) con soporte panorámico de 180°.

La NBM2-H6 soporta zoom digital con paneo digital y con parámetros preseleccionados, y puede rendir con hasta cuatro flujos de perfil para responder a diferentes propósitos y crear zonas programables.

Saborit: nueva versión de DrugWipe 5 S, test de saliva para la detección del consumo de drogas

Saborit ha lanzado al mercado una nueva versión del test de drogas DrugWipe 5 S®, con dos mejoras destacables: permite obtener resultados en un máximo de 5 minutos, además de proporcionar resultados más visibles, al aparecer las líneas de resultados, distintivas para cada tipo de droga, de forma más clara y legible.

DrugWipe 5 S® es un método indiciario que detecta mediante la saliva el consumo de 5 sustancias estupefacientes (cocaína, marihuana, opiáceos y anfeta-/ metanfetaminas), siendo actualmente el test más utilizado a nivel internacional para el uso en controles policiales de carretera.

Su alta especificidad y fiabilidad (más del 95%), confirmadas mediante estudios de laboratorio, hacen que este test sea el más idóneo para aplicaciones en Seguridad Vial y de Seguridad en el Trabajo.

Concretamente en España, el test está siendo utilizado con gran éxito por la Dirección General de Tráfico (DGT-Guardia Civil), la Policía Local de Madrid, Ertzaintza y la Policía Foral de Navarra, entre otros cuerpos policiales, para detectar el consumo de drogas en conductores.

Los tests DrugWipe S®, fabricados por la empresa alemana Securetec Detektions SystemeAG, son de lectura directa, por lo que no precisan de ninguna máquina lectora adicional para obtener resultados. Son limpios e higiénicos, muy fáciles de usar y no necesitan mantenimiento.

El casete del test está diseñado para un transporte seguro y su tamaño reducido permite llevarlo en el bolsillo del pantalón.

Sony mejora su gama de videovigilancia con las nuevas cámaras en red con sensores CMOS Exmor R

Sony ha anunciado el lanzamiento de ocho nuevas cámaras de videovigilancia Full-HD como complemento de su última gama, que constituye la sexta generación (G6) de la familia de cámaras en red, como respuesta a la creciente demanda del mercado de la videovigilancia para ofrecer una mayor claridad de imagen.

Las nuevas cámaras de videovigilancia de la serie V y E incluyen:

- Serie V: SNC-VB640, SNC-VB642D, SNC-VM641, SNC-VM642R.

- Serie E: SNC-EB640, SNC-EB642R, SNC-EM641, SNC-EM642R.

Gracias a la avanzada tecnología de imágenes, las cámaras de Sony ofrecen a los profesionales de la seguridad detalles nítidos y una mayor visibilidad, gracias a una excelente sensibilidad con poca luz, ideal para una amplia gama de aplicaciones exigentes, entre las que destacan la vigilancia urbana, comercial y el transporte.

Mucho más allá de ilustrar la experiencia de Sony en tecnologías clave, estas mejoradas cámaras de G6 incorporan sensores de imagen de alto rendimiento, objetivos y procesadores de imagen.

Contactos de empresas, p. 7.

ÍNDICE

MATERIALES, EQUIPOS Y SISTEMAS DE SEGURIDAD

- ALARMA Y CONTROL
- BLINDAJES. PRODUCTOS
- CALZADO DE SEGURIDAD
- CENTRALIZACION DE ALARMAS
- COMUNICACIONES
- CONTROL DE ACCESOS. ACTIVO
- CONTROL DE ACCESOS. PASIVO
- DETECCIÓN DE EXPLOSIVOS
- DETECCION DE MATERIALES Y OBJETOS
- EQUIPOS DE PROTECCIÓN INDIVIDUAL
- EVACUACIÓN Y SEÑALIZACIÓN
- EXTINCION DE INCENDIOS
- ILUMINACION DE SEGURIDAD
- INFORMATICA DE SEGURIDAD
- MATERIAL POLICIAL
- PROTECCION CONTRA EXPLOSIONES
- PROTECCION CONTRA INCENDIOS. ACTIVA
- PROTECCION CONTRA INCENDIOS. PASIVA
- PROTECCION CONTRA INTRUSION. ACTIVA
- PROTECCION CONTRA INTRUSION. PASIVA
- PROTECCION CONTRA CONTAMINACION
- PROTECCION CONTRA ROBO Y ATRACO. ACTIVA
- PROTECCION CONTRA ROBO Y ATRACO. PASIVA
- PROTECCION CONTRA VANDALISMO
- PROTECCION DE LA INFORMACION. SEGURIDAD DOCUMENTAL
- PROTECCION PERSONAL
- SANIDAD
- SEGURIDAD LABORAL
- SEGURIDAD VIAL
- VEHICULOS BLINDADOS
- VEHICULOS CONTRA INCENDIOS
- VIGILANCIA POR TELEVISION
- VARIOS. SEGURIDAD ACTIVA
- VARIOS. SEGURIDAD PASIVA

SERVICIOS DE SEGURIDAD

- APLICACIONES INFORMATICAS
- ASOCIACIONES
- CENTRALES DE RECEPCION Y CONTROL
- CUSTODIA DE VALORES
- EVENTOS DE SEGURIDAD
- FORMACION DE SEGURIDAD
- INGENIERIA Y CONSULTORIA
- INSTALACION
- INVESTIGACION PRIVADA
- MANTENIMIENTO DE SISTEMAS
- MENSAJERIA Y TRANSPORTE
- ORGANIZACION Y GESTION
- PUBLICACIONES Y AUDIOVISUALES
- VIGILANCIA Y CONTROL
- TRANSPORTE DE FONDOS Y VALORES
- VARIOS. SERVICIOS DE SEGURIDAD

ALARMA Y CONTROL

Techco Security
C/ Barbadillo 7
28042 Madrid
+34 91 312 77 77
www.techcosecurity.com
tcs@techcosecurity.com

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

Tyco Integrated Fire & Security

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

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

FUNDADA EN 1966
INSTALACIONES A SU MEDIDA
ISO 9001
Antoñita Jiménez, 25
28019 Madrid
Tel.: 91 565 54 20 - Fax: 91 565 53 23
seguridad@grupoaguero.com
www.grupoaguero.com

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

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

Calle López de Neira, nº3, oficina nº 301
36202 Vigo España
Tel.: +34 986 220 857 / 693 422 688
FAX: +34 986 447 337
www.aforsec.com
aforsec@aforsec.com

CONTROL DE ACCESOS ACTIVO

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

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

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

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

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

BIOSYS
(Sistemas de Tecnología Aplicada)

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

bydemes
avanzando juntos hacia el futuro

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

RISTER
PRESENTCO®

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

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

accesor

Soluciones integrales en control de Accesos y seguridad

DDS

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

info@accesor.com
www.accesor.com

DORLET

DORLET S. A. U.

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

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

setelsa link
Sistemas Electrónicos y Telecomunicación S.A.

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

DETECCIÓN DE EXPLOSIVOS

COTELSA

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

TECOSA

TELECOMUNICACIÓN, ELECTRÓNICA Y CONMUTACIÓN

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

TARGET TECNOLOGIA

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

SISTEMAS DE EVACUACIÓN

OPTIMUS
SOUND & COMMUNICATION

OPTIMUS S.A.

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

info@optimus.es
www.optimusaudio.com

PROTECCIÓN CONTRA INCENDIOS. ACTIVA

detnov

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

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

www.detnov.com
info@detnov.com

bydemes
avanzando juntos hacia el futuro

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

aguilera

GRUPO AGUILERA

FABRICANTES DE SOLUCIONES PCI DETECCIÓN Y EXTINCIÓN DE INCENDIOS

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

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

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

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

pefipresa
FIRE, SAFETY & SECURITY

PEFIPRESA, S. A. U

INSTALACIÓN Y MANTENIMIENTO DE SISTEMAS DE SEGURIDAD Y CONTRA INCENDIOS

www.pefipresa.com

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

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

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

El directorio es la zona más consultada de nuestra revista.

Módulo: 660€/año*

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

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

PROTECCIÓN CONTRA INCENDIOS. PASIVA

solexin

Calle Alberto Alcocer, 28, 1º A
28036 Madrid
Tel. 913 685 120
info@solexin.es
www.solexin.es

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

PROTECCIÓN CONTRA INTRUSIÓN. ACTIVA

bydemes
avanzando juntos hacia el futuro

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

DAITEM

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

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

Tecnoalarm
Hi-Tech Security Systems

TECNOALARM ESPAÑA

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

VANDERBILT

VANDERBILT ESPAÑA Y PORTUGAL

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

PROTECCIÓN CONTRA ROBO Y ATRACO. PASIVA

AGA
LA INDUSTRIA DE LA CERRAJERÍA

TELECOMUNICACIONES

Alai Secure

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

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

VIGILANCIA POR TELEVISIÓN

HIKVISION

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

SAMSUNG
WISENET

Hanwha Techwin Europe Ltd
Avda. De Barajas, 24, Planta Baja, Oficina 1
28108 Alcobendas (Madrid)España(Spain)
Tel.: +34 916 517 507
www.hanwha-security.eu
hte.spain@hanwha.com

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

dahua
TECHNOLOGY

DAHUA IBERIA
C/ Juan Esplandiú 15 1-B. 28007
Madrid
Tel: +34 917649862
sales.iberia@global.dahuatech.com
www.dahuasecurity.com

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

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

A Western Digital® Company

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

Josep Estivill, 67-69
08027 Barcelona, Spain.
www.ata98.com
info@ata98.com
Tel. +34 931 721 763

ASOCIACIONES

Expertos en VIDEOVIGILANCIA

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

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

Viladecans Business Park
Edificio Australia. C/ Antonio Machado 78-80, 1ª y 2ª planta
08840 Viladecans (Barcelona)
Web: www.ingrammicro.es
Teléfono: 902 50 62 10
Fax: 93 474 90 00
Marcas destacadas: Axis y D-Link.

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

info@uaseguridad.es
www.uaseguridad.es

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

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

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

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

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

C/ Emiliano Barral, 43
28043 Madrid
Tel 91 564 7884 • Fax 91 564 7829
www.aecra.org

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

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

EVENTOS DE SEGURIDAD

ASOCIACIÓN ESPAÑOLA DE INGENIEROS DE SEGURIDAD

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

DALLMEIER ELECTRONIC ESPAÑA
C/ Princesa 25 – 6.1 (Edificio Hexágono)
Tel.: 91 590 22 87
Fax: 91 590 23 25
28008 • Madrid

dallmeierspain@dallmeier.com
www.dallmeier.com

Grupo Alava Ingenieros
Área Seguridad

C/Albasanz, 16 – Edificio Antalia
28037 Madrid
Telf. 91 567 97 00 • Fax: 91 567 97 11
Email: alava@alava-ing.es
Web: www.alavaseguridad.com

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

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

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

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

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

ASOCIACIÓN NACIONAL DE TASADORES Y PERITOS JUDICIALES INFORMÁTICOS (ANTPJI)
C/ Juan de Mariana, 5
28045 Madrid
Tlf 91 / 469.76.44
www.antpji.com
contacto@antpji.com

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

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

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

FORMACIÓN DE SEGURIDAD

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

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

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

Homologado por el Ministerio del Interior y la Junta de Andalucía.
Avda de Olivares 17 • Plg. Industrial PIBO.
41110 Bollullos de la Mitación (Sevilla).
Tlfno. 902194814 – 954108887
Fax. 954002319
gerencia@gruporomade.com

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

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

ASOCIACIÓN DE JEFES DE SEGURIDAD DE ESPAÑA
Avd. Meridiana 358. 4ºA.
08027 Barcelona
Tel. 93-3459682 Fax. 93-3453395
www.ajse.es presidente@ajse.es

CENTRALES DE RECEPCIÓN Y CONTROL

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

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

ASOCIACIÓN VASCA DE PROFESIONALES DE SEGURIDAD
Parque tecnológico de Bizkaia
Ibaizabal Kalea, 101
sae@sae-avps.com
www.sae-avps.com

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

INTEGRACIÓN DE SISTEMAS

ARQUERO SISTEMA CORPORATIVO

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

INSTALACIÓN Y MANTENIMIENTO

TECOSA

Telecomunicación, Electrónica y Conmutación

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

Techco Security
C/ Barbadillo 7
28042 Madrid
+34 91 312 77 77
www.techcosecurity.com
tcs@techcosecurity.com

SEGURIDAD LEVANTE
Homologación de registro D.G.S.E. nº 432

INSTALACIÓN Y MANTENIMIENTO
INTRUSIÓN – CCTV – INCENDIO – ACCESOS
SUBCONTRATACIÓN
ALICANTE, VALENCIA, MURCIA, ALBACETE

www.seguridadlevante.com
902 400 022
info@seguridadlevante.com

AGÜERO Proyectos e Instalaciones, S.L.
FUNDADA EN 1966

INSTALACIONES A SU MEDIDA

Antoñita Jiménez, 25
28019 Madrid
ISO 9001
Tel.: 91 565 54 20 - Fax: 91 565 53 23
seguridad@grupoaguero.com
www.grupoaguero.com

PUBLICACIONES WEB

PUNTO SEGURIDAD.com

PUNTOSEGURIDAD.COM
TF: 91 476 80 00

info@puntoseguridad.com
www.puntoseguridad.com

INSTALSEC

Avda. Manzanares, 196
28026 Madrid
Tel.: 914 768 000 - Fax: 914 766 057
publi-seguridad@epeldano.com
www.instalsec.com

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

MATERIAL POLICIAL

SABORIT INTERNATIONAL

Avda. Somosierra, 22 Nave 4D
28709 S. Sebastián de los Reyes (Madrid)
Tel.: 913 831 920
Fax: 916 638 205

www.saborit.com

VIGILANCIA Y CONTROL

SECURITAS SEGURIDAD ESPAÑA

C/ Entrepeñas, 27
28051 Madrid
Tel.: 912 776 000
email: info@securitas.es

www.securitas.es

Grupo RMD

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

TRANSPORTE Y GESTIÓN DE EFECTIVO

LOOMIS SPAIN S. A.

C/ Ahumaos, 35-37
Poligono Industrial La Dehesa de Vicálvaro
28052 Madrid
Tlf: 917438900
Fax: 914 685 241

www.loomis.com

KEEP CALM AND

spain

Homsec

2017

10 YEARS CONCERNED WITH THE INTERNATIONAL SECURITY & DEFENSE

6th International Exhibition
of Security & Defense Technologies

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

March 14-16, 2017
Madrid, Spain

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

SECURITY FORUM 2017

BARCELONA • 17 y 18 de mayo

Security Forum celebra este año su quinta edición. Un evento que se ha posicionado como un referente en el sector de la seguridad gracias a sus valores diferenciales: exposición, congreso, paneles de expertos y premios Security Forum.
Fechas: 17 y 18 de mayo de 2017.
Horario: de 10:00 h a 18:30 h.
Lugar: Centro de Convenciones Internacional CCIB.
Pza. de Willy Brandt, 11-14, Barcelona.
Periodicidad: anual.
Organiza: Peldaño.
Áreas de Exposición: CCTV, integración de sistemas, seguridad lógica, control de accesos, Ip/redes, protección contra robo e intrusión, ciberseguridad, etc.
Más información: www.securityforum.es

AXIS SOLUTION CONFERENCE

MADRID • 8 y 9 de marzo

Axis Communications presenta la II Edición del Axis Solution Conference. Tras el éxito de la primera edición, vuelve el evento de referencia en soluciones de seguridad. Un evento con un formato dinámico y visual para conocer un mundo de soluciones sectoriales a través de demostraciones en vivo. Un formato pionero que ofrece un mundo de soluciones para cada uno de los mercados verticales: Ciudades Inteligentes y Seguras, Infraestructura Críticas e Industria Retail y Logística, Plataformas de Integración: Vídeo, control de accesos y audio.
Fechas: 8 y 9 de marzo de 2017.
Horario: de 09:00 a 18:00h.
Lugar: Hipódromo de la Zarzuela (A-6) km 8, 28023 Madrid.
Más información: www.axis.com

ASLAN 2017. CONGRESS & EXPO

MADRID • 15 Y 16 de marzo

El papel de la tecnología y de los expertos IT cambiará más en 2017 que en los últimos diez años. Estamos en el punto de inflexión impuesto por el fenómeno de la digitalización. Responsables IT, partners tecnológicos, service providers y startups tienen la oportunidad de liderar la Transformación Digital aportando su talento, experiencia y conocimiento tecnológico. Conocer las últimas innovaciones tecnológicas, y cómo alinearlas con el negocio es el gran reto en la nueva era digital y el foco principal de ASLAN2017.
Fecha: 15 y 16 de marzo
Horario: día 15, de 9:00 h a 19:00 h.
día 16, de 9:00 h a 15:00 h.
Lugar: Palacio Municipal de Congresos.
Avda. de la Capital de España, 7. Madrid
Más información: www.aslan.es

II CONGRESO NACIONAL DE JEFES DE SEGURIDAD

BARCELONA • 5 de abril

Ante la nueva realidad legislativa en materia de seguridad –y a la espera del desarrollo reglamentario de la Ley de Seguridad Privada– y los retos a los que se enfrenta la figura del Jefe de Seguridad, PELDAÑO y la Asociación de Jefes de Seguridad de España organizan el II Congreso de Jefes de Seguridad, que tendrá lugar el próximo 5 de abril en Barcelona.
Fecha: 5 de abril.
Horario: 10:00 h a 18:00 h.
Lugar: Colegio Oficial de Agentes Comerciales de Barcelona
Más información: www.congresojefesdeseguridad.com

¿ESTÁS PREPARADO?

CCIB
Centro de Convenciones
Internacional de Barcelona

17 y 18 de mayo
BCN**2017**

www.securityforum.es

Security FORUM
International Security Conference & Exhibition

HIKVISION

UN PARTNER SÓLIDO, COMPROMETIDO, INNOVADOR, FIABLE, PRESENTE.

El valor de un partner tecnológico se mide por su capacidad de generar ventaja competitiva, así como por su actitud y el poder de transmitir determinación, entusiasmo, y motivaciones siempre nuevas. Hikvision garantiza profesionalidad, solidez empresarial, compromiso, fiabilidad tecnológica, innovación continua y un alcance global con presencia local.

Hikvision Spain
C/ Almazara, 9
28760 Tres Cantos (Madrid)
T +34 91 7371655
F +34 91 8058717
info.es@hikvision.com

www.hikvision.com