

CUADERNOS DE SEGURIDAD

Núm. 303 • SEPTIEMBRE 2015 • 10 euros

 PUNTOSEGURIDAD.com

Seguridad en entidades bancarias

Servicios de seguridad

 Congreso de
Seguridad Privada
EUSKADI
Segurtasun
Pribatuko Batzarra

Bilbao
30SEP2015

Con un paso a **HD Analógica**

- 1080P, 720P
- Cable Coaxial Existente
- Plug & Play
- Transmisión a Larga Distancia

HDCVI – La Interfaz de Video Compuesto de Alta Definición es un estándar de transmisión de video HD analógica por cable coaxial, que permite transmisión en alta definición confiable a larga distancia y a menor costo mientras es aplicable una implementación compleja. Con más de 10 millones de seguidores fieles de 150 países en todo el globo, HDCVI ahora lidera la innovación en HD analógica.



España



iPTECNO

Portugal



CE FC CC UL ISO 9001:2000

DAHUA TECHNOLOGY CO., LTD.

No.1199 Bin'an Road, Binjiang District, Hangzhou, China. 310053
Tel: +86-571-87688883 Fax: +86-571-87688815
Email: overseas@dahuatech.com
www.dahuasecurity.com



II CONGRESO DE SEGURIDAD PRIVADA EN EUSKADI

Seguridad, en continuo proceso de cambio

El Azkuna Zentroa será escenario el próximo 30 de septiembre del II Congreso de Seguridad Privada en Euskadi. El encuentro, organizado por PELDAÑO, refuerza en esta su segunda edición el objetivo principal de convertirse en un foro que reúna al sector de la Seguridad en el País Vasco, en un idóneo entorno donde analizar los nuevos retos a los que se enfrenta la Seguridad Privada.

Bajo el lema «Seguridad, un trabajo de todos», la organización, que ha contado con la colaboración del Gobierno Vasco, la Ertzaintza y otras entidades, ha trabajado en un denso programa de ponencias y mesas de debate donde los profesionales puedan conocer, compartir e intercambiar conocimientos sobre la realidad y necesidades más actuales a las que se enfrenta un sector en general y, en este caso de forma más concreta el de la Seguridad Privada en el País Vasco, en continuo proceso de cambio y adaptación tras la aprobación hace ya más de un año de la nueva Ley de Seguridad Privada.

Dirigido a directores y gestores de seguridad de entidades públicas y privadas, profesionales de las empresas de seguridad, así como miembros de las Fuerzas y Cuerpos de Seguridad, el II Congreso de Seguridad Privada en Euskadi abordará, entre otros, los siguientes temas: «Planes de coordinación entre la Seguridad Pública y la Seguridad Privada»; «Infraestructuras Críticas: Sistema PIC en Euskadi y desarrollo de los Planes Estratégicos Sectoriales»; «Retos en la Certificación de Equipos, Sistemas y Empresas de seguridad»; «Ciberseguridad: desarrollo de un CERT en las corporaciones»; y «La Seguridad Privada frente a la amenaza del Islamismo Radical».

Un evento que, en su segunda convocatoria, vuelve a convertirse en la oportunidad idónea para intercambiar ideas y conocimiento, y para buscar mecanismos y protocolos de coordinación y mejora en aquellos temas de máxima actualidad, que más preocupan e interesan al sector de Seguridad Privada, con el objetivo de asentar las bases para una efectiva comunicación intersectorial, que recaerá en beneficio de la seguridad en general.

Y, por otro lado, el equipo de PELDAÑO ya ha empezado a trabajar en la cuarta edición de Security Forum que tendrá lugar los días 25 y 26 de mayo en Barcelona. Puesta toda la maquinaria en marcha, y a la vista de los resultados de la tercera edición –más de 5.500 visitantes profesionales, 73 expositores y 245 congresistas–, Security Forum 2016 volverá a congregarse a los más destacados expertos en materia de prevención y seguridad, así como la mayor oferta comercial nacional e internacional representada a través de las empresas más avanzadas en el campo de la innovación y desarrollo en seguridad.

Una vez más, PELDAÑO, manteniendo su objetivo prioritario de servicio al sector, escucha y atiende a la demanda e intereses de los profesionales de la seguridad con la puesta en marcha de encuentros e iniciativas que tratan de aproximar la realidad más actual y futura de un sector que reclama encuentros de estas características para revitalizar su tejido empresarial.

3 EDITORIAL

— Seguridad, en continuo proceso de cambio.

8 II CONGRESO DE SEGURIDAD PRIVADA EN EUSKADI

- *Todo listo para el II Congreso de Seguridad Privada en Euskadi.*
- Entrevista: **Rodrigo Gartzia Azurmendi**. Director de Coordinación de Seguridad. Gobierno Vasco.
- Entrevista: **Francisco Llana Prieto**. Jefe de la Unidad de Seguridad Privada. Ertzaintza.

20 SECURITY FORUM

— La cuarta edición de Security Forum se celebrará el próximo mes de mayo.

22 EN PORTADA

SEGURIDAD EN ENTIDADES BANCARIAS

El avance de la sociedad -y en estos momentos la situación de incertidumbre económica- ha propiciado que las entidades bancarias hayan tenido que ir adaptándose a los continuos cambios de la misma, y en el caso que nos ocupa, en el ámbito de la seguridad. Un avance que ha conllevado la implantación de una serie de medios y medidas de seguridad, concretamente de prevención y protección. Medidas que también tienen su punto de apoyo en las tecnologías que avanzan rápi-

damente. Y han sido concretamente éstas las que han modificado -y siguen haciéndolo- la oferta de operar y de servicios que ofrecen las entidades bancarias, lo que ha derivado en la aparición de nuevos riesgos y amenazas, conocidos ya como cibercriminales. Y ahora toca preguntarnos ¿Cómo ha cambiado la seguridad de las corporaciones bancarias en estos últimos años? ¿Cómo gestionan en estos momentos los directores de Seguridad de estas entidades bancarias la seguridad integral?



ENTREVISTAS:

- **José María Arana**. Director de Seguridad. Laboral Kutxa.
- **José Enrique López Regueira**. Director de Seguridad Física. Abanca.
- **José Antonio Soler de Arespachaga**. Director de Seguridad de Liberbank.
- **Andrés Martín Ludeña**. Director de Seguridad. EVOBanco.

ARTÍCULOS:

- Un golpe de timón necesario, por **Juan Manuel Rodríguez Zarco**.
- Renovarse o morir, por **Eduard Zamora**.

CUADERNOS DE SEGURIDAD

www.puntoseguridad.es

Nº 303 • SEPTIEMBRE 2015

Peldaño

Avda. del Manzanares, 196 • 28026 MADRID
www.peldano.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@peldano.com Emilio Sánchez.
Imagen y Diseño: Eneko Rojas.
Producción y Maquetación: Miguel Fariñas, Débora Martín, Andrea Hidalgo.

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

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

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



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

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

- El Reglamento que viene, por **Francisco Guerrero**.
- Los riesgos en la videovigilancia de los cajeros automáticos, por **Ana Marzo**.
- El director de Seguridad y el cumplimiento normativo, por **José Ignacio Olmos**.
- Protección de redes, esencial para la seguridad de entidades financieras, por **José Luis Romero**.
- Sistemas de control y gestión centralizada para contenedores de efectivo, por **Fernando Martínez**.
- Estudio Kaspersky Lab y B2B International.

60 SERVICIOS DE SEGURIDAD

ENTREVISTAS

- **Luciano Valladares**. Director Nacional de Eulen Seguridad.
- **Jesús Gordillo**. Director del Área de Tecnología de Securitas Seguridad España.



ARTÍCULOS

- El sector cae por sexto año consecutivo, por **Ángel Córdoba**.
- Tecnología NFC: control de rondas y presencia para las empresas de seguridad, por **August Jiménez**.

73 CIBERSEGURIDAD

- Ciberseguridad: cambio, desarrollo y evolución, por **Jorge Christian Durán y Juan Carlos Guel**.

76 SEGURIDAD

ENTREVISTAS:

- **Javier López Ferrer**. Director general de Videocode.
- **Jesstin Zhou**. Director general del departamento Internacional. Uni-view.

ARTÍCULOS:

- Seguridad Corporativa, un desafío para las empresas, por **Megan Miller**.
- Dahua desarrolla la aplicación del estándar de compresión H.265.
- Mesa Redonda del Comité de Detección de Tecnifuego-Aespi en Valencia: Seguridad contra Incendios en el hogar.

89 FERIAS

- Sicurezza: soluciones verticales, estrellas de esta edición.
- Sicur 2016: mayor oferta y representación internacional.
- Trafic 2015: soluciones de movilidad con vehículos seguros y eficientes.

92 ACTUALIDAD

- Arecont: Scott Schafer recibe el premio SIA.
- Tecnifuego-Aespi: nuevo folleto sobre protección pasiva contra incendios.
- Barcelona: XII Edición del Día de la Seguridad Privada.
- Siemens: mantenimiento de los sistemas de seguridad de los aero-

- puertos de AENA.
- Ilunion Seguridad: formación.
- El Instituto Nacional de Ciberseguridad (INCIBE) gestionó en el primer semestre cerca de 28.000 incidentes cibernéticos.
- Ingram Micro, nuevo mayorista.
- Casmar apuesta por el mercado de Chile y Colombia.
- Diid y Paradox alcanzan un acuerdo de distribución en España y Portugal.

101 EQUIPOS Y SISTEMAS

- Innovative ofrece mapas y direcciones basadas OpenStreetMap.
- Tyco IF & S: app, seguridad.
- Delta Informática: escáner fotográfico de reconocimiento de pasaporte.
- Samsung: nuevos videograbadores de red con PoE+ integrado.
- Mobotix: MxMC, nuevo software de gestión de vídeo.
- Etc.

114 UN CAFÉ CON

- **Eduard Zamora**. Director de Seguridad Corporativa de Banc Sabadell.



OCTUBRE 2015 - N° 304

EN PORTADA

SEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS

Hace poco más de cuatro años que entró en vigor la Ley 8/2011, de 28 de abril, por la que se establecen las medidas para la protección de las infraestructuras críticas, y que tiene por objeto establecer las estrategias y estructuras adecuadas, que permitan dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en materia de protección de infraestructuras críticas, previa identificación y designación de las mismas, para mejorar la prevención, preparación y respuesta de nuestro Estado, frente a atentados terroristas u otras amenazas que afecten a las mismas. Tras la constitución de la Comisión Nacional para la Protección de las Infraestructuras Críticas, que aglutina a todos los departamentos, organismos y administraciones con responsabilidades en la materia, ésta celebró su primera sesión con la aprobación de los cinco Planes Estratégicos Sectoriales (electricidad, gas, petróleo, nuclear y financiero). Ahora llega el turno para aprobar nuevos Planes Estratégicos Sectoriales para el transporte (aéreo, marítimo, ferroviario y terrestre), y para las tecnologías de la información y comunicaciones y el agua. ¿Cómo se ha ido implantando esta normativa en los sectores estratégicos? ¿Qué aspectos comprenderán estos nuevos planes?



TECNOLOGÍA IP APLICADA A SEGURIDAD

La tecnología está presente hoy en día en todos y cada uno de los ámbitos y sectores, y no cabe duda, de que en el de la seguridad también. Una herramienta que se ha convertido en factor y elemento imprescindible. Y si hablamos de tecnología IP, en unos años se ha convertido en herramienta fundamental a aplicar en cualquier tipo de instalación, con el objetivo de cubrir todas y cada una de las necesidades específicas que requiera.

Estos y otros temas serán analizados en las páginas de nuestro próximo número de la mano, como ya viene siendo habitual, de expertos y especialistas en la materia.

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
ARECONT	92	18189370700	www.arecont.com
AVIGILON	23	900838630	www.avigilon.com
AXIS COMMUNICATIONS	21,97	918034643	www.axis.com
BAUSSA	47	946749099	www.baussa.com
BOSCH	104	902121497	www.boschsecurity.es
BUNKER SEGURIDAD	87	902196649	www.bunkerseguridad.com
BY DEMES	93	934254960	www.bydemes.com
CASESA	4ª CUB	902010406	www.casesa.es
CASMAR	98	933406408	www.casmar.es
CONGRESO SEGURIDAD EUSKADI	3ª CUBIERTA	914768000	www.congresoseguridadeuskaadi.com
CYRASA	27	902194749	www.cyrasa.com
DAHUA	2ª CUB,80	865718768883	www.dahuasecurity.com
DALLMEIER	103	915902287	www.dallmeier-electronic.com
DELTA INFORMÁTICA	101	932151036	www.deltainformatica.es
DIID	99	902565733	www.diid.es
E-MOVILIA	71	936674017	www.emovilia.com
EULEN SEGURIDAD	62	916310800	www.eulen.com/es/seguridad
EUROCLOUD	61	910113303	www.eurocloudspain.org
FLIR SYSTEMS	45	615734827	www.flir.es
HIKVISION	13,15,17	917371655	www.hikvision.com
HONEYWELL SECURITY	103	913136272	www.honeywell.es
ILUNION SEGURIDAD	94	914538200	www.seguridad.alentis.es
INNOVATIVE	101	937895205	www.innovative.es
KABA-SAFE LOCKS	56	902224111	www.kaba.es
KASPERSKY	58	913983752	www.kaspersky.es
MNEMO	73	914176776	www.mnemo.com
MOBOTIX	102	911115824	www.mobotix.com
MORSE WATCHMANS	25	20326494949	www.morsewatchmans.com
PANTER	105	965310613	www.panter.es
ROMBULL RONETS	105	966758130	www.rombullronets.com
SABORIT INTERNATIONAL	35	913831920	www.saborit.com
SAMSUNG TECHWIN	54,102	916517507	www.samsungsecurity.co.uk
SECURITAS SEGURIDAD ESPAÑA	19,68	912776000	www.securitas.es
SEGURIDAD INTEGRAL CANARIA	59	902226047	www.seguridadintegralcanaria.com
SETELSA	37	942544354	www.setelsa.net
SICUR	67	902221515	www.ifema.es/sicur_01
SIEMENS	82,94	915148000	www.siemens.es
SYNOLOGY	104	886225521814	www.synology.com
TECOSA	31	915147500	www.tecosa.es
TESA	79	943669100	www.tesa.es
TYCO IF & S	101	916313999	www.tyco.es
UNIVIEW	78		www.uniview.com/en
VIDEOCODE	76	935650156	www.video-code.es
VIVOTEK	105	886282455282	www.vivotek.com

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



ÍNDICE DE ANUNCIANTES

Avigilon.....	23
Axis.....	21
Baussa.....	47
Bunker seguridad.....	87
Casesa.....	4ª cubierta
Congreso seguridad Euskadi.....	3ª cubierta
Cyrasa.....	27
Dahua.....	2ª cubierta
Eurocloud.....	61
Flir systems.....	45
Hikvision.....	13,15,17
Morse Watchmans.....	25
Saborit international.....	35
Securitas.....	19
Seguridad Integral Canaria.....	59
Setelsa.....	37
Sicur.....	67
Tecosa.....	31
Tesa.....	79

EL ENCUENTRO, ORGANIZADO POR PELDAÑO, SE CELEBRARÁ EL 30 DE SEPTIEMBRE EN EL AZKUNA ZENTROA DE BILBAO

Todo listo para el II Congreso de Seguridad Privada en Euskadi

Bajo el lema «Seguridad, un trabajo de todos», el programa analizará entre otros temas los planes de coordinación entre Seguridad Pública y Privada.

AZKUNA Zentroa será escenario el próximo 30 de septiembre de la segunda edición del Congreso de Seguridad Privada en Euskadi, un encuentro que, organizado por Peldaño, cuenta con la colaboración del Gobierno Vasco, el Ayuntamiento de Bilbao, la Ertzaintza, SAE y otras entidades.

Tras el éxito de la primera edición, celebrada en 2013, el II Congreso de Seguridad Privada en Euskadi, bajo el lema «Seguridad, un trabajo de todos», volverá a ser un foro donde se reúna al sector de la Seguridad en el País Vasco, en un encuentro de trabajo, en el que se analizarán los nuevos retos a los que

se enfrenta la Seguridad Privada, y donde los profesionales puedan compartir e intercambiar conocimientos, ideas y puntos de vista, así como los asuntos y temas de más actualidad.

El II Congreso se desglosará en un amplio programa de ponencias y mesas de debate donde se abordarán los siguientes temas:

- Planes de coordinación entre la Seguridad Pública y Privada.
- Infraestructuras Críticas: sistema PIC en Euskadi y desarrollo de los Planes Estratégicos Sectoriales.
- Retos en la Certificación de Equipos, Sistemas y Empresas de Seguridad.

- Protección de Datos y Seguridad Privada.
- La Seguridad Privada frente a la amenaza del Islamismo Radical.
- Ciberseguridad: desarrollo de un CERT en las corporaciones.

El encuentro contaba al cierre de esta edición con el patrocinio de Casesa, Cueva Valiente, Delta Seguridad, Dorlet, Eulen Seguridad, Ikusi, Kaba, Securitas Direct y Segway.

En la web www.congresoseguridadeuskadi.com se facilita información puntual sobre la preparación y el desarrollo del Congreso, así como las inscripciones. ●

Fotos: Azkuna Zentroa



PROGRAMA

9:15 h	Acreditación y entrega de documentación.
10:00 h	Bienvenida y presentación. D. Ignacio Rojas, presidente de Peldaño.
10:10 h	Acto de apertura del Congreso. Representante Departamento de Seguridad. Gobierno Vasco.
10:30 h	Planes de coordinación entre la Seguridad Pública y Privada. D. Francisco Llana. Jefe USP Ertzaintza.
11:00 h	Descanso. Café.
11:30 h	Mesa debate Infraestructuras Críticas: Sistema PIC en Euskadi y desarrollo de los Planes Estratégicos Sectoriales. Modera: Dña. Verónica Villanueva. Ingeniera en MKV Medialab y directora de seguridad. D. José Ignacio Carabias. Jefe de área del CNPIC (Centro Nacional de Infraestructuras Críticas). D. José Manuel Betanzos. Protección de Infraestructuras Críticas de Euskadi (PICEUS). D. José Juan Meaza. Responsable de Seguridad de Bahía de Bizkaia Gas.
12:30 h	Protección de datos y Seguridad Privada. D. José Ignacio Pariente de Prada. Director de la Agencia Vasca de Protección de Datos.
13:00 h	Mesa debate Retos en la Certificación de Equipos, Sistemas y Empresas de Seguridad. Modera: D. Javier Larrañeta. TECNALIA. Secretario General de PESI. D. Carlos Alonso. Dirección de Certificación de producto de AENOR. D. Víctor del Corte. Oficial Jefe de Área de la Unidad de Seguridad Privada. Ertzaintza. D. Iñigo Ugalde. Director Comercial de Baussa. Vicepresidente de SAE. D. Eduard Zamora. Director de Seguridad Corporativa del Banco Sabadell.
14:00 h	Descanso. Almuerzo.
16:00 h	La seguridad privada frente a la amenaza del Islamismo Radical. D. Luis de la Corte Ibáñez. Profesor UAM. Miembro de ADESYD.
16:30 h	Mesa Debate Ciberseguridad: Desarrollo de un CERT en las corporaciones. Modera: D. Iván Rubio. Director del Área de Seguridad de Peldaño. D. Miguel García-Menéndez. Responsable de Gobierno Corporativo y Estrategia del CCI. D. José María Arana. Director del departamento de Inmovilizado, Seguridad y Servicios Generales de Laboral Kutxa. Presidente de SAE. D. Ricardo Cañizares. Director de Consultoría. Eulen Seguridad. D. Ángel Barrio. Responsable de Seguridad de Sistemas de Euskaltel.
17:45 h	Entrega de distinciones Cuadernos de Seguridad.
18:00 h	Acto de clausura del Congreso. D. Tomás del Hierro. Concejale de Seguridad del Ayuntamiento de Bilbao.
18:20 h	Fin del programa de ponencias.
19:00 h	Recepción y cóctel en el Ayuntamiento de Bilbao.
20:30 h	Despedida y cierre.

¡INSCRÍBETE!
60€



Rodrigo Gartzia Azurmendi

Director de Coordinación de Seguridad. Gobierno Vasco

Nacido en la localidad vizcaína de Ermua, Rodrigo Gartzia Azurmendi es licenciado en Filosofía y Letras por la Universidad de Deusto. Ha desempeñado distintos puestos de responsabilidad en el Gobierno Vasco, y desde abril de 2013 está al frente de la Dirección de Coordinación de Seguridad (Viceconsejería de Seguridad).

Podrías explicarnos, a grandes rasgos, cuáles son los objetivos del Plan General de Seguridad Pública de Euskadi 2014-2019? ¿Cuáles son los ejes

«La seguridad privada es un sector en alza con el que colaboramos permanentemente»

Sobre la base de dos objetivos principales, la cercanía a la ciudadanía y reforzar el trabajo conjunto entre la seguridad pública y seguridad privada, Rodrigo Gartzia Azurmendi, director de Coordinación de Seguridad del Gobierno Vasco, analiza en esta entrevista los objetivos y ejes principales del Plan General de Seguridad Pública de Euskadi 2014-2019, al tiempo que incide en la apuesta por potenciar, a través de diferentes herramientas y acciones, la colaboración entre el sector público y privado.

estratégicos sobre los que se establece?

—La Ley de Ordenación del Sistema de Seguridad Pública de Euskadi define una concepción integral de un sistema que abarca además de la Policía Vasca, que está compuesta por la Ertzaintza con 8.000 efectivos, los 81 cuerpos locales con 3.300 agentes, todo el entorno de las emergencias, la seguridad vial, la seguridad en espectáculos y eventos deportivos. El máximo órgano de participación que define esta ley es el Consejo de Seguridad Pública, que bajo la presidencia de la Consejera reúne a todos los departamentos del Gobierno Vasco, a las diputaciones forales, a los representantes de los ayuntamientos de las capitales, que cuentan con servicios de extinción de incendios y salvamento y también están presentes jueces, fiscales, Eudel...

Este Consejo aprueba el Plan General de Seguridad Pública de Euskadi, que recoge todos los riesgos y amenazas a los que tenemos que hacer frente y establece los ejes y objetivos estratégicos que debemos implementar en el periodo

2014-2019. Estos ejes principales son el servicio a la ciudadanía, la planificación, la coordinación, la formación y la comunicación. Además, en el marco de este Plan se han creado dos grupos de trabajo específicos, uno entre la judicatura, la fiscalía y la Ertzaintza, y otro de protección de las infraestructuras críticas.

—El departamento de Seguridad cuenta hoy en día con una importante herramienta de comunicación, bautizada bajo el nombre ENBOR_Sarea, ¿qué servicios se ofrecen a través de esta iniciativa? ¿Cuáles son sus pilares básicos?

—El departamento de Seguridad dispone de una red de comunicaciones TETRA por radio, que es propia y hemos denominado ENBOR_Sarea, que da servicio a todas las emergencias, los cuerpos de bomberos, el voluntariado de protección civil, Cruz Roja, DYA, Federación Vasca de Montaña, el grupo de perros de Salvamento, y está coordinada a su vez con Osakidetza. Todo ello bajo un único número de atención que es el 112. Cada uno de esos agen-

tes dispone de su canal de comunicación, pero además hemos puesto en marcha canales comunes que permitirán desarrollar operaciones conjuntas. Ocurre lo mismo en el ámbito policial. La Ertzaintza dispone de sus propios canales de comunicación y cada Policía Local tiene el suyo, que se le ha proporcionado desde el departamento de Seguridad. Pero recientemente hemos previsto la asignación de canales comunes para poder coordinar actuaciones incidentales o planificadas.

La Ertzaintza es una policía que está dentro del ámbito europeo de Schengen. En este momento, disponer de información de terceros países, especialmente en todo lo relacionado con los riesgos del islamismo radical, es primordial. La Ertzaintza está estructurando toda la información a la que accede y, a su vez, facilita datos sobre personas, vehículos y objetos a las Policías Locales de Euskadi. Hemos avanzado en coordinación y establecido operativas conjuntas de actuación ante casos como, por ejemplo, una orden europea de detención. Ese grado de coordinación entre las diferentes policías como el que tenemos en Euskadi no existe en ningún otro lugar de nuestro entorno.

—Veo que inciden especialmente en el ámbito de la coordinación. ¿Por qué?

—El ámbito de la seguridad es multiagencia y hace frente a una realidad interdependiente. Es fundamental por tanto coordinarlo y colaborar con cada uno de estos agentes. Una de nuestras principales prioridades es la de ahondar en las relaciones con los nuevos ayuntamientos recién constituidos. Ya lo veníamos haciendo, tenemos suscritos convenios de colaboración con las po-

licías locales y desde la Policía Científica de la Ertzaintza se les facilita el análisis de las drogas incautadas por las policías locales. Les estamos también ofreciendo el análisis de muestras salivales por presencia de drogas en la conducción, y también nuevos protocolos de reseñas de huellas dactilares con las policías locales de los municipios que tienen más de 50.000 habitantes. Además, este intercambio de huellas también se

conjuntas que requieren incluso de un intercambio de información en tiempo real; un ejemplo de ello es el proyecto piloto DATAPOL que estamos avanzando con la Policía Municipal de Bilbao.

—¿Uno de sus principales objetivos es la cercanía a la ciudadanía y poder interactuar con ellos?

—Afortunadamente la sociedad vasca es segura, con niveles de delincuencia

«Afortunadamente la sociedad vasca es segura, con niveles de delincuencia moderados, pero tenemos que seguir incidiendo en un aspecto tan básico como el de la cercanía a la ciudadanía»

efectúa con el resto de Fuerzas de Seguridad del Estado, Mossos y Policía Foral y estamos trabajando en un centro de compensación de datos de detenidos por todos estos cuerpos policiales.

Por otra parte, el Gobierno Vasco acaba de aprobar un decreto que regula todas las comisiones de coordinación de Ertzaintza y Policía local en el ámbito local: tienen que reunirse al menos una vez al año y tiene que haber una comisión en el ámbito de cada demarcación. También estamos trabajando en la delimitación de funciones de cada cuerpo policial y en el análisis de operativas

moderados, pero tenemos que seguir incidiendo en un aspecto tan básico como el de la cercanía a la ciudadanía, en ese patrullaje a pie, nuestras conocidas KORRIKAK, que nos hacen ser más visibles y convivir mejor con la ciudadanía. Además, la información, la transparencia e interactuar con el ciudadano o la ciudadana gracias a las nuevas tecnologías van a mejorar a buen seguro la percepción de seguridad. En este sentido, un estudio del London Home Office concluye que el 80% de la delincuencia es descubierta y comunicada por las propias víctimas,



Reunión del Consejo de Seguridad Pública de Euskadi junto a la Consejera, el Viceconsejero y el Director de la Ertzaintza

por la ciudadanía en definitiva, así que tenemos que hacer que la colaboración ciudadana con la policía sea una realidad creciente. Twitter y las aplicaciones para móviles, como la nueva App de la Ertzaintza que próximamente presentaremos, nos acercan a las nuevas generaciones, pero no debemos olvidar que nuestra sociedad está cada vez más envejecida; las sociedades con una amplia población mayor probablemente delinquirán menos, pero a su vez son mucho más vulnerables. Como ve no nos falta trabajo pero no nos faltan ganas y nos acompaña un magnífico equipo de profesionales.

—Bajo su opinión, ¿qué papel y labor desempeña el sector de la Seguridad Privada en el País Vasco?

—El decreto de regulación del ejercicio de competencias del País Vasco en materia de seguridad privada, que aprobamos hace unos meses, marca el inicio de una nueva era en las relaciones entre los cuerpos policiales y el mundo profesional del sector privado. La ley promulgada el año pasado otorga a la Viceconsejería de Seguridad la potestad de autorización, control, inspección y sanción de todas las actividades de la seguridad privada.

—¿Cree que es necesario potenciar la colaboración y coordinación entre Seguridad Pública y Seguridad Privada? ¿Cómo calificaría el actual nivel de colaboración de las empresas y profesionales de la Seguridad Privada con la Ertzaintza?

—El plan de colaboración «Lagundu», diseñado desde la Unidad de Seguridad Privada de la Ertzaintza, plantea algunas iniciativas que ya han cristalizado, como las relacionadas con la información y el asesoramiento. De hecho, un experto de la Policía Autónoma impartió a finales de abril una charla sobre islamismo radical a un centenar de responsables de seguridad privada. Además, son frecuentes las reuniones con la Comisión Mixta de Seguridad Privada de Euskadi, el órgano en el que están representados todas y todos los agentes, directores y jefes de seguridad

y aquellas empresas obligadas a disponer de especiales medidas de protección como farmacias, joyerías, banca... Precisamente en el Security Forum celebrado el pasado mes de mayo en Barcelona, en el que estuvimos presentes, se incidió en la necesidad de reforzar

«El II Congreso de Seguridad Privada en Euskadi es una magnífica oportunidad para poder intercambiar ideas y experiencias con profesionales y empresas de seguridad privada»

el trabajo conjunto y coordinado entre el sector público y privado. Estamos en ello y ese es el futuro, porque estamos en una situación de interdependencia muy importante en un mundo globalizado.

—Bilbao volverá a ser escenario el próximo 30 de septiembre del II Congreso de Seguridad Privada en Euskadi, ¿qué espera que aporte esta segunda edición a la seguridad en su conjunto en el País Vasco?

—Es una magnífica oportunidad de acercarnos al sector, de poder intercambiar inquietudes, ideas, conocimientos y experiencias con los profesionales y empresas de la Seguridad Privada. Acogemos con mucho interés este II Congreso de Seguridad Privada en Euskadi y confiamos en la consolidación de este foro de encuentro y de participación con un sector en alza con el que estamos colaborando permanentemente y seguiremos haciéndolo porque se trata de una alianza estratégica importante para la seguridad pública de Euskadi. ●

TEXTO: Gemma G. Juanes

FOTOS: Dirección de Coordinación de Seguridad.



HIKVISION

TURBO **HD** TRIBRID SYSTEM

La tecnología Turbo HD de Hikvision marca un hito en la evolución de la era analógica. Los usuarios de CCTV analógico van a poder disfrutar de una resolución Full HD sin necesidad de cambiar el cableado de las instalaciones analógicas ya existentes. Permite la transmisión de vídeo sin retardo en 1080P a través de cable coaxial y es compatible con cámaras analógicas tradicionales, cámaras IP de Hikvision y dispositivos con el estándar HDTVI.

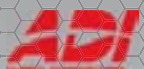
**¡ABROCHÉNSE LOS CINTURONES,
EL HÍBRIDO ANALÓGICO HD HA PUESTO EL TURBO!**



First Choice for Security Professionals

HIKVISION SPAIN - C/ Almazara, 9 - 28760 Tres Cantos (Madrid). Tel. +34 91 7371655 - Fax +34 91 8058717
info.es@hikvision.com - www.hikvision.com

España



www.es-eshop.adiglobal.com

Distribuidores Oficiales



www.casmar.es



www.hommaxistemas.com

Portugal



www.bernardodacosta.pt

FRANCISCO LLANEZA PRIETO. JEFE DE LA UNIDAD DE SEGURIDAD PRIVADA. ERTZAINITZA

«La nueva Ley de Seguridad Privada pretende abarcar toda la realidad del sector y lo prepara para el futuro»



TRAS la entrada en vigor de la nueva Ley de Seguridad Privada desde la Unidad de Seguridad Privada de la Ertzaintza nos planteamos entre otros objetivos, el firme propósito de reforzar la colaboración entre la Ertzaintza y los distintos agentes implicados en el sector» explica Francisco Llaneza, jefe de la Unidad de Seguridad Privada de la Ertzaintza, quien a lo largo de la entrevista analiza las pautas y competencias del Decreto 207/2014 de regulación del ejercicio de competencias de la CA de Euskadi en materia de Seguridad Privada, así como las iniciativas puestas en marcha para potenciar la colaboración entre ambas seguridades, pública y privada.

—Tras la entrada en vigor de la nueva Ley de Seguridad Privada hace poco más de un año, ¿qué

objetivos se plantearon desde la Unidad de Seguridad Privada de la Ertzaintza?

—El primer objetivo que nos marcamos fue la modificación del Decreto 309/1996, de 24 de diciembre, que reguló por vez primera el ejercicio de las competencias que correspondían a la Comunidad Autónoma de Euskadi en materia de seguridad privada. Desde la aprobación del citado Decreto se habían producido cambios tanto en el sector como en la normativa que regula la materia, por lo que resultaba necesaria su adecuación a las nuevas competencias derivadas de la Ley 5/2014. El segundo objetivo lo centramos en el desarrollo de nuevos cometidos y actividades, especialmente en lo que se refería a los centros de formación, a los que teníamos que inscribir en el Registro de Seguridad Privada de Eus-

kadi, y la supervisión de los despachos de detectives, ya que con la anterior legislación la actividad de este personal no se circunscribía de manera única al control de la Ertzaintza.

El tercer objetivo es el referido a las comunicaciones de los contratos, servicios y altas y bajas del personal de seguridad privada. Hasta la entrada en vigor de la Ley 5/2014 no todas estas comunicaciones se realizaban a la Ertzaintza; cuestión que para nosotros era imprescindible para el efectivo control de las actividades, funciones y servicios de seguridad privada que se desarrollan en la Comunidad Autónoma.

Por último, y no menos importante, citaría el firme propósito de reforzar la colaboración entre la Ertzaintza y los distintos agentes implicados en el sector.

—¿Qué valoración haría de la nueva normativa de seguridad? ¿Cuál cree que es su pilar fundamental?

—Como expone en su Preámbulo, la nueva ley representa un tratamiento total y sistemático de la seguridad privada en su conjunto, que pretende abarcar toda la realidad del sector, al tiempo que lo prepara para el futuro. El principio de subordinación de la norma anterior es superado, dando paso a la necesaria, y deseada, complementariedad basada en la cooperación y corresponsabilidad, lo cual, de manera segura, aprovechará todas las potencialidades que la seguridad privada puede ofrecer. Un aspecto novedoso es el referente

HIKVISION

 smart



FISHEYE



VISIÓN DE 360° **APLICACIONES DE 360°**

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

First Choice for Security Professionals

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

España

Distribuidores Oficiales

Portugal



www.es-eshop.adiglobal.com



www.casmar.es



www.hommaxistemas.com



Bernardo da Costa

www.bernardodacosta.pt

a la sustitución, en los casos contemplados en la ley, del procedimiento de autorización administrativa por el de declaración responsable; cuestión que se valora de forma positiva desde esta Unidad. Respecto a la formación del personal, se abren nuevas vías de acceso a la profesión, lo cual no puede sino redundar en una mejora de los servicios y valoración de los mismos por parte de la sociedad.

Por otra parte, en relación al intrusismo, tanto de empresas como de personal no habilitado, se facilita el soporte necesario para que desde las distintas administraciones se articulen las herramientas idóneas para una eficaz lucha

—**Hace casi un año se aprobó el Decreto 207/2014, de 21 de octubre, de regulación del ejercicio de competencias de la Comunidad Autónoma de Euskadi en materia de Seguridad Privada, ¿qué pautas, procedimientos y competencias establece el texto?**

—El objetivo de esta norma es recoger en un texto las competencias de ejecución que atribuye la nueva normativa estatal a nuestra Comunidad Autónoma en materia de seguridad privada, determinando los órganos dentro del departamento de Seguridad a los que corresponde ejercitarlas.

Con carácter general, la actividad ad-

Se crea mediante este Decreto el Registro de Seguridad Privada de Euskadi, en el cual se inscriben una vez autorizados o prestada la declaración responsable: las empresas de seguridad; los despachos de detectives privados; los centros de formación del personal de seguridad privada. También se inscribirán, las sanciones impuestas en materia de seguridad privada, las comunicaciones de los contratos y sus modificaciones, etc. En relación con el Registro, el Decreto prevé que en un futuro próximo y dado las características del sector, determinadas comunicaciones se hagan exclusivamente a través de la dirección electrónica de la Sede Electrónica <https://euskadi.net>.

—**El Plan Lagundu fue una de las grandes iniciativas de cooperación y colaboración entre Seguridad Pública y Privada en el País Vasco, ¿podría explicarnos a grandes rasgos cuáles fueron sus objetivos principales?**

—El Plan Lagundu se enmarca dentro de nuestro Plan Estratégico Horizonte 2016 y, en concreto, se centra en reafirmar la presencia y el apoyo de la Ertzaintza en el desarrollo de las actividades privadas de seguridad. Es indiscutible la importancia y trascendencia para la seguridad pública del valor de la información que dichas actividades pueden aportar, a la vez que, en sentido inverso, las posibles contribuciones de la Ertzaintza pueden favorecer las condiciones en que se desarrollen los servicios y la coordinación de los mismos.

El plan nace con el objetivo de desarrollar bases sólidas para una efectiva relación entre todos los sectores implicados en la seguridad dentro de la Comunidad Autónoma Vasca, estableciendo los mecanismos necesarios para una fluida comunicación bidireccional a distintos niveles, entre la Seguridad



contra ese tipo de actividades.

Es esperable, en definitiva, una mejora de la eficacia en la prestación de los servicios en lo relativo a organización y planificación. A la vez que, en determinadas circunstancias y supuestos, se posibilita y se da amparo legal a la realización de diferentes servicios de vigilancia y protección que la legislación anterior dejaba sin cobertura, y que en la actualidad, tanto por el desarrollo tecnológico como por la propia evolución social, se vislumbran a todas luces lógicas y oportunas.

ministrativa que genera la seguridad privada recae en el director de la Ertzaintza (autorizaciones, recepción de declaraciones responsables, control y registro de Seguridad Privada de Euskadi...).

Así mismo, instrumenta mecanismos de colaboración entre la Ertzaintza y el sector de seguridad privada para el intercambio de informaciones que faciliten la valoración de riesgos, profundizando en la línea de cooperación iniciada con la creación de la Comisión Mixta de Seguridad Privada de Euskadi.

HIKVISION



Msmart



COVERT

C A M E R A

SE ADAPTA A CUALQUIER LUGAR TODO LO VE

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

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

First Choice for Security Professionals

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

España

Distribuidores Oficiales

Portugal



GLOBAL DISTRIBUTION
www.es-eshop.adiglobal.com



SISTEMAS DE SEGURIDAD
www.casmart.es



www.hommaxistemas.com



Bernardo da Costa

www.bernardodacosta.pt

Pública representada por la Ertzaintza y la Seguridad Privada, a fin de lograr una mejora de la seguridad ciudadana.

—Desde la Unidad de Seguridad Privada de la Ertzaintza, de la que usted es su máximo responsable, siempre se ha apostado por reforzar y potenciar la cooperación y colaboración, ¿qué iniciativas se han llevado a cabo con el sector de la Seguridad Privada?

—La aprobación el año pasado de la Ley de Seguridad Privada nos sirvió de impulso para ampliar esta relación con el sector, que desde hace muchos años llevábamos ejerciendo.

En el año 2014, hemos impartido varias charlas informativas a todas las partes implicadas, tanto sobre la Ley 5/2014 como del Decreto 207/2014, todo ello con finalidad divulgativa acerca del alcance del cambio normativo y la nueva relación, que en algunos casos, se establece con esta Unidad a consecuencia de las modificaciones derivadas del artículo 13 de la Ley.

Así mismo, canalizamos la asistencia a distintas acciones formativas que se imparten en la Academia Vasca de Policía y Emergencias de Arkaute, que dentro

de las Jornadas Parez Pare se imparten sobre distintas materias de interés, como por ejemplo, materias referentes a Protección del Patrimonio Histórico y el Medio Ambiente, principios Teóricos y Operativos del Perfil Criminológico, Mediación, etc.

Dado la notoria actualidad y amenaza que representa el terrorismo internacional, durante este año 2015, y enmarcadas en esta relación de colaboración y cooperación, en el mes de abril hemos organizado un primer seminario sobre Islamismo Radical, impartido por nuestros expertos de la Oficina Central de Inteligencia, dirigido a directores de departamentos de Seguridad, empresas y detectives. Debido a la gran acogida en el sector hemos planificado acciones similares, durante los meses de octubre y noviembre, al objeto de hacer más extensivo el conocimiento sobre dicha problemática.

—¿Podría facilitarnos datos del sector de la Seguridad Privada en el País Vasco –número de empresas, vigilantes, detectives...?

—En lo referente a establecimientos obligados a disponer de medidas de seguridad, controlamos 4.172 estable-

cimientos, entre entidades bancarias, loterías, gasolineras, etc.

Actualmente están inscritas en el Registro Vasco de Seguridad Privada, 30 empresas de seguridad de ámbito autonómico; 27 de ellas dedicadas a instalación y mantenimiento, y 3 a vigilancia y protección. Además, contamos con 32 centros de formación.

De ámbito nacional tenemos contabilizados 36 despachos de detectives, 41 empresas con sede en la Comunidad Autónoma y 54 delegaciones de empresas.

En cuanto a personal de seguridad privada, están dados de alta en nuestro registro 4.111 vigilantes de seguridad, 231 escoltas y 45 detectives privados.

—El próximo 30 de septiembre se celebrará el II Congreso de Seguridad Privada en Euskadi, ¿qué aporta al sector iniciativas como éstas donde se potencia el intercambio de ideas y debate?

—Desde la Unidad de Seguridad Privada de la Ertzaintza acogemos con gran interés la celebración en Bilbao de este II Congreso de Seguridad Privada de Euskadi. Por un lado, constituye la consolidación de este foro de encuentro con el sector en el País Vasco y, por otro lado, como garantes directos de la seguridad pública en Euskadi, entendemos que es una gran oportunidad para el intercambio de ideas, inquietudes, conocimientos y experiencias.

Iniciativas como ésta constituyen en sí mismas un valioso instrumento de acercamiento y aproximación entre todos aquellos, que desde distintos ámbitos, interactuamos con la finalidad de que la Seguridad, como pilar básico de la convivencia, alcance los niveles de garantía que exige una sociedad moderna. ●

TEXTO: Gemma G. Juanes.

FOTOS: USP Ertzaintza





Su negocio es nuestra prioridad



Tecnología



Vigilancia Móvil



Soluciones de Video Remoto



Vigilancia Presencial



Protección Contra Incendios

Con Securitas Óptima, solo tendrá que preocuparse por ofrecerle el mejor servicio a sus clientes.

La combinación de la tecnología inteligente y de nuestros conocimientos sobre seguridad hace posible una eficacia sin precedentes a la hora de proteger sus instalaciones 24 horas los 7 días a la semana.



Más información en

902 10 00 52

info@securitas.es
www.secureitas.es

EL CENTRO DE CONVENCIONES INTERNACIONAL DE BARCELONA (CCIB) VOLVERÁ A SER ESCENARIO DEL ENCUENTRO

La cuarta edición de Security Forum se celebrará el próximo mes de mayo

El evento tendrá lugar los días 25 y 26 de mayo

Tras tres ediciones, Security Forum se ha consolidado como un evento de referencia en el sector de la seguridad. Así es, en la pasada edición el encuentro superó todas sus expectativas con la asistencia de más de 5.500 visitantes profesionales, 245 congresistas y 73 expositores. Como un encuentro vivo que evoluciona adaptándose a las necesidades de los profesionales de la seguridad, la organización ha puesto en marcha toda la maquinaria para la celebración de una nueva convocatoria de Security Forum. El Centro de Convenciones Internacional de Barcelona (CCIB) será escenario los próximos 25 y 26 de mayo de Security Forum 2015, donde se seguirá apostando por reforzar el tejido empresarial de un sector en continua evolución.

SECURITY Forum ha sido durante tres ediciones el catalizador y generador de actividad empresarial incentivando las ventas y promoviendo debates, ideas, maneras de ver y de resolver aspectos alrededor de los complejos problemas del sector de la Seguridad. Por eso, ante esta nueva convocatoria, Security Forum, volverá a convertirse en un evento ágil, flexible y orientado a la creatividad, que responderá al espíritu emprendedor y audaz que caracteriza a las empresas y profesionales del sector de la Seguridad. Esa es la prioridad de la organización que ya prepara contenidos especializados e innovadores que se adapten a las inquietudes y demandas de los profesionales de la seguridad.

En Security Forum 2016 volverán a potenciarse los cuatro ejes clave que han caracterizado en sus anteriores ediciones:

- **Negocio:** Security Forum es una oportunidad para generar actividad económica en torno al sector de la Seguridad.
- **Conocimiento:** Security Forum ayuda a comprender los cambios, a ordenar el exceso de información y a gestionar conceptos e ideas que luego serán oportunidades.
- **Networking:** Security Forum ofrece un gran potencial de relaciones y posibilidades de contacto infinitas entre un gran número de profesionales, empresas, entidades y colaboradores asistentes.



- **Innovación:** Security Forum potencia la colaboración entre empresas, universidades, startups y centros tecnológicos.

Además, Security Forum 2015 volverá a contar con una zona expositiva donde las empresas mostrarán las últimas innovaciones en equipos y sistemas en CCTV, integración de sistemas de seguridad física, seguridad lógica, control de acceso, IP/redes, protección contra incendios, y protección contra robo e intrusión.

De manera paralela a la exposición se desarrollará de nuevo Diálogos Security Forum que entre sus objetivos destaca el analizar los nuevos riesgos y amenazas en un entorno global como el actual; conocer el estudio de las necesidades actuales de los mercados; intercambiar conocimientos y establecer vínculos de colaboración interprofesionales; y disponer de una visión sobre las principales tendencias en materia de seguridad. ●



Miramos por ti.



Lo que ocurre en las carreteras está en tus manos. Suceda lo que suceda (atascos, accidentes o inclemencias meteorológicas), tu trabajo consiste en que todo el mundo continúe desplazándose. Y el nuestro es ayudarte. Nuestras soluciones inteligentes de supervisión del tráfico te ayudarán a ver exactamente lo que ocurre en la carretera para que puedas adoptar las medidas adecuadas en cada momento.

Este camino empieza aquí,
visite www.axis.com/yourtraffic

Visítanos en la feria
TRAFIC en el stand
5E04 del 29 de
Septiembre al 2 de
Octubre en Ifema.



NORMATIVA, TECNOLOGÍA, FORMACIÓN...

Seguridad en entidades financieras

Directores y responsables de Seguridad analizan el momento actual de la seguridad en las instalaciones bancarias

EL avance de la sociedad -y en estos momentos todavía de incertidumbre económica- ha propiciado que las entidades bancarias hayan tenido que ir adaptándose a los continuos cambios de la misma, y en el caso que nos ocupa, en el ámbito de la seguridad. Un avance y adaptación que ahora también vendrá de la mano de la nueva Ley de Seguridad Privada ya en vigor, y del tan esperado Reglamento de Seguridad Privada. Por eso, son ellos, una vez más, los directores de

Seguridad de las entidades bancarias quienes toman la palabra para explicarnos, entre otros aspectos, su visión profesional ante los cambios que se avecinan con esta nueva normativa. Pero también la implantación de nuevos medios y medidas de seguridad, concretamente de prevención y protección. Medidas que también tienen su punto de apoyo en las tecnologías que avanzan rápidamente. Y han sido concretamente éstas las que han sido y continúan modificando la oferta de operar y

de servicios que ofrecen las entidades, lo que ha derivado en los ya conocidos como delitos cibernéticos.

Por eso ahora toca preguntarnos ¿Cómo ha cambiado la seguridad de las corporaciones bancarias en estos últimos años? ¿Cómo gestionan en estos momentos los directores de Seguridad de estas entidades bancarias la seguridad integral? ¿Qué aspectos del futuro Reglamento de Seguridad Privada afectarán al sector de la Seguridad Bancaria? ●



Presentando la primera cámara 7K de la industria

Uniéndose a la familia de Cámaras
HD Pro de 4K, 5K y 6K de Avigilon

Conoce más en avigilon.com

7K



MÁXIMA
CLARIDAD

MÍNIMO
ALMACENAMIENTO
Y ANCHO DE BANDA

avigilon™



JOSÉ MARÍA ARANA. DIRECTOR DE SEGURIDAD. LABORAL KUTXA

«Si nos dirigimos hacia la banca digital, tendremos que trabajar por la ciberseguridad»

UN modelo de seguridad integral propio para Caja Laboral - Laboral Kutxa, es el ambicioso proyecto en el que se encuentra inmersa actualmente la entidad, «en el que consigamos coordinar todos nuestros esfuerzos en seguridad física, corporativa, lógica, medios de pago, canales, prevención y seguridad laboral, cumplimiento normativo y otros», explica José María Arana, director de Seguridad de Caja Laboral - Laboral Kutxa, quien a lo largo de la entrevista expone la estructura del departamento que dirige, los riesgos a los que hacen frente, así como sus deseos de cara al Reglamento de Seguridad Privada, entre otros temas.

—**A grandes rasgos, ¿podría explicarnos los orígenes de Caja Laboral-Laboral Kutxa, así como nú-**

mero de oficinas, trabajadores,...?

—Caja Laboral forma parte de la Corporación Mondragón cuya estructura se configura en tres grandes grupos: Financiero, Industrial y Distribución, y que aunque funcionan autónomamente participan de una misma estrategia de conjunto.

Fue fundada en la llamada «primera etapa» del cooperativismo vasco en 1959, junto con otras cooperativas que nacieron siguiendo la filosofía cooperativista del sacerdote e impulsor de Mondragón Corporación Cooperativa (MCC) José María Arizmendiarieta.

Arizmendiarieta concibió Caja Laboral como una entidad financiera, que promoviera el ahorro popular para posteriormente canalizar los recursos hacia el desarrollo cooperativo. Fue la primera entidad financiera en España en abrir sus oficinas por la tarde y la primera

institución financiera europea en recibir la «Q» de oro en calidad de gestión siguiendo el modelo EFQM. Su cuota de mercado en el País Vasco ronda en torno al 18% y cuenta con 368 oficinas bancarias distribuidas entre las comunidades de País Vasco, Navarra, Castilla-León, Madrid, Cantabria, Asturias, La Rioja, Aragón y Cataluña.

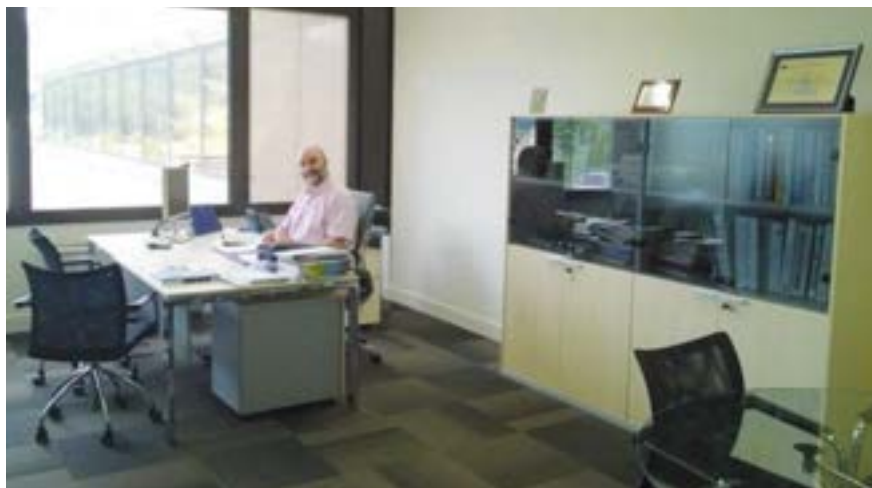
En la actualidad Caja Laboral Popular Coop. de Crédito, se presenta con el nombre comercial de «Laboral Kutxa» y sus ratios principales son:

– Core Capital (tier 1)	13,69%
– Liquidez (loan top deposit)	94,50%
– Morosidad	8,44%

—**¿Cuál es la estructura e infraestructura actual del área/departamento de Seguridad de Caja Laboral-Laboral Kutxa? ¿Podría concretarnos las funciones específicas del área?**

—El actual departamento de Seguridad de Caja Laboral está compuesto por 5 personas fijas en plantilla, de las cuales 2 de sus miembros son preventivistas y 2 técnicos competentes en autoprotección. Asimismo contamos con CRA con back-up propios y un servicio de vigilancia subcontratado, compuesto por 1 jefe de seguridad, 29 vigilantes y 2 azafatas-recepcionistas.

En estos momentos estamos inmersos en un ambicioso proyecto para conseguir un modelo de seguridad integral



propio para nuestra entidad, en el que consigamos coordinar todos nuestros esfuerzos en seguridad física, corporativa, lógica, medios de pago, canales, prevención y seguridad laboral, cumplimiento normativo y otros.

Bajo nuestra responsabilidad están la gestión y protección de los activos físicos (inmuebles, bienes y personas), la gestión de los centros de control y CRA, organización de los operativos especiales, control de accesos, CCTV, vigilantes, PCI, planes de autoprotección (gestión de continuidad, planes de contingencias, emergencias, etc.), control de altas-bajas de personal, representación corporativa en materia de seguridad y relación con juzgados, Fuerzas y Cuerpos de Seguridad, etc.

Colaboramos activamente en materia de prevención y seguridad laboral y con otros departamentos como cumplimiento normativo, auditoría interna, asesoría jurídica, RRHH, etc.



—¿Qué medios y medidas de seguridad cree que son necesarias en instalaciones como las de Caja Laboral- Laboral Kutxa?

—Desde hace dos años todas nuestras instalaciones están en GRADO III y estamos cumpliendo con un plan muy

ambicioso de sustitución de los cajeros automáticos y recicladores de efectivo. Nuestras oficinas cuentan con un alto grado de domotización y control remoto de instalaciones, tales como iluminación, clima, accesos tanto externos como internos (hemos sustituido



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

Tenemos el **toque**

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

piense dentro de la caja.



las llaves por tarjetas de proximidad), controlamos todos los movimientos de dinero entre contenedores de efectivo, tenemos una media de 10 cámaras por oficina, etc., y aunque todo es mejorable y contamos con unas muy buenas instalaciones de seguridad, tal vez nos haría falta algo más de procedimiento, formación y entrenamiento.

—¿Cuáles son los riesgos y problemas a los que tiene que hacer frente el responsable de Seguridad de Caja Laboral Kutxa en sus instalaciones bancarias?

—Entiendo que son similares a los que afrontan mis compañeros de otras entidades y, además de las preocupaciones clásicas, en los últimos tiempos nos está tocando lidiar con problemas relacionados con la situación social del país y el deterioro de la imagen de la banca en general.

—Hoy en día, el sector apuesta por la convergencia de la seguridad como concepto integral, ¿cree que las grandes corporaciones financieras están preparadas para asumir este nuevo tipo de concepto?

—Efectivamente, se trata de un concepto nuevo que lo que pretende es básicamente dos cosas.

Impregnar de Seguridad toda la actividad de la empresa.

Estructurar mediante un Plan Director, la coordinación de los distintos procedimientos de seguridad (física, informática, reputacional, corporativa, prevención y salud laboral, planes de autoprotección, medios de pago, continuidad del negocio, etc.) para que con el necesario cumplimiento normativo, podamos evitar que cada uno vaya siempre por libre provocando problemas competenciales, ineficiencias y en definitiva, inseguridad.

Los nuevos riesgos a los que nos estamos enfrentando, nos llevan inexorablemente por este camino, aunque en muchos casos no resulte fácil ya que la tendencia natural es que cada uno tienda a refugiarse en su propia parcela.

—Desde un punto de vista profesional, ¿cuál cree que es actualmente el nivel de seguridad de las entidades financieras de nuestro país, en relación con Europa?

—Aunque la Seguridad Privada en España, en algunos aspectos está siendo un ejemplo para la Europea, en la actualidad los mayores riesgos para la banca provienen del medio en el que nos movemos. Si nos movemos hacia la banca digital como parece, si caminamos cada vez más a través del ci-

berespacio, nos tendremos que cuidar del e-crimen y trabajar por la ciberseguridad. Se trata de un espacio sin banderas, ni españolas, ni europeas y tanto el riesgo como las regulaciones normativas y legales para protegernos de él son cada vez más internacionales.

—Entrando en temas de legislación y normativos, ¿que aspectos le gustaría que recogiese el Reglamento de Seguridad Privada?

Me gustaría que se desarrollará teniendo en cuenta:

- Los avances tecnológicos.
- El Ciber-crimen.
- La optimización de recursos entre la seguridad pública y la privada.
- Que ponga luz en determinados conceptos jurídicos relacionados con otras legislaciones como la LOPD en el tratamiento de imágenes, la libertad de información con respecto a la intimidad, etc.

—¿Cree que han cambiado los riesgos y amenazas de las corporaciones bancarias españolas, sobre todo en cuanto a aspectos de ciberseguridad?

—Rotundamente sí. Hoy nos preocupa más la confidencialidad de la información propia y la de los datos de nuestros clientes, el fraude en general pero también el que se realiza a nuestros clientes o el que proviene a partir de ellos, de proveedores externos o de otras entidades, el uso de identidades falsas en las transacciones, estafas a nuestros clientes y a otras entidades a través de muleros, la seguridad en los medios de pago (banca electrónica segura, Wallets, pagos por móvil, etc.), los riesgos reputacionales y en general todos los posibles ataques que pudieran venir desde el ciber-espacio. ●

TEXTO: Gemma G. Juanes.

FOTOS: Caja Laboral -Laboral Kutxa





CYRASA

ALQUILER DE EQUIPAMIENTOS PARA EVENTOS

Alquiler de equipos por días-mes-año

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

✓ **Cobertura nacional**

ESPECIALISTAS

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

ABSOLUTO COMPROMISO

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

OTROS SERVICIOS:

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

¡¡Contacte con nosotros!!

cyrasa@cyrasa.com

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



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

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

JOSÉ ENRIQUE LÓPEZ REGUEIRA. DIRECTOR DE SEGURIDAD FÍSICA. ABANCA



«La seguridad es un concepto integral que debe aportar valor a la entidad y a sus empleados»

La seguridad debe englobar necesariamente todos los aspectos posibles: seguridad en las operaciones, procesos, en el puesto de trabajo, y en las instalaciones. Este modelo de seguridad integral debe estar necesariamente alineado con los usuarios», son palabras de José Enrique López Regueira, director de Seguridad Física de ABANCA, quien explica a lo largo de esta entrevista, entre otros aspectos, los problemas a los que tiene que hacer frente su departamento o el nivel de seguridad de la entidades bancarias de nuestro país en relación a Europa.

—**A grandes rasgos, ¿podría explicarnos los orígenes de ABANCA, así como número de oficinas, trabajadores,...?**

—ABANCA nació en 2014 como un nuevo proyecto de banca minorista para empresas y familias, prudente, innovador, multicanal y con vocación de servicio al cliente. En España dispone de cerca de 700 oficinas, de las cuales más del 80% están ubicadas en Galicia y las demás están repartidas por el resto del territorio español, con especial presencia en Asturias y León.

ABANCA es fruto de un proyecto muy ambicioso en el que los cerca de 4.700 empleados que componen la plantilla son la piedra angular de un enfoque vol-

cado fundamentalmente en el cliente. En este sentido, nuestras oficinas están experimentando un cambio radical en el diseño de sus instalaciones para adaptarse a las necesidades de nuestros clientes.

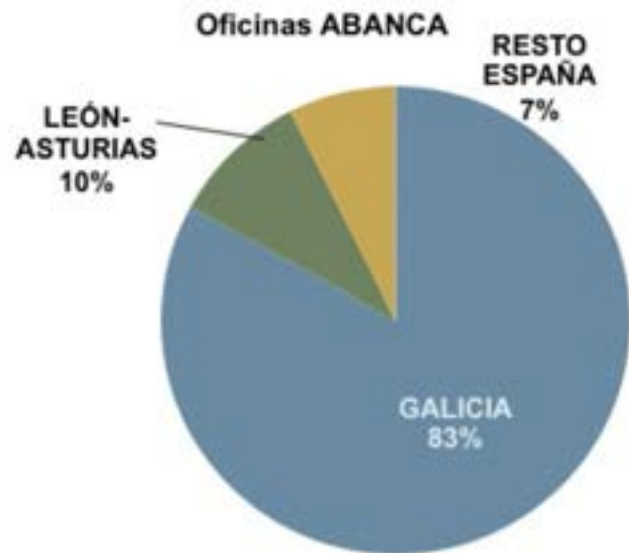
Es una nueva forma de ver la banca, es la búsqueda de un ambiente amigable y cercano que haga que entrar en un banco se convierta en una nueva experiencia.

Todo esto forma parte de un concepto que en ABANCA denominamos «Sentir Común».

—**¿Cuál es la estructura e infraestructura actual del área/departamento de Seguridad de ABANCA? ¿Podría concretarnos las funciones específicas del área?**

— El departamento de Seguridad Física de ABANCA depende directamente de la dirección general de Control Corporativo y Riesgos, y está integrado en el Área de Prevención de Pérdidas, Continuidad de Negocio y Seguridad. Además del departamento de Seguridad Física, cuyas funciones están claramente definidas por la ley, dentro del Área de Seguridad se encuadran el departamento de Seguridad Tecnológica, que desarrolla el Programa de Seguridad y Gestión de Riesgos de la Información para prevenir y/o responder





a cualquier amenaza que pueda poner en peligro los activos de información y la infraestructura que los soporta, el departamento de Depositaria y Gestión de Efectivo, que gestiona todos los procesos relacionados con el ciclo de efectivo, euro y billete extranjero, el departamento de Continuidad de Negocio que lidera la implantación de un sistema de gestión que permita prevenir y/o responder ante cualquier amenaza que pueda poner en peligro la consecución de los objetivos del banco, así como poner en peligro su supervivencia y, finalmente una gerencia de reciente creación para el análisis y tratamiento del fraude: la Oficina de Prevención de Pérdida y Fraude.

—¿Cuáles son los riesgos y problemas a los que tiene que hacer frente el responsable de Seguridad de ABANCA en sus instalaciones bancarias?

—A priori podría pensarse que, por la actividad que desarrollamos como entidad financiera, el principal riesgo al que tenemos que enfrentarnos es el atraco. Sin embargo, el ratio de atracos de ABANCA es de los más bajos del sector. Sin duda, a raíz de la sentencia del Tribunal Supremo de 2008 en la que

se consideraba el atraco como un accidente laboral, la entidad ha avanzado mucho en la respuesta a este tipo de riesgo. Así, casi el 100% de los trabajadores han sido formados en materia de atracos y éstos se han incluido como riesgo dentro del Plan de Autoprotección con el que cuenta cada una de nuestras oficinas.

Además, en colaboración con un centro universitario se está trabajando en un nuevo modelo de Evaluación del Riesgo de Atraco y Butrón en las oficinas, que determinará el nivel de riesgo en cada oficina teniendo en cuenta una serie de parámetros de partida, basados en los factores de riesgo implícitos a una entidad bancaria.

Por otro lado, para combatir los distintos tipos de fraudes y estafas por Internet se ha procedido a la creación de un departamento específico para el fraude.

En otro orden de cosas, dado que ABANCA es un proyecto de nueva creación que ha integrado a entidades preexistentes, el departamento de Seguridad ha abordado el reto de elaborar unas políticas de seguridad, alineadas con la nueva estrategia empresarial, que establezcan una cultura de seguridad común para todos los trabajadores.

Este es uno de los proyectos en los que nos encontramos inmersos y cuyo resultado será el Plan Estratégico y Operativo del departamento de Seguridad. Por último, el mayor hándicap al que nos enfrentamos en la actualidad los directores de Seguridad de las entidades bancarias es la adaptación de las instalaciones a la nueva Ley de Seguridad Privada, lo que supone un importante aporte económico para llevar a cabo una renovación de los sistemas, que deberán pasar a Grado III en un período de 10 años desde la aprobación de la ley.

—Hoy en día, el sector apuesta por la convergencia de la seguridad como concepto integral, ¿cree que las grandes corporaciones financieras están preparadas para asumir este nuevo tipo de concepto?

—Sin duda ese es el camino. La seguridad es un concepto integral presente en todos los niveles y operaciones del banco y debe aportar valor a la entidad y a sus empleados.

Recordemos que para el ser humano la seguridad está sólo por detrás de las necesidades básicas: necesitamos sentirnos seguros.

La seguridad debe englobar necesariamente todos los aspectos posibles: seguridad en las operaciones, procesos, en el puesto de trabajo, en las instalaciones. Este modelo de seguridad integral debe estar necesariamente alineado con los usuarios.

Es por ello que la formación en materia de seguridad es un factor muy importante para obtener unos resultados exitosos.

En este sentido, ABANCA apuesta firmemente por la información (formación+información) permanente para sus empleados. Además de cursos presenciales en materia de seguridad se dispone de un curso on-line, y de forma periódica se publican píldoras informativas como respuesta a un riesgo identificado, o como medida preventiva a posibles amenazas de las que se tiene conocimiento.

—Desde un punto de vista profesional, ¿cuál cree que es actualmente el nivel de seguridad de las entidades financieras de nuestro país, en relación con Europa?

—Los riesgos a los que se enfrentan los distintos países en Europa no son los mismos, y por tanto las comparaciones en materia de seguridad deben hacerse con cierta cautela.

En el caso concreto de nuestro país, la

ley se ha actualizado y establece unos niveles de seguridad y unos estándares para los sistemas que aportan un alto nivel de seguridad a los establecimientos obligados, dejando solo al factor humano el posible ataque a los sistemas.

—Entrando en materia de legislación y normativa, ¿que aspectos le gustaría que recogiese el Reglamento de Seguridad Privada?

—Mayor claridad y sencillez, para que no dé lugar a distintas interpretaciones locales o autonómicas.

En cuanto a las actuaciones de control periódico de las instalaciones, deberán adaptarse a las nuevas tecnologías. La inspección policial debería centrarse en el buen funcionamiento de las medidas de seguridad instaladas, dejando el control administrativo a inspecciones periódicas en los departamentos de Seguridad y en las empresas de instalación y mantenimiento homologadas. No tiene sentido enviar la documentación a las oficinas para su custodia, disponiendo también de esta documentación en el departamento en formato digital.

Por último, el papel del director de Seguridad debe tener mayor protagonismo como representante de la ley.

Así, al igual que recae en su figura to-

do el peso penal y administrativo de la ley ante alguna irregularidad, debe disponer de un rango de actuación más amplio que le atribuya mayores competencias y capacidad de actuación en las funciones que la ley le ha asignado.

—¿Cree que han cambiado los riesgos y amenazas de las corporaciones bancarias españolas, sobre todo en cuanto a aspectos de ciberseguridad?

—Con la llegada de Internet los avances tecnológicos son mayores. Si a esto le unimos el abaratamiento de la tecnología, se amplían las posibilidades de que se produzcan ataques.

Y un banco es una víctima muy atractiva para Black hats y otros esquemas fraudulentos como el phishing bancario, e-mails de estafa nigeriana, cheques falsos...

Si bien es cierto que las entidades bancarias cuentan en la actualidad con auténticos «muros de contención» capaces de reconocer y bloquear los malware con los que son atacados, hay una parte indiscutible de información a los empleados que no debe obviarse. ●

TEXTO: Gemma G. Juanes.

FOTOS: ABANCA





Innovación al servicio de la seguridad

- Equipos de inspección por rayos X
- Detectores de metales
- Equipos de inspección por ondas milimétricas

Excelencia en calidad y servicio post-venta.

TECOSA, la empresa de seguridad del Grupo Siemens, contribuye con sus productos y soluciones a hacer del mundo un lugar más seguro.



TECOSA

Telecomunicación,
Electrónica y Conmutación, S.A.
Grupo Siemens

w w w . t e c o s a . e s

JOSÉ ANTONIO SOLER DE ARESPACOHAGA. DIRECTOR DE SEGURIDAD DE LIBERBANK



«La prioridad que Liberbank tiene para clientes y empleados hace que la inversión en seguridad sea una apuesta real»

RESPECTO a los niveles de seguridad sobre instalaciones de oficinas, clientes, personal trabajador y efectivo, estamos a un magnífico nivel en nuestros departamentos de Seguridad, en relación con Europa», matiza José Antonio Soler de Arespacochaga, director de Seguridad de Liberbank, quien además hace hincapié en que «el cibercrimen es una de las principales amenazas en la actualidad».

—A grandes rasgos, ¿podría explicarnos datos concretos de Liberbank como por ejemplo, número de oficinas, trabajadores...?

—Liberbank es una entidad financiera producto de la integración de tres en-

tidades del sector de las Cajas de Ahorros: Cajastur, que a su vez era propietaria del 75% de CCM, Caja Cantabria y Caja Extremadura. En la actualidad contamos con 1.049 oficinas con un número total de empleados de algo más de 5.200.

La Entidad opera en todas las Comunidades Autónomas excepto Canarias, La Rioja y Navarra, e igualmente Ceuta y Melilla.

—¿Cuál es la estructura e infraestructura actual del área/departamento de Seguridad de Liberbank? ¿Podría concretarnos las funciones específicas del área?

—El departamento de Seguridad está

constituido conforme a la Ley de Seguridad Privada como establecimiento obligado que es Liberbank. Al ser operativo en prácticamente todo el territorio nacional, es necesario contar con personal desplazado in situ, en nuestro caso contamos con delegados de seguridad o responsables funcionales en Asturias, Cantabria, Extremadura y Castilla la Mancha, además de la dirección de Seguridad en Madrid.

Las funciones del departamento son igualmente, como no podría ser de otra forma, las definidas en la Ley con todas sus connotaciones referidas a una entidad del sector financiero.

—¿Qué medios y medidas de seguridad cree que son necesarias en instalaciones como las de Liberbank?

—Bueno sin querer ser reiterativo, serían los desarrollados en el Reglamento de la Ley de Seguridad Privada, aunque debo matizar que en los análisis de riesgos que se conforma en cada instalación, se complementan dichas instalaciones con las medidas que fueran necesarias y siempre por encima de las definidas en el citado Reglamento. Los plazos de adecuación a los niveles de seguridad que la nueva Ley marca están establecidos para su consecución, como igualmente a los plazos



marcados por las anteriores Órdenes Ministeriales.

Todas nuestras instalaciones estarán dotadas de las medidas reglamentadas, pero haciendo referencia de nuevo a que en algunos casos, por el análisis de riesgos que se efectúa individualmente en cada instalación, se dotarán de las medidas complementarias, orientadas siempre a la protección en primer lugar de nuestros clientes y nuestros empleados, manteniendo siempre el espíritu esencialmente social de una Entidad proveniente de las Cajas de Ahorros, las cuales se caracterizaron principalmente por su carácter social.

—**¿Cree que las grandes corporaciones financieras siguen apostando actualmente por la inversión en seguridad?**

—Sin duda, las grandes corporaciones siguen apostando por esta inversión, desterrando el antiguo criterio de ser un gasto, por el de una inversión. Liberbank, igualmente, sigue apostando por tanto. La prioridad que la entidad tiene para sus clientes y empleados, hace que sea una apuesta real. Igualmente comentar que los riesgos aparecen con cada nuevo servicio o producto o, podríamos decir más, con cada nueva tecnología. Los análisis que se realizan nos llevan al estudio de nuevas medidas que son necesarias en aras de la protección de los diferentes activos de Liberbank.

Lo cambiante de las nuevas tecnologías hace que igualmente seamos muy dinámicos en la adopción de diferentes formas de protección específicas en cada caso.

—**Hoy en día, el sector apuesta por la convergencia de la seguridad como concepto integral, ¿cree que las grandes corporaciones financieras están preparadas para asumir este nuevo tipo de concepto?**



—Sin duda el sector de la Seguridad naturalmente que ha evolucionado en los últimos años, producto de la multiplicación de los riesgos y como he comentado, estos riesgos han evolucionado con los nuevos productos y servicios de las grandes corporaciones. La totalidad de ellos está basado en la utilización de nuevas tecnologías de información y comunicación, lo que significa la utilización de redes de datos, públicas o privadas, por las que circulan billones de datos de operaciones y códigos de transacciones.

Esto da como resultado que una operación fraudulenta sobre este tráfico, multiplica exponencialmente el quebranto que anteriormente se podría producir en un atraco o robo e incluso en un asalto a una cámara acorazada. Consiguientemente se apuesta por integrar las diferentes fracciones de la seguridad de una gran corporación que hasta este momento afloraban en este sector en los últimos años.

Es muy común encontrar en las entidades pequeños grupos dedicados y especializados en la seguridad de diferentes áreas, como pueden ser los medios de pago, banca telefónica, o para no ser prolijo, en la denominada seguridad lógica. Todo esto sin entrar en el capítulo del riesgo reputacional al que se está sometido en el caso de

por ejemplo una violación en bases de datos de tarjetas o de números secretos de identificación, sistemas contables, etc. Sobre si estamos preparados, yo apuesto por un sí determinante, lo que hay que hacer es integrar los diferentes grupos aludidos, bajo una única dirección de seguridad, como marca la Ley, quien deberá estar preparado para gestionar los diferentes y variados recursos que esto conforma, lo que en algunos casos podrá traer cambios en los perfiles humanos y formativos de estas direcciones.

La evolución en este sentido, tanto en EEUU como en los principales países europeos, viene marcada por la incorporación en la cúpula del área de seguridad de la Entidad, de personas procedentes del mundo de las tecnologías, especialistas en sistemas operativos, redes de comunicación, etc. alejándose del perfil de los expertos en las protecciones denominadas de seguridad física, tanto para edificios, personas o efectivo.

—**Desde un punto de vista profesional, ¿cuál cree que es actualmente el nivel de seguridad de las entidades financieras de nuestro país, en relación con Europa?**

—Sin duda respecto a los niveles de seguridad sobre instalaciones de ofi-

cinas, clientes, personal trabajador y efectivo, estamos a un magnífico nivel en nuestros departamentos de Seguridad. Simplemente ver las estadísticas sobre hechos delictivos a lo largo de estos últimos años en nuestras corporaciones, con su repercusión en el quebranto económico o igualmente en el transporte de efectivo o valores, etc., así lo demuestra.

Que duda cabe que mucha culpa de ello la tiene la evolución igualmente de las Fuerzas de Seguridad del Estado y Autonómicas, donde tanto la Unidad Central de Seguridad Privada del Cuerpo Nacional de Policía, como el SEPROSE de la Guardia Civil, ha desarrollado una nueva legislación para el siglo XXI, dejando constancia así mismo de su preparación.

Pero respecto a esos mismos niveles de seguridad sobre sistemas de tecnolo-

gías de información y comunicación, desde mi punto de vista, habrá que esperar a la integración referida en la pregunta anterior, para poder efectuar una comparación real con el resto de países del primer mundo. Se puede afirmar que, por los resultados que se conocen, no estamos a un nivel muy diferente, pero la integración nos dará una visión real de dónde estamos.

—**Entrando en temas de legislación y normativos, ¿qué aspectos le gustaría que recogiese el Reglamento de Seguridad Privada?**

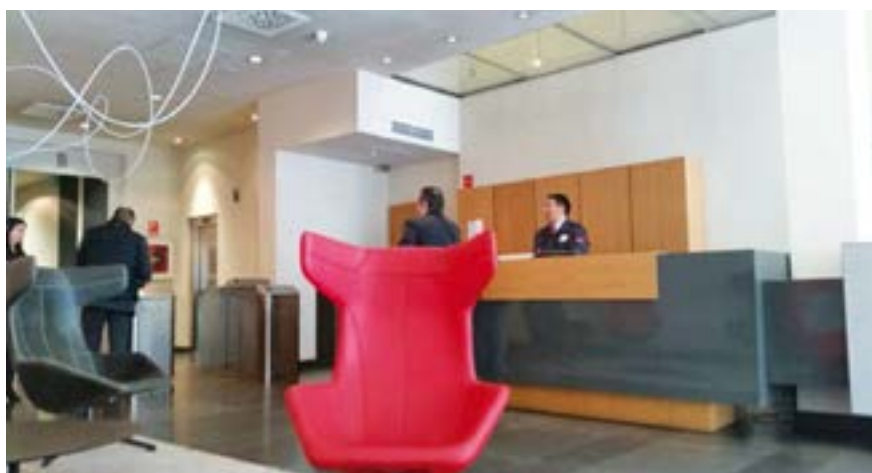
—Precisamente al hilo de lo comentado en las anteriores preguntas, me gustaría que se profundizara en los aspectos de la seguridad de las nuevas tecnologías de información y comunicación, al nivel de las especificaciones que se recogerán sobre los elementos de protección

puramente físicos. Hay que decir para ser justos, la gran dificultad que esto supone, pues es sumamente difícil de profundizar por la inmensa variedad existente de sistemas operativos, tipología de redes, desarrollos establecidos o simplemente las filosofías sobre la utilización de Internet, que no olvidemos se creo como una red libre sin seguridad ni limitaciones de uso.

Pero de cualquier forma estoy convencido que será el próximo paso, pues las amenazas son reales e importantes, lo que sin duda desembocará en una legislación acorde con este, digamos, nuevo entorno.

—**¿Cree que han cambiado los riesgos y amenazas de las corporaciones bancarias españolas, sobre todo en cuanto a aspectos de ciberseguridad?**

—Por favor claro que han cambiado. En las contestaciones anteriores lo he comentado, pero sobre este tema de la ciberseguridad o el ciberespacio, le agradezco la pregunta, pues como sabe siempre ha sido uno de mis capítulos preferidos y de los que más me han demandado en cursos o conferencias. Seguramente mi procedencia profesional del mundo informático me ha llevado a ello intentando ser especialmente sensible y estudioso sobre este particular. Pero yo no dejaría estos cambios en los riesgos únicamente en las grandes corporaciones bancarias, estas amenazas se ciñen sobre todo tipo de instalaciones, bancarias, industriales e incluso gubernamentales. Cuántas noticias nos llegan sin explicación alguna sobre ataques cibernéticos a países y gobiernos o instalaciones industriales. Uno de los resultados ha sido el desarrollo de la Ley de Protección de Infraestructuras Críticas. No tengo la menor duda que el cibercrimen es una de las principales amenazas en la actualidad. Para entender esto fácilmente, pue-



do ponerle muchos ejemplos, uno de ellos la explosión de un gaseoducto en Rusia. ¿Cómo se puede producir? Pues generando en la red de datos de dicha instalación una ficticia baja de presión en el transporte del gas. Esto genera la reacción automática de un aumento de presión en dicho transporte, que al ser ficticia la bajada, origina una explosión por sobrepresión.

¿Quién nos puede asegurar, la inviolabilidad de un sistema informático en una aeronave?, pues la alteración de rutas y parámetros, sin percepción en los indicadores de a bordo, llevaría a dicha aeronave a un lugar indeterminado y de difícil descubrimiento. Quizás pueda asociarlo a algún caso que le suene ¿verdad?

En definitiva no quiero ser reiterativo por lo mucho que me apasiona este tema, sobre una posible ciberguerra, pero qué duda cabe que no es el futuro, muchos hechos nos dice que es



el presente y por eso es necesario ponerse las pilas, actualizarse, para que lo que ahora se vislumbra más como un tema de película, no llegue a ser un hecho irreparable, y que dentro de un tiempo las noticias que hoy tenemos se queden como un mal recuerdo.

Agradezco a Cuadernos de Seguridad su constante labor divulgativa en favor de

la Seguridad que a la postre desemboca en una mejor calidad de vida y una tranquilidad en las obligaciones y servicios de nuestras Entidades, como así mismo la oportunidad de aparecer en vuestra prestigiosa publicación, gracias. ●

TEXTO: Gemma G. Juanes.

FOTOS: LIBERBANK

NUEVO CoSOFT PATROL CONTROL

Su móvil con tecnología »NFC» será su Control de Rondas



- Captura y envío de datos e imágenes y posición GPS en tiempo real.
- Visualización y generación de informes desde la web.
- Utilizable en rondas interiores y exteriores.
- Ideal para patrullaje móvil.
- Permite vigilancia remota.
- Compatible con la mayoría de los teléfonos Androide con tecnología NFC, y con puntos de fichaje Benzinger.



ANDRÉS MARTÍN LUDEÑA. DIRECTOR DE SEGURIDAD DE EVOBANCO

«El futuro de la Seguridad Privada pasa por la formación»



EN EVO partimos de la ventaja de disponer de un equipo humano que tiene un fuerte compromiso con la marca y con el proyecto, escenario que facilita mucho el trabajo del departamento de Seguridad», explica Andrés Martín Ludeña, director de Seguridad de EVO Banco, quien asienta en tres pilares fundamentales una adecuada seguridad bancaria: emotividad, focalización y proactividad.

—¿Cómo ha variado la seguridad, en cuanto a estrategia y logística, en las grandes entidades bancarias de nuestro país en los últimos años?

—Desde el año 2009, el sistema financiero español está acometiendo una reordenación muy agresiva. En este periodo de tiempo han teni-

do lugar fusiones y absorciones entre entidades, hemos visto desaparecer el modelo español de las Cajas de Ahorro —muchas de ellas centenarias—, subastas, segregaciones, liquidaciones, nacimientos de nuevas entidades, aterrizajes en España de entidades extranjeras que aún no tenían presencia y salidas del país de otras.

Nada de lo dicho es ajeno a los departamentos de Seguridad, por el contrario, su trabajo se ha multiplicado, complicado y enredado hasta niveles que eran impensables en el año 2008. Ello nos ha obligado a adaptarnos a estos tiempos y hacer de la urgencia y la excepcionalidad algo ya cotidiano; de la necesidad virtud; de la crisis oportunidad y de la experiencia y las mejores prácticas una herramienta imprescindible.

A lo anterior hay que sumar la com-

plejidad de la integración de diferentes culturas de seguridad heredadas para un tiempo de transición; tiempo que todavía sigue abierto y sin fecha de caducidad visible. Hemos tenido que enfrentarnos a un escenario de nuevas amenazas que en nada se parecen al mapa anterior al año 2009. Hemos sufrido mucho con la pérdida de reputación del sector, motivada por la crisis financiera internacional. Hemos visto la pérdida de talento por la marcha de excelentes profesionales, motivada por los procesos de liquidaciones y prejubilaciones anticipadas.

Para terminar de complicar la situación descrita nos hemos visto obligados a trabajar y construir en escenarios de severas limitaciones presupuestarias y con un factor que ha crecido de manera exponencial, me refiero al «apetito de riesgo» de las organizaciones.

En resumen, todos los departamentos de Seguridad de entidades financieras—sin excepción— nos hemos visto obligados a trabajar durante el último lustro en un «escenario de batalla» donde la ejecución, la urgencia y la austeridad han primado sobre la planificación y este es un lastre que arrastramos aún. EVO es un banco joven, lleno de ilusiones y con marcada vocación de servicio al cliente. Nacido en fecha 9 de noviembre de 2013, con un crecimiento importante desde esa fecha. Su realidad diaria no difiere en mucho de la que tienen otras entidades financieras; si bien, nuestros problemas están acordes con nuestro tamaño. Partimos de la ventaja de disponer de un equipo humano que tiene un fuerte compro-

miso con la marca y con el proyecto, escenario que facilita mucho el trabajo del departamento de Seguridad.

—**¿Cómo es el día a día, en cuanto a planificación y organización para el responsable de una entidad bancaria como EVO Banco?**

—Crear un banco nuevo en España es una oportunidad única para tratar de volcar en el proyecto toda nuestra experiencia y conocimientos.

Es la ocasión de generar un laboratorio de ideas en el que de manera transversal todos los actores de la marca participan y aporten.

Es un momento singular para cimentar ideas y objetivos con solidez y para disfrutar de la profesión.

—**Entrando en temas normativos y de legislación, ¿qué aspectos le gustaría que recogiese el Reglamento de Seguridad Privada?**

—El futuro Reglamento de Seguridad Privada debería reflejar el nivel de madurez alcanzado por el sector en España, sin olvidar que el apetito de riesgo de las organizaciones es cada día mayor y por ello conviene fijar un capítulo de mínimos, sin los cuales no esté permitido desarrollar una actividad profesional concreta.

Tampoco debería dejar sin atar algunos apartados que considero importantes:

- El engarce de la seguridad de la información en las organizaciones.
- El nuevo mapa de sujetos obligados.
- El catálogo de medidas de seguridad físicas, electrónicas e informáticas a implementar en cada caso.
- El catálogo de medidas organizativas a desarrollar por los sujetos obligados, huyendo del concepto «planes» para abordar el de «sistemas de gestión».
- El modelo de cualificación y el de habilitación exigido a los profesionales y a las empresas según presten servicios para Infraestructuras Críticas, para otros sujetos obligados o para aquellos que, sin estar obligados, desean disponer de servicios o sistemas de seguridad en sus instalaciones.

—**¿Se han llevado a cabo en los últimos**

años mejoras en cuanto a infraestructuras de seguridad en las diferentes sucursales de EVO Banco?

—Las mejoras en los sistemas e instalaciones son continuas, ya que parte de las mismas estaban en nivel dos en el momento del nacimiento del banco, y por ello las vamos migrando a nivel tres de manera paulatina. Aunque reconozco que hemos sido muy cautos a



SOLUCIONES AVANZADAS PARA LA GESTIÓN TÉCNICA DEL EDIFICIO

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

DIVISION DE CONTROL DE EDIFICIOS



www.setelsa.net



la espera del desarrollo del nuevo Reglamento de Seguridad Privada.

—¿Cree que han cambiado las amenazas y riesgos de las entidades bancarias, sobre todo en cuanto a aspectos de ciberseguridad?

—La evolución de las nuevas tecnologías está siendo tan rápida que apenas da tiempo a la amortización de los equipos que las soportan.

Este ritmo de crecimiento necesita de un acompañamiento de la misma velocidad de evolución y de respuesta en los equipamientos de seguridad.

Pese a ello y a las constantes inversiones realizadas, a la formación continua que se realiza y a la alta concienciación de los empleados, de cuando en cuando se presenta una incidencia que hay que identificar, bloquear y analizar para evitar su proliferación.

Es un trabajo que no tiene fin, que requiere de una alta especialización y de una vigilancia continua.

—¿Cuáles considera que son hoy en día los pilares sobre los que debe asentarse una adecuada seguridad bancaria?

—Los pilares son tres:

- «Emotividad», entendida como la vocación y preparación para enfrentarse a los problemas y el empeño en resolverlos.
- «Focalización», que es la capacidad para distinguir de manera innata lo importante de lo que no lo es.
- «Proactividad», en lo referente a ir por delante en materia de prevención, innovación, formación y planificación.

—¿Qué papel cree que debe ocupar la formación actualmente en el ámbito de los profesionales de la Seguridad Privada?

—El futuro de la Seguridad Privada pasa por la formación, no caben atajos en esta materia.

«El futuro Reglamento de Seguridad Privada debería reflejar el nivel de madurez alcanzado por el sector en España»

Debemos ser muy exigentes en ello, de lo contrario no veo posibilidad de crecimiento para el sector y cada vez seremos más marginados y menos valorados.

En el desarrollo de la Ley 5/2014 faltó decisión a la hora de separar la cualificación de la habilitación y en exigir un mejor nivel académico.

A mi juicio la cualificación debería ser competencia exclusiva del Ministerio de Educación y Cultura, por el contrario la habilitación debería ser competencia exclusiva del Ministerio del Interior.

No entiendo que a los Vigilantes de Seguridad no se les exija un nivel

académico de Formación Profesional. Tampoco entiendo que a los directores y jefes de Seguridad no se les exija el Grado Universitario en Seguridad. En ambas actividades hay suficientes materias para el estudio, y es evidente que la respuesta que espera la sociedad de nosotros obliga a una formación mucho más exigente y rigurosa.

Tampoco entiendo que determinados puestos de directores de Seguridad no tengan una exigencia de experiencia acreditada en el desempeño profesional de, al menos, cinco años. Me refiero concretamente en las infraestructuras críticas y en los sujetos obligados; sin ésta exigencia estamos haciendo un flaco servicio a la Seguridad Nacional y soy consciente que, al decir esto, no estoy haciendo amigos precisamente, pero tras más de 30 años dedicados a la seguridad pública y la seguridad privada me considero con suficiente autoridad moral y conocimiento para decirlo. ●

TEXTO: Gemma G. Juanes

FOTOS: EVOBanco



Déjate enganchar por **nuestra red**



Descubre en nuestros canales online todo lo que necesitas saber sobre el sector de la Seguridad.

 [cuadernos-de-seguridad](#)

 [@PuntoSeguridad](#)



JUAN MANUEL RODRÍGUEZ ZARCO. DIRECTOR DE SEGURIDAD Y GESTIÓN DEL EFECTIVO. BANKIA

Un golpe de timón necesario

PARA hablar del futuro de la seguridad en las entidades financieras, como es la tarea que me ha encargado la redactora-jefe de Cuadernos de Seguridad, dejaremos a un lado la Ley de Seguridad Privada y su Reglamento que nadie sabe cuándo verá la luz; dejaremos de lado las fuertes inversiones que se están llevando a cabo para actualizar a grado la seguridad física y electrónica antes de 2021 (¿o 2024?) y dejaremos los clásicos asuntos del sector porque hoy es necesario hablar -y mucho- del presente, pues en él se está desarrollando una discreta pero tenaz pugna por dirigir las distintas funciones

que afectan a los riesgos actuales y, sobre todo, de los próximos años.

Puestos de responsabilidad

Para ahondar un poco en este pulso no es necesario recurrir a los cada vez más crecientes puestos de responsabilidad de los nuevos riesgos en los países anglosajones o de su área geográfica de influencia, en los que los CISO, CSO, CIO, CRO y otros acrónimos detrás de los que está la seguridad en sus distintas vertientes, tratan de determinar la evolución de aquellas situaciones que pueden originar impacto en

sus empresas, en la mayoría de las ocasiones utilizando similares recursos técnicos o fuentes de información o análisis en los que se mezclan datos que corresponden a distintas funciones y especialidades, en un confuso laberinto del que cada día se sale con más dificultades, lo que no tardará en animar a las empresas a simplificar sus esquemas de protección.

Ataques a cajeros automáticos, estafas...

Para envenenar más la partida, el mundo criminal no entiende de especialidades o, mejor dicho, le importa muy poco, actúa allí donde ve un buen beneficio: a distintos niveles jerárquicos, interviene en ataques a cajeros automáticos, hackea, estafa, participa en redes de prostitución o vende kalashnikov a lobos solitarios que buscan su minuto de gloria en nombre del DAESH, en una Europa con fronteras muy permeables, que no sólo facilita y agiliza el comercio y los negocios, sino la trashumancia de toda suerte de delincuentes. Y combatirlos, en la medida que lo hacen las empresas privadas, no será fácil hacerlo con pequeñas plantillas y aislamiento de las distintas responsabilidades en el tratamiento de los riesgos.

Para el Ministerio del Interior español, cuyas últimas normas intuyen este panorama y se están dirigiendo, quizá con excesiva cautela, hacia una centra-



lización de funciones de aquellas actividades de prevención que tienen que hacer frente a delitos que se entremezclan con independencia de su origen o naturaleza. En definitiva, hacia una deseada seguridad integral. El robo de identidad o de datos de empresas o particulares puede empezar en Malasia, Lituania, Estonia o China, pero una

la búsqueda de soluciones integrales de servidores, almacenamiento y centros de control que hagan frente a una desbordante capacidad de tratamiento informático y envío de información, debido al vertiginoso aumento en el número y calidad de sus equipos de filmación y grabación, o las nuevas aplicaciones que permiten efectuar un amplio tra-

cuando se accede a determinadas páginas de la «deep Web» o Internet profundo conteniendo relaciones interminables de datos de ciudadanos.

La tabla de nuevos riesgos que empiezan a detectar las entidades convierte en un difícil enfrentamiento las estructuras clásicas que hoy rigen en la mayoría, y que son de complicada coordinación, hacen necesario un replanteamiento de las funcionalidades aglutinándolas en una única cabeza rectora, cuya plasmación debe estar alejada de bienintencionados comités.

Este golpe de timón nos recuerda, en fin, que la formación de los directores de Seguridad debe ser, de una vez por todas, universitaria (produce sonrojo su ausencia en la lista de nuevos estudios de grado) con una amplia gama de conocimientos técnicos que les permitan gestionar, con los equipos adecuados, tan complicado puzzle de riesgos. ●

«La tabla de nuevos riesgos que empiezan a detectar las entidades convierte en un difícil enfrentamiento las estructuras clásicas que hoy rigen en la mayoría»

vez que el troyano ha hecho su devastador efecto, alguien (una «mula» o un delincuente) tiene que «mover» el producto de la transacción fraudulenta.

En este contexto, las entidades financieras españolas, foco de todo tipo de organizaciones delictivas por la mercancía que manejan, no son ajenas a esa estrategia de sus colegas anglosajonas con la creación de nuevas funciones que también tienen como objetivo la gestión del riesgo, pero sería injusto no señalar que, paralelamente, están haciendo un esfuerzo presupuestario ante el cada vez más preocupante desarrollo de la delincuencia cibernética, que si bien dirige en gran medida sus acciones hacia particulares o pymes, no es extraño que cada vez con más frecuencia evalúen el nivel de protección de los sistemas de información de las propias entidades, con ataques de denegación de servicio u otros, hasta ahora infructuosamente.

Tecnología

La tecnología, encaminada a colaborar eficazmente en muchos campos de la seguridad de las empresas, como

tamiento de inteligencia empresarial cuyo objetivo está aumentando notablemente la prevención de delitos o de situaciones conflictivas, la tecnología, digo, no pide señas de identidad a los que la utilizan y puede asegurarse que es fácil sufrir un inquietante cosquilleo

Fotos: *Designed by freepik.com.*





EDUARD ZAMORA. DIRECTOR DE SEGURIDAD CORPORATIVA.
GRUPO BANCO SABADELL

Renovarse o morir

¿Cómo afecta a la Dirección de Seguridad de una entidad bancaria como Banco Sabadell la notable expansión desarrollada por la entidad?

S entre la febril actividad de fusiones que se ha dado en los últimos años en el sector financiero hubiera que destacar alguna entidad como paradigmática, sin duda, esta sería Banco Sabadell.

La notoriedad ganada por el Grupo, ya en el cuarto lugar entre las entidades financieras privadas españolas, algo impensable para aquellos empleados de la entidad que hace ya 25 años nos integramos en la misma, evidencia que, afortunadamente, todo es posible en el mundo empresarial. Tan sólo hay una premisa básica, gestionar la empresa como el entorno actual exige:

de manera eficiente, adaptada a los requerimientos del mercado y a las necesidades de nuestros clientes, reforzando la modernización de las actividades designadas como «core» de la entidad.

Estas condiciones tan elementales en toda empresa me sirven para entrar ya en la materia que la editorial me pide hoy tratar, reconociendo, en primer lugar, la dificultad de muchas entidades para reconocer entre sus actividades prioritarias, en su «core», a lo referente a seguridad y, por ende, ubicarlas orgánicamente en el lugar adecuado para facilitar el mejor desarrollo de sus funciones-misiones.

En otras, como afortunadamente ha sido nuestro caso, se toma conciencia de que la seguridad, como otras parcelas de gestión y gobierno que no son

estrictamente «productivas», han de atenderse con el máximo rigor, estableciendo las políticas de mayor efectividad en cada una de ellas, adaptándolas a las necesidades del momento, justo en un periodo como el que vivimos en que no tan sólo debe ya primar el rendimiento económico por encima de todo y a cualquier precio, sino que aquél debe conjugarse con un alto grado de aplicación de las mejores y más correctas políticas de «gobernanza», responsabilidad social corporativa, imagen reputacional, auditoría y control internos, cumplimiento normativo y, cómo no, todas ellas acompañadas de una mínima repercusión delictiva en todos sus ámbitos, tanto de los que puedan cometerse por los integrantes de la entidad, como los que afecten a la misma desde el exterior, además de minimizar los impactos a los clientes, que deben percibir que la actividad bancaria ofrece unos parámetros adecuados de seguridad operativa, puesto que no hay que olvidar que existimos con el objetivo de disponer del máximo de clientes y de operativa de los mismos, conjugados con las correctas políticas internas antes comentadas.

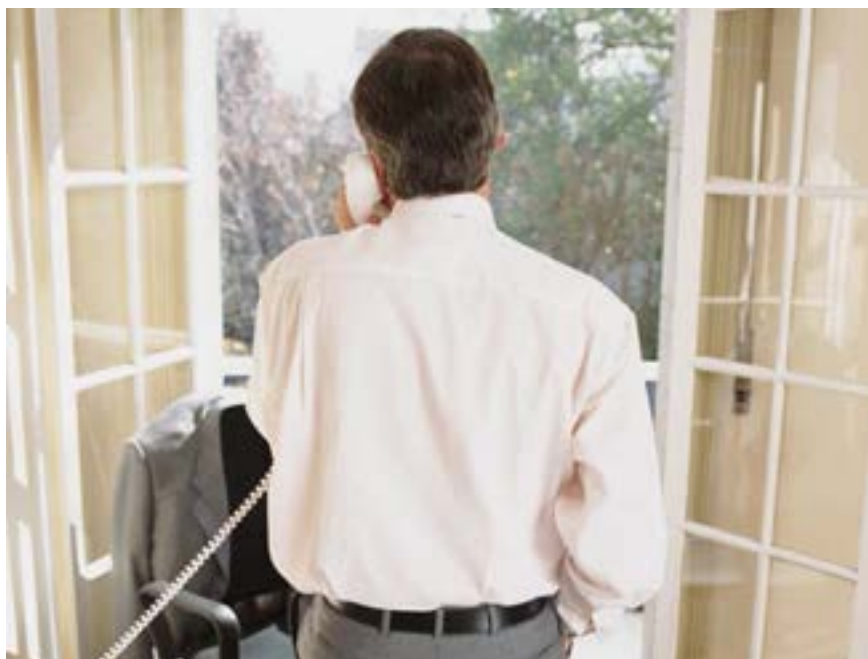
Entrando ya en materia más propia de la Dirección de Seguridad, este ámbito ha de potenciar su estatus en el organigrama, puesto que la ubicación adecuada imprime a su actividad una relevancia y credibilidad que se dificul-



taría de estar en la banda más baja del esquema organizativo de la empresa.

También hemos de olvidarnos de trabajar como un «lobo solitario» dentro de la entidad, puesto que, cada vez más, nuestra interrelación con el resto de ámbitos de la misma es más necesario para el logro de nuestros objetivos globales y nuestra efectividad se verá, sin duda, repercutida en la medida en que seamos capaces de lograr esa correcta cooperación con el resto de actividades del Grupo, con el objetivo final de que todo producto, procedimiento y servicio que implanten dispongan del correcto punto de equilibrio entre nuestra responsabilidad en materia de seguridad y sus objetivos intrínsecos. Con frecuencia ésta es una de las funciones de mayor dificultad: la de lograr ese equilibrio idóneo entre la seguridad y los intereses propios de cada Dirección del Grupo.

En relación a evitar esta «solitud», y ahora desde el punto de vista externo, hemos de reorganizar nuestra interrelación con el resto de entidades sectoriales y con la Administración. Con todas ellas ha de ser una tarea fácil, puesto



da una de las direcciones del Grupo, por lo que, obligatoriamente, hemos de reinventarnos. Tan sólo así podremos aportar el mayor valor añadido a nuestras entidades.

Ha llegado el momento de pensar en nuevos organigramas de las Direcciones de Seguridad, en nuevas funciones, en implantar departamentos de innovación,

do nuevos riesgos y nuevas realidades delictivas, que nos llevarán a implantar nuevas y mejores medidas, ya muy alejadas de los estereotipos anticuados que tan sólo nos asociaban con los vigilantes y las alarmas.

Hoy hemos de convivir con los más altos y universales riesgos, además de con las más estrictas normativas y regulaciones jurídicas al respecto de los mismos.

Si no somos capaces de adaptar nuestras estructuras a todo este nuevo entorno y necesidades empresariales, no nos haremos mercedores de la mejor consideración dentro de nuestras entidades, recibiendo el castigo de «subsistir» por imperativo legal, pero nunca estar valorados en la justa medida, en lo que considero personalmente que ha de ser un alto estatus, dado lo mucho que podemos aportar a la empresa. En definitiva, «renovarse o morir», como reconoce el refrán basado en la frase de Unamuno «el progreso consiste en renovarse», o como dijo Newton: «si he podido ver más lejos ha sido gracias a los gigantes en cuyas espaldas me he subido». ●

«Ha llegado el momento de pensar en nuevos organigramas de las Direcciones de Seguridad, en nuevas funciones»

que todos tenemos los mismos objetivos y todos-todos deberíamos olvidar disputas de «egos», oscurantismos o voluntad de perjuicio de ningún tipo. Tan sólo trabajando al unísono, con reciprocidad, mejoraremos nuestro conocimiento del mercado delictivo y, en consecuencia, las valoraciones de riesgos y determinación de medidas preventivas y reactivas aplicables.

En cuanto a la organización interna de la Dirección de Seguridad, no podemos vivir al margen de la modernización organizativa y funcional de ca-

tanto tecnológica como organizativa; de valoración de la repercusión de la seguridad en los muchos proyectos de la empresa; de seguimiento de la efectividad de las medidas de seguridad, organizativas o materiales, en los mismos; etc.

Entidades como Banco Sabadell, en continuo crecimiento e implantación en nuevos sectores y mercados, tanto nacionales como internacionales, como el desembarco en otros países, algo cada vez más habitual en las grandes corporaciones, nos permiten ir aprendiendo-mejorando cada día, conociendo-

Fotos: Archivo.



FRANCISCO GUERRERO. DIRECTOR DE SEGURIDAD.
UNICAJA BANCO

El Reglamento que viene

TRAS más de un año desde que entró en vigor la Ley 5/2014, de 4 de abril, estamos a la espera de que vea la luz el nuevo Reglamento de Seguridad Privada que la desarrollará.

Para la Ley anterior, la 23/1992, de 30 de julio, tuvimos que esperar casi año y medio a la publicación del aún vigente Reglamento de Seguridad Privada, y sin embargo, las previsiones no cumplidas para el nuevo Reglamento eran que vería la luz en estas semanas en las que estamos.

Todos los sectores están expectantes ya que se intuyen cambios importantes. Se prevé un Reglamento extenso y que, al igual que la ley, defina conceptos aparte de regular la actividad de las empresas y personal de seguridad, así como de las entidades de obligado cumplimiento.

Esto es especialmente importante para el sector de las entidades financieras ya que nada dice la nueva Ley sobre la seguridad en este tipo de entidades, por lo que prácticamente toda la legislación en este asunto vendrá de la mano del Reglamento.

A pesar de las numerosas incógnitas que plantea el desarrollo de la Ley 5/2014, una norma extensa en comparación con su antecesora, una primera idea sobre los cambios en el nuevo Re-

glamento la encontraremos en la definición que realiza de las funciones del director de Seguridad (art. 36), y que supone una novedad importante con respecto a la legislación anterior, que nada decía al respecto; de hecho no aparece la figura del director de Seguridad en la Ley, dejando al Reglamento su inclusión y definición, y el Reglamento tampoco la define limitándose a equipararlas con las recogidas para el jefe de Seguridad con la excepción de la gestión de las armas de los vigilantes de seguridad.

En este sentido, y comparando las funciones recogidas en la actual Ley para el director de Seguridad con las del

Reglamento para el jefe de Seguridad, encontramos algunos cambios sutiles, o no tan sutiles, como por ejemplo, y sin ánimo de ser exhaustivo:

El art. 95.1.b) del Reglamento recoge: «La organización, dirección e inspección del personal y servicios de seguridad privada», y el art. 36.1.a) de la Ley «La organización, dirección, inspección y administración de los servicios y recursos de seguridad privada disponibles».

Otro ejemplo lo tendríamos en el art. 95.1.a) del Reglamento que recoge «El análisis de las situaciones de riesgo y la planificación y programación de las actuaciones precisas para la implanta-



ción y realización de los servicios de seguridad», frente al art. 36.1.b) de la Ley: «La identificación, análisis y evaluación de situaciones de riesgo que puedan afectar a la vida e integridad de las personas y al patrimonio».

Esto en cuanto a las aparentemente ligeras diferencias de definiciones en los preceptos que ya existían en la norma anterior, hay otros que son de cuño nuevo en la Ley 5/2014, como el art. 36.1.h) que recoge: «La interlocución y enlace con la Administración, especialmente con las Fuerzas y Cuerpos de Seguridad, respecto de la función de seguridad integral de la entidad, empresa o grupo empresarial que les tenga contratados, en relación con el cumplimiento normativo sobre gestión de todo tipo de riesgos», en una sola frase se incluyen conceptos no vistos anteriormente como interlocución con la Administración, seguridad integral, y cumplimiento normativo.

O, sin duda el más esperado art.

36.1.e) sobre la validación previa del director de Seguridad sobre las medidas de seguridad instaladas en una oficina hasta tanto aprobación definitiva, que era una situación demandada por el sector y que elimina los efectos de una tramitación engorrosa aportando

tos tendrán que tener medidas de seguridad y cuáles serán estas medidas, eso sí, una habilitación mucho más extensa y detallista que la realizada en la Ley anterior, donde solo le dedicaba 3 líneas. En el caso actual se llega a incluir hasta una asignación de respon-

«El Reglamento que viene está siendo objeto de una gran expectación y promete ser extenso e intenso»

más eficiencia a la actuación profesional del director de Seguridad.

No obstante, el verdadero nudo gordiano del futuro Reglamento vendrá por la habilitación que realiza el art. 51 de la Ley 5/2014 y el contenido del art. 52 del mismo cuerpo legal.

En el primer caso, art. 51, se trata de una habilitación al Gobierno para que pueda determinar qué establecimien-

sabilidades entre empresas y usuarios, y se diferencia entre medidas de seguridad obligatorias y medidas de seguridad adicionales, por ejemplo.

Por medio de este precepto se habilita legalmente a que sea el futuro Reglamento el que relacione cuáles serán los establecimientos obligados a contar con medidas de seguridad, y en qué consistirán esas medidas de seguridad.



Detección excelente. En todo momento.

FLIR TDX™

MINICÁMARA TÉRMICA

LA CÁMARA DE DETECCIÓN DE MOVIMIENTO MÁS PRECISA DISPONIBLE.

- Reduzca las falsas alarmas con una detección de movimiento más fiable
- El sistema de detección de intrusos y verificación de alarmas de vídeo más asequible
- Fácil integración: PoE/12 VCC, IP/MPX(HDCVI)/analógico, ONVIF

Más información en www.flir.com



Las imágenes que aquí se incluyen solo tienen fines ilustrativos y pueden no haber sido tomadas con la cámara descrita. ©2015 FLIR Systems, Inc.

No deja de llamar la atención que la actual ley habla del Reglamento en tiempo verbal futuro cuando actualmente ya hay un Reglamento que no ha sido derogado en lo que no contradiga a la Ley 5/2014, por lo que las medidas reglamentarias no es que existirán, sino que ya existen.

Encontrar un equilibrio entre los riesgos que se quieren prevenir y sobre los que se quiere actuar y cuáles serán las medidas que «obligatoriamente» tendremos que instalar, no es una tarea fácil, es más, opino que hasta ingrata, pero confiemos en que este nuevo Reglamento que viene, sea un Reglamento equilibrado.

Por último, otra importante novedad que incluye la Ley que será incluida en el futuro Reglamento, es el ya referido art. 52 que, de forma novedosa, relaciona qué tipos de medidas de seguridad entran dentro del ámbito de aplicación de seguridad privada, y por ende, de la Ley 5/2014, y así diferencia los siguientes tipos de medidas de seguridad:

- Físicas.
- Electrónicas.
- Personal.
- Informática.
- Organizativa



En la anterior norma no se relacionaba de forma expresa ningún tipo de medida, si bien, del texto del Reglamento de Seguridad Privada se podía extraer una regulación de las tres primeras. Los otros dos tipos de medidas son totalmente novedosas en la regulación de seguridad privada, con lo que será difícil aproximarse al desarrollo que pueda haber en el Reglamento. Si acudimos al Preámbulo de la Ley, hay una breve referencia a las medidas de seguridad informática, que no

arroja mucha luz sobre el contenido final, recogiendo la idea que no se trata de una materia exclusivamente a realizar por empresas y personal de seguridad, pero que sí podrán ser realizadas por éstos, reservándose la posibilidad de someter a los actores intervinientes a ciertas reglas motivadas por la incidencia directa en la seguridad de las empresas, lo que hace presumir que el Reglamento que viene incluirá algún apartado a regular ciertas normas para proveedores y usuarios.

No hay referencia en el preámbulo a las medidas de seguridad organizativas, entendiéndose que lo que hará el Reglamento será potenciar la habitualidad y transversalidad de los Planes de Seguridad.

En definitiva, el Reglamento que viene está siendo objeto de una gran expectación y promete ser extenso e intenso; esperemos que también sea equilibrado, aunque no hay nada que indique que no lo vaya a ser.

Parfraseando a Sir Francis Bacon, «el argumento se asemeja al disparo de una ballesta, es igual de efectivo dirigido a un gigante que a un enano». ●



Fotos: Unicaja/Designed by Freepik

CONTROL TOTAL

SPIDER, el completo sistema multifunción de alta seguridad, diseñado para el control, apertura y cierre de cajas fuertes, cajeros, dispensadores y otros elementos de almacenamiento seguro.

La última tecnología en electrónica, hardware y software, para un **CONTROL TOTAL**.



SPI_{IDER}
Full Control Included

VdS

www.baussa.com

BAUSSA
INDUSTRIAS DE SEGURIDAD

ANA MARZO. SOCIA WHITAN LAW TECH

Los riesgos en la videovigilancia de los cajeros automáticos

AUNQUE ya estamos acostumbrados a que el coche de google nos grabe en un semáforo, al encontrarnos en alguna calle de alguna ciudad en Street View parece que no vemos con los mismos «buenos ojos» que la entidad financiera de la esquina recoja nuestra imagen cuando pasamos por delante de un cajero automático.

¿Puede una entidad financiera grabar las imágenes de los viandantes en una calle o vía pública?

La respuesta no es sencilla. Como es bien sabido la seguridad en bancos, cajas de ahorro y demás entidades de crédito tiene su propia regulación sujeta a reglas específicas derivadas del Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada (en adelante Regla-

mento de Seguridad Privada).

Concretamente el Reglamento de Seguridad Privada exige la instalación de cámaras y videocámaras en dichos establecimientos y determina las condiciones para la puesta en marcha y funcionamiento de dicha instalación.

Pero con la irrupción de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD) y la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, la normativa específica quedó ampliada también a los requisitos regulatorios de estas leyes.

Lo cierto es que no siempre es una tarea fácil interpretar la normativa espe-

cífica de seguridad para bancos, cajas de ahorro y demás entidades de crédito en conexión con la LOPD y sus normas complementarias y de desarrollo.

En todo caso, el Reglamento de Seguridad Privada define las siguientes peculiaridades en su régimen jurídico:

- Las imágenes grabadas únicamente podrán ser utilizadas como medio de identificación de los autores de delitos contra las personas y contra la propiedad.
- Las imágenes deben estar exclusivamente a disposición de las autoridades judiciales y Fuerzas y Cuerpos de Seguridad, a quienes deben facilitar inmediatamente aquellas que se refieran a la comisión de hechos delictivos.
- El contenido de los soportes con las imágenes es estrictamente reservado.
- En principio las imágenes sólo podrán ser visualizadas por las Fuerzas y Cuerpos de Seguridad, los jueces y tribunales, por la Inspección de la Agencia Española de Protección de Datos en ejercicio de sus competencias y por el personal legitimado por la Ley de Seguridad Privada.
- En los ficheros que se generen, debido a las anteriores restricciones, el derecho de acceso de los afectados no es posible, sin perjuicio de que pese a ello, los interesados puedan solicitar la tutela de la Agencia Española de Protección de Datos.
- La cancelación debe llevarse a cabo transcurridos quince días desde la grabación a excepción de aquellos casos en que se hubiese dispuesto lo contrario por las autoridades judicia-



les o las Fuerzas y Cuerpos de Seguridad competentes.

Volviendo a nuestra pregunta inicial, entre las peculiaridades no se encuentra el hecho de que las entidades financieras puedan instalar cámaras para grabar la vía pública, sino que la legitimación para el uso de instalaciones de videovigilancia se ciñe a la protección de entornos privados.

Como es bien sabido, la prevención del delito y la garantía de la seguridad en las vías públicas corresponden en exclusiva a las Fuerzas y Cuerpos de Seguridad del Estado y, por tanto, la regla general es la prohibición de captar imágenes de la calle desde instalaciones privadas.

No obstante, en algunas ocasiones la protección de los espacios privados sólo es posible si las cámaras se ubican en espacios como las fachadas e incluso a veces también resulta necesario captar los accesos, puertas o entradas, de modo que aunque la cámara se encuentre en el interior del edificio, resulta imposible no registrar parte de lo que sucede en una zona de vía pública que de forma inevitable se capta.



lancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida».

Pero esto no debe llevarnos a engaño. El citado artículo 4.3 de la Instrucción 1/2006 no constituye una habilitación para captar imágenes en espacios públicos. Todo lo contrario. Para que esta excepción resulte aplicable, será preciso que no exista una posibilidad de instalación alternativa.

de prevención de actos delictivos contra dichas instalaciones y evitación de riesgos directos para empleados y clientes de las mismas, siendo la entidad financiera responsable del tratamiento y/o fichero quien deberá adecuar el uso de la instalación, de modo que el impacto en los derechos de los viandantes sea el mínimo posible.

Así por tanto, dichas entidades deberán adecuar el uso de la instalación, de modo que el impacto en los derechos de los viandantes sea el mínimo posible, porque en ningún caso se admitirá el uso de prácticas de vigilancia más allá del entorno objeto de la instalación y en particular en lo que se refiere a los espacios públicos circundantes, edificios contiguos y vehículos distintos de los que accedan al espacio vigilado.

Sin embargo, con más frecuencia de la debida, seguimos encontrando supuestos en los que se comprueba que en las oficinas bancarias que cuentan con cámaras y cajeros exteriores, se produce un tratamiento de datos personales que excede del ámbito o entorno privado de las propias instalaciones al que debe ceñirse, recogiendo imágenes procedentes de las vías públicas de forma extremadamente amplia y emplazando no sólo los bienes objeto de protección (zonas de accesos y cajeros), sino también personas que transitan por los

«Lo cierto es que no siempre es una tarea fácil interpretar la normativa específica de seguridad para bancos, cajas de ahorro... en conexión con la LOPD»

¿Entonces volvemos a preguntarnos, es legal en estos casos?

Como indica la Agencia Española de Protección de Datos (en adelante AEPD) en su doctrina éste es el motivo por el que el artículo 4.3 de la Instrucción 1/2006 dispone que «las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos, salvo que resulte imprescindible para la finalidad de vigi-

Bueno, pues parece que a criterio de la AEPD, este caso es el que precisamente se refleja de forma clara en la instalación de las cámaras de seguridad para vigilar el uso de los cajeros automáticos de los bancos y entidades financieras.

Ahora bien, «no todo vale». En estos casos las zonas aledañas que sean grabadas deberán limitarse al área imprescindible para responder a las funciones

espacios públicos enfocados por dichas cámaras, vehículos que circulan o se encuentran estacionados y edificios próximos, todo ello con extremada amplitud y de forma desproporcionada al amparo de los criterios de la AEPD.

Ello suele ser causa de imputación por parte de la AEPD de una infracción de la vulneración del principio del consentimiento, porque como hemos mencionado con anterioridad la instalación de videocámaras en lugares públicos es competencia exclusiva de las Fuerzas y Cuerpos de Seguridad, cuando con la instalación de cámaras en cajeros exteriores, fachadas y accesos a bancos, cajas de ahorro y entidades financieras se constata que desde dichas cámaras se captan con total nitidez a los viandantes que se encuentran en las zonas de la vía pública videovigilada, se recoge la anchura total de las aceras y gran parte de las calzadas, se llega incluso a enfocar no sólo los vehículos que circulan por dichas calzadas, sino también los edificios situados enfrente de las cámaras de videovigilancia y, en definitiva, cuando el ángulo de enfoque de las cámaras instaladas no está reducido al mínimo imprescindible.

¿Qué deberían tener en cuenta los

bancos, cajas de ahorro y entidades financieras para evitar estos incumplimientos?. Pues sencillamente llevar a cabo la programación de los parámetros técnicos de las cámaras situadas en las fachadas para limitar el enfoque a un ámbito concreto en respuesta a la exigencia de proporcionalidad en el tratamiento de los datos personales y para la adopción de medidas tendentes a no captar imágenes de la vía pública con un alcance mayor del que resulte necesario para garantizar la seguridad de las instalaciones. Ello requerirá un análisis detallado por parte de la entidad.

Pero no todo queda ahí. Además otra conducta reprochable que los bancos, cajas de ahorro y entidades financieras deberán prevenir es la que deriva de la difusión en tiempo real de las imágenes de videovigilancia captadas por las cámaras de los sistemas de seguridad, las cuales se muestran a través de monitores colocados en lugares perfectamente visibles del interior de dichos establecimientos financieros, de tal modo que tales imágenes son accesibles a cualquier persona que se encuentre en dichas oficinas.

La AEPD ha sancionado ya en varias ocasiones a entidades financieras por

este tipo de prácticas. En este sentido es importante destacar que el hecho de que la entidad financiera permita a sus empleados y usuarios o clientes de las oficinas el acceso indiscriminado a las imágenes, es una infracción sancionable dado que, en principio, únicamente dichas imágenes (aún en tiempo real) deben estar a disposición exclusiva de las Autoridades Judiciales y Fuerzas y Cuerpos de Seguridad, y sólo podrán ser visualizadas por las Fuerzas y Cuerpos de Seguridad, los jueces y tribunales, la Inspección de la AEPD en ejercicio de sus competencias y por el personal legitimado por la Ley de Seguridad Privada, como pudiera ser personal propio de la entidad financiera con la categoría de director de Seguridad.

En conclusión, esta difusión de datos de carácter personal resulta excesiva en relación con el ámbito y las finalidades de seguridad y videovigilancia que justifican su tratamiento, sin que el hecho de que se trate de imágenes o situaciones que puedan ser captadas por las personas presentes en las propias oficinas ampare que su visualización pueda realizarse a través de los reseñados monitores por personas no autorizadas para ello.



Por lo tanto, aquellos bancos, cajas de ahorro y entidades financieras que a día de hoy aún lleven a cabo este tipo de prácticas, deberán tener en cuenta que la visualización a tiempo real por parte de los empleados, clientes y usuarios de las oficinas de la entidad financiera de las imágenes del interior de dichos establecimientos captadas por cámaras de videovigilancia, entre las que se encuentran las imágenes de los propios usuarios de las instalaciones, se considera innecesaria a los efectos y fines de seguridad y supone una vulneración del principio de proporcionalidad de la LOPD. ●



Fotos: *Designed by freepik.com.*

SI NO TIENES MÁS ESPACIO

Toda la actualidad
del sector en la palma
de tu mano

Síguenos también en  



App oficial

**CUADERNOS DE
SEGURIDAD**

¡Descárgatela ya
en tu móvil!

Disponible para:



JOSÉ IGNACIO OLMOS. DIRECTOR DE SEGURIDAD. EXPERTO EN PREVENCIÓN DE BLANQUEO DE CAPITALES

El director de Seguridad y el cumplimiento normativo

LAS entidades bancarias y de crédito han de disponer, como establecimientos obligados, de un departamento de Seguridad conforme al artículo 119.1 del Reglamento de Seguridad Privada, aún vigente en lo que no se oponga a la Ley 5/2014, de Seguridad Privada. Lógicamente al frente de dicho departamento y con la estructura y delegaciones necesarias estará un director de Seguridad habilitado.

Precisamente en el artículo 36 de la Ley de Seguridad Privada de 2014 se establecen las funciones de los directores de Seguridad. Al margen de que, más allá de lo que se señala en ese artículo, el director de Seguridad desempeñe otras funciones más o menos relacio-

nadas con su actividad y con la propia gestión del departamento (gestión de presupuestos, de los recursos humanos, materiales, etc.), en el universo particular que al final es cada corporación, me gustaría resaltar los apartados b) y c) de la citada normativa:

«Artículo 36. Directores de Seguridad.

1. En relación con la empresa o entidad en la que presten sus servicios, corresponde a los directores de Seguridad el ejercicio de las siguientes funciones:

b) La identificación, análisis y evaluación de situaciones de riesgo que puedan afectar a la vida e integridad de las personas y al patrimonio.

c) La planificación, organización y

control de las actuaciones precisas para la implantación de las medidas conducentes a prevenir, proteger y reducir la manifestación de riesgos de cualquier naturaleza con medios y medidas precisas, mediante la elaboración y desarrollo de los planes de seguridad aplicables.»

Estos preceptos, entendidos en un sentido amplio, se acercan al concepto imperante en el mundo anglosajón modernamente y que creo que es a lo que debe tender todo departamento-director de Seguridad: el concepto de gestión de riesgos.

Con la estructura, dependencias y apoyos especializados que se considere necesaria en cada corporación y, a pesar de la gran especialización de la seguridad, su gestión no se puede realizar de forma diferente según los apellidos que esta tenga, sino de forma integral; no tendría mucho sentido ocuparse por ejemplo de grafiteros o ladrones de poca monta, cuando hoy día el daño patrimonial que le puede ocasionar a una empresa una inadecuada gestión de una crisis en redes sociales es cuantitativa y cualitativamente mayor.

Por tanto, el director de Seguridad ha de constituirse como un gestor de riesgos que trata de evitar o minimizar todo tipo de daños para su compañía.

El cumplimiento normativo y la responsabilidad penal

En el mundo empresarial está surgiendo con fuerza también proveniente



del mundo anglosajón el concepto de compliance, que como bien ha afirmado el experto Enrique de Madrid «no es más que el cumplimiento normativo, es decir, la función específica que permite a las empresas, a través de procedimientos adecuados, como el establecimiento de políticas de actuación en determinadas materias, detectar y gestionar los riesgos de incumplimiento de las obligaciones regulatorias internas y externas, mitigando los riesgos de sanciones y las pérdidas que deriven de tales incumplimientos».

Muchas compañías, y desde luego las entidades financieras, cuentan con su departamento de cumplimiento normativo, debido por un lado a la ingente cantidad de normativa de obligado cumplimiento en muy distintas materias y por las correspondientes sanciones económicas, penales y de otra índole que pueden afectar a su patrimonio, al margen del daño reputacional que afectará de diversas formas a su negocio en el ámbito de la responsabilidad social corporativa.

Todo esto apoyado en las reformas del Código Penal, la de 2010 que establece la responsabilidad penal de las personas jurídicas, y la actual de 2015 en vigor desde el 1 de julio, en la que se establece un triple ámbito: perso-

na jurídica, gestores e incluso empleados por la culpa «in vigilando». En la presente reforma penal se deja claro que la persona jurídica puede quedar exenta de tal responsabilidad al implementar un modelo de prevención (compliance program), cuya supervisión debe encargarse a un órgano de control autónomo (compliance officer).

«El director de Seguridad ha de constituirse como un gestor de riesgos que trata de evitar o minimizar todo tipo de daños»

El director de Seguridad y los programas de cumplimiento normativo

En este contexto y con este nuevo modelo de control en las empresas, el director de Seguridad debe trabajar estrechamente con este departamento de cumplimiento en el sentido que antes mencionábamos de gestionar riesgos y evitar daños, ya que el perfil del responsable de cumplimiento ha venido siendo eminentemente jurídico o relacionado con el departamento de Auditoría, pero también de-

be tener nociones financieras, criminológicas (sobre todo de ciertos delitos de corrupción) y de investigación (fraude interno...).

De alguna manera muchos directores de Seguridad ya se ocupan de estos aspectos procurando cumplir con normativas diversas (seguridad privada, protección contra incendios, protección de datos de carácter personal,

prevención de blanqueo de capitales, etc.).

Sería pues deseable potenciar esa colaboración y que el director de Seguridad se acercase a esos aspectos y se formase en ellos; y al hilo de esta cuestión, con la nueva formación prevista en la Ley 5/2014, dejo caer la idea, para el que la quiera recoger, de la inclusión de esta materia en ese posible Grado en Seguridad.

Si lo veremos o si veremos el propio Grado el tiempo nos lo dirá... ●

Fotos: *Designed by Freepik*

Síguenos en twitter

@PuntoSeguridad 



JOSÉ LUIS ROMERO. GENERAL MANAGER SAMSUNG TECHWIN
SPAIN & PORTUGAL

Protección de redes

Esencial para la seguridad de entidades financieras

LOS bancos han utilizado la video-vigilancia durante muchos años para detectar, supervisar y grabar imágenes de posibles actividades delictivas como actos vandálicos, agresión directa al personal bancario, clonación de tarjetas en cajeros automáticos y robos con arma, así como para supervisar, de manera remota, las instalaciones fuera del horario comercial.

La existencia de sistemas de video-vigilancia basados en redes IP ha transformado el modo en que los directores de Seguridad de los bancos aprovechan al máximo los recursos para garantizar que sus activos están protegidos y que

su personal trabaje en un entorno seguro. Una de las características clave de la tecnología de vídeo sobre IP es la capacidad de controlar las cámaras y visualizar imágenes grabadas o en directo desde cualquier punto de la red. Esto significa que el jefe de Seguridad de una sucursal bancaria se puede encontrar en cualquier lugar del mundo y tener, no obstante, acceso inmediato a imágenes de alta resolución que le permitirán analizar cualquier incidente y, en caso de necesidad, enviar las pruebas a la policía con fines judiciales.

Uno de los principales retos de los bancos es cómo capitalizar los bene-

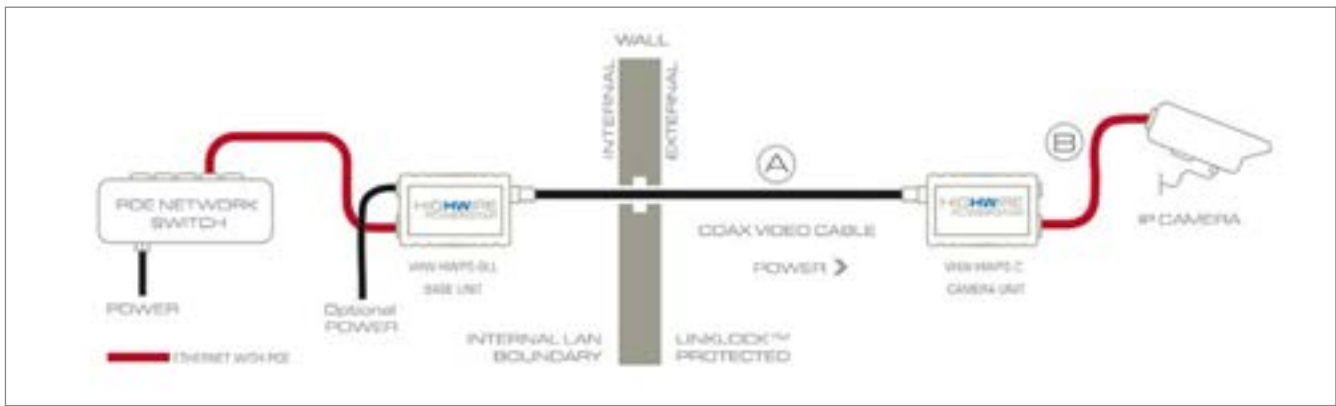
ficios de un sistema de vídeo sobre IP sin crear una oportunidad para que criminales puedan hackear la red. Debido a que los bancos utilizan cada vez más domos y cámaras de red IP de alta definición para capturar imágenes de la actividad en sus oficinas centrales y sucursales, existe la posibilidad de que estafadores puedan acceder a información confidencial y valiosa.

Implementación de cámaras IP

La implementación de cámaras IP externas requiere la existencia de una conexión de red externa al dispositivo de cámara IP, y estas conexiones externas podrían estar sujetas a sabotajes cuya finalidad sería acceder a la red del banco. Aunque se pueden tener en cuenta muchos aspectos para proteger y aislar las conexiones de la red con un interruptor de red completamente gestionado, e incluso con la implementación de una red independiente para el sistema de vigilancia, siempre seguirá habiendo riesgos.

Estas preocupaciones son de especial relevancia cuando fuera posible, en teoría, desconectar una cámara IP montada externamente, acceder a la red a través de esta conexión y detectar potencialmente y desactivar las otras cámaras y/o incluso la grabadora de vídeo de la red. Si se establece un puente entre la red de videovigilancia,





o parte de esta, y la red principal, podría suceder que un criminal experto y bien preparado pudiera acceder o manipular, de alguna manera, otros sistemas de la red.

Tecnología al rescate

Afortunadamente, en la actualidad hay una solución disponible que corta en seco cualquier intento criminal de hackear una red a través de un sistema de videovigilancia basado en una red IP.

Fabricada por la empresa inglesa Veracity y comercializada en exclusiva por nuestra compañía, una solución de tecnología exclusiva e innovadora llamada LINKLOCK™ ofrece una barrera total a todos los accesos de red no autorizados, mediante el bloqueo absoluto de conexiones a cables o equipos que hayan podido ser manipulados o desconectados. Funciona llevando a cabo la desconexión íntegra de datos y alimentación del enlace del cable coaxial, con el consiguiente aislamiento total del enlace afectado. Esto la convierte en la medida de protección ideal para instalaciones en las que la seguridad es clave, tales como bancos, en las que el equipo o el cableado de red deben localizarse fuera de las instalaciones.

Esta solución de tecnología exclusiva, que se comercializa como opción en la gama Highwire Powerstar de Veracity de los adaptadores coaxiales Ethernet y POE over Ethernet puede utilizar-

se con cualquier marca, modelo o tipo de cámara IP.

¿Cómo?

En un sistema de videovigilancia estándar, tener un enlace cifrado o seguro en el cable coaxial no impide las intrusiones, ya que el enlace Ethernet a la cámara seguiría estando abierto y sin protección. La conexión coaxial de la gama Highwire utiliza un protocolo de banda base exclusivo seguro de punto a punto únicamen-

na o la interfaz coaxial. Para volver a activar un modo de funcionamiento normal, la unidad base de Highwire del interior del edificio debe restablecerse físicamente a través de un interruptor de cierre de contactos en las clemas de la unidad.

Esta protección no depende de la cámara IP que está recibiendo alimentación por PoE. Si recibe alimentación de un suministro de alimentación local, la cámara IP seguirá funcionando cuando se active el modo de bloqueo de la solución, pero no habrá ningún

«Uno de los principales retos de los bancos es cómo capitalizar los beneficios de un sistema de vídeo sobre IP sin crear una oportunidad para que criminales puedan hackear la red»

te. La conexión Ethernet se mantiene continuamente activa incluso cuando el enlace está inactivo. No obstante, cualquier intento de intrusión o desconexión de estas conexiones es detectado por la solución, que inmediatamente activa el modo de bloqueo. Como consecuencia, todo el equipo externo se aísla de inmediato de la LAN interna.

Seguridad añadida

El modo de bloqueo de la solución no puede invertirse a través de la red exter-

tipo de comunicación a través del cable coaxial. El modo de bloqueo seguirá activo aún cuando un criminal trate de suministrar alimentación a una cámara de manera externa para manipularla. Esto se debe a que la señal Ethernet o la señal coaxial de la citada gama debe volver a conectarse físicamente o a introducirse para poder conectar un dispositivo (del criminal) de otra marca. Esto se detectará como una anomalía y activará el modo de bloqueo. ●

Fotos: Samsung

FERNANDO MARTÍNEZ. RESPONSABLE COMERCIAL. KABA- SAFE LOCKS



Sistemas de control y gestión centralizada para contenedores de efectivo

LOS sistemas digitales para el control de contenedores de efectivo aportan soluciones de flexibilidad, organización y, sobre todo, una reducción de costes, y garantizan al departamento de Seguridad la posibilidad de disponer del control total sobre sus contenedores de efectivo.

Las nuevas generaciones de sistemas de cerraduras IP para contenedores de efectivo permiten la integración digital en una sola plataforma de gestión, ser comandadas desde sistemas de control de acceso o, prioritariamente por centrales de alarma digitales de última generación. Posibilitan la gestión local y centralizada y, sobre todo,

la capacidad de adaptarse a cada una de las circunstancias particulares de cada cliente y de las características de cada uno de los centros de trabajo de los que dispone.

La Norma UNE-EN 50131-1 establece cuatro grados de seguridad en función del riesgo, por lo tanto las cerraduras digitales IP permiten la integración digital, como un módulo adicional, en las CRA de Grado 3 y 4, ser bloqueadas y desbloqueadas remotamente, pero sobre todo posibilitan gestionar a través de ellas alarmas de diferentes tipos, monitorizar aperturas y cierres, elevando la seguridad por encima de los estándares hasta ahora utilizados.

Soluciones para cajas fuertes homologadas en Grado IV bajo Norma UNE-EN 1143-1:2012, con la capacidad de ser tele-gestionadas vía IP existen en el mercado desde hace tiempo, pero también existen productos homólogos para cajas o puertas de grado superior, gracias a las cerraduras electrónicas homologadas en Clase C bajo Norma UNE EN 1300:2014, quedando las largas llaves de cerraduras mecánicas de Clase C obsoletas, pasando del Siglo XVIII al XXI directamente, eliminando la necesidad de instalar dos unidades de cerradura de Clase B, ahorrando en costes de adquisición, de instalación y de mantenimiento.

La modularidad de las soluciones digitales permite a las entidades bancarias gestionar sus sistemas de forma local y/o centralizada, permitiendo realizar inversiones de forma escalonada, instalando en primera instancia sistemas en modo autónomo y migrando a IP posterior y gradualmente.

Las novedades introducidas en los sistemas permiten ahora una modularidad que no existía hasta el momento, pues dispone de características tan interesantes como:

- Posibilidad de personalizar el acceso al sistema para diferentes usuarios, gracias a la configuración de distintos retardos, periodos de bloqueo horario, interrupciones de retardos y



bloqueos o usos en modos duales, caducidad de códigos de usuario o la posibilidad de inhibir temporalmente el código a empleados que se encuentran de vacaciones o ausentes por una baja laboral.

– Interconexión digital con elementos de control, bloqueo y desbloqueo como CRA, sistemas de control de acceso, exclusas, pulsadores, lectores, puertas o elementos periféricos que se requieran conexas, así como lectores con Smart Keys, Smart Phones que permiten el acceso a cerraduras por medio de ciertos usuarios. Autorizaciones de acceso ligada a credenciales de autorizaciones del sistema de control de acceso es otra de las posibilidades que brindan los sistemas IP.

– Códigos especiales que permiten controles horarios, apertura de compartimentos interiores, códigos de servicio de un uso, de bloqueo y desbloqueo o alarma silenciosa.

– Módulos para uso de códigos para personal de compañías de transporte de fondos o empresas externas que realizan labores de mantenimiento, con la posibilidad de apertura de contenedores mediante códigos de un uso, Códigos Dinámicos o en modo dual (código fijo de empleado + código de transporte de fondos), lo que proporciona que el uso de códigos siempre se encuentra jerarquizado y bajo total control, y garantiza que nadie externo a la entidad dispone de código alguno válido para abrir contenedor alguno. Además gracias a las características de estos módulos y su funcionamiento off line, la gestión de los contenedores no se encuentra supeditada a la conectividad de red, por lo que pueden ser instalados en equipos de áreas remotas en las conexiones que no son lo deseablemente buenas para garantizar una correcta tele-gestión.

– La importancia de conexiones seguras viene garantizada por proto-



los de encriptación, es importante que vengan garantizados por algoritmos cifrados con un mínimo de AES de 256 bits o superior. La seguridad de la información que se transmite vía red es de vital importancia, por ello existen sistemas que disponen de certificación VdS, en la que se garantiza el grado de seguridad de todo el sistema y no solo de las cerraduras.

Las soluciones digitales para contenedores de efectivo alcanzan un nivel de seguridad superior cuando se instalan cerraduras de apertura y cierre con pestillo motorizado, pues garantizan, mediante los switches internos de final de carrera y externos de puerta, que la puerta y la pestillería se abren y cierran correctamente y gracias a las características del monitorizado IP, la información puede ser controlada en tiempo real desde aquellos puntos que sean de interés para la entidad bancaria, posibilitando la gestión y control, local y centralizado, de alarmas debido, por ejemplo, a puertas de cajas

que se encuentran abiertas por encima del tiempo establecido por el protocolo marcado por el departamento de Seguridad.

Las posibilidades de gestionar cambios, dar de alta o baja códigos, conocer estado de baterías o realizar auditorías de forma remota, reporta al banco un importante ahorro en costes temporales de empleados, así como en los relativos a actuaciones de servicio técnico de empresas que realizan labores de mantenimiento de equipos y contenedores de efectivo.

La integración de sistemas en una única plataforma que permite el control, la gestión, la organización y la seguridad de los contenedores de efectivo es la respuesta que los sistemas de gestión IP para contenedores de efectivo ofrecen al mercado bancario, una inversión en seguridad con una clara continuidad en el tiempo que garantiza una seguridad adicional desconocida hasta su llegada. ●



Fotos: Kaba

ESTUDIO REALIZADO POR KASPERSKY LAB Y B2B INTERNATIONAL

El 36% de los españoles cree que las sucursales bancarias son más seguras que los bancos online

El 36% de los usuarios españoles de Internet piensa que los bancos tradicionales son más seguros que los bancos online, según un estudio realizado por Kaspersky Lab y B2B International. A pesar de estos miedos, la mayoría hace pagos online pero muchos fallan a la hora de tomar medidas básicas de seguridad, poniendo su dinero y la reputación de los bancos en riesgo.

Una de las formas más sencillas que tienen los cibercriminales para acceder a las cuentas bancarias online es hacerse pasar por el dueño de la cuenta. Esto se puede hacer obteniendo información de la cuenta, creando una página phishing donde los usuarios introduz-

can sus nombres de usuarios y contraseñas sin darse cuenta, o interceptando estos nombres y contraseñas con un troyano bancario cuando los usuarios se registren en las páginas legítimas de sus bancos. Los ordenadores y los dispositivos móviles son vulnerables a estos ataques.

La encuesta muestra que un número significativo de usuarios, el 55%, se siente vulnerable cuando realiza transacciones financieras online. Por otra parte, el 46% de los españoles cree que hacer pagos offline es más seguro que pagar online, y el 36% está de acuerdo en que los bancos tradicionales offline son más seguros que los bancos en línea.

Sin embargo, a pesar de estos miedos, la mayoría de los internautas realiza pagos online: el 85% de los españoles encuestados usan sus ordenadores o portátiles para realizar pagos online, el 56% usa sus tablets, el 46% sus smartphones y el 9% de los propietarios de una smart TV admite que la utiliza para este tipo de operaciones. Al mismo tiempo, de acuerdo con este estudio, un 19% no hace nada por proteger sus datos financieros online.

«Si los clientes eligen la banca tradicional, por temor a ser víctimas de fraude por Internet, obstaculizará la adopción de sistemas de alto margen online y de pago móviles. Mientras tanto, entre los que han adoptado los pagos online y móviles, existe un problema de seguridad persistente, ya que pueden estar poniendo su dinero - y la reputación del banco - en un innecesario riesgo. Es por eso que hoy en día es de vital importancia que los bancos inviertan en tecnología para garantizar un entorno bancario seguro para sus clientes.

Este enfoque no sólo tranquiliza a los que prefieren las sucursales bancarias a las online y les convence de que la banca móvil es segura, sino que también reducirá el riesgo para los clientes descuidados, que de otro modo podrían perder datos financieros importantes», ha asegurado Alfonso Ramírez, director general de Lab Iberia. ●



Fotos: Kaspersky Lab



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

24h/365 días.



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



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



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



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

El sector cae por sexto año consecutivo

Aunque con expectativas de estabilización

El sector de la Seguridad Privada en España siempre ha seguido la misma evolución que la economía del país, con crecimientos positivos hasta el segundo semestre de 2008 en que, con la aparición de una de las mayores crisis de los últimos tiempos, las empresas de seguridad privada sufrieron un impacto económico negativo superior a la media. De hecho, en los últimos seis años han acumulado una caída del 24,08% en su facturación total.

Adía de hoy, dicha crisis sigue incidiendo sobre la gran mayoría de las empresas del sector, aunque empiezan a aparecer ciertas expectativas de una muy leve recuperación. Dicho esto, en 2014 el sector volvió a cerrar con una bajada del -0,24 con respecto al volumen de negocio del año anterior.

Por otra parte, la aprobación del nuevo marco legal (derivado de la nueva Ley de Seguridad Privada 5/2014 del 20 de marzo de 2014) supone, sin lugar a duda, una noticia positiva, ya que esta nueva normativa ha ayudado a adaptar la legislación a las nuevas realidades, y rejuvenecen una ley de hace más de dos décadas que en muchos aspectos

se había quedado obsoleta.

Como consecuencia de este cambio legislativo, que desde APROSER hemos estado reclamando durante mucho tiempo, al sector se le presentan nuevas oportunidades que podrían ayudar a su recuperación.

Reglamento de acompañamiento

Pero para ello, la implantación de un buen reglamento de acompañamiento es condición indispensable con la finalidad de que el sector se pueda reestructurar y mostrar sus verdaderas potencialidades, y la demora que se está produciendo empieza a ser altamente preocupante.

Finalmente, deben recuperarse los niveles de demanda, tanto en cantidad como en calidad, de los años inmediatamente anteriores al inicio de la crisis, e incrementarse el escandallo de productos y servicios, cada vez más integrados pero sin renunciar a una necesaria especialización. ●



Fotos: Aproser/
Designed by Freepik



#EuroCloudForum

I EUROCLOUD FORUM BARCELONA

7th - 9th OCTOBER, 2015

VI EuroCloud Congress
The Future of Cloud in Europe



Barcelona
Imagina Center



EUROCLOUD EUROPE

AUSTRIA CROATIA GERMANY FRANCE ITALY LUXEMBOURG MALTA NETHERLANDS POLAND
PORTUGAL ROMANIA SLOVAKIA SLOVENIA SPAIN SWEDEN SWISS UK

LUCIANO VALLADARES. DIRECTOR NACIONAL. EULEN SEGURIDAD

«La tecnología e innovación están alineadas con nuestra forma de entender la seguridad»



«En EULEN Seguridad, la innovación continua, permanentemente actualizada, así como la vocación de servicio, han sido factores diferenciadores de nuestra peculiaridad durante toda nuestra historia», explica Luciano Valladares, director nacional de EULEN Seguridad, quien a lo largo de la entrevista recuerda los inicios de una compañía con 40 años de andadura en el sector de la Seguridad, y que en un mundo globalizado y altamente tecnificado ha apostado por la especialización para «ser capaces de defender los intereses de nuestros clientes contra todos los riesgos que les amenazan».

EN plena celebración del 40 aniversario de EULEN Seguridad, ¿podría hacernos un breve recorrido de la historia de la compañía? ¿Qué valoración haría de la andadura de la empresa por el sector de la Seguridad?

—EULEN Seguridad es una empresa que forma parte del Grupo EULEN; es una compañía familiar, de capital 100% español, que fue fundada hace más de 50 años, en 1962, por David Álvarez, para nosotros D. David, quien sigue presidiendo hoy la empresa.

El Grupo comenzó su andadura con la actividad de limpieza, seguida de la de seguridad, la segunda que se pone en marcha cuando en 1974 se crea la marca PROSE, S. A., con el número nueve

en el Registro de Empresas de Seguridad inscritas en el Ministerio del Interior. A día de hoy, las ocho empresas registradas con anterioridad han desaparecido, por lo que podemos afirmar

que nuestra empresa es la decana del sector.

La idea brota en la mente de nuestro Presidente en el mismo momento en que lee en el BOE el Decreto que establece la obligatoriedad de

servicios de seguridad para los bancos, cajas de ahorro y demás entidades de crédito. El 25 de marzo de aquel año, tres semanas después de la publicación de aquel Decreto, se constituye Prosesa, con un capital de 2.000.000 de las antiguas pesetas.

Apoyándose en la estructura territorial que EULEN ya poseía en esas fechas y en la experiencia acumulada por sus gestores y directivos, el negocio de la seguridad avanzó paralelo al de la limpieza.

Así, EULEN Seguridad fue y es pionera en muchos as-

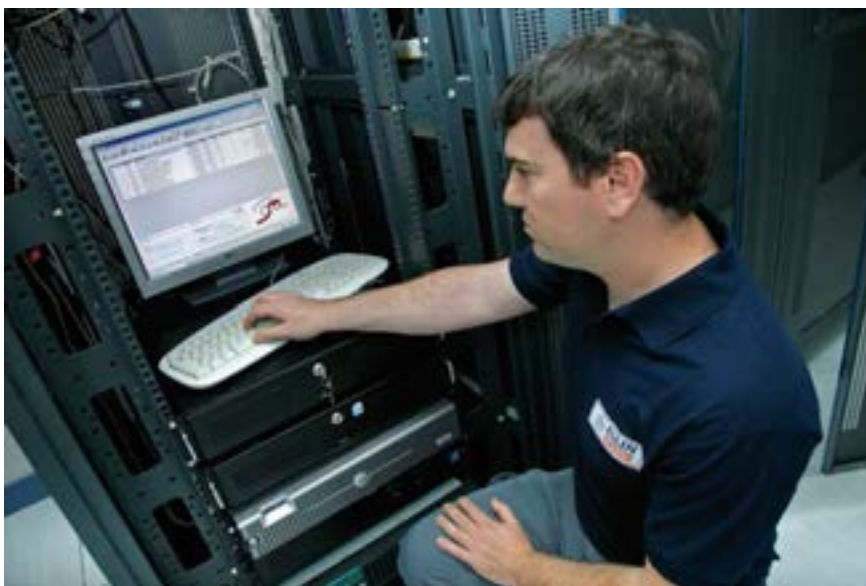


pectos, pero sin duda cabe destacar que fuimos pioneros en la formación de empleados en un centro propio, La Berzosa, que permanece en la memoria de los más antiguos como sinónimo de rigor, profesionalidad y seriedad.

Entonces, para formar parte de nuestra prestigiosa plantilla había que superar un duro proceso de selección, exigiendo entre otras cualidades, una estatura mínima de 1,80 metros. Tras un curso presencial de un mes de duración, los alumnos hacían prácticas junto con el vigilante titular en nuestros servicios durante quince días, doblando el puesto, y si el informe de ese periodo era favorable, se volvía a La Berzosa donde -tras una semana más de curso- se obtenía el diploma final que facultaba al alumno a presentarse a examen ante la Policía. En caso de superarlo, se conseguía el título de Vigilante Jurado. Aquéllos eran tiempos en los que el rigor en la formación, los procedimientos de todas nuestras actividades y tareas, así como la supervisión frecuente y profesional de los servicios eran la «marca de la casa». Para importar el conocimiento necesario, establecimos una alianza con The Wackenhut Corporation, la empresa norteamericana más prestigiosa y avanzada de aquella época. Nuestros directivos viajaron a EEUU y otros países para aprender de los que llevaban haciendo seguridad muchos años. De aquellos tiempos queda, en el imaginario colectivo de todo el sector, la imagen de Prosesa como sinónimo de buen hacer y de profesionalidad.

En la actualidad, las cosas han cambiado en muchos sentidos, aunque el espíritu inicial de seriedad y profesionalidad permanece invariable. Mientras en el año 1980 contábamos con 1.500 vigilantes, hoy tenemos 22.000.

Asimismo, sólo dábamos servicio en España y hoy lo podemos hacer en 14 países. Por otra parte, además de las actividades tradicionales de vigilancia,



sistemas y consultoría, trabajamos en ciberseguridad, inteligencia, continuidad de negocio, vigilancia digital, videovigilancia remota, etc. Contamos con un Centro de Control de Seguridad Integral que gestiona alarmas del mundo físico y del mundo cibernético; igualmente estamos presentes como ponentes en todos los foros en los que se debate el futuro de la seguridad.

Por todo ello, podemos decir que somos líderes en innovación de servicios, así como elemento tractor en el modelo de seguridad integral, refrendado por los últimos cambios legislativos (Ley de PIC y nueva Ley de Seguridad Privada), y que hoy trata la seguridad como un proceso productivo más de la empresa, y cuya finalidad fundamental es conseguir la continuidad de los negocios, es decir, «que no se pare la máquina», ser un facilitador de la actividad empresarial.

En un mundo globalizado y altamente tecnificado, es necesario especializarse y ser capaces de defender los intereses de nuestros clientes contra todos los riesgos que les amenazan. Esto es precisamente lo que hace EULEN Seguridad, tal y como reza en nuestro lema empresarial: ante cualquier amenaza, en cualquier escenario.

Son innumerables los hitos alcanzados por nuestra empresa, y seguro que muchos recordaréis uno de los más recientes, cuando EULEN Seguridad fue autorizada por el Ministerio del Interior para la prestación de servicios de vigilancia y protección de buques con bandera española, fuera de nuestras aguas territoriales.

Asimismo, también debemos mencionar la adjudicación de importantísimos contratos internacionales como el Aeropuerto Internacional de Ciudad de México, para el que tenemos destinados más de 1.200 empleados; la vigilancia y protección para la industria salmonera en altamar e industria minera, ambas en Chile; o la vigilancia marítima contra la piratería, así como un largo etcétera. Sin embargo, aunque es complejo enumerar la consecución de todas aquellas metas por las que hemos trabajado a lo largo de todos estos años, lo que si podemos asegurar es que, todas ellas, se han alcanzado fruto del empeño de mucha gente que se ha dedicado de lleno a adaptar nuestros recursos a las necesidades de los clientes.

Esta celebración de nuestro 40 Aniversario lo consideramos como un escenario perfecto para rendir un emocionado homenaje a todas aquellas

personas que han hecho posible que EULEN Seguridad continúe siendo, hoy igual que ayer, una de las empresas más queridas y admiradas del sector; igualmente quiero agradecer a todos nuestros clientes, por haber confiado en nosotros durante todos estos años, lo que nos ha dado el impulso y ánimo necesarios para seguir mejorando día a día.

—Abordando aspectos normativos y de legislación, ¿qué deseaba que contemplase el Reglamento de Seguridad Privada de cara a las empresas de servicios de seguridad? ¿Cómo cree que afectará al mercado de los Servicios de Seguridad y Vigilancia?

—Muchos son los aspectos que deberían acotarse o aclararse en el nuevo reglamento. Aspectos que por un lado deberían incidir en la lucha contra el intrusismo de empresas de servicios en actividades de seguridad, y por otro en la liberalización de controles por parte de la Administración, de manera que se posibilitara una mayor flexibilidad en la prestación y operativa de servicios. De esta manera podríamos destacar los siguientes:

– Sería deseable que el desarrollo reglamentario acotase el art. 6.2 en lo relativo a las actividades compatibles, evitando una posible sustitución indebida de actividades desempeñadas por empresas de seguridad hacia empresas de servicios.

– Avanzar en el concepto de seguridad integral, atendiendo a la reclamación de un sector necesitado de un cambio regulatorio, sin encorsetar la inabarcable casuística que se plantea con los servicios de inteligencia, ciberseguridad, videovigilancia y vigilancia remota, sistemas de control, etc.

– Acotar y definir de manera flexible y ágil la tramitación y mantenimiento de las acreditaciones del personal de seguridad acreditado, esto es operadores e ingenieros y técnicos, de manera que no pueda suponer una problemática adicional en la adecuación a las demandas del mercado.

– La regulación de la videovigilancia, debe poder distinguir claramente entre los servicios que deben prestarse por empresas de seguridad y los que no, y no debe acotar el muy probable crecimiento exponencial de estos servicios, con restricciones conceptuales o tecnológicas que puedan quedar desbordadas en pocos años.

– El Reglamento debería regular la subcontratación tal y como la recoge actualmente el art. 14.3 del Reglamento vigente, estableciendo que la subcontratación sólo podrá llevarse a cabo por una empresa inscrita en el Registro correspondiente y autorizada para la prestación del servicio o actividad objeto de la subcontratación.

– En lo que respecta a la profesionalización del sector en la protección de infraestructuras críticas, sería aconsejable que el reglamento profundizara en lo que la ley ya apunta, sumando a esas garantías administrativas, laborales o de Seguridad Social o Tributarias a las que se hacen referencia en la Ley de Seguridad Privada 5/2014 (art. 19.4) otras que incorporen criterios de solvencia técnica y operativa, tanto en la prestación de servicios como en la instalación de cualquier tipo de medidas, ya sean estas físicas, electrónicas, organizativas, de seguridad informática o de seguridad personal.

– Los Servicios de Ronda o Vigilancia discontinua deberían poder establecerse con mayor flexibilidad huyendo de rigideces que dificulten la eficacia y operatividad del servicio; y sean lo menos limitativos y restrictivos posibles desde el punto de vista de la administración, de manera que su prestación no sea ineficaz, porque de lo contrario se convertirían en servicios condenados a su desaparición.

– Esperamos que la prestación de servicios de seguridad en espacios públicos, polígonos industriales y urbanizaciones sea lo más aperturista posible, toda vez



que son los servicios más demandados, y el sector está en disposición de prestarlos desde el punto de vista garantista que se requiere.

— Asimismo, nos gustaría que la protección jurídica al personal de seguridad privada, análoga a la de los agentes de la autoridad tenga una cobertura muy amplia.

— Y, por último, una mayor agilidad en los trámites administrativos relativos a autorizaciones, documentación y solicitudes.

Esta liberalización conceptual va en la línea de la nueva filosofía de colaboración que la nueva ley otorga a la Seguridad Privada y que previsiblemente proporcionará mayores oportunidades de negocio para los servicios de seguridad y una mayor implicación a las empresas en su desarrollo.

—¿Cree que en los últimos años ha variado la estrategia y necesidades de las compañías a la hora de solicitar servicios de seguridad?

— Sin duda, la administración y los principales clientes han sufrido de forma muy acusada la crisis y ello ha hecho que se reformulen todos los presupuestos de seguridad en los últimos años. Hemos tenido que dar una vuelta al enfoque de nuestros servicios para hacer frente a este hecho. En este momento, en el que se atisba un escenario de recuperación, observamos que el cliente vuelve a valorar el valor añadido y el compromiso que puede aportararle la compañía de seguridad.

—EULEN Seguridad apuesta por un concepto novedoso: convergencia de la seguridad, ¿podría explicarnos qué engloba esta nueva visión de la seguridad?

— El paradigma de la convergencia de la seguridad, hoy en día ya no es algo novedoso, cada día lo adoptan más empresas, y la nueva legislación le otorga

la relevancia que hoy en día tiene; novedoso lo fue allá por el año 2008 cuando comenzamos a avanzar por este camino.

La convergencia de la seguridad o seguridad integral trata la seguridad como un proceso de negocio, orientado a garantizar la continuidad de las operaciones de la compañía, protegiendo todos sus activos, tanto tangibles como intangibles, de todas las amenazas a las que están expuestos, independientemente de su origen, sean del mundo físico o del ciberespacio.

Esta visión holística de la seguridad, permite el tratamiento integrado de los riesgos (riesgos de seguridad, ciber riesgos, riesgos legales, riesgos de negocios, riesgos tecnológicos...), con el fin de garantizar la protección del ciclo productivo completo.

—¿Cuáles son las grandes unidades de negocio con que cuenta actualmente EULEN Seguridad?

— Los servicios de vigilancia son por volumen la primera unidad de negocio, a continuación destacan los proyectos y servicios de instalación y mantenimiento de sistemas de seguridad; contamos además con Central Receptora de Alarmas propia y llevamos a cabo servicios de videovigilancia remota desde nuestro Centro de Control de Seguridad Integral.



Por último, con menor volumen de ventas, pero con un gran crecimiento en los últimos meses, tenemos los servicios de Consultoría de Seguridad en la que EULEN Seguridad desarrolla 4 grandes actividades: ciberseguridad, unidad de Inteligencia, protección de infraestructuras críticas y, por último, todo lo relacionado con la seguridad corporativa.

—¿Qué papel juega la tecnología e innovación en los servicios que ofrece EULEN Seguridad?

— En la actualidad, la seguridad está condicionada por tres factores:

- Las amenazas, condicionadas por la tecnología.
- La propia tecnología, condicionada a su vez por las amenazas.

– Y en tercer lugar, el regulador, con la Ley de Protección de Infraestructuras Críticas de 2011 y la Ley de Seguridad Privada de 2014.

De esta manera, las empresas se enfrentan a nuevas amenazas y nuevos retos, entre los que destacan:

- La protección de activos tangibles e intangibles.
- La protección de su reputación e imagen (activo intangible).
- El ciberespacio y las ciberamenazas.
- El tratamiento integrado de los riesgos (riesgos legales, riesgos de negocios, riesgos tecnológicos...).
- La protección del ciclo productivo completo.

En definitiva, la seguridad se concibe en la actualidad como una actividad integral e integradora, siendo un proceso más del negocio, lo que hace que la seguridad pase de ser un coste a una inversión.

En EULEN Seguridad, también la innovación continua, permanentemente actualizada, así como la vocación de servicio, han sido factores diferenciadores de nuestra peculiaridad durante toda nuestra historia. Desde las históricas soluciones basadas en el binomio hombre-sistemas hasta los más actuales planteamientos de

convergencia, en EULEN Seguridad hemos apostado por innovar en procesos, integrando las últimas tecnologías contrastadas. La tecnología y la innovación están alineados con nuestra forma de entender la seguridad, con soluciones fiables, adaptadas a cada necesidad e integradas con los intereses particulares de cada uno de nuestros clientes.

Actualmente, estamos trabajando en el desarrollo del servicio de vigilancia con vehículos aéreos no tripulados (drones), para algunos sectores muy específicos. Este proyecto lo tenemos ya muy avanzado y en breve será una realidad.

Las soluciones de videovigilancia, gestión remota de servicios, ciberseguridad e inteligencia exigen una adecuación constante al vertiginoso ritmo de la tecnología en las instalaciones productivas de nuestros clientes. De esta manera, la irrupción del mundo digital ha catalizado nuevas propuestas de soluciones en la nube que también abordamos desde EULEN Seguridad y para el que venimos trabajado en un nuevo concepto de seguridad integral, física y lógica, desde el Centro de Control de Seguridad Integral, donde hacemos convivir de manera coordinada servicios de Central Receptora de Alarmas,

del Centro de Operaciones de nuestro personal de Seguridad, del Centro de Operaciones de Videovigilancia, del Centro de Operaciones de Ciberseguridad y del Centro de Operaciones de Inteligencia.

—¿Cuáles son los mercados donde EULEN Seguridad tiene mayor presencia en España?

—Nuestra compañía atiende todos los sectores de actividad de los principales contratistas de servicios de seguridad de nuestro país. Destaca nuestra implantación en aeropuertos, el sector energético y los sectores de real estate y retail.

—¿Han cambiado en los últimos años las necesidades de los usuarios y clientes en cuanto a aspectos de ciberseguridad?

—Sí, cada vez es mayor la integración del mundo físico y el ciberespacio, y el uso que se le da a la tecnología tanto en el mundo empresarial como en la vida diaria de las personas, por lo tanto cada vez es mayor la necesidad de garantizar la seguridad del ciberespacio; un ejemplo claro de ello es la aparición de «Internet de las cosas» IOT, al que es necesario proteger de las amenazas que se ciernen sobre él.

Por otra parte, la profesionalización de los ciberdelincuentes es el mayor reto al que nos enfrentamos, el ciberdelito es un «negocio» que proporciona pingües beneficios. Este hecho ha motivado que cada vez más nuestros negocios y nuestra propia actividad personal esté expuesta a amenazas más sofisticadas y peligrosas, en las que en muchos casos los delincuentes tradicionales, del mundo físico, trabajan codo con codo con los ciberdelincuentes, los delincuentes del ciberespacio. ●

TEXTO: GEMMA G. JUANES.

FOTOS: EULEN SEGURIDAD





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

23-26
FEBRERO
February
2016

ORGANIZA / ORGANISED BY



IFEMA
Feria de
Madrid



Seguridad
contra incendios
y emergencias
Fire safety
and emergency



Seguridad laboral
Safety and health
at work



Security



Defensa
Defense

www.sicur.ifema.es

LÍNEA IFEMA / IFEMA CALL CENTRE

LLAMADAS DESDE ESPAÑA / CALLS FROM SPAIN
INFOIFEMA 902 22 15 15

LLAMADAS INTERNACIONALES (34) 91 722 30 00
INTERNATIONAL CALLS

FAX (34) 91 722 57 88

sicur@ifema.es

JESÚS GORDILLO. DIRECTOR DEL ÁREA DE TECNOLOGÍA. SECURITAS SEGURIDAD ESPAÑA

«La tecnología nos permite desarrollar soluciones inmediatas, eficaces y a un coste asumible»



«Hoy en día los clientes buscan un servicio de seguridad que les proporcione una protección de calidad pero no sólo desde el punto de vista de la eficacia operativa, sino también desde una perspectiva de eficiencia de los recursos utilizados y, en ese sentido, la tecnología es la gran aliada, es la que nos permite incrementar el nivel de seguridad ajustando al máximo el coste», asegura Jesús Gordillo, director del Área de Tecnología de Securitas Seguridad España, quien además hace hincapié en que el vigilante de seguridad es y será en el futuro una figura muy importante en el escenario de un servicio de seguridad, «pero hace ya tiempo –puntualiza– que es un elemento más que, junto con la tecnología, integra el servicio».

COMENZAMOS esta entrevista abordando aspectos normativos y de legislación, ¿qué aspectos desearía que contemplase el reglamento de Seguridad Privada de cara a las empresas de servicios de seguridad?

—Desearíamos que el reglamento de Seguridad Privada fuese lo suficientemente flexible como para que las compañías que ofrecemos este tipo de servicios podamos atender a las peticiones de los usuarios, dentro de un marco amplio que contemple la realidad actual. A nadie se le escapa la velocidad a la que evoluciona la tecnología, una herramienta fundamental a la hora de desarrollar soluciones de seguridad eficaces y eficientes, capaces de resolver las necesidades de los clientes. El vigilante de seguridad es y será en el futuro una figura muy importante en el escenario de un servicio de seguridad,

pero hace ya tiempo que es un elemento más que, junto con la tecnología, integra el servicio.

Hoy en día el componente tecnológico de la seguridad es evidente, y su capacidad y velocidad de evolución tremen-

da, de ahí la flexibilidad que reclamamos al futuro reglamento.

—¿Cómo cree que afectará al mercado de los Servicios de Seguridad y Vigilancia?



—Es difícil prever cómo afectará al mercado sin saber el contenido del futuro reglamento, pero sí sabemos lo que los clientes nos están reclamando y que la tecnología tiene un peso específico fundamental en la ecuación.

—La especialización es una de las grandes apuestas de Securitas Seguridad España para adaptarse a las necesidades de los clientes, ¿cuáles son los grandes segmentos de clientes a los que la compañía ofrece sus servicios? ¿Podría explicarnos a grandes rasgos los servicios más demandados?

—En los últimos años nos hemos esforzado por realizar grandes cambios dentro de nuestra compañía. Ese esfuerzo ha dado sus frutos y hemos conseguido transformar nuestra forma de hacer y ofrecer soluciones de seguridad, tanto de cara a los clientes como desde el punto de vista de la organización interna.

Securitas ofrece en la actualidad una de las ofertas más completas del mercado en lo que a soluciones de seguridad se refiere, entendiendo por éstas un servicio integral, que engloba vigilancia especializada, tecnología, servicios Mobile, gestión remota de la seguridad desde el COS (Centro de Operaciones de Servicios), y toda una serie de herramientas asociadas a la gestión de la seguridad, que permiten tanto al cliente como a nuestros gestores de seguridad saber lo que está ocurriendo en sus instalaciones en cada momento, así como identificar tendencias y poner el foco en nuevos riesgos y amenazas.

—¿Cree que en los últimos años ha variado la estrategia de las compañías a la hora de solicitar servicios de seguridad?

Hoy en día los clientes buscan un servicio de seguridad que les proporcione una protección de calidad, pero

no sólo desde el punto de vista de la eficacia operativa, sino también desde una perspectiva de eficiencia de los recursos utilizados y en ese sentido la tecnología es la gran aliada, es la que nos permite incrementar el nivel de seguridad ajustando al máximo el coste. Los usuarios de seguridad privada se están dando cuenta de que el modelo de la vigilancia tradicional, la vigilancia presencial

a secas, es más costoso y menos eficaz que, por ejemplo, la combinación de ésta con la tecnología. Con nuestras Soluciones de Vídeo Remoto, por ejemplo, cuando se produce una alarma un vigilante de Securitas se conecta a la cámara y al resto de las existentes en la instalación, verifica lo que ocurre en las instalaciones del cliente para tomar la decisión más adecuada, que unas veces será avisar al vigilante más cercano para que acuda inmediatamente con su vehículo al lugar u otras veces será avisar directamente a los bomberos, a la policía, al propio cliente... Además, creo que los usuarios de seguridad privada cada vez son más conscientes del valor añadido que puede aportar un servicio de seguridad de calidad a la actividad de su negocio, no sólo porque permite la continuidad de su negocio (con todo lo que ello implica en cuanto a ahorro de costes) sino porque hay toda una serie de



actuaciones que puede llevar a cabo una compañía de seguridad como la nuestra. Por ejemplo, nuestro producto Trailback está basado en tecnología GPS y se puede aplicar tanto al área de seguridad como a logística, procesos, trazabilidad y gestión de recursos, entre otros, por lo que pueden ayudar a mejorar la propia cuenta de resultados del cliente.

—Securitas Seguridad España cuenta con tres áreas con mucho peso en la compañía: PCI, Trailback y Soluciones de Vídeo Remoto, ¿podría explicarnos a grandes rasgos los elementos característicos y servicios que ofrecen?

—Efectivamente, forma parte de nuestra estrategia que estas tres áreas tengan un gran peso en la compañía. En todos estos casos la tecnología nos ha permitido desarrollar servicios de seguridad que proporcionan al cliente



Sabemos que hoy en día la tecnología permite casi a cualquier usuario medio poner una cámara en su casa o en su negocio y visionar lo que allí ocurre desde su propio terminal móvil, eso es evidente; pero lo que nosotros ofrecemos va mucho más allá, es un servicio completo en el que el vídeo está conectado al sistema de alarma y a nuestro propio COS. Desde allí nuestros vigilantes especializados en SVR no sólo gestionan la Vídeo Verificación de Alarmas de Intrusión o de Incendio, si no que de manera proactiva, previo acuerdo con el cliente, realizan Rondas de Vigilancia Remota con capacidad de interactuar

En este sentido, y buscando tanto una mayor diferenciación sobre nuestros competidores, como la capacidad de ofrecer a nuestros clientes un abanico más amplio de soluciones y servicios, la creación del Área de PCI hace ahora un año representó un paso adelante en la puesta en práctica de nuestra estrategia de ofrecer soluciones capaces de satisfacer las necesidades de seguridad de nuestros clientes de manera transversal, incluyendo también la Protección Contra Incendios. La rápida identificación de alarmas de incendio es crítica para iniciar los procedimientos de actuación y es evidente que la combinación de los sistemas de seguridad con los de detección y alarma de incendios, todos ellos centralizados en nuestro COS, mejora sustancialmente el nivel de protección que Securitas ofrece a sus clientes, y evidentemente el de la intervención. Resulta poco útil blindar cualquier instalación con la mejor solución de seguridad si no se tienen en cuenta las medidas adecuadas para evitar el inicio y propagación de un incendio, así como sus consecuencias. Por esa razón vimos necesario completar nuestra oferta de servicios también con el área de PCI. ●

soluciones inmediatas, eficaces y a un coste asumible para la pequeña y mediana empresa.

Nuestras Soluciones de Vídeo Remoto (SVR) están muy consolidadas, pues se encuentran entre los primeros servicios que pusimos en marcha cuando entró en funcionamiento nuestro COS (Centro de Operaciones de Servicios).

en parámetros técnicos de la ubicación. También es de destacar tanto la Gestión Remota de Accesos o la Escolta Remota de Empleados.

Por otro lado, la combinación del mencionado Trailback u otros productos con el resto de soluciones de Securitas marcan la diferencia de nuestra compañía frente a otras empresas del sector.

FOTOS: SECURITAS SEGURIDAD ESPAÑA





AUGUST JIMÉNEZ. DIRECTOR DE TECNOLOGÍA. E.-MOVILIA

Tecnología NFC

Control de rondas y presencia para las empresas de seguridad

Desde que en el año 2007 apareciera en el mercado el primer móvil con tecnología NFC incorporada, el Nokia 6131, pasando por el Nexus de Google en 2010, hasta nuestros días, la tecnología NFC ha estado en constante evolución, y la incorporación del NFC en los móviles ha ido en aumento. En cuanto al uso del NFC en los teléfonos, hasta hace poco tiempo, los fabricantes de móviles pensaban que serviría, únicamente, para realizar pagos, como si fuera una tarjeta bancaria. Sin embargo, ahora son conscientes de que existen muchas otras formas de sacarle partido a esta tecnología, como por ejemplo, para el control de rondas y de presencia, en tiempo real.

EL NFC (siglas de Near Field Communication) es, básicamente, una tecnología de comunicación inalámbrica de corto alcance, que permite el intercambio de datos entre diferentes dispositivos. Trabaja en la banda de los 13.56 MHz, y la tasa de transferencia

puede alcanzar los 400 kb/s.

Debido a sus características técnicas, está pensado, fundamentalmente, para dispositivos móviles, ya que trabaja a pocos milímetros de distancia, y permite una rápida velocidad de transmisión. A diferencia de otras tecnolo-

gías, no se requiere un emparejamiento previo entre los dispositivos, y la transmisión y la recepción de datos pueden hacerse simultáneamente.

Conviene tener en cuenta que no es un sistema adecuado para la transmisión de grandes cantidades de información, ya que la velocidad de comunicación está pensada para un escenario de proximidad.

El NFC ofrece dos tipos de comunicación:

Activa, en el que los dos dispositivos que participan en la comunicación disponen de su propio chip NFC activo, por ejemplo, los teléfonos móviles.

Pasiva, en el que sólo hay un dispositivo que dispone de chip NFC activo. El otro, es un elemento que contiene un chip NFC pasivo, por ejemplo, una etiqueta NFC, que no requiere alimen-



tación eléctrica y en la que puede grabarse diferente información para que, posteriormente, pueda ser leída por un teléfono con NFC.

Para qué se puede utilizar el NFC.

Estos son algunos ámbitos que más han aprovechado esta tecnología, dadas sus características:

«La tecnología NFC permite el control de personas en movilidad, por ejemplo, para el control de rondas, personal de seguridad, etc»

Permite utilizar el terminal móvil para la identificación de personas y el acceso a edificios, zonas restringidas y transporte, por citar algunos.

Intercambio de información entre diferentes dispositivos y periféricos, como teclados, impresoras y ordenadores, por ejemplo.

Ejecución en acciones inmediatas, mediante la lectura de etiquetas NFC, de manera que cuando sean leídas, se ejecuten acciones concretas, como por ejemplo, acceder a una página Web, conectarse automáticamente a una red Wi-Fi, guardar los datos de un contacto en la agenda, etc.

Realización de pagos desde el teléfono móvil.

Control de personas en movilidad, por ejemplo, para el control de rondas, control asistencial en domicilios, personal de seguridad, etc.

Qué necesidades se pueden cubrir con el NFC en las empresas de seguridad

Gracias a la instalación de una aplicación en un terminal móvil, con

tecnología NFC, es posible controlar determinadas zonas, salas u objetos, mediante la lectura de unas etiquetas situadas en diferentes puntos. De esta forma, el personal de seguridad, a medida que va completando la ronda de control asignada, acerca su terminal móvil a estas etiquetas, y la aplicación envía la información leída a un centro de control Web, junto con la geolocalización, en el que su supervisor cono-

cerá, en tiempo real, el estado en el que se encuentra el servicio prestado a su cliente. Todas las lecturas quedan almacenadas en el servidor, y pueden ser consultadas en cualquier momento y desde cualquier dispositivo. Si no se realiza una lectura de una etiqueta, el sistema genera una alarma y envía una notificación, inmediatamente. También se pueden configurar todas las opciones de los diferentes servicios creados.

Existen funcionalidades adicionales, como por ejemplo, la gestión de días festivos en los turnos, la asignación de tareas en puntos concretos, envío de fotos e incidencias y geolocalización de todas las lecturas realizadas.

Ventajas de la tecnología NFC en entornos empresariales.

Las ventajas de utilizar el NFC son muchas y variadas, dependiendo de la utilidad y del sector en el que se aplique, pero si nos centramos en el de la seguridad, y la acompañamos de un software adecuado, las ventajas son claras:

- Disponibilidad de la información relacionada con las lecturas de las etiquetas NFC, en tiempo real.
- Ahorro en costes por la tramitación de las posibles incidencias en los servicios.
- Seguridad en las comunicaciones.
- No requiere instalación.
- No se necesita ningún dispositivo adicional, salvo el propio teléfono móvil.
- Tecnología transparente para el usuario y fácil de utilizar.
- Control del personal desplazado.
- Bajo coste debido a la fácil y rápida implantación.
- Facilidad en la automatización de procesos en la recogida de información.

Estas y otras ventajas son aplicables a otros sectores, como por ejemplo, empresas de mantenimiento o de facility services.

En definitiva, el NFC es una tecnología que ha llegado para quedarse, y de la que iremos viendo nuevas y variadas aplicaciones, tanto a nivel particular como empresarial. ●

Fotos: E-movilia



JORGE CHRISTIAN DURÁN, DIRECTOR DE SEGURIDAD; Y JUAN CARLOS GUEL, DIRECTOR CORPORATIVO DE SEGURIDAD DE GRUPO MNEMO

Ciberseguridad: cambio, desarrollo y evolución

Los eventos maliciosos también podrían ser llamados delitos cibernéticos, pero esta concepción no puede ser mundialmente aceptada, pues existen países que tienen deplorables leyes para la atención de los delitos que se cometen con el uso de recursos cibernéticos, otros países ni siquiera se han preocupado. A diferencia de los anteriores, países en Europa y otros desarrollados como Estados Unidos y Canadá sí han tomado conciencia de la problemática y han ajustado sus marcos regulatorios para tratar los eventos maliciosos del ciberespacio como delitos cibernéticos, de lo contrario sólo podrían referirse con el primer nombre.

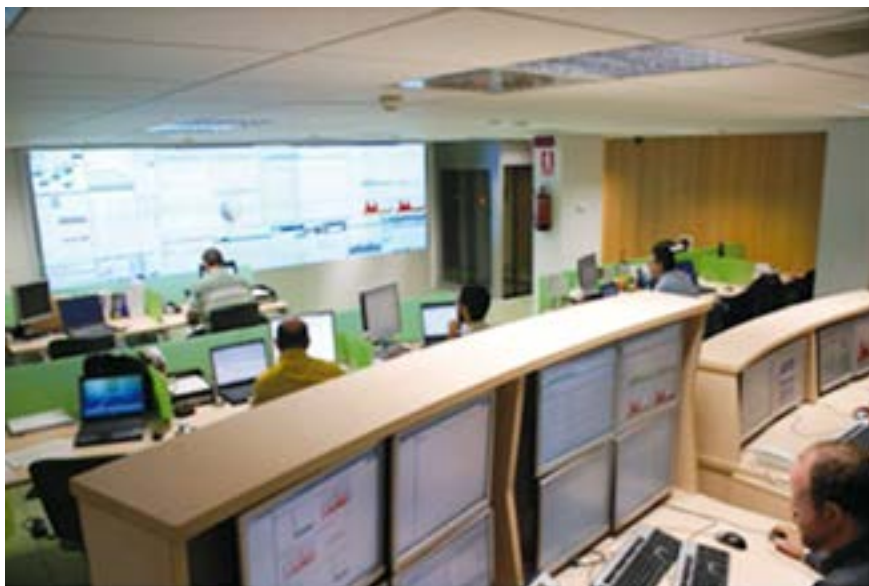
El problema se centra sobre el uso de la red de redes por la población mundial; pues Internet es hoy día la red más utilizada del planeta que brinda acceso a diferentes plataformas y recursos, de ahí su peligrosidad; incluso podríamos referirnos a Internet como un sub-mundo alterno con su

propio territorio (virtual), sus diversas condiciones e incluso sus diferentes civilizaciones. Una estadística condensada sobre el volumen de su uso se documenta en el sitio Internet World Stats, el cual indica que más de 3 mil millones de personas en el mundo tienen acceso, lo que representa más del 40% de la

población mundial (7,264,623,793 personas). Ver la tabla 1 (Figura 1) del sitio mencionado con estas cifras. Pero ese no es el único reto de exposición al que se enfrenta la industria de la Ciberseguridad hoy en día, pues la ITU ha documentado en alguno de sus estudios que existen casi 7 mil millones de suscripciones de telefonía móvil en el mundo, representando una penetración del 96% sobre la población mundial. Lo anterior no sería un problema si solamente se tratara de comunicaciones por telefonía celular, pero 2.3 mil millones de los usuarios son también suscriptores de banda ancha móvil, es decir acceden a Internet por su dispositivo móvil y esta cifra crece año con año a razón de un porcentaje expresado en doble dígito, lo cual significa que los usuarios de telefonía celular están añadiendo el empleo de datos móviles en sus servicios de telecomunicaciones. Un panorama ampliamente positivo para las empresas de telecomunicaciones al generar más negocio, pero al mismo tiempo señala un claro espectro más amplio de amenazas y riesgos contra la seguridad de todos los usuarios de Internet sin distinción de personas, empresas o gobiernos.

En Mnemo nos gusta llevar los conceptos a la práctica y bajo la filosofía de la simpleza para que cualquier persona pueda entenderlo. Por ello hemos definido a la Ciberseguridad como sigue:

«Parte de la seguridad que se ocupa de detectar, analizar, documentar, responder y solucionar los eventos mali-



ciosos ocurridos en el ciberespacio, llevándolos por un proceso integral de atención que permita la prevención de futuros incidentes de seguridad en mayor y menor medida. A su vez visualizando los siguientes elementos principales:

Cyber Inteligencia: detección y gestión de las nuevas amenazas y vulnerabilidades para dar una respuesta actualizada y dinámica frente a los riesgos a los que está expuesta una organización.

«La inversión en Ciberseguridad ha tenido, tiene y tendrá un impacto importante en el negocio al mitigar pérdidas tangibles e intangibles»

Cyber Investigaciones: proceso en el cual se emplean técnicas especiales sobre el ciberespacio y en combinación con el método científico para resolver problemas o tratar de explicar determinadas observaciones.

Cyber Malos: todos aquellos individuos que ocasionan los eventos maliciosos y llamados de diferentes maneras: hackers, crackers, intrusos, entre otros».

La Ciberseguridad en las Organizaciones

La inversión en Ciberseguridad ha tenido, tiene y tendrá un impacto importante en el negocio al mitigar pérdidas tangibles e intangibles. Se trata de una práctica que está transformando el diario acontecer de las empresas, puesto que en los últimos años han estado registrando pérdidas monetarias millonarias por causa de las brechas de seguridad.

Un problema que se visualiza recientemente es el evidente desgaste de las estructuras corporativas, que demuestran ya no tener efectividad frente a los incidentes de seguridad actuales al no ofrecer soluciones viables y contundentes a los problemas.

Aunque pudiera parecer un poco ridículo se deberá empezar por rebautizar puestos de trabajo y segregar funciones que se derivarán en la crea-

ción de posiciones con responsabilidades específicas, que requieren atención particular. El Chief Información Security Officer debería cambiar su nombre, y por supuesto también sus funciones, a Chief Risk Security Officer. También será necesario contar con la custodia de los datos, el cual podrá ser comúnmente llamado Chief Data Protection Officer. Finalmente será importante nombrar la figura del Head of Intelligence quien deberá mejorar la calidad de la información para mejorar la seguridad.

Paradigmas que romper

¿Las organizaciones deberán crear su propia área de inteligencia?

Cuando surge un problema que atacar en una corporación el camino común suele ser crear la estructura que sea necesaria. No obstante, ello podría suponer un alto costo y los resultados serán a mediano y largo plazo, debido a la curva de aprendizaje por el que deberá pasar la nueva área. Adicionalmente, la organización que así lo determine, deberá contemplar los recursos necesarios de espacio, capacitación, certificaciones y herramientas.

En materia de inteligencia no intrusiva la actualización de conocimientos y herramientas es constante, por lo



Tabla 1

WORLD INTERNET USAGE AND POPULATION STATISTICS DEC 31, 2014 - Mid-Year Update

World Regions	Population (2015 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2015	Users % of Table
Africa	1,158,353,014	4,514,400	318,633,889	27.5 %	6,958.2 %	10.3 %
Asia	4,032,654,624	114,304,000	1,405,121,036	34.8 %	1,129.3 %	45.6 %
Europe	827,566,464	105,096,093	582,441,059	70.4 %	454.2 %	18.9 %
Middle East	236,137,235	3,284,800	113,609,510	48.1 %	3,358.6 %	3.7 %
North America	357,172,209	108,096,800	310,322,257	86.9 %	187.1 %	10.1 %
Latin America / Caribbean	615,583,127	18,068,919	322,422,164	52.4 %	1,684.4 %	10.5 %
Oceania / Australia	37,157,120	7,620,480	26,789,942	72.1 %	251.6 %	0.9 %
WORLD TOTAL	7,264,623,793	360,985,492	3,079,339,857	42.4 %	753.0 %	100.0 %

NOTES: (1) Internet Usage and World Population Statistics are preliminary for Dec 31, 2014. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the [US Census Bureau](#) and local census agencies. (4) Internet usage information comes from data published by [Nielsen Online](#), by the [International Telecommunications Union](#), by [GfK](#), local ICT Regulators and other reliable sources. (5) For definitions, disclaimers, navigation help and methodology, please refer to the [Site Surfing Guide](#). (6) Information in this site may be cited, giving the due credit to [www.internetworldstats.com](#). Copyright © 2001 - 2015, Miniwatts Marketing Group. All rights reserved worldwide.

que será muy difícil que exista un punto de madurez en el corto plazo. Entonces, considerar romper el paradigma de creación de nuevas estructuras podrá ser una decisión acertada para evitar un gran desgaste e inversión a la organización.

Un ejemplo muy ilustrativo resulta de imaginar a esa nueva área de la organización encargándose del contenido de la Deep Web, considerando que se trata de una sub-plataforma web de información oculta, no accesible por los métodos tradicionales, se accede mediante una red de datos anonimizada con avanzados algoritmos matemáticos y computacionales, así como también contiene sitios que los motores de búsqueda no pueden indexar.

¿Contratar una compañía?

La Ciberseguridad puede apreciarse como outsourcing para empresas y gobiernos. Existen gobiernos y compañías que han comenzado a hacerlo al verse rebasados y al analizar el alto coste de crear y mantener áreas dedicadas. Una ventaja de esto es que la compañía que brinde el servicio tendrá la labor y la capacidad de mantenerse actualiza-

da. Su equipo especializado podrá resolver casos que los corporativos, simplemente, no tienen la capacidad. Las empresas que tomen este papel deberán proponer y acordar los protocolos apropiados de interacción.

¿Cómo manejar la información?

La inteligencia se venía entendiendo como tener gran cantidad de datos protegidos de salir a la luz. Sin embargo, en Ciberinteligencia la clave es compartir. Los usuarios maliciosos comparten técnicas de ataques y modus operandi. Fomentar la cultura de compartir generará la oportunidad de contrarrestar y cerrar puertas a los intrusos. Con nuevos exploits y APTs que surgen cada día se afecta la capacidad de reaccionar. Por ello, debemos cambiar el paradigma. Dejar de ser un cuerpo de inteligencia del pasado y comenzar a compartir lo que obtengamos del ciberespacio, desde luego empleando los protocolos de seguridad adecuados.

Conclusiones

Es necesario evolucionar la estructura de seguridad de las organizaciones.

Dejar de percibir los problemas como parte de sistemas o dispositivos de seguridad. Lo que se ofrece en este artículo es una propuesta, al final son las mismas organizaciones quienes deben adaptar esta propuesta en su interior. La seguridad es usar otras herramientas y considerar otros riesgos para los que no estamos preparados.

Se vuelve esencial unir esfuerzos y diseñar los protocolos para combatir los ataques y juntos romper viejos y desactualizados paradigmas. El diferencial ya no es el modus operandi porque la velocidad a la que las amenazas mutan es tan demasiado rápida que en poco tiempo han evolucionado de un estado a otro. Muchas son las veces que las empresas realmente no saben que su información está a la venta, por ejemplo en la Deep Web. Hay que evolucionar las áreas de investigación y desarrollo, pero de la mano de empresas especializadas y apoyarse siempre de ellas. Al final esas empresas podrán resolver los casos más complejos y en un tiempo menor que con capacidades internas. ●

Fotos: Mnemo

JAVIER LÓPEZ FERRER. DIRECTOR GENERAL. VIDEOCODE

«Videocode nace con vocación de ser el mejor aliado para los proyectos de vídeo»

VIDEOCODE apuesta por productos y soluciones donde además de la calidad de los mismos, el calor humano, la cercanía del fabricante, la atención del equipo que forma el canal de distribución, instalación y el propio cliente final, sea el bastión para sobrevivir a la crisis», así lo asegura Javier López Ferrer, director general de la compañía, quien a lo largo de la entrevista analiza la estrategia empresarial de cara a los próximos años, así como las novedades que han incorporado a su catálogo de soluciones.

—**A grandes rasgos, ¿podría explicarnos los orígenes de la compañía y cuáles fueron sus objetivos prioritarios?**

—Tras la desaparición y/o la disminución de actividad de algunas empresas españolas fabricantes de sistemas de

vídeo (CCTV), nos encontramos con un desánimo general por la falta de colaboradores, partners, para la mayoría de empresas del sector, y de muchos clientes finales.

La gente (instaladores, integradores, clientes finales) necesita de socios tecnológicos en los que apoyarse, que les acompañen en los proyectos importantes de un sector cada vez más duro, donde solo la calidad de las soluciones puede hacer que este sector siga funcionando. Empresas españolas, con personas cercanas, hombro a hombro, espalda con espalda.

Así nace VIDEOCODE, con vocación de ser el mejor aliado para los proyectos de vídeo.

—**¿Cuáles son los elementos diferenciales de VIDEOCODE en relación a compañías que operan en el mismo ámbito?**

—En VIDEOCODE tenemos un producto de gran calidad, pero a la vez muy versátil, un LEGO, que se adapta a las necesidades del proyecto y del cliente final; soluciones completas, pero también soluciones adaptables a otras piezas que no son VIDEOCODE, bien porque existen, bien porque están resueltas desde otros fabricantes.

—**¿Cómo ha sido su evolución en el ámbito de la gestión y análisis de vídeo en los últimos años?**

—VIDEOCODE fabrica una solución de análisis de vídeo, ANALYZ, que aprende el escenario de manera continua, y analiza los objetos que aparecen, siguiendo unos complejos algoritmos, los clasifica y según las reglas programadas actúa.

ANALYZ puede ser una solución completa, analiza, graba (es grabador), y viene con un software de gestión que puede ser autónomo o una pasarela a un Centro de Control o CRA; pero también puede ser una pieza dentro de un proyecto global, conviviendo con cámaras IP, analógicas, visibles, térmicas, con otros DVR, con barras, sistemas de sonido para cuñas de audio, etc. VIDEOCODE, también desarrolla su propio gestor de vídeo, VMS, llamado VISORCODE, sistema



Parte del equipo de VIDEOCODE. ((de derecha a izquierda: Cesar González, Sergi González, Marc Cabrerizo, Xavier Vergés, y Javier López-Ferrer).

abierto y polivalente, con capacidad para ser la pieza principal, y gestionar sistemas de otros fabricantes, o bien para ser una pasarela a plataformas mayores.

—**¿A qué mercado se dirigen actualmente y a cuál les gustaría llegar?**

—VIDEOCODE, tiene soluciones para diferentes mercados, actualmente queremos convertirnos en un referente como socio tecnológico en proyectos de Seguridad, con ANALYZ, GRAVO, y VISORCODE, pero hay mercados como el retail, donde ya tenemos soluciones de fusión de datos, VIDEOPOS; de conteo de personas, FLUENCY, etc., y donde queremos crecer, en posicionamiento y en soluciones a ofrecer.

—**En una situación de crisis económica como la actual, ¿con qué dificultades se encuentra el sector en el que su compañía opera?**

—El sector está cambiando y muchas empresas tienen que decidir dónde quieren llegar, y dónde se situarán en los próximos años. Los distribuidores deben decidir si quieren mover cajas o dar valor añadido. Las empresas instaladoras e integradoras, si van a ofrecer productos y soluciones donde su aportación como instalador o integración tiene un valor, o no. Y los clientes finales no deberían de apostar por la gama más barata del mercado, si tienen necesidades específicas o quieren



un trato especial.

Muchas veces el atractivo de un precio muy barato, destruye el objetivo del proyecto.

VIDEOCODE apuesta por productos y soluciones donde además de la calidad de los mismos, el calor humano, la cercanía del fabricante, la atención del equipo que forma el canal de distribución, instalación y el propio cliente final, sea el bastión para sobrevivir a la crisis

—**¿Qué estrategia empresarial tiene planeado VIDEOCODE de cara a los próximos años?**

—VIDEOCODE lo que planea es ser el mejor aliado para los proyectos de vídeo, por supuesto mejorar en productos y soluciones, en rango de productos, en calidad de servicio; pero sobre todo en crear una red de colaboradores, partners, con empre-

sas instaladoras, que sean los que nos ayuden a formar esa melé de rugby imparables en su avance.

—**¿Qué novedades han incorporado o quieren incorporar a su catálogo de soluciones?**

—VIDEOCODE, presentó en Security Forum su nueva plataforma de grabación, GRAVO-H, que permite indistintamente cámaras IP y analógicas, y que es una plataforma de grabación abierta a instalar las licencias del resto de soluciones que fabricamos como ANALYZ, VIDEOPOS, FLYENCY...; es decir el cliente decide cuantos canales quiere de grabación, de análisis de vídeo, de POS, etc. ●

Fotos: VIDEOCODE

Plataforma de grabación GRAVO-H.



JESSTIN ZHOU. DIRECTOR GENERAL DEL DEPARTAMENTO INTERNACIONAL. UNIVIEW

«En Uniview tenemos productos de alta calidad y profesionales líderes en capacidad innovadora»



Cuál es la historia de Uniview desde sus inicios hasta hoy?

—Uniview comenzó su negocio de videovigilancia en 2005. Pero en ese momento, Uniview era un departamento de H3C, que es el fabricante número 1 en TI y dispositivos de comunicación en China. Con una profunda herencia en la tecnología de TI de la empresa anterior, Uniview fue fundada en 2011 y se convirtió en el tercer fabricante en China en un año. De acuerdo con el informe de IHS, Uniview es la 12ª compañía en el mercado mundial en 2014. Uniview solo se centra en la vigilancia de vídeo IP. Uniview es un experto para proporcionar una solución global de vigilancia de vídeo para ciudades

«Uniview es una compañía experta en proporcionar soluciones globales de vigilancia de vídeo para ciudades seguras, universidades, aeropuertos, empresas y autopistas en China», explica Jesstin Zhou, director general del departamento Internacional de la compañía, quien adelanta en esta entrevista el objetivo de Uniview de avanzar en el mercado extranjero con la presencia de sus innovadoras soluciones que se caracterizan por su facilidad de uso, alta calidad y sistemas estandarizados.

seguras, universidades, aeropuertos, empresas y autopistas en China.

En 2014, Uniview decidió avanzar en el mercado extranjero. Tenemos productos de alta calidad que han sido probados miles de veces en China. Y tenemos un equipo de profesionales de I + D líderes en capacidad innovadora. Ahora estamos buscando socios a nivel mundial que quieran crecer juntos con Uniview.

—¿Cuáles son los objetivos globales de la empresa para el próximo año?

—Uniview es una empresa joven en el mercado internacional. Si bien para la mejora de nuestros productos, estamos buscando socios en cada país y región. El año que viene, vamos a llegar a acuerdos con «socios de desarrollo en la mayoría de los países» como objetivo principal. Esperamos que nuestros socios nos puedan ayudar a ampliar el mercado local, nos proporcionen apoyo local y servicio a los clientes. Uniview también hace negocio OEM.

Nos gustaría cooperar con empresas que tengan fuerza y experiencias enriquecedoras.

—¿Qué beneficios ofrecen sus soluciones de CCTV a sus clientes?

—Los productos y soluciones de Uniview tienen principalmente estos tres beneficios:

- Facilidad de uso: La solución SMB de Uniview es muy fácil de utilizar. Se puede agregar la cámara IP en el NVR escaneando el código QR de la cámara IP. La solución también soporta plug and play y la mejora en cloud.
- Alta calidad: En IFSEC, Uniview ha desmantelado cámaras y NVR para mostrar los diseños interiores de forma precisa. Esto demuestra nuestra confianza en los productos. El vidrio antirreflejante IR utilizado en el domo PTZ y las cámaras bala puede aumentar un 7% de transmisión IR. Los LEDs IR de doble cristal incrustados dentro la cámara bala de la serie IPC212x y el domo fijo de la serie IPC323x puede producir una mejor imagen, mientras

Empresas

se utilizan sólo 2 LEDs IR. Con los LED de tercera generación seleccionados por Uniview, la luz IR puede alcanzar hasta 30 metros. Con un diseño único y resistente al agua utilizado en la serie fija IPC323x permite disponer de carcasa con protección IP66. Uniview también mostró su placa PCB a nivel industrial en sus NVR, demostrando completamente que Uniview tiene la capacidad de fabricar productos de alta calidad.

–Sistemas estandarizados: Desde que Uniview entró en el mercado internacional, se ha esforzado por ser más abierto y estandarizado. En 2015, Uniview se convirtió en uno de los miembros de pleno del estándar ONVIF. Uniview también está haciendo esfuerzos para la integración de productos. Ahora, los productos de Uniview son compatibles con software de terceros, muy conveniente para nuestros clientes.

—En su opinión, ¿cuáles serán las tendencias en tecnologías de circuito cerrado de televisión para los próximos años?

—En comparación con hace diez años, la videovigilancia IP se ha desarrollado enormemente. En mi opinión, en el futuro, la videovigilancia IP continuará extendiéndose, más y más personas aceptarán y utilizarán cámaras IP y NVR. La segunda tendencia es la tecnología de ultra-alta resolución. Una resolución más alta significa más información. También las funciones de inteligencia que puedan prevenir crímenes de antemano, o ayudar para encontrar información clave. Estas tecnologías tienen una gran importancia para los clientes. ●

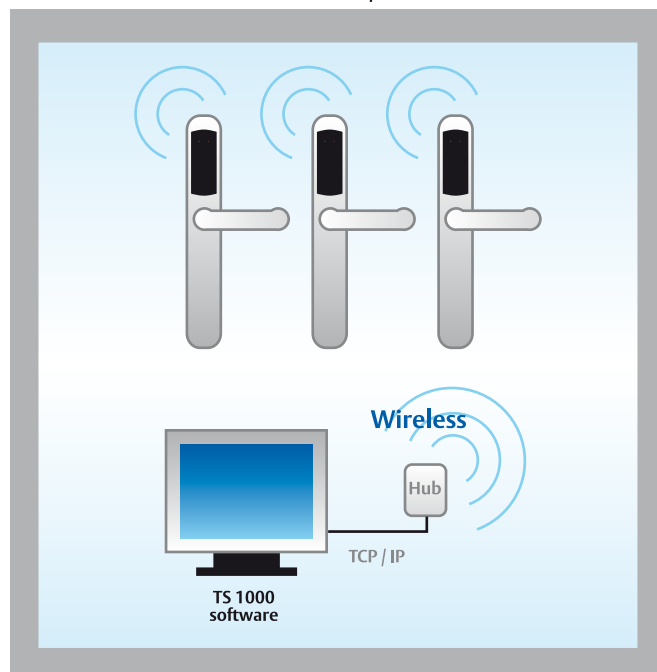
Fotos: Uniview



SMARTAIR

control de accesos sin cables: abra su mente a una nueva dimensión.

Más información en www.tesa.es/SMARTair



Entre con TESA en una nueva dimensión.

Haciendo uso de la tecnología wireless bi-direccional Tesa - Assa Abloy ofrece al mercado una solución integral, compacta y sin cables para el control de puertas. El sistema incorpora comunicaciones de radiofrecuencia encriptadas para la transferencia de información entre las puertas y el servidor, ofreciendo la mayor flexibilidad, comodidad y seguridad en el control de los accesos.



ASSA ABLOY

ASSA ABLOY, the global leader
in door opening solutions.

TESA Talleres de Escoriaza, S.A.U.
Barrio Ventas, 35 E-20305 Irun · Guipúzcoa
Tel.: +34 943 669 100 · Fax: +34 943 633 221
www.tesa.es

DAHUA DESARROLLA LA APLICACIÓN DEL ESTÁNDAR DE COMPRESIÓN H.265

H.265, el sombrero del mago

Impulsada por la siempre creciente demanda de alta definición y el desarrollo del procesamiento de imágenes, 4k es sin duda una palabra de moda en el mercado, jugando un papel cada vez más importante en la videovigilancia, especialmente en aplicaciones como ciudades seguras, estacionamientos, puertos, plazas y otros lugares de grandes dimensiones. Tiene una fuerte demanda en el detalle de captura que, al mismo tiempo, incide en la decodificación y en el almacenamiento. Por suerte, vemos un futuro allí con la introducción y desarrollo del H.265, que brinda amplias posibilidades y optimismo a la industria, abordando problemas como la escasez de ancho de banda, lo que mejora la eficiencia de la transmisión y proporciona otros beneficios.

High Efficiency Video Coding (HEVC), también conocido como H.265, es un estándar de compresión de vídeo, sucesor del H.264 / MPEG - 4 AVC (Advanced Video Coding), actualmente en fase de desarrollo conjunto por ISO/IEC Moving Picture Experts Group (MPEG) e ITU-T Video Coding Experts Group (VCEG).

En comparación con la corriente actual AVC H.264 estándar, H.265 es capaz de reducir aún más de un 50% la velocidad de datos requerida para la codificación de vídeo de alta calidad. La velocidad de transferencia de datos destaca por descargar entre un 40 % y un 50% a 1080p, mientras presta una excelente calidad de imagen.

En resumen, H.265 puede reducir el tamaño de las imágenes de vídeo en gran medida, mientras reproduce de forma fluida con poco ancho de banda, y todos estos beneficios adicionales llevan más allá la demanda del mercado en 4K / Ultra HD. En segundo lugar, con el rápido desarrollo de 4G y la tecnología móvil, la integración entre las dos industrias dispondrá de opciones mucho más sorprendentes.

Línea de productos

A pesar de todas las ventajas, el momento actual parece un poco limitado para H.265 ya que este estándar de compresión es todavía nuevo para la industria de videovigilancia, lo que signifi-



ca que va a tardar algún tiempo en ser adoptado y adaptado. Dahua Technology, como empresa líder e innovadora, no puede resistirse a su encanto y perspectiva, a tener la imagen azul no sólo en la mente, sino también llevada ya a la realidad. La empresa ha adoptado H.265 en su última gama de productos, incluyendo la cámara de red, NVR, dispositivos de transmisión, así como en sistemas de videowall.

Por comenzar con las cámaras, Dahua acaba de lanzar una cámara de red ultra-inteligente 5.0 megapíxeles que utiliza código dual H.265 / H.264, lo que permite usar un 40% menos de ancho de banda, mientras que la calidad de imagen es excepcional. Por otra parte, con sus funciones, como el defog ultra ROI, y las detecciones inteligentes, la cámara puede hacer que la vigilancia sea más clara, más inteligente y más fluida; sobre la base de esta tendencia, podemos prever que muchas más cámaras H.265 en diferentes resoluciones están en camino.

Cuando se trata de dispositivos de back-end, Dahua fue la primera compañía en la industria en introducir una línea completa de productos H.265 NVR 4K, que cubren diversas deman-



das, incluidas las pequeñas y medianas, así como aplicaciones de gran escala. Estos son los NVR con capacidad de decodificación de hasta 12.0 megapíxeles, soporte 1080P @ 60fps y H.265 de vista previa de reproducción; 4 canales 4K de tiempo de visualización en vivo y reproducción. Mientras tanto, sus funciones de inteligencia, incluyendo análisis de comportamiento, detección facial, etcétera, también son compatibles. Es importante mencionar que el equipo de I + D tuvo en cuenta el consumo de energía en la fase de planificación, para hacer el producto respetuoso con el medio ambiente.

Además, Dahua también introdujo una plataforma de control de M70 con el estándar H.265. Esta plataforma puede decodificar múltiples canales de vídeo H.265 al mismo tiempo, y gracias al diseño modular, M70 puede maximizar para manejar hasta salidas de vídeo UHD de 40 canales con cada decodificación H.265 de apoyo. Y lo que es más, estas salidas de vídeo de alta definición se pueden presentar como una imagen integrada mediante la combinación de salidas de alta definición.



H.265 ofrece más posibilidades

«Obviamente, el H.265 es una de las normas principales de compresión que nos permiten implementar soluciones UHD, como 4K o incluso 8K, que es sin duda la tendencia de la videovigilancia», afirmó James Wang, director de Producto de Dahua Tecnología.

«Los beneficios que trae H.265 no se limitan a lo anterior» –continuó Wang–, «al igual que el sombrero de un mago, se puede esperar mucho más de él, por ejemplo, nuestro departamento de I + D ha llevado a cabo algunas grandes actuaciones sobre el control de veloci-

dad de bits, el equilibrio de la calidad de imagen, así como de análisis inteligentes y seguimiento».

«Siempre me siento emocionado con las cosas y tecnologías nuevas, ya que tienen el potencial para alimentar muchas nuevas posibilidades, para llevar los productos, la industria e incluso la sociedad a un mejor estado», añadió Wang. «H.265 es sólo un caso, confiamos en aprovechar el potencial de esta norma y hacer pleno uso de ella, así que mi consejo es quedarse con nosotros, quedarse con la última tendencia y ver cómo la utilizamos como magia». ●

FOTOS: DAHUA



Contactos de empresas, p. 7.

MEGAN MILLER. RESPONSABLE DE MERCADO. SIEMENS BUILDING TECHNOLOGIES

Seguridad Corporativa, un desafío para las empresas

Los conceptos de seguridad empresarial deben ser tan diversos como lo son las empresas, los mercados y las industrias a las que se aplican. Cuando se trata de implantar estas soluciones, todas tienen una cosa en común: el factor humano, el cual juega un papel fundamental en el éxito de cualquier tecnología aplicada. Dado que cada vez es mayor el número de empleados, visitantes o contratistas que se mueven por toda la empresa, esto adquiere todavía más importancia. Teniendo esto presente, las soluciones de seguridad física viables se fusionaron con las medidas técnicas y organizativas que deben implementarse, de forma que sean aceptadas por todos los miembros de la empresa, permitiendo realizar las operaciones diarias de forma simple y fácil.

LOS conceptos de seguridad han estado presentes desde que existen las empresas. En el pasado, las medidas de seguridad eran relativamente simples, se utilizaban vigilantes de seguridad o barreras físicas como vallas. El objetivo principal ha sido siempre el mismo: la protección efectiva de las personas y los activos para evitar riesgos específicos y escenarios de amenazas. Sin embargo, en la actualidad, los responsables de la Seguridad Corporativa (CSOs) se enfrentan a nuevos desafíos especialmente apremiantes.

Globalización

Cuando las empresas se convierten en multinacionales, sus ubicaciones, divisiones y filiales se expanden por todo el mundo, cada una con sus necesidades específicas, incluyendo los requisitos de seguridad locales o las regu-

laciones gubernamentales. Al mismo tiempo, los empleados cada vez tienen más movilidad y con frecuencia ya no están atados a una ubicación fija de la empresa. Esto requiere unos estándares de seguridad uniformes en toda la empresa para satisfacer los requisitos locales, así como las políticas de dirección corporativas que requieran una gestión remota.

Delitos cibernéticos y seguridad TI

Los datos son uno de los activos más valiosos de una empresa, y en muchos casos los más vulnerables. Los estudios muestran que más del 50% de las organizaciones que pierden información crítica quedan fuera del mercado en menos de dos años. Pasar de los activos físicos a los activos basados en la información y una creciente tendencia hacia el almacenamiento online de los

datos, la seguridad TI es cada vez más compleja. Esto tiene un impacto claro sobre la seguridad empresarial tradicional dado que muchas de las violaciones de seguridad correspondientes a los datos, las redes y la infraestructura de TI se originan internamente. Incluso el cortafuegos más potente no puede proteger a una empresa de este tipo de amenaza interna o espionaje. Las soluciones de seguridad tienen que coordinarse de forma precisa y relacionar el acceso físico con los procesos de TI para que la seguridad física y lógica confluyan.

Presión competitiva, imagen y conformidad

En el competitivo entorno actual, las empresas confían cada vez más en el mantenimiento de la continuidad de los negocios y en gestionar su reputación con sus principales interesados. Todos los incidentes de seguridad deben gestionarse cuidadosamente para evitar daños en la marca corporativa. Los incidentes relevantes exigen una rápida respuesta para mantener un nivel de seguridad adecuado local o globalmente. Un tiempo de parada prolongado es inaceptable bajo cualquier circunstancia y debe evitarse todo acceso no autorizado a los datos o información de los clientes. Además, tienen que documentarse todos los eventos y medidas activadas para su posterior información, y debe ser posible hacer un seguimiento para fines de auditoría con el objetivo de cumplir con los requisi-

tos regulatorios gubernamentales, industriales o locales.

El factor humano

Los responsables de la Seguridad Corporativa se enfrentan a escenarios cada vez más exigentes usando con-

les. Además, pueden surgir problemas cuando se despliegan una variedad de soluciones de acceso en diversos edificios o ubicaciones. Las tarjetas o llaves de acceso pueden perderse fácilmente o ser robadas; si esto no se detecta durante un largo periodo de tiempo, pone a la empresa ante un nuevo ries-

evoluciona la empresa y ofrecer capacidades de automatización para dar soporte a los usuarios. Otro aspecto es la aceptación de los controles de seguridad que están vigentes. En otras palabras, lo que importa no es tanto la propia tecnología como la forma en la que la utilizarán los usuarios.

«Los datos son uno de los activos más valiosos de una empresa, y en muchos casos los más vulnerables»

ceptos de seguridad holísticos creados en base a análisis de riesgos estandarizados, teniendo siempre en cuenta a los usuarios. Puesto que las personas siguen siendo uno de los puntos débiles más importantes que pueden plantear un riesgo potencial, es importante conocer a las diferentes personas involucradas y combinar procesos y políticas como parte de las estrategias de gestión de riesgos. Solo cuando los empleados de cualquier nivel de la empresa se ven a sí mismos como parte del concepto de seguridad es posible solucionar las carencias de seguridad que no pueden tratarse únicamente con tecnología.

La tecnología debe ser apropiada para las operaciones diarias

Las soluciones de seguridad son una parte esencial de una cultura de seguridad, pero deben alinearse con los procesos y requisitos empresariales. La tecnología debe ayudar a los empleados a cumplir con los estándares de seguridad en sus operaciones diarias. La gestión de acceso es un ejemplo práctico de ello. Si las soluciones aplicadas no son fáciles de usar en la vida diaria, los empleados encontrarán formas de eludir los estándares y regulaciones actua-

go. Sin embargo, si se aplica la tecnología correcta, intuitiva, modular y fácil de usar, los empleados la utilizarán correctamente como parte de su rutina normal.

Los CSOs o Responsables de Seguridad Corporativa actuales tienen que adaptarse a los cambios de tecnología y asegurar que las inversiones sean a prueba de futuro. Un factor fundamental es la tecnología apropiada; tiene que proporcionar flexibilidad a medida que

La seguridad corporativa como concepto

En muchas empresas, las soluciones o disciplinas de seguridad se gestionan individualmente o compartimentadas, lo que genera un aumento de los recursos y los costes. Históricamente, este suele ser el resultado de una fusión o adquisición, donde los sistemas son «heredados» por la empresa existente. Muchas veces se debe también a que los diferentes departamentos o ubicaciones tienen distintos requisitos. Las soluciones tipo silo siguen siendo comunes, lo que supone una pérdida de los estándares de seguridad y un aumento de los gastos de administración,



mantenimiento y formación.

Siemens ha respondido a estos escenarios heterogéneos con un enfoque holístico a la seguridad corporativa. Estas soluciones se centran en grandes empresas internacionales con ubicaciones muy dispersas, así como clientes en un espacio de mercado competitivo que otorga un alto valor estratégico a aspectos de seguridad. Siemens ofrece soluciones de seguridad personalizadas e integradas y servicios que dan soporte a un marco completo de análisis de riesgos, consultoría y planificación para la implementación, mantenimiento y actualizaciones futuras.

Esto proporciona a las empresas estándares de seguridad universales que

tenerse en cuenta. Después de que se haya definido y documentado todo esto, son necesarias contramedidas técnicas, estructurales y organizativas que se adapten con precisión a situaciones individuales y a los requisitos actuales. La clave es crear una cultura de seguridad en toda la empresa que englobe a todos los interesados a todos los niveles.

Estructuras de seguridad centrales

En un estudio de mercado de seguridad internacional realizado por Siemens, el 83% de los CSOs o Responsables de Seguridad Corporativa estudiados reconocieron la tendencia



pueden aplicarse en toda la empresa y en todo el mundo.

Para implementar este tipo de solución de seguridad, en primer lugar, es importante comprender la actividad de la empresa y seguir con una estrategia específica para la misma. Tienen que tenerse en cuenta las condiciones y especificaciones locales para asegurar que la estrategia global general no interfiera con la privacidad aplicable o con otras regulaciones de protección de datos. El desarrollo comienza comprendiendo el negocio principal de la empresa, seguido por un análisis de los procesos y políticas corporativos. La siguiente fase es la identificación de escenarios de amenaza específicos y los riesgos que deben

hacia las soluciones de seguridad corporativa organizadas de forma centralizada. El desplazamiento a la seguridad corporativa orientada estratégicamente y alineada centralmente no puede realizarse de forma adecuada usando tecnologías aisladas o soluciones tipo silo. Un enfoque holístico permite a los profesionales de la seguridad, a nivel operativo y estratégico, obtener un impulso y aumentar su capacidad, según sea necesario, para responder rápida y fácilmente, si se produce un incidente.

Un ejemplo de un enfoque holístico es el concepto «Una Tarjeta» para el control de acceso en toda la empresa: una sola tarjeta de ID de empleado multifuncional satisface las necesidades

de los visitantes, empleados y contratistas. La tarjeta sirve como una llave electrónica para todas las entradas, puertas y portones, y también puede usarse para opciones de autoservicio, como el pago sin tarjeta para servicios de cafetería, acceso a aplicaciones de software o archivos sensibles y muchas otras necesidades especializadas. Los empleados aceptan fácilmente la tecnología cuando les proporciona valor añadido y les permite más independencia dentro de la empresa. La solución de «Una Tarjeta» ofrece también seguridad adicional, cuando se requiere, para instalaciones, recursos o infraestructuras críticos, que necesitan un enfoque de software uniforme y centralizado.

En empresas muy grandes, las soluciones de «Una Tarjeta» de nuestra compañía facilitan el movimiento de los empleados por toda la empresa en cualquier lugar y permiten un acceso seguro a las redes y a la información. El sistema gestiona todas las identidades y autorizaciones, eliminando de este modo los procesos manuales. Los datos de los portadores de tarjetas tienen que introducirse solo una vez y se sincronizan automáticamente con la base de datos corporativa en tiempo real, ahorrando tiempo y dinero. Las ubicaciones de sucursales individuales pueden decidir gestionar independientemente sus soluciones o disciplinas de seguridad, pero pueden elegir configurarlas centralmente para abarcar múltiples ubicaciones. Si se pierde o se roba una tarjeta ID o de acceso, los datos del usuario pueden recuperarse inmediatamente de una base de datos central, permitiendo al personal de seguridad anular rápidamente las credenciales y crear una nueva ID. Esto minimiza las carencias de seguridad y los esfuerzos administrativos cuando se emite una ID sustitutoria y evita duplicados. ●

Fotos: Siemens

MESA REDONDA DEL COMITÉ DE DETECCIÓN DE TECNIFUEGO-AESPI EN VALENCIA

Seguridad contra incendios en el hogar

El Comité de Detección de Tecnifuego-Aespi organizó en Valencia su Mesa Redonda anual sobre Protección contra Incendios en Viviendas, en general, y detección y alarma, en particular. Este foro reunió a profesionales reconocidos (ingeniería, fabricante, instalador, receptora de alarma, administración pública) para debatir sobre los retos presentes y ofrecer una perspectiva futura de desarrollo.

EN 2015, la mesa redonda organizada en Valencia ha centrado el enfoque del debate en desarrollar la conciencia individual acerca del riesgo inherente de incendio en los edificios de viviendas. Para el profesional esta es una cuestión obvia, pero, sin embargo, hoy día sigue siendo un reto el reconocimiento de este riesgo por parte de la mayor parte de la población.

Tras el interesante debate, Juan de Dios Fuentes, coordinador del Comité de Detección de Tecnifuego-Aespi, recogió algunas de las conclusiones más importantes a tener en cuenta. Se destacan:

- Necesitamos demostrar que existe el riesgo de incendio, y generar inquietud para alertar a la sociedad sobre la necesidad de protección.
- En la Comunidad Valenciana, casi la mitad de las viviendas son anteriores a los años 80, y una cuarta parte tiene más de 50 años. Todas ellas anteriores a la legislación (NBE-CPI y CTE). Estas viviendas son las prioritarias a proteger.
- Debería haber un manual de seguridad contra incendios en vivienda a disposición de los vecinos.

- La conciencia no llega hasta que no se vive un suceso de emergencia.
- Hay que plantear también la detección de gases domésticos y tóxicos.
- Existen limitaciones normativas para hacer confluir la Safety y la Security.
- Es llamativo el bajo nivel de dotaciones de protección contra incendios, PCI, en vivienda.
- En la Comunidad Valenciana, la guía sobre las condiciones básicas de la

vivienda existente incluye la Seguridad contra Incendios.

En un momento clave

- El momento clave para incrementar la seguridad contra incendios en vivienda es al realizar reformas y rehabilitaciones.
- Se debe desarrollar el plan de evacuación global del edificio para integrar el interior de las viviendas y las zonas comunes.
- Todo sistema de detección que no está conectado al exterior o que está aislado, tiene mayor potencial de degradarse con el tiempo.
- Trabajar en concienciación y reglamentación no deberá ser excluyente, sino complementario. ●

Fotos: Tecnifuego-Aespi





JAVIER TORMOS. RESPONSABLE SECTOR SEGURIDAD PÚBLICA Y EMERGENCIAS. INTERGRAPH ESPAÑA, S. A.

La gestión de grandes emergencias

Las labores de rescate en el accidente de avión de Germanwings ponen de nuevo de manifiesto la importancia de una buena planificación en la gestión de grandes emergencias. A este tipo de tragedias, que se generan como consecuencia del factor humano, se suman los desastres naturales como resultado de fenómenos ambientales extremos que, como muestran las estadísticas, son cada vez más frecuentes, intensos, dinámicos y complejos. Además de la capacidad destructiva de estos sucesos, las consecuencias que tienen sobre las personas y los bienes se ven amplificadas debido al proceso de ocupación y transformación del territorio y a la inexistencia, en algunos casos, de una evaluación adecuada de los riesgos y las vulnerabilidades de estos espacios.

La magnitud y complejidad de este tipo de incidentes requieren unos niveles de comunicación, interacción y articulación muy elevados entre los diferentes servicios involucrados, para los que los sistemas de mando y control habituales no están específicamente

diseñados.

Los sistemas de gestión de grandes emergencias requieren de datos que deben estar organizados con antelación y que permitirán reaccionar ante las situaciones que se presenten de forma ágil y efectiva. Dichos datos reco-

pilados durante la fase de prevención son, entre otros, los mapas de riesgos que permitirán conocer a qué peligro se está siendo expuesto actuando en la zona afectada, los organigramas y datos de contacto de cada organización que se encuentra involucrada o afectada, los datos de censos o instalaciones de interés geolocalizadas, los modelos digitales del terreno, etc.

Asimismo, estos sistemas también incorporan datos precargados que incluyen los planes de emergencia y protocolos que hay que seguir, según el tipo de incidente y el nivel de emergencia del que se trata.

Qué Plan de Emergencias debe activarse

Según todo esto, el sistema aportará la inteligencia de la que carecen los documentos impresos: indicando qué plan de emergencias debe activarse, asistiendo en la ejecución y seguimiento de todas las tareas a realizar y permitiendo realizar análisis geoespaciales (sobre población afectada u otras variables involucradas), y lo más importante: optimizando la coordinación, entre todos los agentes involucrados. De este modo, cada servicio de emergencias podrá compartir su información con los demás servicios, permitiendo la difusión, en tiempo real, de las decisiones y los datos clave y pertinentes, con todas las organizaciones e individuos involucrados (sobre la ubicación de re-



curios, las tareas que hay que realizar, etc.), y la información de ámbito público y de especial interés, (como partes meteorológicos, planos de interior de edificios, etc).

cia, encaminadas a restaurar las funciones críticas de la comunidad o la zona afectada.

Actualmente ya existen en el mercado sistemas que materializan este

de carga y resistencia, para ejecutar un sistema de misión crítica. Se trata de plataformas web, accesibles a cualquier agente que interviene en la gestión de la emergencia, que no requieren instalación previa y cuentan con capacidad de trabajo offline, en el caso de pérdida momentánea de las comunicaciones.

En resumen, la implantación de este tipo de sistemas permite una mayor colaboración entre los diferentes actores involucrados en los procesos de gestión de emergencias, redundando en una mejor comunicación y coordinación, una toma de decisiones más rápida y una respuesta mucho más eficiente. ●

«Los sistemas de gestión de grandes emergencias requieren de datos que deben estar organizados con antelación y que permiten reaccionar de forma ágil y efectiva»

En este esquema es fundamental la integración con otros sistemas habituales de gestión (geolocalización de vehículos y recursos, mando y control para despacho de medios), pero también la posibilidad de operar sin ellos, cuando no exista integración, o en el caso de que se produzca una pérdida de comunicaciones.

concepto e incorporan la arquitectura fundamental que proporciona todas las características necesarias de disponibilidad, fiabilidad, redundancia, balanceo

Fotos: Intergraph

Gestionar la recuperación

Los sistemas de gestión de grandes emergencias también deben permitir gestionar otra fase clave del proceso: la recuperación, que hace referencia a todas aquellas actividades que continúan más allá del período de emergen-



Contactos de empresas, p. 7.



**NUEVAS BARRERAS DE IR
DE 4 HACES DE OPTEX
PARA NUESTRA
FAMILIA RESIDENCIAL**



CUADERNOS DE SEGURIDAD PARTICIPA EN UN CURSO ORGANIZADO POR ADESyD

Medios de comunicación y movimientos sociales

Bajo el título «40 Años de Democracia en Seguridad y Defensa (1975-2015) Balance y retos de futuro», la Asociación de Diplomados Españoles en Seguridad y Defensa (ADESyD) celebró el pasado mes de julio la cuarta edición de sus cursos de verano, donde Cuadernos de Seguridad tuvo la oportunidad de participar y aportar su visión sobre el tema «Los medios de comunicación y movimientos sociales».

El objetivo del curso era promover entre los alumnos el conocimiento del papel que los distintos gobiernos democráticos han desarrollado en la España constitucional, y profundizar en las relaciones e interacciones entre diplomacia, Fuerzas Armadas y Fuerzas y Cuerpos de Seguridad del Estado, así como su relación con otros actores sociales (medios de comunicación, movimientos sociales).

Con gran éxito de participación, como en ediciones anteriores, el curso contó expertos de primera talla vinculados al mundo de la Seguridad.

Bajo la dirección de Miguel Ángel Ruiz de Azúa, decano del Colegio Nacional de Doctores en Ciencias Políti-

cas y Sociología, y María Angustias Caracuel, presidenta de ADESyD, durante cuatro jornadas, los alumnos asistieron a ponencias y mesas redondas donde se analizó desde distintos puntos de vista el proceso de consolidación de la democracia en España en sus ámbitos de seguridad y defensa; su relación con otros escenarios geográficos (Europa, EE.UU., el Mediterráneo, Iberoamérica, África y Asia) y la interacción con distintos actores nacionales, internacionales y la sociedad civil.

El primer día estuvo dedicado a la *Transición y modernidad en Seguridad y Defensa*. El programa se inauguró con la conferencia sobre Democracia y Representatividad, a cargo de Jordi Mar-

sal, adjunto civil al director del CESEDEN y miembro del Consejo de Honor de ADESyD.

Durante la jornada también se habló sobre El modelo policial en la España constitucional, La Guardia Civil como Cuerpo de Seguridad Pública y Las Fuerzas Armadas, entidad única.

En la segunda jornada se trató el tema de *La Seguridad y la Defensa hoy*, centrándose en El Sistema de Seguridad Nacional y La Acción Exterior española.

Una mesa redonda sobre los Nuevos riesgos, nuevas amenazas, abrió la sesión del tercer día, que se completó con distintas ponencias sobre la influencia de las cuestiones de género y La cooperación seguridad pública-seguridad privada: una sinergia necesaria.

El curso se cerró con una sesión dedicada a *La implicación de la ciudadanía en Seguridad y Defensa*, con una charla sobre la Comunicación en Seguridad, y una mesa redonda sobre Medios de comunicación y movimientos sociales –moderada por Alfredo Crespo–, que contó con la participación de Miguel Ángel Benedicto, secretario general del Movimiento Europeo; Carmen Chamorro, periodista y directiva de ACPE, y Julia Benavides, directora de Contenidos de Peldaño, editora de CUADERNOS DE SEGURIDAD.

Los ponentes debatieron sobre la importancia de los medios de comunicación a la hora de difundir el mensaje de los movimientos sociales, y analizaron la compleja situación social y política que vive Europa, y concretamente España, en la actualidad. ●



ORGANIZADO POR IFEMA SE CELEBRARÁ DEL 23 AL 26 DE FEBRERO

SICUR 2016: mayor oferta y representación internacional

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

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

Además, todo apunta a que SICUR 2016 crecerá en todos sus parámetros. El buen ritmo de contratación registrado hasta la fecha, y la labor que viene desarrollando la organización del Salón para potenciar la presencia de profesionales y usuarios de seguridad, nacionales e internacionales, abren expectativas muy positivas para la próxima convocatoria. En este sentido, y al margen del gran atractivo que despierta la oferta del Salón, se está trabajando en un ambicioso programa de jornadas técnicas que, en el marco de FORO SICUR, abordará temas transversales de interés para los usuarios de la seguridad de todos los sectores de la actividad, con un formato muy dinámico y orientado al debate.

La oferta de SICUR se presentará en distintas áreas monográficas representativas de la Seguridad Contra Incen-

dios y Emergencias, en la que se enmarcan las empresas especializadas en la protección activa y pasiva contra el fuego, así como en las soluciones para mejorar la respuesta en situaciones de emergencia; la Seguridad Privada y Pública, en el sector Security y un contenido fuertemente marcado por el avance tecnológico al servicio de la protección de bienes y vidas; la Seguridad Laboral, en SICUR Prolabor, con lo último en Equipos de Protección Individual –EPIs–, así como en medidas de prevención y salud laboral, y el sector de Defensa, que acogerá a las empresas suministradoras de productos para el ámbito naval, aeronáutico, espacial, ar-

mamento, soluciones electrónicas e informáticas, vehículos terrestres, industria auxiliar, así como otros desarrollos realizados para el mercado civil adaptados al ámbito de Defensa.

Exposiciones, exhibiciones, demostraciones operativas...

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

Fotos: Sicur



EL SALÓN SE CELEBRA DEL 29 DE SEPTIEMBRE AL 2 DE OCTUBRE EN FERIA DE MADRID

Trafic 2015: soluciones de movilidad con vehículos seguros y eficientes

El Salón Internacional de la Movilidad Segura y Sostenible, TRAFIC, organizado por IFEMA, se celebrará del 29 de septiembre al 2 de octubre en la FERIA DE MADRID. Una convocatoria que, en su décimo cuarta edición, se presenta más completa que nunca, incorporando a las últimas novedades en infraestructuras y aparcamientos, un combinado de flotas públicas y privadas con los estándares tecnológicos de última generación para atender la creciente demanda de las corporaciones locales.

EN esta próxima edición, la Feria pondrá el foco en la movilidad en vías interurbanas y urbanas, a través de una oferta articulada en torno a la eficiencia energética, el equipamiento y la sostenibilidad en carreteras, la seguridad vial y los sistemas inteligentes de transporte, como e-call. Un contenido amplio e integrador del sector, que concitará la atención muy especialmente de los nuevos responsables de movilidad y tráfico, de las re-

cién constituidas corporaciones locales de toda España, que tendrán la posibilidad de exponer y compartir públicamente, en un foro institucional y muy profesionalizado, sus modelos de movilidad sostenible.

Por otro lado, TRAFIC también ha abierto el plazo de presentación de productos para la Galería de la Innovación que, de nuevo, ha encontrado gran aceptación entre las empresas participantes en la Feria. El Jurado

constituido al efecto procederá en breve a seleccionar los admitidos.

Asimismo, se está trabajando ya en la programación de la agenda de conferencias y otros encuentros profesionales que integrarán una nueva edición del FORO TRAFIC. En esta ocasión, destaca como novedad la convocatoria, dentro de dicho espacio de debate, de la II Jornada de Seguridad Vial Urbana – Cuartos Premios de Seguridad Vial para los Policías Locales, que organiza la Unión Nacional de Jefes y Directivos de Policía Local, UNIJPOL.

Una convocatoria que, en su décimo cuarta edición, se presenta más completa que nunca, incorporando a las últimas novedades en infraestructuras y aparcamientos, un combinado de flotas públicas y privadas con los estándares tecnológicos de última generación para atender la creciente demanda de las corporaciones locales.

Todo ello está generando gran expectación en el sector, como se refleja en la excelente respuesta que está encontrando entre las empresas la nueva convocatoria de TRAFIC, que ha iniciado su comercialización con un buen ritmo. ●



Fotos: Trafic

EL ENCUENTRO SE CELEBRARÁ EN FIERA MILANO DEL 3 AL 5 DE NOVIEMBRE

Sicurezza: soluciones verticales, estrellas de esta edición

El camino hacia SICUREZZA 2015 continúa con muchos regresos importantes y una oferta amplia orientada hacia tecnologías personalizadas para contextos específicos. Un formato que sigue creciendo y, en tres ediciones - 2015, 2017 y 2019 - pretende convertirse en el evento de referencia en el sector para el área mediterránea.

UNA vuelta a la muestra de muchas empresas importantes, un regreso de marcas que no han estado en la feria durante unos años, un enfoque en nuevos temas que se ven en el futuro inmediato del mercado y abren interesantes oportunidades de negocio. Con unos pocos meses todavía por delante antes de la apertura de la feria, SICUREZZA 2015 (en Fiera Milano del 3 al 5 de noviembre) se perfila de nuevo para ser el evento clave para los profesionales del sector de la seguridad y prevención de incendios, una exposición internacional única prevista para el segundo semestre de este año.

Esta edición, que se celebrará en unas fechas poco frecuentes del calendario, está proponiendo un formato que se orienta cada vez más hacia soluciones en línea con los requisitos de los expositores y de todas las empresas del sector, y es probable que crezca en las próximas exposiciones programadas para 2017 y 2019.

Mientras tanto, las empresas se están inscribiendo para la exposición a un ritmo importante: una vez más, las empresas de videovigilancia estarán presentes, pero también existe una cada vez mayor oferta de soluciones y productos para la seguridad pasiva –fabricantes– y empre-

sas de control de acceso, por mencionar algunos de los sectores con mayor número de expositores.

«Sicurezza se perfila para ser el evento clave para los profesionales de la seguridad»

Otro factor clave es la presencia en la feria de un número considerable de empresas líderes del mercado, que han optado por este evento, ya que está en contacto con sus mercados de referencia y proporcionará oportunidades potencia-

les para los nuevos acuerdos comerciales.

Pero SICUREZZA 2015 no sólo ofrecerá una visión completa de tecnologías y soluciones a través de las propuestas que ofrece de primera mano por los mayores fabricantes italianos e internacionales, sino también a través de iniciativas verticales centradas en un mundo de aplicaciones en constante crecimiento. De esta forma se guía a los profesionales del sector que visitan

la feria, proponiéndoles la opción que mejor se adapte a sus necesidades y ayudándoles a comprender el potencial de las tecnologías. ●

Fotos: Sicurezza



Arecont: Scott Schafer recibe el premio SIA

ARECONT Vision®, especialista en la industria de tecnología para cámaras con resolución megapíxel basada en IP, ha anunciado que el vicepresidente ejecutivo Scott Schafer ha sido galardonado con el premio de la SIA por su exitoso liderazgo y sus contribuciones a la organización.

Schafer trabajó en la Junta de Directores de la SIA, en el Comité Ejecutivo y desempeñó funciones como presidente de Afiliación y secretario.

«SIA otorga un valor inconmensurable a sus miembros y a la industria de la seguridad en general, y es realmente gratificante poder colaborar con el



crecimiento de esta industria junto al personal de la asociación, al equipo de miembros y a la Junta de Directores de SIA», dijo Schafer. «Recibir el premio es un enorme honor y le agradezco a SIA por este reconocimiento».

V. John Stroia, presidente de la Junta en SIA, le hizo entrega del premio a Schafer en el Centro de Convenciones Sands Expo en Las Vegas, durante la feria anual de SIA en el ISC Oeste 2015.

«Scott está siempre presente sin importar el tipo de proyecto o programa en el que estemos trabajando», dijo Stroia durante la ceremonia. También se reconoció a Arecont Vision® por sus diez años de compromiso y membresía empresarial en la SIA en el evento.

Tecnifuego-Aespi: nuevo folleto sobre protección pasiva contra incendios

EL Comité de Productos de Protección Pasiva de Tecnifuego-Aespi ha elaborado un nuevo folleto para dar a co-

Barcelona: XII Edición del Día de la Seguridad Privada

La delegada del Gobierno en Cataluña, Llanos de Luna, presidió el pasado 11 de junio en L'Auditori de Cornellà de Llobregat el acto de celebración del Día de la Seguridad Privada, en el que se hizo entrega oficial de las menciones honoríficas a los diversos profesionales de la Seguridad Privada que, en el último año, han destacado por su singular comportamiento, total entrega al servicio, profesionalidad y colaboración con las Fuerzas y Cuerpos

de Seguridad del Estado.

La delegada del Gobierno estuvo acompañada por el General Jefe de la VII Zona de la Guardia Civil, el Jefe Superior de Policía, y por los Subdelegados del Gobierno en Barcelona, Girona, Lleida y Tarragona, entre otras personalidades.

Durante el acto, se han entregado 300 menciones por servicios destacados.

En su intervención, la delegada del

Gobierno en Cataluña subrayó que «en España, la seguridad privada se configura como auxiliar y colaboradora de las Fuerzas y Cuerpos de Seguridad, a las que complementa en su labor de proteger y garantizar la seguridad de los ciudadanos». «La profesionalidad demostrada por la seguridad privada en beneficio de una seguridad común la ha hecho merecedora de un generalizado reconocimiento por parte de la sociedad española».



nocer las ventajas de utilizar este tipo de soluciones para la seguridad contra incendios de los edificios.

El nuevo folleto está disponible en versión on line y también en papel para todos los profesionales interesados que lo soliciten o quieran descargarlo gratuitamente.

La protección pasiva comprende todos aquellos materiales, sistemas y productos de la construcción, diseñados para:

- Prevenir la aparición de un incendio.
- Evitar que se propague un incendio (compartimentación).
- Mantener la estabilidad del edificio (protección estructural).

En protección pasiva hay que distinguir entre la protección del continente (edificio) y del contenido (cortinajes, alfombras, muebles, electrodomésticos, etc.).

Está regulada por la normativa (Código Técnico de la Edificación y Reglamento de Seguridad contra Incendios en los Establecimientos Industriales), que determina la instalación de sistemas de protección que garanticen la estabilidad de la estructura de la construcción y la sectorización de la misma. La responsabilidad de la protección del continente corresponde al promotor, al proyectista y al constructor del edificio.

Representa la carga de fuego propia-



Hyundai se une con by DEMES

Hyundai Corporation, Korea, ha anunciado su incursión en el mercado de España con una alianza estratégica con by DEMES S.L., distribuidor especializado y de referencia de productos de seguridad en España. Como parte de la asociación, by DEMES será el distribuidor exclusivo en España, Francia, Portugal, Italia y Holanda para toda la gama de productos de soluciones de seguridad que incluyen cámaras analógicas y grabadores de vídeo digital Hyundai. En este sentido, DM Kim, vicepresidente de Hyundai Corporation, señaló que «estamos encantados de la asociación con by DEMES y esperamos fortalecer nuestra presencia en España y otros países a través de una amplia red de contactos y la gran calidad de servicio.» Además, añadió que «estamos completamente equipados y preparados para proporcionar soluciones de seguridad de primer nivel y de la más alta calidad, con productos técnicamente superiores al resto a un precio súper competitivo, realizados a medida conforme a los requerimientos de los clientes, lo cual complementará y fortalecerá a ambas partes, y así mismo nos harán fuerte en estos territorios».

La gama de soluciones de seguridad Hyundai incluye una amplia variedad de productos tales como:

- Cámaras y equipos de grabación basados en tecnología HDCVI (720P y 1080P) HD over Coax.
- Cámaras y equipos de grabación

mente dicha. A diferencia de otros países de nuestro entorno, la regulación al respecto se limita a butacas y asientos fijos tapizados en cines, teatros, etc.

Cuatro son las cualidades fundamentales de la protección pasiva:

- Productos y sistemas no combusti-



basados en tecnología HDTV (720P y 1080P) HD over Coax.

- Cámaras y equipos de grabación en RED basados en tecnología IP (1, 2 y 4 Megapixels).

Todos los equipos están diseñados con los máximos estándares para proporcionar imágenes de alta calidad, sin sacrificar en capacidades de almacenamiento y de red. Todos los productos de esta gama se han desarrollado de acuerdo con el entorno y las condiciones de España y Europa, teniendo en cuenta los requisitos de los mercados locales y verticales.

Por su parte, Ricardo Rubi, CEO de by DEMES S.L., dijo que «a través de los años hemos logrado el liderazgo indiscutible del mercado de seguridad electrónica. Nos enorgullece establecer relaciones y vínculos con Hyundai Corporation, compañía global líder de Corea. Hyundai ha entrado en el campo de la solución de seguridad mediante el desarrollo y fabricación de sistemas de seguridad de vanguardia, y esta colaboración nos permitirá ofrecer a los consumidores españoles y de Europa soluciones completas de seguridad».

bles.

- Actúa como una barrera contra el fuego.
- Permite confinar el fuego.
- Responde de forma natural, sin necesidad de intervención humana, ni automatismos electrónicos de ningún tipo.

Nuevas publicaciones de AENOR

CÓMO implantar un SGSI según UNE-ISO/IEC 27001: 2014 y su aplicación en el Esquema Nacional de Seguridad, es la nueva publicación de AENOR, cuyos autores son Luis Gómez Fernández y Pedro Pablo Fernández Rivero. Esta publicación facilita la comprensión de todos los conceptos desarrollados en la norma UNE-ISO/IEC 27001:2014, para la implantación efectiva de un Sistema de Gestión de Seguridad de la Información (SGSI).



Asimismo, incluye un capítulo descriptivo de otra herramienta importante para la implantación de los requisitos de la Norma UNE-ISO/IEC 27001, la Norma ISO/IEC 27002, que ofrece un conjunto de recomendaciones y buenas prácticas para la implantación de las medidas de seguridad seleccionadas.

Además, entre otros contenidos este libro analiza:

- Cómo dar cumplimiento al Esquema Nacional de Seguridad (ENS), reglamento de obligado cumplimiento en el ámbito de la Administración Electrónica, mediante un SGSI.
- El proceso de certificación del SGSI.
- La relación entre los apartados de la norma y la documentación del sistema.
- La correspondencia entre las Normas UNE-ISO/IEC 27001:2007 y UNE-ISO/IEC 27001:2014.

Pedro Pablo Fernández uno de los autores junto a Luis Gómez Fernández, ambos expertos en seguridad de la información en Start Up explica «Con esta guía pretendemos ayudar a los responsables de implantar y mantener un SGSI a comprender los requisitos de la norma UNE-ISO/IEC 27001 y llevarlos a la práctica a través de ejemplos».

Siemens: mantenimiento de los sistemas de seguridad de los aeropuertos de AENA

Tecosa, compañía del Grupo Siemens, especializada en la integración de sistemas de seguridad, ha sido la adjudicataria por parte de AENA del contrato de mantenimiento de los equipos CEIA y Smiths Heimann, durante al menos un año. Este servicio se llevará a cabo en el conjunto de los aeropuertos de la red de AENA, que asciende a 47. Los retos a los que se enfrentan hoy quienes toman las decisiones respecto a la seguridad de los aeropuertos son cada día más complejos, ya que tienen que considerar procesos adicionales que tradicionalmente han estado fuera del foco de su desempeño. Entre ellos se incluyen la gestión del flujo de pasajeros, una mayor capacidad de la aeronave, llevar a cabo el criterio de seguridad de clasificación de los pasajeros, el cumplimiento de la legislación o la

creciente presión por la disponibilidad operativa y la optimización de los beneficios. Para lidiar con éxito todos estos factores, la red de Aena cuenta con una serie de sistemas de detección, utilizados tanto en el control de seguridad como en la inspección de equipajes de mano y bodega. Entre ellos se encuentran arcos detectores de metales, detectores de metales de calzado, dispositivos convencionales de rayos X y equipos automáticos para la localización de explosivos. La colaboración de Siemens-Tecosa con Aena data de 1977, año en que la tecnológica suministró a la entidad sus primeros equipos de seguridad. AENA confía una vez más en Siemens para garantizar una respuesta rápida y efectiva a los retos que conlleva la gestión segura de un gran flujo de viajeros y equipajes a diario.

Ilunion Seguridad: formación

EL Área de Incendios y Emergencias de ILUNION Seguridad, que este año cumple su 25 aniversario, forma a personal operativo del Consorcio Provincial de Bomberos de Castellón (Valencia) para que puedan actuar en determinadas situaciones peligrosas y urgentes en el nuevo aeropuerto de la provincia.

Se trata del Curso de Formación de

La Guardia Civil desarticula una organización criminal que asaltaba viviendas

La Guardia Civil, en el transcurso de la operación BACARÁ desarrollada en Almería, ha detenido a cuatro personas y ha imputado a otras cuatro, toda ellas de nacionalidad rumana, kosovar y serbia, por llevar a cabo asaltos a viviendas ubicadas en zonas rurales de Almería y Murcia en las que empleaban violencia extrema sobre sus moradores.

El grupo criminal, cuya base de operaciones se encontraba en Garrucha (Almería), estaba dirigido por un miembro que tomaba las decisiones, planificaba, coordinaba y dinamizaba la actividad delictiva. El resto de los miembros de la organización quedaban bajo su control.

La red, que disponía de gran movilidad geográfica en sus desplazamientos, adoptaba importantes medidas de seguridad con el fin de dificultar su seguimiento y localización.

Los asaltos se llevaban a cabo en viviendas ubicadas en zonas despobladas,



cuyos moradores eran personas de avanzada edad. Los delincuentes, ataviados con pasamontañas, tras neutralizar mediante inhibidores de frecuencia los sistemas de alarma, accedían al interior de las viviendas atando y amordazando a los moradores hasta conseguir todo el dinero en efectivo, objetos de valor y vehículos de su propiedad.

Los vehículos sustraídos eran trasladados a un garaje que la organización poseía en la localidad de Palomares (Almería). En este lugar, se realizaba un reportaje fotográfico de estos que posteriormente servía como

catálogo para mostrarlo a compradores potenciales de países del este de Europa.

En el transcurso de la operación se han practicado 3 registros domiciliarios en Garrucha, Vera y Palomares (Almería), en los que se ha intervenido los siguientes efectos:

- 3 vehículos sustraídos.
- Inhibidores de frecuencia.

- Ropa, guantes, linternas y herramientas para la comisión de robos.

- Efectos de joyería.
- Material electrónico.

Hasta el momento los investigadores han esclarecido más de una veintena de hechos delictivos.

La investigación, dirigida por el Juzgado de Instrucción núm. 1 de Vera (Almería), ha sido realizada por el Equipo Contra el Crimen Organizado (ECO) de la Unidad Central Operativa de la Guardia Civil con sede en Málaga y el por Equipo de Policía Judicial del mismo Cuerpo de Garrucha (Almería).

Bombero de Aeropuerto, en el que se formarán un máximo de 90 profesionales de dicho consorcio (30 por cada una de las tres ediciones).

Organizado y financiado por el Consorcio de Bomberos de Castellón, este curso tiene dos partes, una teórica y otra práctica. La primera tiene una duración de 35 horas y se imparte en las instalaciones en Castellón del parque de bomberos de Oropesa del Mar.

La segunda, compuesta por 40 horas lectivas, se imparte en el Centro de Formación Contra Incendios y Emergencias que ILUNION Seguridad tiene en Brunete (Madrid), uno de los mejores de Europa y especialmente diseñado para la formación, entrenamiento y reciclaje del personal, tanto del sector público como del privado, dedicado a cualquier tipo de intervención en emergencias.



Siemens, en la central nuclear de Cofrentes

SIEMENS, compañía global especializada en tecnología, está trabajando en la sustitución del actual sistema de extinción de incendios, basado en

halón, de la central nuclear valenciana de Cofrentes. Para ello, utiliza la solución integral Sinorix 1230, que emplea el agente extintor Novec 1230 de 3M, la ciencia de la compañía se aplica a hacer la vida de las personas más fácil y ayudar a las empresas a ser más productivas. De este modo, Siemens reemplaza al Halón 1301 por una solución integral que abarca todo el proceso

de protección frente al fuego; desde la evaluación de riesgos y diseño del sistema, hasta su puesta en marcha y mantenimiento. Sinorix 1230 es un sistema muy efectivo –extingue el fuego en 30 segundos- y limpio –no produce residuos ni emisiones contaminantes-, especialmente en riesgos eléctricos y electrónicos. La extinción del fuego se lleva cabo mediante la última genera-

El Instituto Nacional de Ciberseguridad (INCIBE) gestionó en el primer semestre cerca de 28.000 incidentes cibernéticos

El ministro del Interior, Jorge Fernández Díaz, visitó el pasado mes de julio en León el Instituto Nacional de Ciberseguridad (INCIBE), centro tecnológico «imprescindible para la seguridad de nuestro país», que durante el primer semestre de 2015 ha gestionado cerca de 28.000 incidentes cibernéticos, lo que supone un considerable incremento respecto a 2014, año en el que se registraron 18.000 incidentes. También en 2015 se han resuelto satisfactoriamente más de 40 ataques contra infraestructuras críticas, mientras que en 2014 fueron 67 en todo el año.

Además, el ministro del Interior destacó la importancia de este centro en la lucha contra la amenaza yihadista.

Este tipo de terrorismo se «caracteriza por su predilección hacia las nuevas tecnologías con las que son capaces de crear terror con sus acciones, pero también las utilizan para adoctrinar, radicalizar y reclutar a futuros terroristas. Si antes el proceso de radicalización tenía lugar en mezquitas y otros espacios físicos, hoy se calcula que el 80 % de los procesos de captación se llevan a cabo a través de Internet y las redes sociales».

El Instituto Nacional de Ciberseguridad de España (INCIBE), que depende del Ministerio de Industria, Energía y Turismo (MINETUR), es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza di-

gital. Además, operado por el INCIBE se encuentra el CERT de Seguridad e Industria -centro de respuesta a incidentes de ciberseguridad-, en cuya gestión participa de manera muy activa el Ministerio del Interior. Fernández Díaz afirmó que es el «centro tecnológico del Ministerio del Interior para responder de forma efectiva al complejo escenario cibernético al que se enfrenta España y para proporcionar ciberseguridad a la población española».

Asimismo, Fernández Díaz resaltó que el CERT de Seguridad e Industria, que atesora una amplia experiencia, es el centro más potente y con mayores posibilidades tecnológicas de España, contando en la actualidad con una plantilla de la que forman parte más de un centenar de profesionales de los ministerios del Interior y de Industria, Energía y Turismo.

El ministro del Interior también subrayó la labor de la Oficina de Coordinación Cibernéticas que, como parte integrante del CERT de Seguridad e Industria, asegura «la imprescindible relación de las capacidades que aporta este centro con otros elementos que contribuyen, desde otras perspectivas, a garantizar la ciberseguridad pública en España».



Curso de Extensión Universitaria: Protección al consumidor en los servicios de seguridad privada

Con la colaboración de AECRA y Dirección General de Comercio y Consumo de la Comunidad de Madrid, la Universidad Nacional de Educación a Distancia ha convocado la I Edición del Curso «Protección al consumidor en los Servicios de Seguridad Privada», que tendrá lugar del 8 de octubre al 9 de diciembre.

Ya está abierto el plazo de matrícula para el Curso de Extensión Universitaria sobre la protección al consumidor en los servicios de seguridad privada. El curso cuenta con una carga lectiva de 50 horas y con dos créditos ECTS, impartido en formato de formación a distancia se inicia el próximo día 8 de octubre en sesión presencial y finaliza el 9 de diciembre de 2015.

En el citado curso, adaptado a la nueva Ley 5/2014 de seguridad pri-

vada y Ley 3/2014 de modificación del RD 1/2007 texto refundido de la Ley General de defensa del consumidor, se abordará el contenido de los servicios de mantenimiento de sistemas de seguridad, el régimen contractual aplicable, las condiciones generales de la contratación aplicables a dicho sector empresarial, sus cláusulas contractuales abusivas, requisitos legales exigidos a empresas y usuarios de servicios de seguridad en dichos contratos, así como procedimientos de reclamación y queja ante las OMIC, servicios de Atención al cliente de las Empresas prestadoras de servicios de seguridad.

Conoce el sistema arbitral de consumo como solución para la resolución de conflictos entre la empresa de seguridad y sus clientes.

ción de agentes químicos para este uso, «Novec 1230», un fluido de 3M, no corrosivo ni conductor, que se carga junto con nitrógeno y que al abrir la válvula en caso de incendio se descarga en forma gaseosa. Su alta eficacia permite utilizar bajas concentraciones de diseño de extinción. Cero riesgos, cero impacto en la capa de ozono. La extinción ecológica mediante Sinorix 1230, basada en Novec 1230 de 3M, posee un margen de seguridad muy elevado, incluso más allá de la eliminación del fuego. Este sistema posee uno de los menores potenciales de calentamiento global, una reducida vida útil en la atmósfera –de 3 a 5 días– y ningún impacto en la capa de ozono. Además, la naturaleza no corrosiva ni conductora de este

agente extintor garantiza la protección de los equipos más delicados durante su uso. Asimismo, su baja toxicidad combinada con una baja concentración de diseño, le otorga el mayor margen de seguridad en comparación con los agentes halocarbonados, CO2 o mezclas con gases inertes, lo que le hace inocuo para la salud de las personas, por lo que puede utilizarse en espacios que puedan estar ocupados. En esta misma línea, al no ser tóxico, ni inflamable, ni explosivo, no hay restricción para su transporte. Siemens ya ha suministrado aproximadamente cuatro toneladas de Novec. Los trabajos de sustitución en la central nuclear de Cofrentes comenzaron en 2010 y se prevé que finalicen en 2015.

Ingram Micro, nuevo mayorista de Axis Communication

AXIS Communications, especialista del mercado en vídeo en red, es una compañía con un modelo de comercialización 100% indirecto, por ello, todos sus socios son una prolongación de su propio equipo y desempeñan una función clave en la estrategia de mercado y en el éxito global de la empresa. Esto hace imprescindible que los socios conozcan de primera mano cuáles son las soluciones que ofrecen para cada sector según las necesidades de cada negocio tanto en materia de vigilancia como en analíticas de negocio más completas.

Como novedad, las soluciones de vídeo IP de Axis Communications comenzarán a ser distribuidas y comercializadas por Ingram Micro. Gracias a un acuerdo entre ambas compañías con vigencia desde el 1 de julio, el mayorista utilizará la estructura de ventas en España para ofrecer los productos del fabricante.

«El mercado del vídeo IP ofrece actualmente grandes oportunidades de negocio y la firma de este acuerdo con Ingram Micro es importante para nosotros ya que amplía y complementa la estructura de mayoristas que tenemos a día de hoy, especialmente por la calidad de su base de clientes», afirmó Julio Castillo Sevilla, responsable del canal de distribución de Axis Communications para España y Portugal.

Ingram Micro es una compañía que ofrece un amplio abanico de tecnología y servicios de la cadena de suministro a las empresas de todo el mundo. Fundado en 1979, Ingram Micro es el líder de

innovación en tecnología y servicios de la cadena de suministro.

Con su completa infraestructura global y enfoque en soluciones en la nube, la movilidad, la cadena de suministro y la tecnología, Ingram Micro permite a los socios de negocio operar de la manera más eficiente y con éxito en los mercados en los que operan.

«Desde hace varios meses estamos desarrollando el negocio de valor en Ingram Micro, lanzando al mercado una estrategia muy definida y con un equipo de profesionales certificados que gestionan este negocio tan exigente», concluye Manuel Méndez, Business Manager Physical Security en Ingram Micro.

Casmar apuesta por el mercado de Chile y Colombia

CASMAR Electrónica S.A, empresa española de distribución de material y soluciones de seguridad electrónica, con más de 35 años presentes en el mercado español y de 8 años en Portugal, inaugura una nueva etapa con la apertura de oficinas en Chile y Colombia.

Esta decisión se basó en la apuesta de Casmar por el crecimiento de los países sudamericanos y la aportación de la experiencia de Casmar dentro del mundo de la seguridad.

En los mercados chileno y colombiano hay una gran demanda de soluciones



Cecabank certifica con AENOR la seguridad de su información

Cecabank ha obtenido el certificado de seguridad de la información para los sistemas de información que llevan a cabo la recepción, el procesamiento y transmisión de transferencias y adeudos adaptados a SEPA (Single Euro Payments Area). Este certificado se obtiene conforme a la Norma ISO 27001, y ha sido concedido por AENOR (Asociación Española de Normalización y Certificación).

El sello acredita que Cecabank ha implantado un Sistema de Gestión de Seguridad de la Información (SGSI), que le permite identificar los riesgos de cada activo de información, evaluar sus implicaciones y adoptar los controles más eficaces para mitigarlos.

Además, el SGSI implantado en Cecabank garantiza el adecuado cumplimiento de las exigencias legales de seguridad en materia de protección de la propiedad intelectual, protección de datos personales, y los servicios para la sociedad de la información, y establece una permanente revisión de las medidas implantadas.

La gestión eficaz de la seguridad de la información de Cecabank implica medidas para asegurar:

- su confidencialidad, garantizando que sólo quienes están autoriza-

- su integridad, asegurando que la información y sus métodos de proceso son exactos y completos, y
- su disponibilidad, para que los usuarios autorizados tengan acceso a la información y a sus activos asociados cuando lo requieran.

El Certificado de Registro de Empresa es el nº SI-0023/2015, y lo otorga AENOR a Cecabank como evidencia y reconocimiento, nacional e internacional, de la conformidad de su sistema de gestión con la norma UNE-ISO/IEC 27001:2014.

Para Javier Planelles, director de la División de Operaciones de Cecabank, «la obtención de este certificado ratifica el objetivo de la excelencia en el servicio que ofrecemos a nuestros clientes a través de la continua mejora de la calidad y seguridad de todos nuestros procesos».

Según Manuel Romero, director de Certificación de AENOR «La ISO 27001 se consolida como el referente mundial en seguridad de la información. Cecabank ha implantado la nueva versión de esta norma internacional, que presta mayor atención al contexto de las organizaciones y a los objetivos y riesgos de seguridad».

de seguridad para grandes proyectos y Casmar Electrónica, gracias a su experiencia en el mercado, y a los acuerdos estratégicos con una selección de los mejores fabricantes nacionales e internacionales, ofrece los mejores productos y

soluciones para instalaciones de seguridad electrónica.

Análisis de vídeo, cámaras térmicas, cámaras IP, sistemas contra intrusión, soluciones de integración de seguridad son una pequeña muestra de lo que Casmar ofrecerá, siempre con la garantía de la experiencia y de los acuerdos de distribución con fabricantes estratégicos y de soluciones profesionales.

El malware bancario descende un 18,7% en el segundo trimestre

Según los datos de Kaspersky Lab, sus soluciones han neutralizado más de 379 millones de ataques lanzados desde recursos de Internet ubicados en diferentes países del mundo y se han detectado más de 26 millones de objetos maliciosos únicos durante el segundo trimestre del año. De igual modo, los antivirus de la firma reaccionaron ante más de 65 millones de direcciones URL únicas.

Durante ese periodo, se neutralizaron los intentos de ejecución de malware que roba dinero accediendo a las cuentas bancarias en los equipos de más de 755.000 usuarios. Esta cifra comparada con la del trimestre anterior, cercana a los 930.000, indica que se ha producido un descenso del 18,7% en malware bancario. Sin embargo, el dato es ligeramente superior al de hace un año cuando este tipo de programa malicioso afectó a 735.000 usuarios. En total, los productos de Kaspersky Lab han registrado durante lo que va de año casi seis millones de notificaciones sobre intentos de infección con este tipo de malware.



Respecto a la distribución territorial de los ataques, Singapur, con un 5,28% de usuarios atacados, se sitúa en primer lugar. Suiza y Brasil, con un 4,16% y un 4,07% respectivamente, son segundo y tercero en este particular podio. Completan el top 10 Australia, Hong-Kong, Turquía, Nueva Zelanda, África del Sur, Líbano y Emiratos Árabes Unidos. En cuanto a España, el 2,02% se topó al menos una vez con un troyano bancario.

UNESPA: el seguro atiende 906.000 siniestros en comunidades de vecinos

El sector asegurador atiende 906.000 siniestros en comunidades de vecinos al año. Fruto de estos percances,

las entidades indemnizaron o realizaron reparaciones a los afectados por valor de 372 millones de euros. Esta es una de las conclusiones que se desprenden de la última edición de la Memoria social del seguro elaborada por UNESPA y publicada el pasado junio.

En España hay 743.000 edificios asegurados. Cataluña, con 202.407, es la región donde hay un mayor número de pólizas de este tipo. Su posición también es destacada en términos relativos. Hay 271 inmuebles asegurados por cada 10.000 habitantes. El segundo puesto en términos absolutos lo ocupa Madrid, con unas 111.000 comunidades protegidas. Otros territorios superan a esta última región si se emplea como referencia la cantidad de pólizas por habitante. En Asturias, por ejemplo, hay 207 edificios cubiertos por cada 10.000 habitantes y en La Rioja son 203. En comparación, Madrid tiene 173. A la cola de la presencia de aseguramiento por cada 10.000 habitantes se encuentran Ceuta (53), Extremadura (78) y País Vasco (79).

DiiD y Paradox alcanzan un acuerdo de distribución en España y Portugal

DiiD, empresa especializada en la distribución de material de seguridad, ha anunciado el acuerdo de distribución con Paradox Security Systems para los mercados de España y Portugal. Con esta alianza estratégica, DiiD afianza su liderazgo en la distribución de productos de intrusión en estos países.

El acuerdo se extiende a toda la gama de productos de intrusión de la firma canadiense de reconocido prestigio a nivel mundial. Una vez más, desde DiiD se refuerza la apuesta por incorporar a su proyecto fabricantes

de primer nivel internacional.

En palabras del director general de DiiD, Ignacio Barandiarán «Nos enorgullece contar con Paradox en nuestro portfolio, algo que sin duda, nos sitúa a la cabeza de la distribución en España y Portugal. Seguimos avanzando en el camino de conseguir tener los mejores fabricantes y las últimas innovaciones tecnológicas para ponerlas al alcance de nuestros clientes. Gracias a esta alianza se nos abre una gran oportunidad de crecimiento en el mercado de la seguridad en España y Portugal».

Tyco Retail Solutions adquiere FootFall

TYCO Retail Solutions, la división de seguridad y rendimiento para el sector minorista de Tyco, ha anunciado la adquisición de FootFall, especialista global de inteligencia minorista, de Experian, plc, por £ 38,5 millones de libras esterlinas (US\$60 millones) en efectivo. FootFall, con sede en el

Reino Unido, proporciona a miles de minoristas y propietarios de centros comerciales tecnología «end-to-end», servicios y soluciones de análisis minorista para la recopilación, medición y análisis del tráfico de consumidores en tiendas y propiedades. FootFall administra más de 50.000 dispositivos instalados en aproximadamente 13.000 sitios minoristas, los cuales capturan más de 15 mil millones de visitas de compradores a través de 11 mercados en Europa, Asia Pacífico y América del Norte.

«La adquisición de FootFall además de complementar nuestro portafolio

existente de soluciones de rendimiento en tiendas basado en información para nuestros clientes minoristas, también es consistente con la estrategia de crecimiento e innovación de Tyco», comenta Nancy Chisholm, presidenta de Tyco Retail Solutions. «Esta inversión estratégica posiciona a Tyco como el proveedor líder de soluciones de inteligencia de tráfico a nivel global, mientras fortalece y diferencia nuestras soluciones de Internet de las Cosas (IoT) que ofrecen visibilidad en tiempo real con capacidades predictivas de inventario, merma de inventario y comportamiento del comprador».

General ASDE & Instituto IUMET: certificados psicomédicos para portadores de armas de fuego y Seguridad Privada

Desde General ASDE, S.A., a través de su Centro Investigador de referencia ubicado en Valencia, el Instituto Universitario de Medicina Telemática (IUMET), se está llevando a cabo una importante investigación en materia de Certificados Psicomédicos para Portadores de Armas de Fuego y Seguridad Privada.

El objetivo fundamental de la investigación consiste en la modificación del Anexo de condiciones psicofísicas del vigente Real Decreto 2487/1998, por el que se regula la Acreditación de Aptitud Psicofísica necesaria para la Tenencia y Uso de Armas y para prestar Servicios de Seguridad Privada.

Con esta propuesta se trata de adecuar y diferenciar las necesidades y condiciones de aptitud necesarias para cada una de las actividades profesionales contempladas en las normativas. En el ámbito de la Seguridad Privada, por ejemplo, carece de sentido aplicar los mismos criterios de aptitud para un Director o Jefe de Seguridad que

para un Vigilante o un Escolta Privado, puesto que se no requieren las mismas capacidades para el desempeño de su labor. Se plantea, también, la diferenciación entre uso o no uso de arma según el tipo de habilitación. Actualmente, se hace necesaria una revisión y actualización del cuadro de condiciones de aptitud psicofísica, ya que se trata de una normativa cuyo contenido es inadecuado en multitud de aspectos y por no haber sido actualizada desde hace más de 15 años.

La investigación está dirigida por el Dr. Francisco Tortosa Gil, Catedrático de Psicología de la Universitat de València, director del Grupo PRECOVIR del Instituto Universitario de Tráfico y Seguridad Vial (INTRAS) y miembro de la directiva de la Sociedad Española de Psicología Jurídica y Forense. Entre otras figuras importantes, se cuenta también con el asesoramiento científico-técnico del Dr. Luis Montoro González, Catedrático de Seguridad Vial de la Universitat de València,

presidente de FESVIAL y Director del Grupo FactHum.lab del INTRAS.; y con la colaboración de Juan Antonio Checa Martínez, director de Seguridad y presidente de la Comisión Organizadora de AVADISE.

Para realizar esta tarea investigadora de la manera más completa posible y disponer de una muestra amplia y significativa, es necesario realizar nuevas pruebas psicofísicas -no influyentes en el resultado de las exploraciones- a personas de diferentes agrupaciones, por lo que se considera indispensable la colaboración de colectivos y asociaciones del ámbito de la seguridad pública y privada.

General ASDE S.A. ofrece la aplicación de un 50% de descuento sobre el precio del certificado de reconocimiento médico, en el CRC del Instituto Universitario de Medicina Telemática - IUMET- (C/ Emilio Baró, 33), en el caso de que colaboren con la investigación realizando las pruebas complementarias.

Innovative ofrece mapas y direcciones basadas en OpenStreetMap

Innovative ha anunciado que el módulo de Mapas de interVIEW es ahora compatible con el proyecto de código abierto OpenStreetMap.

Los usuarios de OpenStreetMap actualizan continuamente los mapas y direcciones, lo que garantiza una actualización continua de los mapas en interVIEW.

Los clientes también pueden optar por instalar el servicio de mapas y direcciones localmente. De este modo se enriquecen los datos de Innovative con sus propios datos locales y por lo tanto

se consigue una información extremadamente detallada.

Características seleccionadas:

- Basado en datos geográficos de OpenStreetMap, que se caracterizan por una rápida introducción de cambios y correcciones en sus mapas/direcciones
- La solución de mapas y direcciones de Innovative tiene dos partes: un mapa visual en forma de mosaico (archivos PNG) a diferentes niveles de zoom e información sobre la dirección de búsqueda.



- El servicio de suscripción garantiza datos geográficos actualizados.
- El cliente puede tener la solución instalada y de este modo añadir/fusionar sus propios mapas y direcciones.

Tyco IF & S: app, seguridad

Con el objetivo de ofrecer a los usuarios una mayor flexibilidad y comodidad, Tyco Integrated Fire & Security, empresa especializada en soluciones de seguridad y protección contra incendios, ha anunciado su nueva aplicación para teléfono móvil, disponible para iOS y Android. Con esta app, los clientes de Tyco pueden acceder a todas las prestaciones de su sistema de alarma de forma cómoda, fácil y segura, desde cualquier lugar, gracias a la inmediatez y comodidad que aportan los dispositivos móviles.

Algunas de las principales características de la nueva app de Tyco son:

- Acceso a toda la seguridad y control del hogar o negocio con tan solo un click: Gestión remota del sistema de alarma, incluso si se encuentra fuera de casa o de su negocio, pudiendo conectar y desconectar total o parcialmente el sistema.
- Mediante el sistema clip on demand, los usuarios pueden recibir en su móvil o tablet imágenes en tiempo real de su hogar o empresa y controlar qué pasa en todo momento.
- Control y reporte de la actividad del hogar, etc.

Delta Informática: escáner fotográfico de reconocimiento de pasaporte

Delta Informática, compañía especializada en el desarrollo y comercialización de soluciones de captura y reconocimiento automático de documentos, ha presentado un nuevo escáner para pasaportes y documentos de identidad con tecnología fotográfica, el SmartCam. El nuevo escáner es compatible con el software propio de reconocimiento Delta ID.

El nuevo lanzamiento completa la solución Delta ID en el apartado hardware ya que aporta a la gama tecnología fotográfica, ergonomía y nuevas opciones en seguridad. La captura de la imagen con fotografía permite mayor fiabilidad, ya que se reducen posibles distorsiones de tracción o por el movimiento de documento. Además, una visera fija evita tener que levantar y bajar tapas para escanear.

SmartCam permite añadir un



módulo de RFID para lectura de ePassports, cada vez más vigentes, así como lector de banda magnética y de chip de tarjeta inteligente o DNIe. La fotografía de luz no visible, como infrarrojos, amplía el nivel de seguridad.

Delta ID permite reducir un 60% el tiempo de check-in, mejorando la imagen de la empresa y evitando colas. Actualmente reconoce más de 50 tipos de documentos de identidad y pasaportes de más de 150 nacionalidades. Delta ha sido la primera empresa en incorporar el nuevo DNI 3.0 a la lista de documentos reconocidos.

Samsung: nuevos videograbadores de red con PoE+ integrado

Samsung Techwin ha presentado una nueva gama de videograbadores de red (NVR) a precios competitivos y equipados con un switch integrado PoE+.

La presentación de los nuevos videograbadores de red se produce poco después del lanzamiento de la gama de cámaras WiseNet Lite de Samsung Techwin. La combinación de las nuevas cámaras y los nuevos videograbadores ofrece a los diseñadores de sistemas un amplio abanico de opciones que se ajustan a todo tipo de presupuestos y requisitos de funcionalidad en proyectos de videovigilancia.

Los videograbadores de red de 4, 8 y 16 canales reducen considerablemente los costes de instalación ya que no es neces-

rio contar con fuentes de alimentación y switches individuales. Gracias a la funcionalidad PoE+ integrada, los tres nuevos NVR ofrecen energía suficiente para cualquier cámara PoE+ que cumpla con el estándar ONVIF, incluidos los domos PTZ para exterior.

«Nuestros nuevos videograbadores de red con switches PoE+ integrados suministran energía de forma segura a las cámaras y otros dispositivos mediante cables de datos Ethernet estándar, con la ventaja añadida de que se puede usar PoE en cualquier lugar sin necesidad de tener en cuenta las posibles variaciones en los estándares de suministro local», afirma Tim Biddulph, Product Manager para Samsung Techwin Europe, Ltd.

Los tres nuevos NVR son compatibles con las cámaras de 8 megapíxeles y, por tanto, graban imágenes de una altísima calidad, como las imágenes que capturan las cámaras 4K.

Están equipados con una larga lista de beneficios prácticos e intuitivos que incluyen una interfaz gráfica de usuario en pantalla, muy fácil de usar y disponible en múltiples idiomas.

Los tres nuevos modelos son:

SRN-473S: NVR de 4 canales con 4 puertos PoE+, grabación a 32 Mb/s de ancho de banda, un disco duro interno y compatibilidad con e-SATA.

SRN-873S: NVR de 8 canales con 8 puertos PoE+, grabación a 64 Mb/s de ancho de banda, hasta dos discos duros internos y compatibilidad con e-SATA.

SRN-1673S: NVR de 16 canales con 16 puertos PoE+, grabación a 80 Mb/s de ancho de banda, hasta cuatro discos duros internos y compatibilidad con e-SATA.



Mobotix: MxMC, nuevo software de gestión de vídeo

La primera versión del MxMC ya está disponible de forma gratuita para su descarga. El software de gestión de vídeo MxMC es un producto totalmente nuevo que da especial importancia a una utilización sencilla e intuitiva,

conservando al mismo tiempo la máxima flexibilidad. Algunas de las muchas nuevas ventajas que ofrece este nuevo software son: clic simple y doble, posibilidad de arrastrar y soltar, así como control por gestos, funcionamiento en

varios monitores y visualización directa de eventos. Hay que destacar particularmente las nuevas herramientas de análisis y reproducción, que garantizan que la búsqueda sea rapidísima, al igual que los resultados.

MxMC está perfectamente adaptado a las cámaras Mobotix, con lo cual favorece decididamente las ventajas del concepto descentralizado de Mobotix. MxMC permite acceder de forma controlada a vídeos grabados a través de las cámaras o, posteriormente, acceder directamente al sistema NAS.

Una característica única es la gestión del ancho de banda ajustable, con la que es posible realizar búsquedas en buena calidad incluso en redes con poco ancho de banda.



Dallmeier: nueva appliance de análisis de vídeo DVS 800 IPS

El DVS 800 IPS completa su portafolio de análisis a nivel de iniciación. La appliance de vídeo soporta el análisis de hasta 4 canales de vídeo IP y la grabación de hasta 8 canales de vídeo IP.

El DVS 800 IPS es una appliance de servidor de análisis de vídeo SEDOR® compacta y versátil. Como hardware se utiliza la probada plataforma de la VideoNetBox® II. El software SEDOR® Analysis Server para el análisis así como el software SMAVIA Recording Server para la grabación ya están instalados de fábrica. El DVS 800 IPS soporta el análisis de hasta cuatro canales de vídeo IP y la grabación de hasta ocho canales de vídeo IP.

Tanto el software de análisis como el software de grabación se pueden configurar cómodamente por Ethernet mediante un navegador. Para la evaluación de las grabaciones se ofrece el SMAVIA Viewing Client. Además de la represen-



tación rápida e intuitiva de las imágenes en vivo, el software de cliente soporta funciones sofisticadas de navegación para la reproducción, numerosas funciones de búsqueda para metadatos, el Dallmeier SmartFinder para la búsqueda eficiente de secuencias con movimientos y PRemote-HD para la transmisión con anchos de banda bajos.

Los resultados del análisis pueden ser transmitidos en tiempo real al SMAVIA Viewing Client. Además, pueden ser enviados como mensaje en forma-

to XML o ser utilizados para el control de relés externos vía Ethernet. También es posible una transmisión al cliente de gestión externo PGuard advance. Con el módulo opcional de visualización y evaluación SEDOR® DiViStic, se pueden representar gráficamente o en forma de tabla los resultados de aplicaciones de recuento por Ethernet mediante un navegador.

El DVS 800 IPS dispone de una carcasa compacta y es ideal para el montaje sobre pared.

Honeywell Security: nuevas funcionalidades en la App GX Remote Control

Después del exitoso lanzamiento de la versión 2.1 de la App «GX Remote Control» a principios de año, Honeywell ha anunciado nuevas funcionalidades en la App con la incorporación del control de salidas.

Teniendo en cuenta el gran aumento del uso de smartphones y tabletas, la aplicación ha sido diseñada para ofrecer a los clientes una forma más sencilla e intuitiva de gestionar su sistema de seguridad, independientemente de donde se encuentren. La App, que en la versión anterior ya permitía a propietarios de negocios y viviendas solicitar instantáneamente un informe de estado, armar y desarmar la alarma y revisar el registro de eventos, permite ahora además:

–Control de Salidas, que permite el control de diversos sistemas eléctricos como la calefacción, el aire acondiona-



do, la luz e incluso las puertas a través de la App. Los usuarios pueden controlar estos sistemas de forma remota permitiendo así la automatización de sus hogares y negocios desde cualquier dispositivo.

–Aumento del número de paneles que se pueden gestionar desde un único dispositivo – la nueva versión permite ahora gestionar hasta 20 sistemas a través de la App.

El control de salidas se añadió en respuesta a la creciente popularidad de la automatización del hogar y el aumento del número de clientes que buscan una plataforma única para supervisar y controlar varios sistemas eléctricos en sus instalaciones. La App se ha actualizado también para ser compatible con más dispositivos Android y así permitir a un mayor número de usuarios la gestión remota de sus instalaciones.

Synology: VisualStation, nueva solución de videovigilancia

Synology Inc. ha anunciado el lanzamiento de VisualStation VS360HD, una solución de monitorización de videovigilancia versátil, duradera y compacta. La VS360HD es capaz de decodificar y mos-

trar hasta 36 canales de vídeo sin latencia y en alta definición en un monitor HDMI/VGA cuando se combina con un servidor de grabación de vídeo en red NVR que funcione con el Surveillan- ce Station de Synology. Esta opción lo convierte en la solución perfecta para reemplazar un ordenador y ahorrar costes.

Al no tener piezas móviles, la VS-360HD es más resistente a las vibracio-

nes y a los fallos del hardware. Se trata de una solución ideal para la monitorización de videovigilancia en la recepción de un hotel o de un edificio de oficinas, o en el mostrador de una tienda. La salida de vídeo dual y los puertos USB también hacen de la VS360HD una elección asequible para soluciones de TV Wall (televisión en montaje de pared). Su sólida carcasa externa y su diseño rígido permiten que la VS360HD pueda funcionar en rangos de temperatura de entre -20 y 50 grados, habituales en entornos industriales.



Panasonic: cámara PTZ 4K

Panasonic ha presentado la primera cámara PTZ integrada del sector del vídeo profesional

La AW-UE70 ofrece una resolución de 3.840 x 2.160 a 25p a través de HDMI y tiene capacidad para transmisión en flujo IP 4K y grabación 4K interna. Además del formato 4K 2160/25p, la cámara incorpora una gran cantidad de formatos HD internacionales, como 1080/50p, 1080/50i, 1080/25p, 1080/25PsF y 720/50p.

La nueva cámara UE70 integra funciones esenciales dirigidas a la producción tales como sincronizador, estabilización de imagen

óptica (OIS, por sus siglas en inglés) y filtros de densidad neutra remotos intercambiables. La cámara cuenta asimismo con una interfaz 3G-SDI y salida de vídeo HDMI e incorpora un sensor MOS de tipo 1/2.3 y procesamiento avanzado.



Bosch: familia de cámaras panorámicas Flexidome IP

Con el lanzamiento de su familia de cámaras panorámicas Flexidome IP, Bosch presenta la más alta calidad de imagen en el campo de soluciones panorámicas de videovigilancia. La cámara panorámica de interiores Flexidome IP 7000 MP ofrece una visión panorámi-

ca de 180 grados o 360 grados de un área en particular con un sensor de doce megapíxeles de resolución a 30 imágenes por segundo, en combinación con una lente de ojo de pez. Para aplicaciones de interior y exterior, la cámara panorámica IP Flexidome 5000 MP ofrece la cámara domo de 360 grados más pequeña disponible en el mercado, que combina un sensor de cinco megapíxeles de resolución a 15 imágenes por segundo con una lente de ojo de pez. Ambos modelos garantizan una visión panorámica completa en una sola imagen sin ángulos muertos y una



captura fácil de objetos en movimiento, mejorando significativamente el rendimiento de cualquier solución de videovigilancia. En combinación con el software Video Security Client, el usuario puede seleccionar hasta seis modos diferentes de visualización. La cámara panorámica Flexidome IP 7000 MP cuenta con análisis inteligente de vídeo integrado para garantizar que los operadores son alertados siempre que sea necesario y que la información relevante, tanto en directo como en las grabaciones, sea suministrada de la forma más eficiente.

Panter y Rombull Ronets participarán en A+A presentando sus últimas novedades

Panter y Rombull Ronets, fabricantes nacionales y empresas especializadas en el sector del calzado de seguridad, y en el sector de redes, cordelerías y mallas de seguridad, bricolaje y deporte, participarán entre el 27 y el 30 de octubre en A+A, el Salón Internacional de la Seguridad Laboral y la Prevención de Dússeldorf (Alemania).

Panter presentará en esta nueva cita su completo catálogo de referencias desarrolladas a partir de una minuciosa elección de componentes y materias primas de primera calidad, así como tecnologías de última generación que garantizan total protección y una experiencia de confort inigualable.

Entre las novedades que presentará la marca en A+A destaca su nueva línea de sneakers de seguridad con estética sport-casual de última tendencia denominada Panter Skyline, concebida para aquellos profesionales que demandan un calzado de seguridad diferenciador y compatible con una vestimenta informal, permitiendo su uso



tanto dentro como fuera del trabajo.

Otra novedad es la nueva gama Panter Link, donde podemos encontrar calzado de diseño funcional y atractiva estética casual, adecuado a cualquier uniformidad o vestimenta tanto formal como informal por sus discretos colores. Otra incorporación de vanguardia aplicada en toda la gama de calzado laboral de Panter destinada al sector alimentario y sanitario es el tratamiento antibacteriano Panter Biomaster, que no sólo inhibe el crecimiento de bacterias sino que las elimina al 99'99%.

Por su parte, Rombull Ronets, mostrará sus novedades en cuanto a redes de seguridad, industria y deporte, cor-

delería profesional o bricolaje, mallas de sombreado, ocultación, mosquiteras extraordinariamente duraderas y de fácil montaje, cordelería náutica, pulpos, redes elásticas y correas de amarre, de un acabado excepcional, extraordinaria durabilidad y de montaje rápido y sencillo, a partir de materia prima de primera calidad y alta tecnología, cumpliendo con las más exigentes certificaciones europeas y los más exhaustivos controles de calidad



Vivotek: cámara IP Ojo de Pez de Anti-ligadura

Vivotek ha anunciado el lanzamiento de la cámara IP ojo de pez de anti-ligadura, la CC8370-HV. Esta cámara compacta ojo de pez de 3-Megapíxeles cuenta con el diseño de antiagarre, WDR Pro y la carcasa antivandálica, los cuales aseguran simultáneamente la seguridad de los detenidos y la eficiencia del personal de guardia. La CC8370-HV es especialmente diseñada para ambientes que requieren alta seguridad, tales como los centros de detención, las celdas, las salas psiquiátricas, y los penales.

Debido a los requerimientos aumentados de la vigilancia interior para los ambientes que necesitan seguridad extraordinaria, Vivotek



ha desarrollado la CC8370-HV para alcanzar el desafío de este campo exigente. Con la ventaja de anti-ligadura, la cámara funciona como una salvadora que previene tanto la autolesión como el conflicto. Contando con las vistas panorámicas horizontales de 180° y un ángulo tilt ajustable de 25°, la CC8370-HV permite a los oficiales de seguridad ver todos los eventos en las celdas, sin ningún punto ciego. Gracias a un micrófono incorporado, el sonido dentro del radio de 5 metros puede ser grabado claramente también.

Además, la CC8370-HV está armada con una carcasa robusta IP66 y IK10, para permitir que la cámara resista el agua y el polvo, y para protegerla contra el vandalismo o la manipulación.

ÍNDICE

MATERIALES, EQUIPOS Y SISTEMAS DE SEGURIDAD

- ALARMA Y CONTROL
- BLINDAJES, PRODUCTOS
- CALZADO DE SEGURIDAD
- CENTRALIZACION DE ALARMAS
- COMUNICACIONES
- CONTROL DE ACCESOS. ACTIVO
- CONTROL DE ACCESOS. PASIVO
- DETECCIÓN DE EXPLOSIVOS
- DETECCION DE MATERIALES Y OBJETOS
- EQUIPOS DE PROTECCIÓN INDIVIDUAL
- EVACUACIÓN Y SEÑALIZACIÓN
- EXTINCIÓN DE INCENDIOS
- ILUMINACION DE SEGURIDAD
- INFORMÁTICA DE SEGURIDAD
- MATERIAL POLICIAL
- PROTECCION CONTRA EXPLOSIONES
- PROTECCION CONTRA INCENDIOS. ACTIVA
- PROTECCION CONTRA INCENDIOS. PASIVA
- PROTECCION CONTRA INTRUSION. ACTIVA
- PROTECCION CONTRA INTRUSION. PASIVA
- PROTECCION CONTRA CONTAMINACION
- PROTECCION CONTRA ROBO Y ATRACO. ACTIVA
- PROTECCION CONTRA ROBO Y ATRACO. PASIVA
- PROTECCION CONTRA VANDALISMO
- PROTECCION DE LA INFORMACION. SEGURIDAD DOCUMENTAL
- PROTECCION PERSONAL
- SANIDAD
- SEGURIDAD LABORAL
- SEGURIDAD VIAL
- VEHICULOS BLINDADOS
- VEHICULOS CONTRA INCENDIOS
- VIGILANCIA POR TELEVISION
- VARIOS. SEGURIDAD ACTIVA
- VARIOS. SEGURIDAD PASIVA

SERVICIOS DE SEGURIDAD

- APLICACIONES INFORMATICAS
- ASOCIACIONES
- CENTRALES DE RECEPCION Y CONTROL
- CUSTODIA DE VALORES
- EVENTOS DE SEGURIDAD
- FORMACION DE SEGURIDAD
- INGENIERIA Y CONSULTORIA
- INSTALACION
- INVESTIGACION PRIVADA
- MANTENIMIENTO DE SISTEMAS
- MENSAJERIA Y TRANSPORTE
- ORGANIZACION Y GESTION
- PUBLICACIONES Y AUDIOVISUALES
- VIGILANCIA Y CONTROL
- TRANSPORTE DE FONDOS Y VALORES
- VARIOS. SERVICIOS DE SEGURIDAD

ALARMA Y CONTROL



GAROTECNIA, S.A.
SISTEMAS DE SEGURIDAD

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



Tyco Integrated Fire & Security

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



by demes
avanzando juntos hacia el futuro

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



AGUERO
Proyectos e Instalaciones, S.L.

FUNDADA EN 1966

INSTALACIONES A SU MEDIDA

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



CASMAR
sistemas de seguridad

Accesos CCTV Incendio Intrusión

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

COMUNICACIONES



DYNASCAN
professional radio



Doctor Ramón Solanich
i Riera 13-15
08905 L'Hospitalet-BCN
Tel. 93 334 88 00*
comercial@pihernz.es
www.pihernz.com

CONSULTORIA



MBC-IURIS
Abogados y Consultores

MBC-IURIS
Abogados y consultores
C/Pau Claris, 147, 2º, 2º
08009 Barcelona
Tel. 931 702 417 • Fax. 931 702 416
info@mbciuris.com
www.mbciris.com

CONTROL DE ACCESOS ACTIVO



3M España S. L.
C/Juan Ignacio Luca de Tena, 19-25
28027. Madrid.
Tel. 913 216 416
Fax. 913 216 748
mgonzalez3mmm.com
www.3m.com/es/seguridad



TESA
ASSA ABLOY

TALLERES DE ESCORIAZA, S. A. U.
Barrio de Ventas, 35
E-20305 Irún • SPAIN
Tel.: +34 943 669 100
Fax: +34 943 633 221
tesalocks@tesa.es • www.tesa.es

online

SEGURPARKING

Control de mandos por Internet

Sistemas de seguridad para garajes comunitarios

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



SKL
Smart Key & Lock

SKL Smart Key & Lock
Familias J, Entremat,
2000 MONFRANCOU - SPAIN
+34 943 71 19 52
info@skl.es
www.skl.es
IFAM



**CONTROL DE ACCESO,
HORARIO, TIEMPO Y PRESENCIA**
C/Samonta 21
08970 Sant Joan Despí
Tel.: +34 934774770
info@primion-digitek.es
www.digitek.es



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



BIOSYS
(Sistemas de Tecnología Aplicada)
C/ Cinca, 102-104
08030 BARCELONA
Tel. 93 476 45 70
Fax. 93 476 45 71
comercial@biosys.es - www.biosys.es



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



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

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



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

info@accesor.com
www.accesor.com



DORLET S. A. U.
Parque Tecnológico de Álava
C/Albert Einstein, 34
01510 Miñano Mayor - ALAVA - Spain
Tel. 945 29 87 90 • Fax. 945 29 81 33
e-mail: comercial@dorlet.com
web: http://www.dorlet.com



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



ZKTECO
Camino de lo cortao, Nº 10 Nave 1
208073 • San Sebastián de los Reyes
MADRID
Tel.: +34 91 653 28 91
sales@zktechnology.eu
www.zkteco.eu

DETECCIÓN DE EXPLOSIVOS



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



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, 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 S.A.
C/ Barcelona 101
17003 Girona
T (+34) 972 203 300
info@optimus.es
www.optimusaudio.com



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

PROTECCIÓN CONTRA INCENDIOS. ACTIVA



c/ Alguer nº8 08830 Sant Boi
de Llobregat (Barcelona)
Tel: +34 93 371 60 25
Fax:+34 93 640 10 84
www.detnov.com
info@detnov.com



SOCIO TECNOLÓGICO EN SEGURIDAD
Y PROTECCIÓN CONTRA INCENDIOS
Stanley Security España, S. L. U.
C/ Barbadillo, 7 - 28042 Madrid
Centralita: 91 312 7777 • Fax: 91 329 25 74
scs@niscayah.es
www.stanleysecuritysolutions.es
REDGP. nº 2979 fecha 22-05-01

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

El directorio es la zona más
consultada de nuestra revista.

Módulo: 650€/año*

Más información:

Tel.: 91 476 80 00

e-mail: publi-seguridad@epeldano.com

* Tarifa vigente 2015

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

El directorio es la zona más consultada de nuestra revista.

Módulo: 650€/año*

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

* Tarifa vigente 2015



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



GRUPO AGUILERA

FABRICANTES DE SOLUCIONES PCI
DETECCIÓN Y EXTINCIÓN DE INCENDIOS

SEDE CENTRAL

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

Delegaciones en:

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

Factoría de tratamiento de gases

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

Soluciones y sistemas:

** DETECCIÓN **
Algorítmica • Analógica • Aspiración • Convencional
• Monóxido • Oxyreduct® • Autónomos
• Detección Lineal
** EXTINCIÓN **
Agua nebulizada • Fe-13™ • Hfc-227ea • Co₂



PEFIPRESA, S. A. U

INSTALACIÓN Y MANTENIMIENTO
DE SISTEMAS DE SEGURIDAD Y CONTRA
INCENDIOS

www.pefipresa.com

Oficinas en: A Coruña, Algeciras, Barcelona,
Bilbao, Madrid, Murcia, Santa Cruz
de Tenerife, Sevilla, Valencia y Lisboa.

Atención al cliente: 902 362 921
info.madrid@pefipresa.com

SIEMENS

Siemens, S.A.
División Building Technologies
Área Fire Safety

Ronda de Europa, 5
28760 Tres Cantos (Madrid)
Tel.: 91 514 80 00
Fax: 91 514 07 01
www.siemens.es/buildingtechnologies



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

PROTECCIÓN
CONTRA
INTRUSIÓN.
ACTIVA



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

SIEMENS

Siemens, S. A.
División Building Technologies
Área Fire & Security Products

Ronda de Europa, 5
28760 Tres Cantos (Madrid)
Tel.: 91 514 80 00
Fax: 91 514 07 01
www.siemens.es/buildingtechnologies



C/ Menéndez Pelayo Nº 49
28009 Madrid
Tel. 913 685 120
info@solexin.es
www.solexin.es



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



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



Tyco Security Products
C/ Caléndula, 95 -
Miniparc II, Ed. M, 1ª planta
28109 Alcobendas Madrid
Tf. 91 650 24 72
www.tycosecurityproducts.com
tycoacvssalesiberia@tycoint.com
tycointrusionsalesiberia@tycoint.com



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



Honeywell Security España S. A.
Soluciones integradas de intrusión,
video y control de accesos
Avenida de Italia, 7
C. T. Coslada
28821 Coslada
Madrid
Tel.: 902 667 800 - Fax: 902 932 503
seguridad@honeywell.com
www.honeywell.com/security/es



TECNOALARM ESPAÑA

C/ Vapor, 18 • 08850 Gavà (Barcelona)
Tel.: +34 936 62 24 17
Fax: +34 936 62 24 38
www.tecnoalarm.com
tecnoalarm@tecnoalarm.es

PROTECCIÓN
CONTRA ROBO
Y ATRACO.
PASIVA

PUERTAS Y PERSIANAS
DE ALTA SEGURIDAD



ANTIFRACCIÓN - ANTIBALAS

Collbaix T. 902 496 496
www.collbaixarmorsystem.com

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD



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



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



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

¿No cree...
... que debería estar aquí?
El directorio es la zona más consultada de nuestra revista.
Módulo: 650€/año*
Más información:
Tel.: 91 476 80 00
e-mail: publi-seguridad@epeldano.com
* Tarifa vigente 2015



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



Samsung Techwin Europe Ltd
P. E. Omega - Edificio Gamma
Avenida de Barajas, 24 Planta 5 Oficina 5
28108 Alcobendas (Madrid)
Tel.: 916 517 507
STESecurity@samsung.com
www.samsungcctv.com



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



Dahua Technology Co, Ltd.
No.1199, Bin'an Road, Binjiang
District, Hangzhou
310053 China
+86-571-87688883 • +86-571-87688815
overseas@dahuatech.com
www.dahuasecurity.com



Siemens, S.A.
División Building Technologies
Área Fire & Security Products
Ronda de Europa, 5
28760 Tres Cantos (Madrid)
Tel.: 91 514 80 00
Fax: 91 514 07 01
www.siemens.es/buildingtechnologies



EET SECURITY
European Distributor
C/ Aragoneses, 15
28100 Alcobendas, Madrid
Tlf. 902 902 337
seguridad@eeteuroparts.es
www.eeteuroparts.es



Avda. Roma, 97
08029 BARCELONA
Tel.: 93 439 92 44 • Fax: 93 419 76 73
Delegación Zona Centro:
Sebastián Elcano, 32
28012 Madrid
Tel.: 902 92 93 84



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



Ballerup, Dinamarca.
Tlf. +34 902 65 67 98
ventas@ernitec.com
www.ernitec.com



DALLMEIER ELECTRONIC ESPAÑA
C/ Princesa 25 - 6.1 (Edificio Hexágono)
Tel.: 91 590 22 87
Fax: 91 590 23 25
28008 • Madrid
dallmeierspain@dallmeier.com
www.dallmeier.com



A Western Digital® Company
WD ESPAÑA
4 boulevard des Iles
92130 Issy les Moulineaux · Francia
florence.perrin@wdc.com
Tel.: 00 331 70 74 46 27
www.wdc.com



Canon España, S.A
Avenida de Europa 6
28108 Alcobendas
Madrid
Tel: +34915384500
www.canon.es
camarasip@canon.es



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



AXIS COMMUNICATIONS
C/ Yunque, 9 - 1ªA
28760 Tres Cantos (Madrid)
Tel.: +34 918 034 643
Fax: +34 918 035 452
www.axis.com



GEUTEBRÜCK ESPAÑA
Edificio Ceudas
Camino de las Ceudas, 2 Bis
28230 Las Rozas (Madrid)
Tel.: 902 998 440
Fax: 917 104 920
ffvideo@ffvideosistemas.com
www.geutebruckspain.com

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

El directorio es la zona más
consultada de nuestra revista.

Módulo: 650€/año*

Más información:
Tel.: 91 476 80 00
e-mail: publi-seguridad@epeldano.com
* Tarifa vigente 2015



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



**ADSI - Asociación de Directivos
de Seguridad Integral**
Gran Vía de Les Corts Catalanes, 373 - 385
4ª planta (local B2)
Centro Comercial Arenas de Barcelona
08015 Barcelona
info@adsi.pro • www.adsi.pro



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

ASOCIACIONES



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



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



**Grupo Alava Ingenieros
Área Seguridad**
C/Albasanz, 16 - Edificio Antalia
28037 Madrid
Telf. 91 567 97 00 • Fax: 91 567 97 11
Email: alava@alava-ing.es
Web: www.alavaseguridad.com



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



**ASOCIACION ESPAÑOLA
DE SOCIEDADES DE PROTECCION
CONTRA INCENDIOS**
C/ Doctor Esquerdo, 55. 1º F.
28007 Madrid
Tel.: 914 361 419 - Fax: 915 759 635
www.tecnifuego-aespi.org



**ASOCIACIÓN PROFESIONAL
DE COMPAÑÍAS PRIVADAS
DE SERVICIOS DE SEGURIDAD**
Marqués de Urquijo, 5 - 2ªA
28008 Madrid
Tel.: 914 540 000 - Fax: 915 411 090
www.aproser.org



C/ Alcalá 99
28009 Madrid
Tel. 915765255
Fax. 915766094

info@uaseguridad.es
www.uaseguridad.es



**ASOCIACION ESPAÑOLA
DE DIRECTORES DE SEGURIDAD (AEDS)**
Rey Francisco, 4 - 28008 Madrid
Tel.: 916 611 477 - Fax: 916 624 285
aeds@directorseguridad.org
www.directorseguridad.org



**ASOCIACION ESPAÑOLA
DE LUCHA CONTRA EL FUEGO**
Jacometrezo, 4 - 8º, nº 9
28013 Madrid
Tel.: 915 216 964
Fax: 911 791 859



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



AECRA
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



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



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



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



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



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



**ASOCIACIÓN DE JEFES
DE SEGURIDAD DE ESPAÑA**
Avd. Meridiana 358. 4ª A.
08027 Barcelona
Tel. 93-3459682 Fax. 93-3453395
www.ajse.es presidente@ajse.es



**ASOCIACIÓN VASCA
DE PROFESIONALES DE SEGURIDAD**
Parque tecnológico de Bizkaia
Ibaizabal Kalea, 101
sae@sae-avps.com
www.sae-avps.com

FORMACIÓN DE SEGURIDAD



TECNOSYSTEMS
Formación especializada en video IP
Avenida de Brasil 29, 28020 Madrid
Telf.: 916 323 168
www.videoipformacion.es

CENTRALES DE RECEPCIÓN Y CONTROL



ALARMAS SPITZ S. A.
Gran Vía, 493 - 08015 Barcelona
Tel.: 934 517 500 - Fax: 934 511 443
Cdad. de Barcelona, 210 - 28007 Madrid
Tel.: 914 339 800 - Fax: 914 332 191
Central Receptora de alarmas
Tel.: 902 117 100 - Fax: 934 536 946
www.alarmaspitz.com

INTEGRACIÓN DE SISTEMAS



TELECOMUNICACIÓN, ELECTRÓNICA
Y CONMUTACIÓN

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

APLICACIONES INFORMÁTICAS



Innovative Business Software
C/ Alcoi 106bis, 12A
08225 Terrassa (Barcelona)
Tel.: 93 789 52 05
info@innovative.es
www.innovative.es



Sant Joan de la Salle, 42. 08022.
Barcelona.
Tel.: +34 93 667 40 17
Fax: +34 93 539 47 37
www.emovilia.com
E-mail: comercial@emovilia.com

SERVICIOS AUXILIARES



SEDE CENTRAL

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

INSTALACIÓN Y MANTENI- MIENTO



Homologación de registro D.G.S.E. nº 432

INSTALACIÓN Y MANTENIMIENTO
INTRUSIÓN - CCTV - INCENDIO - ACCESOS
SUBCONTRATACIÓN
ALICANTE, VALENCIA, MURCIA, ALBACETE

www.seguridadlevante.com
902 400 022
info@seguridadlevante.com



SOCIO TECNOLÓGICO EN SEGURIDAD
Y PROTECCIÓN CONTRA INCENDIOS

Stanley Security España, S. L. U.
C/ Barbadillo, 7 - 28042 Madrid
Centralita: 91 312 7777 • Fax: 91 329 25 74
scs@niscayah.es
www.stanleysecuritysolutions.es
REDGP. nº 2979 fecha 22-05-01



TELEFÓNICA INGENIERÍA DE SEGURIDAD
 Don Ramón de la Cruz 82-84 4º
 28006 Madrid
 Tel.: 917 244 022 • Fax: 917 244 052
 tis.clientes@telefonica.es
 www.telefonica.es/ingenieriadeseguridad

PUBLICACIONES
WEB



SABORIT INTERNATIONAL
 Empresa y distribución de equipos para la
 Seguridad, Vigilancia y Defensa
SABORIT INTERNATIONAL
 Avda. Somosierra, 22 Nave 4D
 28709 S. Sebastián de los Reyes (Madrid)
 Tel.: 913 831 920
 Fax: 916 638 205
 www.saborit.com



SEGURSERVI, S. A.
 Empresa de Seguridad
 Moreno Nieto, 9
 28005 Madrid
 Tel.: 902 191 200 - Fax: 913 658 179
 segurservi@segurservi.es
 Web: www.segurservi.es
 Autorizada por la D.G.P. con el n° 1.833



AGUERO
 Proyectos e Instalaciones, S.L.
 FUNDADA EN 1966
INSTALACIONES A SU MEDIDA
 Antoñita Jiménez, 25
 28019 Madrid **ISO 9001**
 Tel.: 91 565 54 20 - Fax: 91 565 53 23
 seguridad@grupoaguero.com
 www.grupoaguero.com



PUNTOSEGURIDAD.COM
 TF: 91 476 80 00
 info@puntoseguridad.com
 www.puntoseguridad.com



Grupo RMD
 Autorizada por la D.G.P. con el n° 729
 Sede Social: Avda. de Espartinas, 5 - Plg. Industrial PIBO
 Industrial PIBO
 41110 Bollullos de la Mitación (Sevilla)
 Tlfno. 902194814 - Fax. 954002319
 http://www.grupormd.com
 comercial@grupormade.com
 SERVICIOS EN TODA ESPAÑA



CIASPROIND, S.L.
 Autorizada por la D.G.P. con el n° 3598
 Avda. de Espartinas, 5 - Plg. Industrial PIBO
 41110 Bollullos de la Mitación (Sevilla)
 Tlfno. 902194814 - Fax. 954002319
 http://www.grupormd.com
 email: comercial@grupormade.com



Avda. Manzanares, 196
 28026 Madrid
 Tel.: 914 768 000 - Fax: 914 766 057
 publi-seguridad@epeldano.com
 www.instalsec.com



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



SEGURIDAD
 Control accesos / Intrusión / CCTV / Detección
 incendios / Megafonía / Interfonía / Consultoría
ENERGÍA
 Eficiencia energética / Gestión inteligente de
 infraestructuras / Electricidad / Climatización
 / Consultoría energética
 www.ambarsye.es
 ambarsye@ambar.es
 902 55 08 01



SECURITAS SEGURIDAD ESPAÑA
 C/ Entrepeñas, 27
 28051 Madrid
 Tel.: 912 776 000
 www.securitas.es



LOOMIS SPAIN S. A.
 C/ Ahumados, 35-37
 Polígono Industrial La Dehesa de Vicálvaro
 28052 Madrid
 Tlf: 917438900
 Fax: 914 685 241
 www.loomis.com

Síguenos en twitter

@PuntoSeguridad





Suscríbete

CUADERNOS DE SEGURIDAD

RELLENE SUS DATOS CON LETRAS MAYÚSCULAS (fotocopie este boletín y remítanoslo)

Entidad: _____ N.I.F.: _____
 D. _____ Cargo: _____
 Domicilio: _____
 Código Postal: _____ Población: _____
 Provincia: _____ País: _____
 Teléfono: _____ Fax: _____
 Actividad: _____
 E-mail: _____ Web: _____

Forma de pago:

- Domiciliación bancaria c.c.c. nº _____
- Cheque nominativo a favor de EDICIONES PELDAÑO, S. A.
- Ingreso en Banco Popular c.c.c. 0075 0898 41 0600233543
- Cargo contra tarjeta VISA nº _____ Caducidad _____

Firma

TARIFAS (válidas durante 2015)

ESPAÑA
 1 año: 93€ 2 años: 165€ (IVA y Gastos de envío incluido)

EUROPA
 1 año: 124€ 2 años: 222€ (Gastos de envío incluido)

RESTO
 1 año: 133€ 2 años: 239€ (Gastos de envío incluido)

INFORMACIÓN SOBRE PROTECCIÓN Y TRATAMIENTO DE DATOS PERSONALES. De acuerdo con lo dispuesto en la vigente normativa le informamos de que los datos que vd. pueda facilitarnos quedarán incluidos en un fichero del que es responsable Ediciones Peldaño, S. A. Avenida del Manzanares, 196. 28026 Madrid, donde puede dirigirse para ejercitar sus derechos de acceso, rectificación, oposición o cancelación de la información obrante en el mismo. La finalidad del mencionado fichero es la de poderle remitir información sobre novedades y productos relacionados con el sector, así como poder trasladarle, a través nuestro o de otras entidades, publicidad y ofertas que pudieran ser de su interés. Le rogamos que en el supuesto de que no deseara recibir tales ofertas nos lo comuniquen por escrito a la dirección anteriormente indicada.



DEPARTAMENTO DE SUSCRIPCIONES: 902 35 40 45
 Avda. del Manzanares, 196 • 28026 Madrid • Tel.: +34 91 476 80 00 • Fax: +34 91 476 60 57
 suscripciones@epeldano.com • www.puntoseguridad.com

Foto: Xavi Gómez



Eduard Zamora

Director de Seguridad Corporativa de Banco Sabadell

Gemma G. Juanes

Aún conserva los ecos de una mirada infantil, mezcla de inocencia y curiosidad. Se pierde en el pasado y futuro con el deseo de recuperar emociones, revivir momentos olvidados y adivinar cercanas aventuras. No es tarea sencilla confesar a viva voz los más íntimos pasajes de tu historia. Pero hoy afronta ante «Un Café con...» la valiente labor de reconstruir, capítulo a capítulo, la semblanza de un hombre de pocos silencios, firmes convicciones y espíritu luchador... Un rebelde incondicional.

Bastan unos instantes para que Eduard Zamora, director de Seguridad Corporativa de Banco Sabadell, reciba con confianza una batería de preguntas descolocadas y, sin darse cuenta, se «despoje» del protocolario traje de ejecutivo. Detrás se descubre a un hombre que, rebasadas tres décadas en el escenario de la seguridad, pública y privada, se declara «un enamorado del mundo de la seguridad». Y a las pruebas nos remitimos. Sus comienzos, en la Jefatura de la Policía Local de Sabadell donde realizó funciones de gestión interna. Años después, el empeño y voluntad por poner en práctica claros principios empresariales le llevaron al área de Seguridad de Banco Sabadell.

«Soy un enamorado del mundo de la seguridad»

Una carrera profesional que «culminó» –«trabajando duro y desde abajo», matiza– asumiendo la dirección de Seguridad de la entidad financiera.

Con una visión siempre optimista de la seguridad privada, Zamora, valiente en el discurso y directo en los mensajes, marca territorio lejos de evasivas o ambigüedades al manifestar que «en el sector debería haber menos regulación. Siempre he pedido que nos dejasen más libertad. ¡Ya nos preocuparemos nosotros de proteger la actividad que está en nuestras manos. Es nuestro objetivo y función!». Inagotable trabajador –ha sido durante 6 años el máximo responsable de la Asociación de Directivos de Seguridad Integral (AD-SI) y es el actual presidente de Security Forum–, solo aspira a ser recordado por un sector, «del que no me jubilaré nunca», como «alguien que se esforzó por mejorarlo y dignificar la figura del director de seguridad».

Por unos minutos retomamos esa mirada infantil que proyecta una vida que palpita a cada segundo. Imágenes de unos padres que abandonaron Sevilla con destino a Cataluña soñando con un futuro mejor o la de aquel chaval que con 14 años dejó los estudios para ponerse a trabajar porque «en casa hacía falta dinero para comer». Inteligente, carismático y cortés, durante la entrevista se descubre como un hombre cariñoso y un entrañable padre de familia. «La felicidad –matiza– es poder disfrutar de la familia. Cada momento de la vida es único y hay que aprender a valorarlo».

Avispado, irónico, y con un gran sentido del humor, se aísla del caótico ajeteo diario tomando el sol y escuchando música –«me gusta el flamenco, la música clásica, Leonard Cohen,...»– y es asiduo al gimnasio. Hombre de buen paladar –«como de todo, menos lo muy picante; si cocino yo, nada de sal ni azúcar», solo se decanta por gin-tonic en la sobremesa. Dice ser un tipo afortunado porque intenta ver el lado bueno de la vida sin negar la realidad. Hoy aprendimos con él que la actitud determina casi siempre el éxito. Él es un claro ejemplo de ello. ●



Congreso de Seguridad Privada
EUSKADI
 Segurtasun Pribatuko Batzarra

Seguridad: un trabajo de todos

Bilbao
 30 SEP 2015

Con el patrocinio de:



CUADERNOS DE SEGURIDAD

Peldaño



Compromiso



Soluciones



Calidad

Nuestras señas de identidad quedan latentes en la nueva imagen de la Compañía. Compromiso, soluciones y calidad. Una imagen renovada con un compromiso hacia nuestros clientes:

Crecemos para estar más cerca