CUADERNOS DE SEGURIDAD

Núm. 323 • JUNIO 2017 • 10 euros

PUNTOSEGURIDAD.com

Seguridad en entidades bancarias

Vigilancia por CCTV

II CONGRESO NACIONAL DE JEFES DE SEGURIDAD

Así fue la segunda edición

Dahua Solución Inte

Banca y

ATM

Evitar alto riesgo de robos, atracos e incursiones. Vigilancia integral. Grabación de videos

Mostrador

Gran volumen de transacciones en efectivo. Son necesarias imágenes faciales de alta definición y registro de transacciones para evitar peligros ocultos

Vestíbulo

Las grandes áreas con multitudes de personas requieren alta definición y sin puntos ciegos

CE FC UL RoHS ISO 9001:2000

DAHUA TECHNOLOGY IBERIA, S.L.
Juan Esplandiú 15-1B-28007 Madrid, SPAIN
Tel: +34 917649862
Fax: +34 917649862
E-mail: sales.iberia@global.dahuatech.com

egrada de Seguridad

Finanzas

Centro de Seguridad

Seguridad de datos. Estabilidad y fiabilidad del sistema. Amplio mecanismo de alarma

Video Wall

Plataforma de gestión de vídeo

Multi-lente Paronámica Cámara

Espacio Exterior

Entorno complicado. El rápido cambio de luz requieren alta definición, ultra gran angular y tecnología Starligh

Smart WDR IR Cámara

Entrada

Imagen facial nítida bajo la luz del sol, el reconocimiento VIP produce una buena sensación en los clientes

demes GROUP iPTECNO CCTV CENTER ADI GLOBAL DISTRIBUTION

Visualiza cada detalle de forma auténtica y natural

Cámara panorámica de 180°sin distorsión de imagen

Características

- Cámara con 3 ó 4 sensores en 1 y 1 dirección IP
- Tecnología de visualización con marcos ultra delgados para una presentación de imagen perfecta
- Angulo de visión de 180° sin distorsión de imagen
- Fácil montaje que evita trabajos de instalación y ahorran costes
- Todos los modelos se presentan con IP67 & IK 10, diseñados para uso exterior

H.265 | 180° Panoramic | TRACKING Smart Tracking | Starlight | WDR | IP67 | Vandal-proof

ISO 9001:2000

DAHUA TECHNOLOGY IBERIA, S.L.
Juan Esplandiú 15-1B-28007 Madrid, SPAIN
Tel: +34 917649862
Fax: +34 917649862
E-mail: sales.iberia@global.dahuatech.com

ENCUENTROS PROFESIONALES. NUEVA NORMATIVA

El sector se mueve...

En poco más de mes y medio el sector de la Seguridad ha tenido a su servicio plataformas de encuentro profesional donde establecer principios, estrategias y herramientas comunes con un único fin: asentar las bases de un futuro prometedor. Sobre el pilar de una nueva realidad normativa y tecnológica, Barcelona fue escenario el pasado mes de abril del II Congreso Nacional de Jefes de Seguridad. El encuentro, organizado por Peldaño –editora de esta revista– y la Asociación de Jefes de Seguridad de España, congregó a más de 150 profesionales, que convirtieron la jornada en un foro de debate y análisis, donde se abordaron los retos de futuro para estos profesionales de la Seguridad Privada ante los nuevos rumbos en el ámbito social, económico y legislativo.

El Congreso, que sirvió de tribuna para reiterar el papel fundamental que desempeña el Jefe de Seguridad como colaborador entre Seguridad Pública y Seguridad Privada, aglutinó un enriquecedor programa de ponencias y mesas de debate donde los asistentes –jefes de Seguridad, directores y responsables de Seguridad de entidades públicas y privadas, así como miembros de las Fuerzas y Cuerpos de Seguridad– pudieron conocer, compartir e intercambiar conocimiento y opiniones sobre la realidad más actual en cuanto a la industria de seguridad, tecnología y protección de datos, entre otros temas, y sobre los retos a los que tendrá que hacer frente el Jefe de Seguridad.

Y al cierre de esta edición otra plataforma de encuentro profesional, organizada por Peldaño, se clausuraba convirtiendo su quinta edición en la mejor de su historia. Así fue: Security Forum 2017 congregaba en dos días en Barcelona –17 y 18 de mayo– a 6.700 profesionales, 65 expositores y 350 congresistas, convirtiéndose en cita de referencia de primer nivel para el sector de la seguridad. Una quinta edición que se ha caracterizado por las oportunidades de negocio generadas y por la cualificación del público asistente, que pudo conocer en la zona comercial las últimas innovaciones tecnológicas en equipos y soluciones de seguridad, así como por la calidad de las ponencias y mesas de debate del Congreso Security Forum, donde se abordaron, bajo el protagonismo del ataque cibernético «wannacry», temas de absoluta actualidad como las nuevas guerras del siglo XXI, la Directiva NIS, la incidencia de la tecnología en la privacidad de las personas o el Reglamento de Seguridad Privada. El encuentro, del que se publicará una amplia crónica en el próximo número de Cuadernos de Seguridad, volvió a contar con un amplio respaldo institucional, así como de empresas, asociaciones del sector y Fuerzas y Cuerpos de Seguridad.

Y aún quedan unas líneas para otra buena noticia: el sector de la Protección contra Incendios está de enhorabuena. El Consejo de Ministro aprobó el pasado 19 de mayo el Reglamento de Instalaciones de Protección contra Incendios (RIPCI). Una normativa muy esperada y largamente demandada (las instalaciones de protección contra incendios se rigen actualmente por una normativa de 1993), que responda a la evolución, tanto de la técnica como del marco legislativo.

Lo dicho, el sector se mueve...¡por fin!

© denisismagilov

CUADERNOS DE SEGURIDAD

www.puntoseguridad.com

Nº 323 • JUNIO 2017

Peldaño

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

Presidente: Ignacio Rojas.
Gerente: Daniel R. Villarraso.
Director de Desarrollo de Negocio: Julio Ros.
Directora de Contenidos: Julia Benavides.
Directora de Marketing: Marta Hernández.
Director de Producción: Daniel R. del Castillo.
Director de TI: Raúl Alonso.
Jefa de Administración: Anabel Lobato.
Jefe del Dpto. de Producción: Miguel Fariñas.
Jefe del Dpto. de Diseño: Eneko Rojas.

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

Distribución y suscripciones:
Mar Sánchez y Laura López.
Horario: de 9,00 a 14,00 y de 15,00 a 18,00 horas)
Viernes: de 8,00 a 15,00 (suscripciones@epeldano.com)

Redacción, administración y publicidad
Avda. Manzanares, 196 - 28026 Madrid
Tel.: 91 476 80 00 - Fax: 91 476 60 57
Correo-e: cuadernosdeseguridad@epeldano.com

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

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

que ha derivado en la aparición de nuevos riesgos y amenazas, conocidos ya como ciberdelitos. Y ahora toca preguntarnos, ¿cómo ha cambiado la seguridad de las corporaciones bancarias en estos últimos años?

ENTREVISTAS:

— **Eduardo J. Álvarez Blázquez**. Security Director Spain. CSIS Spain Citibank.
— **Rafael Madrid García.** Director de Seguridad. Banco de Crédito Cooperativo-Grupo Cooperativo Cajamar.
— **Juan Manuel Zarco.** Director de Seguridad y Gestión del Efectivo. Bankia.
— **Francisco Guerrero.** Director de Seguridad. Unicaja Banco.
— La combinación ideal para la seguridad bancaria, por **Borja García-Albi Gil de Biedma.**
— Viviendo el futuro de la seguridad bancaria, por **Alfonso Mata**.
— Dahua lanza soluciones integradas de seguridad de vídeo para banca y finanzas, por **Dahua**.
— La banca invierte tres veces más en seguridad que el resto de entidades no financieras, por **Kaspersky y B2B**.
— Videovigilancia Inteligente, gana la banca y el cliente, por departamento técnico de **Hikvision**.

JULIO/AGOSTO 2017 - Nº 324

EN PORTADA

CRÓNICA SECURITY FORUM 2017

Security Forum se celebró el 17 y 18 de mayo en el Centro de Convenciones Internacional de Barcelona y, de nuevo, se convirtió en un auténtico escaparate para la exposición de las últimas innovaciones y tecnologías en equipos, productos y servicios, así como en espacio de conocimiento e intercambio de experiencias. Durante dos jornadas los profesionales –que en esta edición alcanzaron los 6.700- acudieron a la exposición y al Congreso Security –las sesiones contaron con la presencia de 350 asistentes-, bajo el tema central «Ver para Crear», donde reconocidos expertos compartieron con los congresistas su visión sobre los nuevos retos a los que se enfrenta la seguridad en la sociedad moderna. De todo esto, y de mucho más, CUADERNOS DE SEGURIDAD publicará en su próximo número una amplia crónica con toda la información de lo acontecido durante los días de duración del evento. Además, el lector podrá encontrar un extenso reportaje gráfico con las imágenes del encuentro que se ha convertido en el evento de referencia de 2017.

SEGURIDAD EN CENTROS COMERCIALES Y RETAIL

Los centros comerciales y grandes superficies se han convertido en un escenario habitual de nuestras ciudades y sus alrededores. ¿Quién no ha acudido alguna vez a una de estas singulares instalaciones y algunas únicas en diseño? Hoy en día son muchos los centros comerciales –no nos vamos a olvidar en este número del sector retail– que abren sus puertas en nuestro país, lugares que se han convertido en centros de visita para todos. En un mismo escenario se trata de conjugar oferta comercial, espectacular diseño, facilidad de accesos.

Se trata de un elemento que tiene y debe quedar integrado en el conjunto del edificio o instalación, pero siempre viendo las necesidades reales de cada centro. De nuevo, volvemos a destacar la figura del responsable de Seguridad, profesional en cuyas manos estará la conjunción de todos aquellos elementos para garantizar una satisfactoria seguridad para este tipo de instalaciones.

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
BAUSSA	97	946749099	www.baussa.com
BOSCH SECURITY SYSTEMS	109	902121497	www.boschsecurity.com/es/
BY DEMES GROUP	35,104	934254960	www.bydemes.com
CASMAR	66	933406408	www.casmar.es
CYRASA SEGURIDAD	49	902194749	www.cyrasa.com
DAHUA	Despl. Int. Cub, 2ª cub,58	917649862	www.dahuasecurity.com
DALLMEIER	47,82	915902287	www.dallmeier-electronic.com
DETNOV	107	933716025	www.detnov.com
DORLET	61,88,105	945298790	www.dorlet.com
DORMAKABA	23	917362480	www.dormakaba.com
FERRIMAX	91	934601696	www.ferrimax.com
FF VIDEOSISTEMAS	31	902998440	www.ffvideosistemas.com
FLIR SYSTEMS	67	31765794190	www.flir.com
FUJINON	13	4921150890	www.fujifilm.eu/fujinon
GENAKER	53	932422885	www.genaker.net
GRUPO IPTECNO	27	902502035	www.iptecno.com
HANWHA TECHWIN EUROPE	68	916517507	www.hanwha-security.eu
HIKVISION	4ª Cubierta, 9,20, 50,51	917371655	www.hikvision.com
HOMMAX	106	961594646	www.hommaxsistemas.com
III CONGRESO DE SEG. PRIV. EN EUSKADI	3ª Cubierta	914768000	www.congresoseguridadeuskadi.com
KASPERSKY	60	913983752	www.kaspersky.es
LSB	70,89	913294835	www.lsb.es
MOBOTIX	78,81,107	911115824	www.mobotix.com
PELCO BY SCHNEIDER ELECTRIC	64,65,101	911234206	www.pelco.com
PRODEXTEC	109	913316313	www.prodextec.es
RISCO GROUP	52	914902133	www.riscogroup.es
SAFIRE	57		www.safirecctv.com
SCATI	54	902116095	www.scati.com
SEGURIDAD INTEGRAL CANARIA	21	902226047	www.seguridadintegralcanaria.com
TECHCO SECURITY	73	913127777	www.techcosecurity.com
TYCO IF & S	102, 104	916313999	www.tyco.es
VISIOTECH	62	911836285	www.visiotechsecurity.com
VIVOTEK	108	886282455282	www.vivotek.com
WHITAN ASOCIADOS	92	965210307	www.whitanabogados.com

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

ÍNDICE DE ANUNCIANTES

EL ENCUENTRO PROFESIONAL SE CELEBRÓ EL 17 Y 18 DE MAYO EN EL CCIB DE BARCELONA

Security Forum celebra **la mejor edición** de su historia

Las empresas participantes han expresado su satisfacción por las oportunidades de negocio y por la cualificación del público asistente

Más de 6.700 profesionales de la seguridad, 65 expositores directos, más de 350 congresistas y una veintena de ponentes han desfilado este año por Security Forum para ver las novedades de la industria y debatir sobre los retos de la Seguridad. Dos jornadas que han servido para convertir a la quinta edición en la más exitosa de su trayectoria, y al evento como una cita de referencia de primer nivel para el sector de la seguridad al que da servicio. En la revista de julio publicaremos la crónica completa del evento.

PERO el éxito de la quinta edición no solo viene avalado por las cifras. Las empresas participantes en la zona comercial han expresado su satisfacción por las oportunidades de negocio generadas gracias al interés de compra y a la alta cualificación del público asistente –de primer ámbito de decisión–, que pudo conocer en la exposición las últimas soluciones en áreas como CCTV, control de accesos o tecnología IP o realidad virtual, entre otras.

Tal y como afirmó el **secretario de Estado de Seguridad, José Antonio Nieto,** en sus palabras de inauguración, «Security Forum es una ventana abierta de la industria y la tecnología aplicada a la seguridad». Asimismo, hizo hincapié en el papel que juega el evento para «servir de cauce de comunicación entre la industria de la seguridad y los clientes finales, tanto del sector público como del sector privado».

Y si el **área de exposición** ha resultado atractiva para las empresas, las ponencias y mesas redondas del **Congreso** Security Forum no lo han sido menos para quienes buscan estar al tanto de las últimas tendencias del sector, como las guerras del siglo XXI, la directiva NIS, el reglamento de Seguridad Privada o la incidencia de la tecnología en la privacidad de las personas. El gran protagonista de ambas jornadas ha sido el reciente ataque cibernético conocido como «wannacry», especialmente analizado en las intervenciones de los expertos participantes en el Ciberday, que ha contado con la presencia de destacados especialistas como el famoso «hacker» Deepak Daswani, entre otros.

Momento especial para el reconocimiento al potencial innovador del sector volvió a ser la ceremonia de entrega de los **premios Security Forum**, a la que asistió el **conseller del Departament d' Interior de la Generalitat de Catalunya, Jordi Jané.** En sus palabras a los asistentes, Jané destacó la importancia de la buena colaboración entre la seguridad pública y privada y su confianza en el futuro del sector.

El cierre final de la última jornada lo puso el **director general d' Administració de Seguretat de la Generalitat de Catalunya, Jordi Jardí**, quien destacó el papel de Security Forum como escenario donde se comparten ideas, visión empresarial y tecnología: «ese intercambio de inteligencia e información es la clave del futuro para evolucionar al mismo ritmo que la sociedad». También subrayó la relevancia del papel de la seguridad privada «al servicio de los ciudadanos» y la necesidad de apostar por políticas de «responsabilidad social corporativa» para mejorar el funcionamiento de las administraciones y actores involucrados en el sector de la seguridad privada.

Fotos: Xavi Gómez

HIKVISION

DARKFIGHTER LITE
¿POR QUÉ CONFORMARSE CON BLANCO Y NEGRO?

En la oscuridad, los colores se difuminan hasta acabar en grises, pero para una seguridad eficaz es necesario entender todos los detalles de cada situación. Con la tecnología Darkfighter, en una situación urbana con un artista del grafiti actuando, no solo se distinguirá su silueta, sino que lucirá con tanto color y detalle como su creación en la pared.
Por muy tenue que sea la iluminación u oscura la escena, ningún color se escapa a la mirada de las cámaras Darkfighter de Hikvision.

Hikvision Spain
C/ Almazara, 9
28760 Tres Cantos (Madrid)
T +34 91 7371655
info.es@hikvision.com

www.hikvision.com

EL ENCUENTRO SE CELEBRÓ EL PASADO 5 DE ABRIL EN BARCELONA

El Jefe de Seguridad, **pieza clave** del sector de la **Seguridad Privada**

Más de 150 profesionales avalan el éxito de un encuentro en el que se abordaron los nuevos retos a los que se enfrenta el Jefe de Seguridad ante una nueva realidad tecnológica y normativa

Más de 150 profesionales acudieron el pasado 5 de abril en Barcelona al II Congreso Nacional de Jefes de Seguridad, jornada que se convirtió en un foro de análisis y debate de la figura del Jefe de Seguridad. El encuentro, organizado por la Asociación de Jefes de Seguridad de España y Peldaño, abordó los retos y futuro de este profesional del sector de la seguridad privada ante una nueva realidad tecnológica y normativa.

EL acto de inauguración corrió a cargo de Jordí Jardí, director general d´Administració de Seguretat del Departament d´Interior de la Generalitat de Catalunya, quien destacó que la Seguridad Privada conforma uno de los elementos imprescindibles y puntal del estado de seguridad, al tiempo que hizo hincapié en la necesidad de trabajar conjuntamente con la Seguridad Pública. Jardí señaló la importancia de potenciar foros para compartir conocimiento y experiencia donde trabajar por una profesión «digna y más profesional».

Antonio Cedenilla, presidente de AJSE e Iván Rubio, director del Área de Seguridad de Peldaño, junto a Jordi Jardí, director general d´Administracio de Seguretat del Departament d´Interior de la Generalitat de Catalunya (en el centro), que inauguró el II Congreso Nacional de Jefes de Seguridad.

Previamente, Antonio Cedenilla, presidente de la Asociación Española de Jefes de Seguridad, señaló que el futuro del sector pasa por la tecnología y la formación que «nos dará una mayor cultura profesional», a la vez que matizó las aportaciones de la Seguridad Privada al bienestar y seguridad de la sociedad. Cedenilla agradeció el apoyo a patrocinadores y entidades, sin los cuales no hubiera sido posible la celebración de un encuentro que tiene como objetivo «aportar un granito de arena en la mejora del sector».

Por su parte Iván Rubio, director del Área de Seguridad de Peldaño, señaló que el II Congreso Nacional de Jefes de Seguridad se convertirá, una edición más, en un espacio de «encuentro sectorial en el que los Jefes de Seguridad serán los protagonistas», y contribuirá a potenciar su posicionamiento como «figura humanitaria del sector».

El congreso tuvo entre sus objetivos crear un punto de encuentro del sector de la Seguridad donde analizar de forma exhaustiva la figura del jefe de Seguridad y sus funciones, los nuevos retos tecnológicos y normativos a los

Vista general del II Congreso Nacional de Jefes de Seguridad.

Un momento de una de las Mesas de Debate.

que se enfrenta, y su papel como colaborador entre la Seguridad Pública y Privada.

El congreso contó además con la intervención del Conseller d´Interior de la Generalitat de Catalunya, Jordi Jané, quien explicó que una «sociedad sin seguridad no garantiza el estado del bienestar», en el que juega un papel fundamental el sector de la Seguridad Privada con el que existe una «sincera voluntad de colaborar y trabajar activamente para la seguridad en su conjunto». El conseller d´Interior de la Generalitat de Catalunya destacó el valor de los jefes de Seguridad, con una importante labor de conexión y colaboración con la Seguridad Pública que hay que intensificar.

Jordi Jané hizo referencia durante su intervención al Código de Buenas Prácticas de la Seguridad Privada aprobado por el Consejo de Seguridad Privada en Catalunya y que prima participar y dar carta de naturaleza a las herramientas necesarias para dar un mensaje de la actuación ética de las actividades de los profesionales de este sector.

Dirigido a Jefes de Seguridad, directores y responsables de la seguridad de entidades públicas y privadas, profesionales de empresas de seguridad, así como a miembros de las Fuerzas y Cuerpos de Seguridad, la jornada se desglosó en diferentes ponencias y mesas de debate en las que se abordaron, entre otros temas: «Presente y futuro de la industria de la seguridad, sus diferentes actividades»; «Los beneficios de la formación en prevención de riesgos laborales para el Jefe de Seguridad»; «La seguridad privada en otros países»; «Últimos avances en sistemas de gestión de vídeo desde el punto de vista del operador y jefe de Seguridad»; «Nuevas tecnologías aplicadas a seguridad»; «El nuevo reglamento general de protección de datos y su adaptación al sector de la seguridad»; o «La figura del Jefe de Seguridad en el entorno normativo actual y futuro: visión de la Administración».

Jordi Jané, conseller d´Interior de la Generalitat de Catalunya, durante su intervención en el Congreso.

Jordi Jardí, director general d´Administració de Seguretat del Departament d´Interior de la Generalitat de Catalunya, durante su discurso de inauguración.

Los coroneles Aledo (4º por la izqda) y Martínez, de la Guardia Civil, junto al comisario del CNP Manuel Yanguas y el subinspector Carles Castellano, Jefe de la Unidad de Seguridad Privada de Mossos d'Esquadra.

Los asistentes cambiaron impresiones sobre lo expuesto en el congreso durante el almuerzo.

El acto de clausura contó con la presencia del delegado del Gobierno en Cataluña, Josep Enric Millo, que comenzó su intervención destacando que la seguridad es la llave que «nos permite disfrutar de la libertad, así como el pilar en el que se asienta la comunidad de una sociedad», al tiempo que insistió en que «los derechos fundamentales no son posible sin seguridad». Tras matizar que España «es un país seguro», Enric Millo destacó los elementos que contribuyen a conseguir este logro: el excelente capital humano formado por la Fuerzas y Cuerpos de Seguridad, la excelente coordinación policial –«la seguridad debe quedar fuera –explicó– del debate político»-, así como los profesionales de la Seguridad Privada, «un sector puntero –indicó–, que proyecta marca España, y que complementa las funciones de los profesionales de la Seguridad Pública».

El delegado del Gobierno, quien hizo hincapié en que una de las máximas prioridades del ministro del Interior es el desarrollo reglamentario de la Ley de Seguridad Privada, alentó a trabajar conjuntamente Seguridad Pública y Seguridad Privada para hacer frente a los nuevos retos, ya que «nadie sobra cuando se trata de garantizar la seguridad de la ciudadanía». Y es que tal y como finalizó «Sin seguridad no hay libertad, derechos ni bienestar».

Para finalizar se procedió a la entrega de los II Premios AJSE a la Seguridad Privada, en las categorías de: Premio «Carrera Profesional»; Premio «Empresa Tecnológica»; Premio «Empresa Responsable»; y Premio AJSE de Honor.

Además se hizo entrega de una placa al Comisario Principal Esteban Gándara, Comisario Principa, por su especial implicación en la mejora del sector de la Seguridad Privada en España, durante su etapa al frente de la Unidad Central de Seguridad Privada.

El Congreso ha contado con el patrocinio de Genaker, Hikvision, P.S.A., Securitas Direct, Shoke-Magnum y Tyco Integrated Fire & Security. ●

Fotos: Xavi Gómez.

El General Gozalo, jefe de la VII Zona de la Guardia Civil de Cataluña (a la izq.), Comisario Anselmo Palma, 2º Jefe de la Brigada Provincial de Seguridad y Protección, y Andrés Sanz, Coronel Jefe del SEPROSE de la Guardia Civil (dcha).

Josep Enric Millo, delegado del Gobierno en Cataluña, que clausuró el encuentro profesional.

FUJIFILM
Value from Innovation

I

magina

una nueva

lente de telezoom

32x con 2 megapíxeles de

resolución para una excelente calidad FULL HD

para todo el rango de zoom e imagínala más y más y más pequeña

Please visit us at booth E630

IFSEC International
SECURING PEOPLE, PROPERTY & ASSETS
20-22 JUNE 2017 EXCEL LONDON UK

La nueva lente Fujinon para 1/1.8" y 2/3"

Day Night
Full HD 2MP

Con su tamaño compacto, imágenes FULL HD, formato de gran sensor, filtro de niebla incorporado y controles, las dos lentes zoom 32x encajan en varias carcasas y son versátiles para una amplia gama de aplicaciones de vigilancia incluso con poca luz y mal tiempo. Escanea para más información o visita www.fujifilm.eu/fujinon — **Fujinon. Para ver más. Para saber más.**

kremer agency

FUJINON

MESA DE DEBATE: «PRESENTE Y FUTURO DE LA INDUSTRIA DE LA SEGURIDAD, SUS DIFERENTES ACTIVIDADES»

Una clara apuesta por un **sector maduro y profesional**

Enrique París, presidente de APROSER Catalunya; Jordi Isern, coordinador de Formación de Tecnifuego-Aespi; Aleix Asna, representante de CAT Formació; Anna Aisa, gerente de ACAES; Jorge Salgueiro, asesor jurídico de ASEFOSP; y Jordi Ortega, asesor jurídico de AJSE.

EL reconocimiento de la seguridad privada como un sector profesional y maduro, fue uno de los objetivos que se plantearon durante el desarrollo de la mesa de debate «Presente y futuro de la industria de la seguridad, sus diferentes actividades», que se desarrolló en el marco del II Congreso Nacional de Jefes de Seguridad, y que fue moderada por Jordi Ortega, asesor jurídico de la AJSE.

Para Anna Aisa, gerente de la Asociación Catalana de Empresas de Seguridad, ACAES, las empresas del sector de la Seguridad Privada tienen que dar cumplimiento a múltiples normativas –Ley de Seguridad Privada, Protección de Datos, legislación de Seguridad Social, etc.-, que en muchas ocasiones no van a la par de las necesidades del sector. «Hoy en día existe diferentes velocidades entre las demandas y necesidades del sector y la normativa aplicable al mismo».

Por su parte Aleix Asna, representante de CAT Formaciò, señaló que el modelo de formación ha cambiado y los centros deben adaptarse a los nuevos requisitos que marca la nueva Ley de Seguridad Privada, entre los que se incluyen cambios en cuanto a las propias instalaciones de los centros, en donde «se han aumentado mucho las exigencias». «Hay ocasiones en que –matizó- es inviable para un centro de formación muchos de los requisitos que se les solicitan. Sería necesario flexibilizar algunos de éstos para que todo fuera más sencillo».

Vista general de la Mesa de Debate «Presente y futuro de la industria de la seguridad, sus diferentes actividades».

Enrique París, presidente de la Asociación Profesional de Compañías Privadas de Servicios de Seguridad, APROSER Catalunya, destacó que la Seguridad Privada es un sector tremendamente tradicional, donde las dos terceras partes de su facturación lo conforman los servicios tradicionales. «Nos encontramos con un sector poco propenso a la innovación».

En un entorno con nuevos retos y amenazas y donde la revolución digital es la protagonista, el sector se verá obligado a incorporar nuevas tecnologías y perfiles profesionales en sus empresas. «Profesionales que habrá que formar o reciclar a ese nuevo escenario digital», señaló París, quien también hizo hincapié en la necesidad del desarrollo reglamentario de la Ley de Seguridad Privada para conocer cómo se abordarán aspectos tan importantes como el intrusismo y los nuevos servicios.

Jordi Isern, coordinador de Formación de Tecnifuego-Aespi, destacó que en el año 2015 se produjeron más de 42.000 incendios en España,

Aleix Asna, representante de CAT Formaciò, y Anna Aisa, gerente de ACAES.

Jordi Isern, coordinador de Formación de Tecnifuego-Aespi.

Jordi Ortega, asesor jurídico de AJSE, y moderador de la mesa de debate (izq.), junto a Enrique París, presidente de APROSER Catalunya.

que ocasionaron pérdidas millonarias, así como el cierre de empresas y la pérdida de empleos. «La protección contra incendios es uno de los elementos fundamentales de la seguridad», apuntó.

El ponente hizo referencia a la necesidad de garantizar el buen mantenimiento de las instalaciones de protección contra incendios para garantizar la seguridad, y es ahí donde los «Jefes de Seguridad tiene una gran responsabilidad de velar por el buen mantenimiento de sus instalaciones».

Por su parte, Jorge Salgueiro, asesor jurídico de ASEFOSP, comenzó su intervención haciendo una valoración sobre el estado del sector donde destacó, principalmente, el fuerte impacto que había tenido la crisis económica en los centros de formación, así como que actualmente existe una confusión del papel de los centros acreditados de seguridad privada respecto a las vías formativas del artículo 29 de Ley de Seguridad Privada.

Salguerio hizo referencia también a los requisitos exigidos a los centros de formación tanto antes de su apertura como durante su funcionamiento recogidos en el artículo 29.4 de la LSP.: acreditación del derecho de uso del inmueble en donde se ejerce la actividad de formación -propiedad o arrendamiento-; licencia municipal de actividad; instalaciones adecuadas al cumplimiento de sus fines -«aquí se aplicarían alguna de las medidas del artículo 52 de la Ley de Seguridad Privada, sustituyendo las establecidas en la orden 318/2011 de 1 de febrero sobre el personal de seguridad privada», explicó.

Para finalizar el ponente planteó algunas de las propuestas de ASEFOSP ante el Reglamento de Seguridad Privada como la existencia de una tarjeta de identificación profesional única para los profesores de los centros de formación, o la unificación a nivel normativo de los requisitos generales y específicos exigidos a los centros de formación para su apertura y funcionamiento cuando se imparta formación de personal de Seguridad Privada (Ministerio del Interior y Empleo).

Durante la mesa de debate se abordaron también aspectos relacionados con situaciones de intrusismo y competencia desleal -«uno de los grandes problemas a los que tiene que hacer frente el sector», apuntó Anna Aisa-, o la problemática de algunos concursos públicos, donde algunos de los participantes destacaron que lo que «se favorece es el precio y no la calidad».

Para finalizar, Jordi Ortega, enumeró algunas de las conclusiones resultado del análisis y debate desarrollado: adaptación del sector a las nuevas amenazas, así como a nuevos perfiles profesionales; un nuevo modelo de contrato; el reconocimiento del sector de la seguridad privada como un sector profesional y maduro; o la necesidad de articular los mecanismos apropiados para contar con profesionales adecuadamente formados a las necesidades de las empresas. ●

Texto: Gemma G. Juanes
Fotos: Xavi Gómez.

Anna Aisa, gerente de ACAES.

Enrique París, presidente de APROSER Catalunya, durante su intervención.

Jorge Salgueiro, asesor jurídico de ASEFOSP.

MÓNICA ROMÁN. VOCAL DE LA JUNTA DIRECTIVA DE AJSE. DIRECTORA Y JEFA DE SEGURIDAD. TÉCNICA SUPERIOR EN PRL.

La formación en **PRL**, fundamental para el **Jefe de Seguridad**

Conferencia sobre «Beneficios de la formación en Prevención de Riesgos Laborales a los Jefes de Seguridad»

BAJO el título «Beneficios de la formación en Prevención de Riesgos Laborales a los Jefes de Seguridad», Mónica Román, vocal de la Junta Directiva de la Asociación de Jefes de Seguridad de España, directora y jefa de Seguridad, así como Técnico Superior en Prevención de Riesgos Laborales, comenzó su intervención, en el marco del II Congreso Nacional de Jefes de Seguridad, señalando que siempre hay que buscar la proactividad dentro de las empresas y «siempre hay que ir un paso por delante».

En este sentido, la ponente explicó el proceso mental en el cumplimiento de las normas, abordando aspectos de no querer: intencionalidad; no poder: incapacidad; no conocer: ignorancia. Y es que, tal y como matizó, el cambio de conducta es «fundamental para conseguir tener una conducta segura».

Por otro lado, Mónica Román abordó la trilogía percepción-riesgo-confianza, donde destacó la importancia de adoptar nuevas costumbres que aportan confianza, y dejar atrás viejos hábitos. De manera muy visual durante toda la intervención, la ponente explicó que hoy en día «no podemos cambiar a la condición humana, pero sí las condiciones en las cuáles trabajan los seres humanos». Existe una línea de confluencia de factores, como pueden ser, entre otros, la comunicación deficiente, formación inadecuada, falta de supervisión, técnica inapropiada,... que derivan de un riesgo a un evento adverso. Ante ello hizo hincapié en que no es «saber quién se equivocó, sino cómo y por qué falló la defensa del sistema». Por eso, precisó, es fundamental contar «con una formación adecuada, rápida y realmente adaptada a lo que necesitamos».

Una formación que tenga entre sus ejes fundamentales la motivación –transmisión de conocimientos y beneficios–. Una formación necesaria para comprender: usabilidades, compatibilidades, aplicaciones y normalización de actividades, que ayudan a tener una visión 360º entre accesos y evacuaciones. Para finalizar, Mónica Román señaló que «el precio de la educación se paga una vez, el precio de la ignorancia se paga toda la vida». ●

Fotos: Xavi Gómez

IGNACIO CARRASCO. SECRETARIO GENERAL DE CLOUD COMMUNITY EUROPE

El **jefe de seguridad** tiene un papel clave para proteger la **estructura computacional de las empresas**

Conferencia «Nuevas tecnologías aplicadas a la seguridad»

TRATAR de proteger la estructura informática de las empresas es una de las funciones que forman parte de la actividad de los Jefes de Seguridad. Se trata, no obstante, de un tema de creciente complejidad debido a que va asociado a un aumento exponencial en la conectividad y en el número de accesos a internet de dispositivos y usuarios.

«Este creciente uso de Internet conlleva la aparición de múltiples peligros para las empresas y los usuarios», afirmó Carrasco. Para contextualizar esta afirmación hizo un recorrido histórico de la evolución de la red de redes para concluir que «cuando se diseñaron muchos de los elementos tecnológicos que sustentan Internet no se pensaba que fueran a tener que soportar volúmenes de datos y número de usuarios como los que se dan actualmente».

En su opinión «El creciente uso de internet está llegando a una medida exponencial y los peligros de Internet son muchísimos». No obstante, explicó Carrasco, «existen alternativas para la ciberseguridad, que pasan por el análisis de riesgos, la implantación de estrategias de protección y la toma de soluciones». Actualmente se está tratando de que haya un uso adecuado de la información y no, como ocurre en muchas ocasiones, un uso perverso de la misma.

Hay una serie de avances tecnológicos que se constituyen como elementos clave para la seguridad y sobre los que el Jefe de Seguridad debe estar informado y alerta:

- El desarrollo de las analíticas de vídeo relacionadas con el reconocimiento facial. Este desarrollo está abaratando los dispositivos de análisis de imágenes lo que, a su vez, está provocando una popularización de su uso y una extensión de su aplicación a múltiples sectores de actividad.
- El crecimiento del uso de las Redes Sociales está permitiendo detectar muchas actividades no muy «legales», que se producen a partir de usos perversos de la información y las propias Redes Sociales.
- Finalmente, el ponente identificó algunas claves asociadas al crecimiento exponencial de la conectividad global: la aparición de nuevos dispositivos que funcionan en red (el Internet of Things, IoT); las nuevas posibilidades de análisis derivadas del uso del Big data y el crecimiento del Cloud como plataforma de computación.

Posteriormente planteó la pregunta: ¿Qué va a ocurrir con los avances tecnológicos en relación a la industria de la Seguridad? Como respuesta inicial y pensando en el futuro más inmediato habló de la importancia de las certificaciones, y dio un repaso a los artículos de la Ley de Seguridad Privada en los que se hace referencia a las TIC. Ya en la exposición de motivos, la Ley 5/2014 dice que «La integración de los sistemas de seguridad debe contemplar el avance tecnológico».

A modo de conclusión, Carrasco invitó al uso de las Tecnologías de la Información: «Las TIC no son una amenaza, apóyense en ellas y asegúrense que la suya es una empresa bien capacitada para un uso adecuado de las mismas». ●

Texto: Mario Gutiérrez
Fotos: Xavi Gómez

MESA DE DEBATE «LA SEGURIDAD PRIVADA EN OTROS PAÍSES»

«Aún queda **un largo camino** en el plano internacional para los **Jefes de Seguridad»**

Javier Ruiz, vocal de Calidad de AJSE y experto en seguridad en países del Magreb; Carmelo Hernando, vicepresidente de International Security Chiefs Association (ISCA) en países árabes; José Meneses, director de Seguridad Makro Cash & Carry Portugal; Tony Arroyo, vicepresidente de ISCA en Francia; y Aitor Agea, vocal de la Junta Directiva de AJSE y presidente de ACC.

EN nuestro país las funciones del Jefe de Seguridad aparecen descritas en el artículo 35 de la Ley 5/2014 de Seguridad Privada. Sin embargo, ¿cómo está regulada esta figura en otros países? Conocer la situación del Jefe de Seguridad en países de nuestro entorno fue el objetivo principal de esta mesa de debate moderada por Javier Ruiz, vocal de calidad de AJSE y experto en seguridad en países del Magreb.

En primer lugar, Carmelo Hernando dio unas pinceladas de la situación del Jefe de Seguridad en los Emiratos Árabes. «En este país es una figura que no existe como tal, sino que sus funciones están englobadas en las del director de Seguridad, un cargo de gran relevancia y cuyas actividades se desarrollan en estrecha colaboración con las Fuerzas y Cuerpos de Seguridad del Estado». Entre los requisitos que deben cumplir las empresas de seguridad en Emiratos Árabes destaca la necesidad de contar con una delegación física en cada uno de los Emiratos en los que quiera operar, y entre las obligaciones de los directores de Seguridad está la de informar diariamente de cada incidencia a las Fuerzas y Cuerpos de Seguridad del Estado.

Es un país con leyes muy estrictas y con cierto nivel de proteccionismo frente a lo exterior, por lo que es necesario contar con un socio local a la hora de constituir una empresa de seguridad. También se precisan licencias específicas para cada una de las actividades que la empresa de seguridad desee desarrollar localmente. Además de reportar a la policía de las incidencias y de los resultados de las investigaciones, el director de Seguridad es el máximo responsable sobre el nivel de calidad de los servicios que se ofrecen a clientes y gobiernos.

Recientemente se ha actualizado la Ley de Seguridad Privada y entre sus no-

Vista general de la Mesa de Debate.

Javier Ruiz, vocal de Calidad de AJSE y experto en seguridad en países del Magreb, que moderó la mesa.

vedades está la actualización de los salarios de los vigilantes, que como comentó Hernando suelen ser profesionales con poca formación y que suelen proceder de países de Oriente Medio y de la India. «Se trata de un país con mucho nivel de control y muy estricto en el cumplimiento de las regulaciones. Se podría pensar que es casi una dictadura pero es muy seguro y tiene uno de los índices de criminalidad más bajos del mundo».

En segundo lugar participó José Antonio Meneses, que informó que en Portugal la Ley de Seguridad Privada existe desde 1986 y que se desarrolló para «controlar un sector que hasta entonces no estaba regulado». En opinión de Meneses «en Portugal el legislador no entiende de seguridad privada» y por eso se puede contratar a la Policía para que lleve a cabo servicios de seguridad privada. «Es el único país de la UE en el que ocurre esto. Es a la vez regulador y tiene competencias en esta materia, y sólo pone limitaciones pero no vela por el sector de la seguridad privada.»

En Portugal, la figura del Jefe de Seguridad tampoco existe como tal, siendo lo más parecido la figura del coordinador de seguridad, que sólo existe para eventos deportivos. El país vecino se encuentra en fase de renovación de su regulación sobre Seguridad Privada y, como parte del proceso regulador, los directores de Seguridad ya han hecho sus aportaciones. «Estamos a la espera de ver cómo queda conformada esta nueva ley».

Tony Arroyo expuso la situación de los Jefes de Seguridad en Francia. Explicó que «la seguridad privada surgió en Francia para complementar las actividades de las Fuerzas y Cuerpos de Seguridad del Estado. En este país los representantes de la Seguridad Privada están armados y hubo algún comportamiento inesperado, por lo que la primera Ley fue de tipo "moral" y se promulgó en 1983, aunque no contemplaba la profesionalización del sector.»

José Meneses, director de Seguridad Makro Cash and Carry Portugal.

Carmelo Hernando, vicepresidente de International Security Chief Association (ISCA) en países árabes

Tony Arroyo, vicepresidente de ISCA en Francia.

Aitor Agea, vocal de la Junta Directiva de AJSE y presidente de ACC.

Las leyes en el país galo han ido evolucionando pero no hay, como en España, una Ley concreta para la Seguridad Privada. En opinión del ponente: «El Estado no ha sido capaz de regular adecuadamente, y hasta ahora no había ninguna intención de formalizar la actividad de las empresas de este sector». Aunque existe formación universitaria en materia de seguridad, no tiene su reflejo en la regulación actual. Existe una nueva dinámica en el mercado que exige llegar a una complementariedad de la Seguridad Privada y la actividad de las Fuerzas y Cuerpos de Seguridad nacionales. Sin embargo en opinión del ponente «la actividad de la Seguridad Privada no está bien definida todavía y las figuras de los diferentes actores se están modificando».

También en Francia se está trabajando en una nueva Ley de Seguridad Privada, aunque aún se está en una fase inicial y no está redactada. Arroyo espera «que la nueva Ley contemple y diferencie lo que es Seguridad Pública, Seguridad Privada y Seguridad Civil».

Finalmente Aitor Agea, vocal de la Junta Directiva de AJSE comentó sus experiencias internacionales en relación a la seguridad en el transporte aéreo de mercancías, quien añadió que «en otros países el concepto seguridad incluye los aspectos que los angloparlantes denominan "safety" y también "security". La concepción de la seguridad en otros países es diferente por lo que es necesario armonizar las legislaciones nacionales y las internacionales».

Agea comentó su experiencia en países como Colombia y Estados Unidos y afirmó que «los países que han sufrido más inseguridad son los que más han avanzado en las regulaciones» y puso también como ejemplo el caso de Israel. «No todas las democracias son homologables a la nuestra y en algunos países se aprecian regulaciones de corte más dictatorial ya que el concepto de seguridad varía mucho dependiendo de cada país», concluyó. ●

Texto: Mario Gutiérrez
Fotos: Xavi Gómez

ROBERTO OTERO. DIRECTOR TÉCNICO DE HIKVISION SPAIN

Tecnología punta en la **gestión de vídeo**

Conferencia sobre «Últimos avances en sistemas de gestión de vídeo»

TRES fueron los temas que Roberto Otero, director técnico de Hikvision Spain, abordó, bajo el título «Últimos avances en sistemas de gestión de vídeo», en su intervención en el II Congreso Nacional de Jefes de Seguridad celebrado en Barcelona. La conferencia se desglosó en Analíticas de Vídeo: Deep Learning; Imagen: cámaras multisensor; y Compresión: algoritmos inteligentes.

El análisis del Deep Learning fue el punto de partida de una conferencia, donde el ponente abordó también aspectos relacionados con la Inteligencia Artificial –«es la tecnología más elemental, ya que responde siempre igual ante los mismos parámetros», explicó-; Machine Learning –«es capaz de autoaprender y corregir errores», apuntó-; para, acto seguido, incidir en el Deep Learning, del que explicó que es «capaz de tomar decisiones en base a los datos» y es «la más compleja de las tres».

De manera práctica planteó la aplicación de las tres tecnologías a la hora de la identificación de la marca y modelos de vehículos que circulan por una calle, y explicó que un sistema de Inteligencia Artificial identificará los coches por su «aproximación» a los datos que conoce, pero no siempre acertará, ya que hay coches con características similares, mientras que un sistema de Machine Learning puede «aprender» de los datos y clasificar con mayor precisión los vehículos. Acto seguido hizo hincapié que un sistema de Deep Learning puede «entrenarse» sobre los datos que va recibiendo. «Emplea los datos que conoce para tomar decisiones sobre datos nuevos; puede emplear un diferenciador erróneo y equivocarse una vez, pero a la siguiente empleará otro para acercarse cada vez al resultado correcto». En definitiva, ¿qué ofrece el Deep Learning?: más información; más aplicaciones; y mayor precisión en aplicaciones como la detección de comportamientos, el conteo de personas 3D, funciones de extracción.

Roberto Otero hizo referencia también durante su intervención a las cámaras multisensor, equipos con doble sensor: uno para imágenes IR que garantiza el brillo de la imagen, y otro para la luz visible que garantiza el color. «Después combina las dos imágenes formadas por los diferentes espectros –señaló- en una sola imagen a todo color».

Para finalizar abordó los algoritmos de compresión –H.264 y H.265– destacando que hoy en día fabricantes de CCTV, como es el caso de Hikvision, invierten recursos para desarrollar algoritmos de compresión más inteligentes que mejoren aún más la tecnología de compresión, como se trata de la compresión H.265+ que ofrece «resolución de ancho de banda y ahorro en almacenamiento». ●

Texto: Gemma G. Juanes
Fotos: Xavi Gómez

SEGURIDAD

SEGURIDAD INTEGRAL CANARIA SA

Líderes en **Seguridad**

Seguridad Integral Canaria, tras 20 años de existencia, es una referencia indiscutible en la vigilancia y protección de bienes e instalaciones, además de representar la apuesta más segura para el transporte de fondos y valores. Inició hace una década su expansión a la Península con una creciente presencia paralela a su prestigio, tanto por la alta cualificación de su personal como la constante incorporación de sistemas de vanguardia, lo que garantiza servicios de protección eficaces adaptados a las necesidades y capacidad de los clientes. Cuenta con los principales certificados de calidad y acreditaciones técnicas.

ISO 9001 · ISO 14001 · OHSAS 18001

T 902 226 047

www.seguridadintegralcanaria.com

RAMÓN ARNÓ. ABOGADO. EXPERTO EN PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN.

«La **privacidad** se venderá como valor añadido»

Conferencia sobre «El nuevo Reglamento General de Protección de Datos (GDPR) y su adaptación al sector de la seguridad»

RAMÓN Arnó centró su ponencia en los elementos del nuevo Reglamento General de Protección de Datos (GDPR) de la UE relacionados con la actividad de los Jefes de Seguridad. Arnó comentó que «aunque hasta mayo de 2018 la nueva Ley no entrará en vigor, las grandes empresas ya están poniendo medidas en sus sistemas de información para adaptarlos a esta nueva Ley. Antes de final de año habrá una nueva LOPD», y la Agencia Española de Protección de Datos (AEPD) está poniendo al servicio de las empresas una serie de herramientas y recomendaciones para facilitar la adecuación de las actividades de las empresas españolas a la nueva regulación europea.

El nuevo Reglamento es una normativa larga, formada por 173 considerandos y 99 artículos, y es compleja, por lo que se está muy pendiente de la transposición que se pueda hacer desde las instituciones españolas en la nueva versión de la actual Ley Orgánica de Protección de Datos.

Algunos de los aspectos de esta ley que son novedad y/o afectan especialmente a la función de los Jefes de Seguridad son: En relación al concepto de dato de carácter personal, Arnó comentó la viabilidad del uso de datos pseudo-anonimizados. También habló de los datos biométricos y dactiloscópicos, que están contemplados como categoría de datos especialmente sensibles y protegidos cuando permitan la identificación o autentificación de una persona. «Las evaluaciones de impacto estarán a la orden del día ya que antes del tratamiento de datos habrá que hacer una evaluación de impacto sobre los datos personales».

Respecto a los principios de la protección de datos informó que la nueva Ley cambia el paradigma, ya que «hasta ahora había que configurar las opciones que afectan a la privacidad y con GDPR, al ir la privacidad desde el diseño y por defecto, ésta se constituirá como un elemento imprescindible». También son novedad la creación de figuras con responsabilidad en el tratamiento de datos, como el delegado de Protección de Datos, imprescindible en las Administraciones Públicas y en algunas empresas, y que será responsable de asesorar a los responsables de los tratamientos de datos, supervisará el cumplimiento de la normativa y cooperará con las autoridades de control.

Finalmente y en relación a los derechos de los afectados por el tratamiento de datos, Arnó comentó que «GDPR crea la figura del Derecho al Olvido, exige el consentimiento expreso de cada persona en la cesión de datos, frente al consentimiento tácito o presunto que existía hasta ahora, y define las características y procedimientos específicos para llevar a cabo acciones de portabilidad de datos entre empresas de tratamiento».

Arnó concluyó su ponencia realizando un repaso de los artículos de la actual Ley de Seguridad Privada afectados de alguna manera por el nuevo Reglamento General de Protección de Datos de la Unión Europea.

Ramón Arnó, abogado y experto en Protección de Datos y Seguridad de la Información (izq.), durante su intervención,junto a Jordi Ortega, asesor jurídico de AJSE.

Fotos: Xavi Gómez

Texto: Mario Gutiérrez

Control de acceso inteligente

Innovación tecnológica y diseño para su oficina bancaria

PRODUCTOS TOTALMENTE INTEGRADOS

Seguridad con la tecnología más avanzada del mercado

dormakaba, con presencia en más de 130 países, es el socio de confianza que ofrece soluciones innovadoras de control de acceso.

Con nuestra experiencia, le podemos asesorar sobre cómo gestionar sus accesos.

Ofrecemos soluciones a medida, integrando cualquier tipo de sistema mecánico, soluciones de control de acceso autónomo, sistemas online o cerraduras de cajas fuertes.

Para más información, póngase en contacto con nosotros.

dormakaba

MESA DE DEBATE: «LA FIGURA DEL JEFE DE SEGURIDAD EN EL ENTORNO NORMATIVO ACTUAL Y FUTURO: VISIÓN DE LA ADMINISTRACIÓN»

«Podéis estar **orgullosos** de vuestra **profesión. La Ley** os otorga **funciones muy importantes»**

Manuel Yanguas. Jefe de la Brigada Central de Empresas y Personal. Unidad Central de Seguridad Privada del CNP; Manuel Luna. Intervención Central de Armas y Explosivos. Guardia Civil.; Carles Castellano. Cap de la Unitat Central de Seguretat Privada. Mossos d'Esquadra; Francisco Llaneza. Jefe de la Unidad de Seguridad Privada de la Ertzaintza; y Jorge Salgueiro, Vicepresidente jurídico de AJSE y presidente de AECRA.

EN la ronda de presentación inicial los representantes de Mossos d'Esquadra, Carles Castellano, y de la Ertzaintza, Francisco Llaneza, realizaron un resumen estadístico aportando datos actualizados respecto al número de vigilantes, jefes de seguridad, empresas de seguridad privada, informes, inspecciones, número de servicios, etc. desarrollados durante el último año en sus respectivas comunidades autónomas. A continuación el Comisario Yanguas comentó el tema del formulario consensuado con ICAE para la validación provisional de sistemas de seguridad e informó de que «por su novedad, al inicio, no fue bien interpretado y fue necesario explicar y reforzar la informa-

Vista general de la mesa de debate, que fue moderada por Jorge Salgueiro, Vicepresidente jurídico de AJSE y presidente de AECRA.

ción relativa al uso que se esperaba le dieran los jefes de seguridad, ya que es una herramienta que se ha puesto a su disposición y han de aprovecharla».

Manuel Luna explicó la función de la Intervención Central de Armas y Explosivos en lo relacionado con la Seguridad Privada y comentó que su misión específica, tal y como indica la normativa, «es planificar, organizar, inspeccionar y controlar las actividades encaminadas al ejercicio de las competencias que sobre armas y explosivos, artículos pirotécnicos y cartuchería que están encomendadas a la Guardia Civil en todo el territorio nacional». En relación al tema de la validación provisional comentó que han recibido quejas de que tardan mucho en la tramitación, sin embargo, «hay que aplicar medidas correctoras que tienen sus procedimientos y llevan su tiempo». En este sentido, «hay que hablar más con el sector y aumentar el nivel de contacto para evitar quebrantos. Y hay que realizar más labores pedagógicas para dar a conocer los criterios que usa la Guardia Civil a la hora de valorar y validar los sistemas de seguridad».

Los participantes en la mesa destacaron de manera unánime la importancia de la formación continuada para los Jefes de Seguridad, que «es responsabilidad de las empresas y debemos hacer lo posible para asegurarnos que todos los trabajadores del sector de la Seguridad Privada la reciben y de forma continuada, especialmente los Jefes de Seguridad». En relación a otras de las quejas que hay el sector se trató el tema del intrusismo sobre el que se comentó «lo más habitual es sustituir a un vigilante de seguridad con un auxiliar, y esta es una situación que hay que denunciar. Las denuncias hasta ahora llegan más vía sindicatos e inspecciones que por las propias asociaciones y las empresas del sector de la Seguridad Privada».

Carles Castellano. Cap de la Unitat Central de Seguretat Privada. Mossos d'Esquadra.

Manuel Luna. Intervención Central de Armas y Explosivos. Guardia Civil.

Manuel Yanguas. Jefe de la Brigada Central de Empresas y Personal. Unidad Central de Seguridad Privada del Cuerpo Nacional de Policía.

Francisco Llaneza. Jefe de la Unidad de Seguridad Privada de la Ertzaintza.

Posteriormente Jorge Salgueiro preguntó acerca de la posibilidad de que el Jefe de Seguridad pudiera ofrecer otros servicios de Seguridad Privada en el nuevo reglamento y el Comisario Yanguas comentó que «podéis estar esperanzados, ya que puede que el nuevo reglamento incorpore novedades en este sentido».

A modo de conclusiones los ponentes aplaudieron las iniciativas de la Administración Pública que buscan acercar las Fuerzas y Cuerpos de Seguridad del Estado al sector de la Seguridad Privada, «ya que cada vez es más necesaria la colaboración».

También resaltaron que es preciso «continuar en la línea y aumentar el trabajo de concienciación sobre seguridad global ya que es fundamental la suma de seguridades (pública + privada). Para ello la formación, la comunicación, la colaboración y la coordinación entre empresas y fuerzas de seguridad del estado son pilares fundamentales». Comentaron que «es recomendable además aumentar el nivel de confianza entre las empresas y el sector de la Seguridad Privada y los Cuerpos y Fuerzas de Seguridad pública, con el objetivo de aumentar el nivel mutuo de confianza. Todo ello redundará en un mayor conocimiento de todos los actores intervinientes y en una mejor coordinación entre todos nosotros».

Además consideraron que sería positivo promover la creación de Códigos Deontológicos y de buenas prácticas, para establecer directrices y líneas de actuación en situaciones concretas y áreas específicas. Citaron como ejemplo a seguir el caso de la nueva Ley Europea de Protección de Datos (GDPR) sobre la que se está preparando un código de conducta. ●

Fotos: Xavi Gómez

Texto: Mario Gutiérrez.

II CONGRESO NACIONAL DE JEFES DE SEGURIDAD

II CONGRESO NACIONAL DE JEFES DE SEGURIDAD

II Premios de la **Asociación de Jefes de Seguridad de España**

En el marco del II Congreso Nacional de Jefes de Seguridad celebrado en Barcelona se procedió a la entrega de los II Premios de la Asociación de Jefes de Seguridad de España a la labor de profesionales, empresas y entidades en pro del sector

Fotos: Xavi Gómez

«Premio AJSE de Honor». Joan Miquel Capell, Director de Seguridad de la Diputación de Barcelona, galardón que fue entregado por el delegado del Gobierno en Catalunya, Josep Enric Millo.

La Asociación de Jefes de Seguridad de España entregó un Premio Especial a Esteban Gándara Trueba, Comisario Principal. Jefe de la Unidad Central de Seguridad Privada, cargo que ocupaba en ese momento, por su especial implicación en la mejora del sector de la seguridad privada.

«Premio Carrera Profesional». Andrés Martín Ludeña, Security Director de Euronet, quien recogió el premio de manos del Delegado del Gobierno en Catalunya, Josep Enric Millo.

«Premio Empresa Responsable». Antonio Molina, Director de Seguridad del Consorcio Zona Franca, quien recogió el premio de mano del delegado del Gobierno en Catalunya, Josep Enric Millo.

«Premio Empresa Tecnológica»: Javier Mirallas, de la empresa ICS Internacional. El premio fue recogido por Enrique París, presidente de APROSER Catalunya, de mano de Josep Enric Millo, delegado del Gobierno en Catalunya.

CÓMO HACER QUE SU SISTEMA DE SEGURIDAD SEA MÁS SEGURO

JOAN BALAGUER
DIRECTOR COMERCIAL GRUPO IPTECNO

Actualmente la palabra ciberseguridad ha dejado de ser una palabra de moda para ser un problema real para todos aquellos dispositivos que estén conectados a internet. La videovigilancia no es inmune a un posible ciberataque, pero aplicando una serie de medidas de protección y cambiando la configuración de los dispositivos conseguirá minimizar la posibilidad de sufrir un ciberataque. A continuación le proponemos una lista de cambios y configuraciones para hacer que su sistema sea más seguro y menos propicio a sufrir un posible ciberataque.

1. Actualice el firmware de manera regular

Mantenga su grabador NVR, DVR y cámara IP constantemente actualizado con las últimas versiones de firmwares disponibles por sus respectivos fabricantes; seguramente estas actualizaciones ya incluyan mejoras y parches que protejan de este tipo de ataques.

2. Cambie la contraseña original y utilice contraseñas más seguras

Esta información no debería ser de dominio público, pero una de los principales motivos por los que un sistema puede ser "hackeado" es porque no se le han cambiado las contraseñas originales que facilita el fabricante. Cualquier fabricante recomienda no utilizar nunca las contraseñas originales una vez instalado el dispositivo y escoger una contraseña lo más segura posible. Se considera una contraseña segura aquella que al menos dispone de 8 caracteres y usa una combinación de símbolos, números y letras mayúsculas y minúsculas.

3. Cambie la contraseña regularmente

Cambie de manera regular la contraseña de sus dispositivos, de este modo se asegurará que solo podrán acceder aquellas personas que conozcan la contraseña y puedan acceder de manera autorizada al sistema.

4. Desactive los servicios de conexión que no utilice

El sistema UPNP intenta establecer una serie de puertos por defecto entre el grabador y el router, que quedan abiertos directamente en el mismo. Normalmente esto debería ser un sistema rápido y sencillo para instalar los dispositivos,pero si se mantienen las contraseñas originales, puede recibir un ataque o tener la visita de un visitante inesperado.

- Si asigna y abre manualmente los puertos HTTP y TCP en el router, debería desactivar esta opción para hacer su Sistema más seguro.
- Si no va a utilizar la conexión por P2P, desactive siempre esta función.
- Desactive la opción SNMP en su dispositivo si no la utiliza, use esta opción sólo de manera puntual y actívela solo cuando tenga que hacer una prueba o rastreo del sistema.

La opción de Multicast se utiliza para compartir el stream de video entre un grupo de dispositivos dentro de una red. Actualmente no hay ningún ciberataque reconocido a través del MULTICAST, pero recomendamos que si no se usa lo desactive.

5. Active la conexión HTTPS/ SSL

Configure una conexión HTTPS en su dispositivo y cree un certificado SSL. Esto encriptará todas las comunicaciones entre las cámaras y grabadores.

6. Cambie la contraseña del ONVIF

Hay cámaras IP antiguas que solo disponen de protocolo de comunicación ONVIF y con las versiones antiguas de ONVIF no se podía cambiar la contraseña. Para este tipo de cámaras necesitará actualizar el firmware a la última versión disponible por el fabricante para actualizar la versión del ONVIF y poder cambiar la contraseña.

7. Habilite el Filtrado de IP

Si habilita el filtrado de IP, bloqueará todas las conexiones a su sistema, excepto a aquellas IP que tenga configuradas como autorizadas para acceder al Sistema.

8. Cambie los puertos HTTP y TCP que vienen por defecto

Cambie los puertos HTTP y TCP que vienen por defecto

- Estos puertos son los más comunes, y lo que es peor, los más conocidos (están en el manual) para comunicar el dispositivo a internet.
- Estos puertos se pueden cambiar y puede usar el rango entre los números 1025-65535. Evitar los puertos predeterminados reduce el riesgo que alguien desde el exterior pueda adivinar qué puertos está utilizando.

9. Revise el Log de eventos

Si sospecha que alguien no autorizado se ha conectado a su Sistema de seguridad, revise el log de eventos. El Log de eventos le mostrará la IP desde la cual se ha conectado un usuario a su sistema.

10. Conecte las cámaras IP POE directamente a los puertos POE del NVR

Conecte las cámaras IP POE directamente a los puertos POE del NVR, además de obtener alimentación fiable por el propio cable de red, también quedan aisladas del resto del mundo y no se podrá acceder a las cámaras desde la WAN ya que el switch POE actuará como un cortafuegos para las cámaras y evitará cualquier conexión.

11. Proteja físicamente el dispositivo

Si desea evitar un acceso no autorizado directamente en el grabador, la mejor manera de evitarlo, es instalar el grabador dentro de un arcón, rack, caja fuerte ventilada, o habitación con cerradura.

12. Abra solo aquellos puertos que utilice

Abra solo los puertos HTTP y TCP que vaya a utilizar. No abra un rango de puertos a la ip de un dispositivo

13. No utilice nunca la opción DMZ del router

No utilice la opción DMZ del router a la dirección IP del grabador, ya que esta suele ser una de los principales métodos utilizado para piratear un grabador. Es el error más común cuando el instalador no dispone del soporte o conocimiento suficiente sobre cómo configurar el router.

Si utiliza esta opción, está dejando el grabador totalmente expuesto a que cualquier hacker intente acceder a su sistema, por lo que no utilice nunca esta opción y abra solo aquellos puertos que necesite. Si no puede acceder a configurar direccionamiento de puertos en el router use la opción P2P suponiendo que no esté filtrada por el router o el operador.

14. Desactive el inicio automático del software de gestión o navegador

Si está utilizando un ordenador conjuntamente con otras personas, asegúrese que la opción de auto-inicio de sesión del programa de gestión está desactivada; y asegúrese que no tiene activada la opción memorizar contraseña en su navegador, a fin de evitar que otro usuario del ordenador pueda acceder al sistema de seguridad.

15. Use nombre de usuario y contraseñas diferentes para cada usuario en el software de gestión

Si alguien le piratea sus cuentas de redes sociales, sus datos bancarios, cuenta de correo electrónico, no querrá que utilicen los datos conseguidos para intentar acceder a su sistema de seguridad. Un nombre de usuario y contraseñas diferentes al resto de cuentas evitará que alguien pueda adivinar la manera rápida de acceder a su sistema.

16. Limite las características de los usuarios invitados

Si el sistema está configurado para varios usuarios, asegúrese de que cada usuario tiene una cuenta diferente que el resto y cada cuenta dispone de las funciones que debe realizar cada usuario.

17. Aísle la red del NVR y cámaras IP

La red en la que están instalados el grabador y las cámaras no debería ser la misma que la red informática. Una forma sencilla de conseguir esto es crear una VLAN. Esto evitará que los visitantes tengan acceso a la misma red que el sistema de seguridad.

El II Congreso Nacional de Jefes de Seguridad reunió a más de 150 profesionales el pasado 5 de abril en Barcelona. Un encuentro que se convirtió en un gran foro de debate y análisis en el que se abordaron los nuevos retos a los que se enfrenta el Jefe de Seguridad ante una nueva realidad tecnológica y normativa. En estas páginas hemos querido ofrecer a nuestros lectores una pequeña crónica gráfica de lo acontecido en un envento donde ponentes, profesionales, representantes de empresas y asociaciones, organismos e instituciones analizaron en primera persona la figura del Jefe de Seguridad. Pasen... y vean

Jordi Jardí, director general d´Administració de Seguretat del Departament d´Interior de la Generalitat de Catalunya, (en el centro de la imagen) durante la inauguración del Congreso, junto a Iván Rubio, director del área de Seguridad de Peldaño (a la dcha.), y Antonio Cedenilla, presidente de la Asociación de Jefes de Seguridad de España (AJSE).

Jordi Jané, Conseller d´Interior de la Generalitat de Catalunya (en el centro de la imagen), durante su intervención.

Mario Gutiérrez, consultor de Comunicación del Área de Seguridad; Gemma G. Juanes, redactora jefe de la revista Cuadernos de Seguridad; Juan Cabral, director de Seguridad de TOUS; y Anna Aisa, gerente de la Asociación Catalana de Empresas de Seguridad (ACAES). (de izq. a dcha.).

Representantes de las Fuerzas y Cuerpos de Seguridad y organismos públicos acudieron al II Congreso Nacional de Jefes de Seguridad.

Josep Enric Millo, delegado del Gobierno en Cataluña, durante el acto de clausura.

Joan Josep Pintado, director de Seguridad del Museu Nacional d' Art de Catalunya, junto a Gemma G. Juanes, redactora jefe de la revista Cuadernos de Seguridad.

Andrés Sanz. Coronel jefe del Servicio de Protección y Seguridad de la Guardia Civil. (SEPROSE)

Jesús Fernández Garrido, inspector jefe. Jefe de la Unidad Territorial de Seguridad Privada de Catalunya.; Anselmo Palma García, Comisario 2º Jefe de la Brigada Provincial de Seguridad y Protección, de Cataluña, y Manuel Yanguas, Comisario del CNP. Jefe de la Brigada Central de Empresas de la UCSP.

Antonio Cedenilla, presidente de la Asociación de Jefes de Seguridad Española, AJSE; Gemma G. Juanes, redactora jefe de la revista Cuadernos de Seguridad; e Iván Rubio, director del Área de Seguridad.

Manuel Yanguas, Comisario. Jefe de la Brigada Central de Empresas del CNP, y Emilio Sánchez, consultor del Área de Seguridad de Peldaño.

Esteban Gándara, Comisario Principal Jefe de la Unidad Central de Seguridad Privada (cargo que ocupaba al cierre de esta edición) y actual Comisario Principal Jefe de la División Económica y Técnica, y Maite Casado, subdirectora general de Seguretat d´Interior. Departament d´Interior de la Generalitat.

Jorge Salgueiro, vicepresidente jurídico de AJSE y presidente de AECRA; y Carles Castellano, subinspector jefe de la Unidad Central de Seguridad Privada de los Mossos d´Esquadra.

Ángel Gózalo, General jefe de la 7 Zona de la Guardia Civil de Cataluña.; Anselmo Palma García, Comisario 2º Jefe de la Brigada Provincial de Seguridad y Protección, y Ándres Sanz, Coronel jefe del Servicio de Protección y Seguridad de la Guardia Civil. (SEPROSE).

Equipo del Área de Seguridad que acudió al II Congreso Nacional de Jefes de Seguridad. Mario Gutiérrez y Emilio Sánchez, consultores de Comunicación del Área de Seguridad; Gemma G. Juanes, redactora jefe de la revista Cuadernos de Seguridad; Iván Rubio, director del Área de Seguridad; y María Gómez, event manager de Peldaño.

GEUTEBRÜCK
Excellence in Video Security

64 bit Aceleración GPU Hasta 256TB Onvif

Nueva generación de grabadores **G-SCOPE**

All in One de Geutebrück

Grabación – Visualización - Gestión – Analítica de vídeo

Rentabilice sus instalaciones con soluciones profesionales

Sistema compatible con protocolos Onvif e integraciones de terceros

Protección de los datos basados en AES256 o SALSA20

Analítica de vídeo desarrollada por Geutebrück de máxima fiabilidad

F.F. Videosistemas
Camino de las Ceudas 2 Bis
CP: 28232 Las Rozas (Madrid)
902 99 84 40
ffvideo@ffvideosistemas.com

F.F. Videosistemas
Distribuidor exclusivo

www.ffvideosistemas.com

EDUARDO J. ÁLVAREZ BLÁZQUEZ. SECURITY DIRECTOR SPAIN. CSIS SPAIN CITIBANK

«La **ciberseguridad** es uno de los **pilares clave** en la seguridad bancaria contemporánea»

AHORA mismo, la información es el activo a proteger más importante dentro de una Corporación, casi por encima incluso del propio efectivo», asegura Eduardo J. Álvarez Blázquez, Security Director Spain. CSIS Spain Citibank, quien además puntualiza en esta entrevista que en un mundo cada vez más globalizado, «la protección de la información es una obligación que no debe ser descuidada por ningún departamento de Seguridad».

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

—El día a día en la vida del director de Seguridad de Citibank, en relación a planificación y organización, pasa por un análisis constante de los riesgos que amenazan a nuestra corporación.

En el actual clima de amenaza constante en el que vivimos (baste ver los últimos ataques terroristas perpetrados en suelo europeo, desde Londres a Bruselas) uno de los principales elementos a considerar es la seguridad física del personal que, o bien trabaja para Citi, o bien son clientes del mismo.

En este sentido, Citi ha desarrollado una potente herramienta de análisis y prospección, el Mando Regional de Control (RCC), que emite diferentes informes que nos ayudan tanto en la evaluación de los riesgos a los que nos enfrentamos, como a la toma de decisiones a la hora de neutralizar o minimizar estas amenazas.

La colaboración y comunicación con Fuerzas y Cuerpos de Seguridad del Estado, y otros organismos de Seguridad resulta vital, tanto para la detección temprana de la amenaza, como su ulterior neutralización. Herramientas digitales tales como las plataformas REDAZUL o COOPERA, desempeñan un trabajo más que digno.

Por otro lado, debemos hacer frente, de manera prácticamente diaria, a otro de los vectores de amenaza que afronta la entidad, y que afecta muy especialmente a su credibilidad e imagen corporativa, como es el fraude. En este sentido, trabajamos en una doble vertiente: por un lado, y en constante comunicación con Fuerzas y Cuerpos de Seguridad del Estado, nueva neutralización del fraude con tarjetas, cuya tecnificación y sofisticación ha resultado extraordinaria en los últimos tiempos; y por otro, el fraude a través de medios tecnológicos, tales como phising, ingeniería social, etc., que si bien compete más a otra figura de la organización, como es el Oficial de Seguridad de la Información (CISO), tiene un componente de Seguridad «pura» bastante elevado.

Una tercera vertiente dentro de las competencias del responsable de seguridad de una entidad como Citi se encuentra dentro del terreno del cumplimiento normativo. Si bien Citi posee un departamento de cumplimiento normativo muy potente (Compliance), con una vinculación estrechísima con el Departamento Legal, existe una

preocupación enorme dentro de la entidad por realizar un trabajo plenamente acorde con la normativa, no sólo del país en cuestión, sino, por ejemplo en nuestro caso, con la legislación de la Unión Europea, y por supuesto, con los estándares normativos de Citi, y sus propias políticas internas.

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

—Evidentemente, los parámetros en los que se desenvuelve la Seguridad Bancaria en la actualidad no tiene prácticamente nada que ver con el de hace, por poner un ejemplo, 20 años. Si bien es cierto que se sigue conviviendo con el delito que podríamos llamar más tradicional (atracos a sucursales, violencia en cajeros automáticos y ATM´s, etc.), el perfil del delincuente bancario se ha tecnificado muchísimo, y preocupa en la actualidad mucho más tipologías delictuales como el hacking, phishing, ingeniería social, etc., como los mayores peligros a los que hacemos frente los departamentos de Seguridad de las diferentes entidades bancarias. Incluso dentro de la delincuencia tradicional, ya no sólo nos encontramos con la sustracción de la tarjeta de crédito, sino también con la clonación de las mismas, o la sustracción de sus datos.

Respecto al otro punto, al cambio de riesgos y amenazas desde el prisma de la Ciberseguridad, podemos decir que actualmente es uno de los pilares clave en la Seguridad Bancaria contemporánea. Ahora mismo, la información es el activo a proteger más importante dentro de una Corporación, casi por encima incluso del propio efectivo. En un mundo cada vez más globalizado, la protección de la información es una obligación que no debe ser descuidada por ningún Departamento de Seguridad, dado que de verse comprometida,

se vería comprometida en igual medida la credibilidad de la institución, con el consiguiente deterioro de su imagen corporativa y su competitividad.

Este aspecto de lucha contra el Cibercrimen se verá incrementado extraordinariamente en los próximos años, debido fundamentalmente a la entrada en escena de la Banca Digital, con una nueva problemática a la que los departamentos de Seguridad tendremos que hacer frente. Este es un mundo nuevo a explorar que, francamente, no sabemos hasta dónde nos va a llevar. Creo honestamente que éste es el mayor de los retos que se nos presenta a corto-medio plazo.

—¿Cuáles considera que son actualmente los elementos fundamentales a la hora de plantear una seguridad integral y convergente en el sector bancario?

—Sinergia, creo que es la palabra que podría definir y englobar más acertadamente ambos conceptos. Este es el elemento en el que más énfasis se debería poner tanto a nivel Seguridad como a nivel Corporación. Ya no podemos considerar la Seguridad como un elemento aislado del resto de la entidad. Debe de ser una herramienta útil, que sirva a los intereses del banco, tanto a nivel de Seguridad propiamente dicha, como a nivel de Cumplimiento Normativo, Fraude, Ciberseguridad, Blanqueo, etc., que puede afectar y perjudicar a nuestra entidad.

En este sentido, se debe realizar una mayor concienciación a nivel usuario de todo lo que la seguridad aporta a la Corporación, no sólo a nivel de Seguridad llamémosla «tradicional», sino también a toda aquella parte de protección de la que los departamentos de Seguridad son responsables y es menos visible (Auditorías, Planes de Contingencia, Continuidad del Negocio, etc.)

—¿Cuáles son las prioridades de seguridad para el responsable de Seguridad de una corporación bancaria como Citibank?

—En primer lugar, desde una perspectiva de seguridad física, una vez más, la protección tanto de personas como de bienes que componen Citi. El principal activo que posee Citi son las personas que la componen, y es nuestra máxima prioridad garantizar su seguridad, no sólo en su puesto de trabajo, sino en su vida cotidiana, cuya esfera puede verse amenazada, más en la situación actual que vivimos.

Actualmente, las amenazas no se están produciendo en países remotos, están aquí, a nuestro lado, en países cercanos, y nos está golpeando brutalmente,

por lo que la percepción de la amenaza es totalmente diferente a la que se tenía hace diez años, por ejemplo.

La protección de la Información. Como hemos señalado anteriormente, un aspecto fundamental en la protección integral de la entidad vendría determinado por la protección de la seguridad que Citi maneja en desarrollo de sus operaciones. Esta información está compuesta no sólo por la aportada por los clientes, sino también por los propios empleados, generándose un volumen de datos cuya protección e integridad deben ser salvaguardadas por la Corporación, y por su departamento de Seguridad.

una buena reputación, pero se tardan 5 minutos en destruirla, y eso es exactamente lo que ocurre en nuestro sector. Es por este motivo por el que el departamento de Seguridad debe permanecer vigilante, a fin de evitar estos deterioros en la imagen de la Corporación, derivada de vulnerabilidades ocasionadas por una falta de protección de los bienes, servicios, o clientes de la entidad. El puntual cumplimiento de esta premisa, por el contrario, redundará en una mejor apreciación de la entidad por parte del cliente.

Otro de los puntos a proteger, y que cada vez está más en desuso, es la protección del efectivo, el capital. Al

> «La lucha contra el cibercrimen se verá incrementada en los próximos años debido fundamentalmente a la entrada en escena de la banca digital»

Otro de los elementos que desde el departamento de Seguridad tratamos de proteger como uno de los principales activos de la compañía es la Imagen Corporativa. Como reza el clásico adagio, se tardan 20 años en construir

fin y a la postre, no dejamos de ser los responsables directos de la seguridad de una entidad financiera. Cierto es que en el caso de Citi, la protección del efectivo físico no mantiene el peso que tenía en el pasado, sobre todo des-

Maksim Kabakon / Shutterstock

de la venta del negocio minorista en el último cuarto de 2014, por la que Citi prácticamente dejó de manejar efectivo. Esto mismo ocurrió con la gestión de seguridad de las sucursales, dado que con su venta, se dejó de proveer de seguridad a las mismas.

Una de las claves para el correcto funcionamiento de un departamento de Seguridad de una entidad bancaria es la relación con Fuerzas y Cuerpos de Seguridad del Estado. En este sentido, el departamento de Seguridad trata de que estos vínculos sean lo más estrechos posibles, participando en diversos foros y ponencias, donde se pongan sobre la mesa los distintos problemas y retos que afronta la Seguridad Bancaria, y que sean tratados desde el prisma de la Seguridad Pública.

El intercambio de información con las distintas Fuerzas y Cuerpos de Seguridad del Estado debe ser constante y fluido, para proveer de una prospección fiable y efectiva a los diferentes departamentos de Seguridad, y proveer al consumidor de seguridad de unas herramientas válidas para desempeñar sus funciones, principalmente en el campo de la prevención. Es aquí donde este flujo de información, entre los distintos cuerpos policiales y los diferentes departamentos de Seguridad resulta crucial, pues si un agente externo golpea a una corporación, la información que pueda derivarse de este ataque, puede ayudar a que no se repita en otra entidad.

—¿Qué papel juega la tecnología a la hora de garantizar y mejorar la seguridad de las corporaciones bancarias?

—Resulta un factor indispensable absolutamente. No se concibe la Seguridad Bancaria ajena a la tecnología. Si nos fijamos en la seguridad del sector en las décadas de los 80 o 90, por ejemplo, veíamos cómo en casi cualquier

HYUNDAI

TECNOLOGÍAS DE ÚLTIMA GENERACIÓN

NEXT GEN

HDTVI HDCVI™

AHD CVBS IP

DESCUBRA NUESTRO MÁS AVANZADO CATÁLOGO DE PRODUCTOS

CÁMARAS Y DVRS HASTA 5 EN 1 · SISTEMAS DE ALARMA

VIDEOPORTEROS · TECNOLOGÍA IP HASTA 4K

bydemes GROUP

DISTRIBUIDOR EXCLUSIVO EUROPEO

SEDE CENTRAL
San Fructuoso, 50-56
08004 Barcelona
Teléfono: 934 254 960 / 934 269 111
Fax: 934 261 904
bydemes@bydemes.com
www.bydemes.com

HYUNDAI

Licensed by Hyundai Corporation, Korea

WWW.HYUNDAI-SECURITY.ES

sucursal, existía un Vigilante de Seguridad que proveía de seguridad al establecimiento. Progresivamente dicho concepto se fue abandonando, dando paso cada vez más a nuevas tecnologías, desde las antiguas CCTV´s, a las esclusas, por no hablar de las cámaras acorazadas y sus propios adelantos tecnológicos. Estos mismos medios, muy probablemente quedarán obsoletos en un futuro no muy lejano, al entrar la Banca Virtual y Digital a sustituir a la sucursal tradicional.

—¿Qué retos debe asumir actualmente un director de Seguridad a la hora de implantar una estrategia de seguridad, en este caso, en el ámbito bancario?

—El principal reto, como en otros departamentos, consiste en conjugar restricción presupuestaria con operatividad. En estos tiempos donde todos son límites al gasto, se trata de intentar hacer lo máximo con lo mínimo. Tenemos que conseguir llegar a cubrir todos los ángulos posibles de la seguridad, con unos recursos cada vez más limitados, teniendo en cuenta que cada vez más elementos pasan a estar gestionados por las áreas de seguridad. Optimizar los recursos al máximo, es el principal reto que asume hoy el director de Seguridad.

El engranar las diferentes legislaciones en juego en materia de seguridad, junto a los diferentes protocolos y directivas internas supone otro reto importante, sobre todo cuando unos y otros se encuentran basados en criterios normativos tan diferentes en muchas materias (derechos fundamentales, seguridad, etc.).

La globalidad de las amenazas, así como su gestión integral, suponen igualmente un reto a la hora de desempeñar nuestras funciones. En un mundo cada vez más globalizado, cualquier amenaza a una parte, aunque no esté localizada geográficamente en un entorno cercano, afecta o puede llegar a afectar, al conjunto de la corporación. Su evaluación y posterior gestión se hace imprescindible en nuestro mundo actual.

> «La globalidad de las amenazas, así como su gestión integral, suponen igualmente un reto a la hora de desempeñar nuestras funciones»

—A grandes rasgos, ¿cuáles considera que son las claves para una seguridad satisfactoria en las corporaciones bancarias?

—Funcionalidad: Una de las características es que debe cumplir con su objetivo prioritario, que no es otro que el de proveer de seguridad, en sus múltiples facetas, a la corporación. Esto implica la toma de decisiones y medidas encaminadas a tal fin, y que sean efectivas, es decir, que realmente consigan neutralizar la amenaza, sea ésta de la naturaleza que sea.

Utilidad: Esta seguridad debe ser útil, es decir, realmente debe de alcanzar los objetivos requeridos, y debe hacerlo de la manera más directa posible, evitando gastos y molestias innecesarias a los usuarios. Aquí el equilibrio entre la propia operatividad de la compañía y la consecución de los estándares de calidad de seguridad es prioritario. Por alcanzar unas óptimas y plausibles

Este hecho tiene mucho que ver también con el cambio en el perfil del usuario, que como es normal, también se está adaptando a las nuevas tecnologías. Creo que se trata de una evolución natural del sector. Es fundamental que el concepto de seguridad, así como el propio departamento, se adapten a los tiempos que viven, teniendo siempre

cotas de seguridad no puede nunca sacrificarse el normal desarrollo de las operaciones del negocio.

-Sostenibilidad: Debe ser sostenible, tanto en el tiempo, como a nivel gasto, y dentro de la propia corporación. Esto implica una gran capacidad para el sacrificio del departamento de Seguridad, que en muchas ocasiones, y debido al panorama de «relativa tranquilidad», así como por la continua evolución técnica y tecnológica que está sufriendo el sector bancario, y que estamos viviendo sobre todo en los países occidentales se han visto en muchas ocasiones muy mermados en sus capacidades operativas, pero cuyos servicios continúan siendo requeridos para cumplir sus objetivos de seguridad y protección.

No obstante, y apelando una vez más a esta capacidad de adaptación de los departamentos, pueden verse incrementados sus recursos y dimensiones en un período de tiempo también extraordinariamente corto, caso que las condiciones de seguridad vayan mutando.

Baste como ejemplo referirse en este punto a los desgraciados ataques terroristas que cada vez con más frecuencia se vienen produciendo en suelo europeo (Gran Bretaña, Alemania, Francia, Turquía, por citar los más relevantes), que ya están provocando en la sociedad, y por supuesto en las corporaciones financieras, una creciente preocupación por la seguridad, con el consiguiente incremento de recursos, tanto materiales como humanos. Uno de los puntos a considerar, y que en mi opinión continuará una línea ascendente, será la creación de más departamentos de Inteligencia y Prospección, sobre todo en entidades con intereses globales.

Una preocupación que, por otro lado, se tenía olvidada al albur de una sociedad cada vez más alejada de la violencia física, pero que el devenir de los acontecimientos ha demostrado lo equivocadas que estaban las sociedades occidentales (principalmente las europeas) en este sentido.

Esta preocupación se ve acentuada en el caso de corporaciones de la naturaleza de Citi al tratarse en primer lugar de una corporación americana, con las implicaciones a nivel seguridad que conlleva este extremo, y en segundo lugar porque al tratarse de una corporación con intereses globales, también las amenazas que afronta son globales. Lo cual hace que los departamentos de Seguridad tengamos que tener unas herramientas de análisis poderosas y una implicación global de los distintos organismos de seguridad para identificar amenazas globalmente.

-Valor añadido: Un departamento de Seguridad de una entidad bancaria de carácter moderno debe además aportar valor añadido a la Corporación. Y este valor añadido debe ser engranado en un doble sentido:

En el orden interno, aportando al trabajador una herramienta fiable y un recurso del que pueda valerse, se trataría en este caso de que existiera una Seguridad «tangible». Este objetivo se consigue a través de un sistema de control de accesos de calidad, con un discernimiento efectivo del personal que puede acceder o no a las diferentes instalaciones. También a través de la elaboración de diferentes notas e informes relativos a asuntos de seguridad que puedan afectar a los usuarios, y a través de diferentes trainings que se elaboran desde el departamento de Seguridad.

En el ámbito externo, un departamento de Seguridad, percibido como potente, con capacidades, por los potenciales agresores, siempre añade un plus a una corporación bancaria. Esa percepción externa pasa por hacer gala de una buena reputación, ganada sobre las sólidas bases de la neutralización de amenazas concretas, de una relación fluida con Fuerzas y Cuerpos de Seguridad del Estado, y por la pertenencia a la Comunidad de Seguridad e Inteligencia tanto a nivel local como regional y global.

Como diría Sun Tzu «No emprendas una guerra que no puedas ganar», máxima que aquellos que pretenden causar daño a nuestras entidades deben tener muy presente.

Texto y Fotos: Gemma G. Juanes.

Wright Studio / Shutterstock

RAFAEL MADRID GARCÍA. DIRECTOR DE SEGURIDAD.
BANCO DE CRÉDITO COOPERATIVO-GRUPO COOPERATIVO CAJAMAR

*«Nuestro objetivo es alcanzar las **máximas cotas de seguridad** con la máxima eficiencia de los recursos disponibles»*

GARANTIZAR la seguridad de su principal activo que son las personas, y también de los bienes, es en palabras de Rafael Madrid García, director de Seguridad del Banco de Crédito Cooperativo- Grupo Cooperativo Cajamar, una de las máximas prioridades de seguridad para el responsable de seguridad de una corporación bancaria, además de, añade, el estar «alineados con las estrategias de negocio y coadyuvar al alcance global de los objetivos del conjunto de nuestra organización, y todo ello dando el mejor servicio posible a nuestros clientes, que no son otros que los empleados del Grupo».

—¿Cómo es el día a día, en cuanto a planificación y organización para el responsable de Seguridad de una entidad bancaria como es el Banco de Crédito Cooperativo-Grupo Cooperativo Cajamar?

—Cada mañana comienza con el repaso de cuanto internamente ha acontecido el día anterior en el ámbito de mi responsabilidad, sin perjuicio de haber sido informado puntualmente de los hechos más relevantes cuando se produjeron. También procuro conocer bien todo lo relacionado con el cambio y la evolución de nuestro entorno de actuación en el más amplio sentido, pero especialmente en los aspectos tecnológico, normativo y del comportamiento y tendencias de la actividad delincuencial. Para ello utilizo fuentes abiertas, publicaciones oficiales y revistas especializadas como Cuadernos de Seguridad.

La planificación me exige de un análisis continuo que permita la elección de las medidas de seguridad más adecuadas, en atención a las características de los bienes a proteger y de las amenazas a las que estén expuestos, y que por normativa o por decisión directiva, se encuentren bajo la responsabilidad de Seguridad. Para ello procuro contar con una estructura adecuada, que debe justificarse ante la dirección del Grupo.

En mi opinión, la esencia de la función directiva es conseguir una actuación conjunta de las personas que componen la organización, dándoles objetivos y valores comunes, ejerciendo una continua orientación para responder a los cambios que se presentan. En ello procuro volcar mis esfuerzos, a la par que otorgo la adecuada discrecionalidad a los responsables de mis oficinas internas para el desarrollo de su propia impronta.

En la actualidad nos encontramos ante un escenario muy dinámico, como es el propio de la actividad financiera, en el que generar ingresos y resultados se ha convertido en una tarea difícil y com-

pleja. La presión sobre los costes que soportamos todos los departamentos es muy alta. Por ello, como responsable de Seguridad, en mi tarea organizativa me enfrento de continuo a un proceso de toma de decisiones a fin de implementar los mecanismos operacionales, de seguimiento y de control adecuados que permitan garantizar y conocer el estado y funcionamiento de los elementos de seguridad y la calidad de los servicios que tenemos contratados, al tiempo que debemos estar coordinados con otros departamentos y oficinas internas para aprovechar las sinergias resultantes de una buena colaboración, manteniéndonos además alineados con las estrategias y necesidades de negocio de nuestro Grupo.

Siempre he considerado que la flexibilidad en los planteamientos y la capacidad de adaptación son los mejores precursores para una eficaz adaptación al cambio y adecuación a las exigencias de la tarea que nos es exigida, y en eso estamos cada día. Afortunadamente los cambios no son diarios, se requiere de un mínimo de estabilidad en los planteamientos, pero sí lo es el ejercicio de preguntarnos qué estamos haciendo y en qué podemos mejorar.

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

—Yo no diría que han cambiado las amenazas y riesgos del sector bancario. Para ello deberían haber desaparecido unas y aparecido otras, cuestión que en mi opinión no es el caso. La realidad es que perduran las amenazas tradicionales, las de siempre, algunas de las cuales incluso se reinventan en manos de determinados colectivos, que consiguen superar las medidas de seguridad en su día implementadas para evitar la materialización de los riesgos. Y junto a éstas, y al abrigo del desarrollo tecnológico y singularmente de las tecnologías de la comunicación, aparecen nuevas modalidades delictivas o amenazas que nos exponen a los riesgos de siempre.

Por supuesto me estoy refiriendo al entorno financiero, donde las actividades delictivas que soportamos pretenden como fin último, principalmente, obtener un beneficio económico apoderándose de lo ajeno y, en algunos casos, causar daños físicos o reputacionales a nuestros activos. Así las cosas, desde mi punto de vista, lo que ha cambiado son los procedimientos y vectores de ataque empleados por los delincuentes para el logro de sus objetivos, de modo que nos enfrentamos a un panorama más amplio que obliga a la adopción de nuevas medidas de seguridad, pero sin que podamos abandonar las existentes.

Sede social de Banco de Crédito Cooperativo-Grupo Cooperativo Cajamar.

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

—Como en otros aspectos de la seguridad, en los últimos tiempos están viéndose fuertemente condicionadas por la contención presupuestaria, tanto en la inversión como especialmente en el gasto. No podemos permitirnos el lujo de cometer errores embarcándonos en proyectos ambiciosos que años más tarde puedan ser desechados, ni incorporar tareas en el ámbito de la entidad financiera que no aporten valor.

Así las cosas, debemos obtener el máximo rendimiento con la mínima estructura, apoyarnos en la tecnología para ser muy eficaces con el menor esfuerzo, ser muy sensatos en la elección del material de seguridad, huyendo a ser posible de los sistemas propietarios, y tener criterios claros de externalización de tareas con una buena selección de empresas proveedoras. Todo ello buscando la máxima eficiencia.

En este sentido, es generalizado el uso de plataformas para la gestión de la negociación y la contratación de proveedores en procesos abiertos y multidepartamentales, pues intervienen con gran peso supradepartamentos, como las centrales de compras, soporte tecnológico, comités presupuestarios, de recursos, de contratación, etc., que a veces encorsetan las negociaciones, condicionando de algún modo la libertad sobre la elección de proveedores, sistemas de seguridad e incluso medidas de seguridad a establecer, con la que tiempo atrás contaban los departamentos de Seguridad.

—¿Cuáles considera que son actualmente los elementos fundamentales a la hora de plantear una seguridad integral y convergente en el sector bancario?

—Por regla general es aceptado, que el resultado armónico de seguridad ha de ser proporcionado por la conjunción de los medios humanos, técnicos y organizativos, como partes integrantes de un

Rafael Madrid, director de Seguridad del Banco de Crédito Cooperativo-Grupo Cooperativo Cajamar, con profesionales del Centro de Gestión de Seguridad.

todo. De ahí que, en lo humano, como he comentado en otras ocasiones, se deben constituir equipos con personas formadas en seguridad, distribuyendo cometidos descentralizados, bajo la dirección del director de Seguridad, para áreas geográficas concretas. Hay que lograr que estas personas desarrollen un fuerte sentimiento de pertenencia y sientan como suyo el bien a proteger. En lo técnico, habremos de elegir los elementos y sistemas, tanto físicos como electrónicos, adecuados a las características del bien a proteger y las amenazas imperantes. Y por último, debemos elaborar planes, normas y estrategias en un marco organizativo que se ajuste al nivel de seguridad deseado y a las necesidades de la entidad, que facilite el ejercicio de las funciones directivas por parte del director de Seguridad y la implementación de una cultura corporativa de seguridad en toda la entidad, siendo una cuestión fundamental para ello dirigir acciones formativas y transmisoras de conocimiento dirigidas a todos los empleados.

—¿Cuáles son las prioridades de seguridad para el responsable de Seguridad de una corporación bancaria como Banco de Crédito Cooperativo-Grupo Cooperativo Cajamar?

—Garantizar la seguridad de su principal activo que son las personas, y también de los bienes. Estar alineados con las estrategias de negocio y coadyuvar al alcance global de los objetivos del conjunto de nuestra organización, y todo ello dando el mejor servicio posible a nuestros clientes, que no son otros que los empleados del Grupo.

Nuestro objetivo es alcanzar las máximas cotas de seguridad con la máxima eficiencia de los recursos disponibles, aplicando criterios de optimización en la doble perspectiva de prevención de riesgos, evitando que se materialicen, y protección ante los riesgos, minimizando las pérdidas y sus consecuencias perjudiciales en el caso de que no los podamos evitar.

—¿Cree que ha llegado el momento de adaptar las estructuras de los departamentos de Seguridad a las nuevas necesidades empresariales?

—A pesar de la incuestionable evolución de los departamentos de Seguridad, todavía son numerosos los casos en los que la seguridad no forma parte del *core business* de las empresas, que con frecuencia la ven como una obligación normativa y centro de gasto, provocando con frecuencia carencias en cuanto a la dotación de personal cualificado, recursos y adquisición de nuevas tecnologías. En la actualidad, los clientes de todos los sectores demandan más servicios y agilidad en entornos extremadamente competitivos. Los tiempos cambian y la forma de relación también, con lo que, si las necesidades empresariales son otras, se presenta como algo incuestionable la necesidad de adaptación de los departamentos de Seguridad.

—¿Qué retos debe asumir actualmente un director de Seguridad a la hora de implantar una estrategia de seguridad, en este caso, en el ámbito bancario?

—La eficiencia impera sobre todo. El reto principal es la adaptación al cambio del modelo de negocio y a la transformación digital. Desde un enfoque puramente físico, vamos hacia una distribución de los locales con espacios de atención discretos que faciliten la labor de asesoramiento al cliente. Con una fuerte reducción de los puestos de caja y operativa administrativa tradicional. Al tiempo que aumentan en espacio y número de elementos las zonas destinadas al autoservicio de los usuarios, que asimismo requieren de medidas de protección. Para ello es fundamental conocer la prospectiva de la entidad, a fin de acertar en la elección de los medios y sistemas de seguridad, adecuando los esfuerzos a lo que serán las necesidades reales.

En este sentido, se hace también muy importante establecer unos muy buenos contratos de mantenimiento, con empresas de absoluta confianza, puesto que ahora cobra especial importancia garantizar el correcto funcionamien-

to de los canales alternativos y equipamientos de autoservicio, a los que se derivan a los clientes en los nuevos modelos de oficina.

Por otra parte, y en relación con la pregunta anterior, en las entidades financieras son recurrentes los procesos de revisión, por departamentos propios o consultoras externas, de las estructuras y composición de las oficinas internas; de la superación de procesos y proyectos bajo múltiples denominaciones como análisis organizativo, eficiencia operativa, gestión del cambio, optimización de servicios, entre otros.

El caso es que la adaptación de la estructura de los departamentos de Seguridad a las necesidades de las entidades financieras es permanente, siendo un gran reto en continua revisión. A todos los directores de Seguridad nos son familiares y hemos debatido y rebatido argumentos referidos al benchmarking, palancas y oportunidades de mejora, oportunidades para la mejora de la eficiencia, descontinuación de tareas, FTEs…, cuyo resultado final habrá condicionado, frecuentemente reduciéndolo, la estructura y composición de nuestros departamentos.

Por ello, desde mi punto de vista, la estrategia debe estar basada en una adecuada prospectiva que permita el establecimiento y mantenimiento de unos criterios de seguridad claros, que formen parte de la cultura de empresa, el diseño de un modelo organizativo con una estructura dotada adecuadamente, y la adopción de una equilibrada política de externalización de servicios; de tal suerte que la falta de criterios, las debilidades de la estructura organizativa o una desmedida externalización, no constituyan en sí mismas amenazas endógenas que añadir a las exógenas existentes.

—Retomando aspectos normativos, ¿qué elementos le gustaría que incluyese el Reglamento de Seguridad Privada que afectasen a la seguridad bancaria?

—Esta cuestión se debate de forma recurrente en distintos foros, siendo claro que el reglamento no puede incluir nada que la ley no contemple, con lo que no procede pedir la inclusión de ningún aspecto nuevo. Dicho esto, y dado que la ley otorga una mayor consideración al director de Seguridad, a quien asigna funciones nuevas, respecto de la legislación anterior, de las que se derivarán las consiguientes responsabilidades, sería deseable que en el reglamento se concrete al máximo y quede bien definido y delimitado el alcance de unas y otras.

Igualmente, por razones obvias, entre las que podríamos incluir la afección a los balances económicos de algunas empresas, espero un sensato y razonable desarrollo reglamentario en cuanto a los sistemas y medidas de protección obligatorias que no lo sean con arreglo a la normativa actual, en especial para los establecimientos obligados a contar con medidas de seguridad.

Estoy seguro de que la Administración está haciendo un gran esfuerzo para armonizar el interés general, en su obligación de garantizar la seguridad y la protección públicas, con las expectativas de los fabricantes, proveedores y empresas de seguridad, y la de los consumidores de seguridad y establecimientos obligados. ●

Texto: Gemma G. Juanes.
Fotos: Grupo Cooperativo Cajamar

Oficina de la entidad bancaria.

Interior de una de las sucursales de Grupo Cooperativo Cajamar.

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

DAESH, «algo que patear»

NO les gusta a los yihadistas la traducción peyorativa que se hace de su acrónimo Daesh, Al-Dawla al-Islamiya al-Irak al-Sham, «algo que pisotear». Ellos comparten con entusiasmo la denominación con la que cada día más sectores de Occidente les identifican, porque es algo así como la matriz de su objetivo territorial perseguido y utópico, el Califato: Estado Islámico (EI), Estado Islámico de Irak y Levante, ISIS (Islamic State of Irak and Siria, etc.). Todo aquello que magnifique las porciones de terreno que actualmente salpican las zonas que ocupan en Siria e Irak, y que en el transcurso de los tres años de guerra que a mediados de marzo cumplieron su sangriento aniversario, va decreciendo mucho más deprisa de lo que hubieran podido imaginar en 2013.

Algunos analistas consideran que el enfrentamiento entre Occidente y Oriente no se remonta a los cruzados, lo que ya de por sí nos trasladaría a épocas remotas (siglos XI a XIII), sino probablemente al instante mismo de que en el año 622 se iniciara la predicación de Mahoma en la Meca, de donde tuvo que huir a Medina porque los comerciantes no aceptaban la nueva religión, una decisión que pasaría a la historia como el Égira.

Shutterstock / Tyler Mckey

En tantos cientos de años, algo llama poderosamente la atención, algo significativamente contradictorio: que las tres religiones monoteístas abrahámicas (Judaísmo, Cristianismo, e Islam), cuyas raíces arrancan del profeta Abraham, no hayan parado de una u otra forma de guerrear.

Si estos ejemplos históricos no fueran suficiente para entender a los que hoy se autodenominan muyahidines, la sucesión de atentados en países occidentales y las estrategias que algunos especialistas les han adjudicado sobre Europa y Occidente en general (convertir al Viejo Continente en Eurabia, un territorio mayoritariamente musulmán, o asesinar al mayor número posible de europeos para que su miedo les lleve a abrazar el Islam), deberían acelerar nuestra puesta al día en análisis preventivos y prospectivos; en una mayor integración europea en defensa y seguridad y en el desarrollo de unas estrategias de comunicación social de mayor calado, por citar algunas de las puntas de lanza más significativas.

Justo es reconocer que la Unión Europea ha avanzado significativamente

en estos apartados en los tres últimos años: fuerte aumento en los trabajos de inteligencia, una mayor integración en seguridad y una importante mejora en la comunicación y neutralización yihadista en las redes sociales. La peor barbarie representada por los videos en ultra definición que con implacable regularidad suben a Internet, demuestran de lo que son capaces y cuál es la intensidad que aplican a sus crímenes: decapitaciones, soldados turcos incinerados poco a poco en medio de sufrimientos atroces, tiros en la nuca a cargo de niños...

No es menos preocupante que de los dos grandes troncos doctrinales del Islam destaque el sunismo abrumadoramente (85%), porque los musulmanes de tradición sunita siguen las enseñanzas y deberes de los hadices, acciones de Mahoma que han conformado el código de comportamiento recogido en la Sunna del profeta, es decir, el perfil más duro, aunque ellos lo definen como el más puro. Pero conviene tener presente que si el yihadismo, que agrupa las ramas más violentas y radicales del islam político o islamismo, es considerado una desviación del salafismo (volver a los orígenes y pureza del Corán) en las filas sunitas, no es menos cierto que ha tenido un gran predicamento también dentro del chiismo. Doble preocupación. Se afirma que en una población musulmana en el mundo de algo más de 1.500 millones de personas, 200 millones de ellas se dice que estarían dispuestos a incorporarse a la Yihad.

Como es sabido, dos organizaciones terroristas se atribuyen el liderazgo actual en su enloquecida Yihad y en la expansión de sus acciones criminales. Al Qaeda, cuya fundación oficial tiene lugar en 1988, se da a conocer diez años antes con su incorporación a la insurgencia durante la invasión rusa de Afganistán. Su atentado más grave pasará a las páginas negras de la Historia con las casi 3.000 víctimas que fallecieron en el derrumbamiento de las Torres Gemelas de Nueva York. No hay palabras suficientes para describir el horror que sentimos millones de ciudadanos con este ataque.


Shutterstock / Drop of Light

Estados Unidos considera a Al Qaeda en la Península Arábiga (AQPA), la rama más peligrosa de la organización. El primer Seal de la presidencia de Trump caído en combate, William Owens, murió en febrero pasado en el curso de un ataque a una base de Al Qaeda en Yemen. Pero la actividad de otras filiales como Al Qaeda del Magreb (AGMI), Boko Haram en Nigeria, Al Shabab en Somalia y otras, no cesa.

Como grupo tutelado por Al Qaeda para implicarlo en la insurgencia, Al-Zarqaui funda Daesh con el inicio de la segunda guerra de Irak, en 2003. De naturaleza fundamentalista yihadista wahabí (movimiento religioso dentro del sunismo), su primer dirigente murió alcanzado tres años más tarde por un misil lanzado por un dron y fue sustituido por Al-Baghdadi, quien pese a los intentos de diversos países por eliminarlo y a sus continuas simulaciones de muerte, sigue liderando esta organización terrorista.

Entre las consecuencias de los esfuerzos por hegemonizar la Yihad global, cabe destacar la serie de atentados en 2015 y 2016 a cargo de ambos grupos en Europa y Estados Unidos, entre otras zonas. Según el Centro de Terrorismo e Insurgencia del Jane's Information Group con sede en el Reino Unido, los atentados han crecido en el mundo un 26% en 2016, pasando de 18.987 a 24.202, de los cuales Daesh ha sido responsable de 4.236 atentados con 18.807 víctimas.

Islamización de los radicales

Un interesante informe de «El País» del mes de febrero último, analizaba las teorías de dos académicos franceses, Olivier Roy y Gilles Kepel, sobre la radicalización. El primero la resumía como «la islamización de los radicales» y el segundo como «la radicalización del Islam». En un término medio se ubica el analista francés Wassim Nasr, quien distingue entre yihadistas occidentales y yihadistas árabes, entre los que es fundamental analizar el historial para determinar el origen del conflicto y la implicación de los actores.

La financiación de ambos grupos es similar, pero se acentúa en el ca-

Shutterstock / Wuthrich didier

so de Daesh por su protagonismo en áreas de recursos petrolíferos, antigüedades, tráfico de personas y drogas e «impuestos» en las zonas ocupadas. Algunas fuentes occidentales han calculado que entre la venta de petróleo y gas y el tráfico de drogas y personas, sólo Daesh alcanza los 1.100-1.200 millones de euros anuales, a lo que hay que añadir la venta de las antigüedades expoliadas y las donaciones de algunos países árabes.

Es particularmente sorprendente su capacidad para la comunicación. Han aprendido muy rápido el valor y alcance de las relaciones en las redes sociales, pero también la comunicación escrita con la publicación de 4 revistas (Dabiq, Rumiyah, Al Risalah y Inspire) e intensos adoctrinamientos en centros de culto, prisiones y casas particulares. Hasta las reivindicaciones de atentados son una oportunidad para su apología salafista.

Repasar los atentados más relevantes llevados a cabo por ambos grupos terroristas o sus filiales, con especial mención al más brutal de todos y cuyo aniversario se ha cumplido hace poco más de tres meses, los atentados del 11-M en España, implica un gran esfuerzo por la brutal cantidad de víctimas y las formas tan sangrientas en que han sido abatidos: durante una tranquila cena en un tranquilo bistró parisino, en una discoteca de moda, en un aeropuerto, en el metro… en definitiva, en todos aquellos lugares donde las personas están más indefensas, donde es más previsible para los terroristas que puedan ser masacradas en mayor número y donde el impacto en los medios de comunicación del mundo entero puedan originar fuertes dosis de terror.

No hay muertes más violentas que otras. Todas son terriblemente crueles y violentas, pero algunas tienen la mala suerte de ser filmadas en un mundo plagado de sistemas de captación de imágenes, especialmente de smartphones, como la ejecución del policía francés de origen musulmán que es abatido cuando yace en el suelo, herido de gravedad, e implora a sus asesinos –quizá en árabe- que no le rematen, tras haber provocado una carnicería en una de las salas de reunión de la revista Charlie Hebdo, en enero de 2015.

Muchos de estos asesinos, como los hermanos Abdeslam, autores de atentados en París y Bruselas, se han criado en barrios de ciudades europeas, con más o menos suerte laboral, pero es difícil imaginar cómo puede haberse desarrollado en ellos tal nivel de odio hacia los pueblos que les acogieron. La evolución del terrorismo en Turquía es también otra sangrienta paradoja, pues tras haber hecho la vista gorda durante algunos años al tránsito de integrantes de Daesh a través de sus fronteras y de haberles apoyado discretamente, ha sufrido de 2003 a 2016 nada menos que 25 atentados con 593 muertos, sin incluir los producidos por el PKK. Sólo en 2016 se han registrado 300 muertos y cientos de heridos.

La llamada Primavera Árabe no parece haber conseguido sus propósitos de abrir la política de los países árabes a la democracia. Libia, Siria, son dos de los ejemplos de hasta dónde puede llegar el descontrol de los Estados, de las Instituciones, del salvajismo más descarnado asumido por grupos que se pretendían políticos y que probablemente son peores que los regímenes que han derrocado. En Túnez, sólo en los atentados del Museo del Bardo y del complejo turístico de Susa, los terroristas de Daesh han asesinado en 2015 a 61 personas y causado decenas de heridos, muchos de ellos turistas occidentales. Y la penetración de Al Qaeda en África no cesa. Bien el contrario, la lucha por la hegemonía se ha recrudecido en el Sahel, con países como Sudán, Chad, Níger, Malí o Mauritania, donde los europeos a duras penas pueden contener la hemorragia terrorista a base de importantes contingentes militares y actuaciones muy discretas pero intensas de los servicios de información occidentales.

Departamentos de Seguridad de las empresas

¿Cómo puede afectar la actividad terrorista de Daesh a los departamento

de Seguridad de las empresas? En algunas reuniones del sector financiero se han realizado formulaciones evaluadoras de la amenaza, desde considerar al sector como un objetivo no prioritario a considerar el terrorismo como la mayor amenaza posible tanto por la imprevisión de los criterios para la selección de objetivos, como por la brutalidad de sus atentados y, en consecuencia, establecer medidas de protección de personas, edificios y locales empresariales, a partir de la ecuación Amenaza= Intención + Capacidad. En vanguardia, la colaboración bidireccional con las Fuerzas y Cuerpos Policiales.

Carlos Vázquez, el siempre reconocido y fino analista director de Seguridad de Barclays, incluía en un reciente análisis de las amenazas derivadas de la actuación de estos grupos, que dentro de la Intención de Daesh se incluyen una clara sucesión de elementos estratégicos, como modificar la políticas de colaboración de los países occidentales, generar sobrerreacciones, aterrorizar a sus sociedades y «vender» entre sus seguidores una masacre como una acción de éxito. La capacidad se obtiene de los combatientes que cada día en mayor número retornan, los individuos de segunda o tercera generación que habitan los barrios marginales, la selección de objetivos fáciles («blandos») y mediáticos, la escasa financiación que requiere la ejecución de no pocos atentados, la inmolación y la estructura de las células terroristas, que no son lobos solitarios como se cree en muchos casos.

Antes de llevar a cabo un atentado, prosigue Carlos, los terroristas realizan algún tipo de reconocimiento para preparar sus planes de ataque, evalúan las probabilidades de que el lugar pueda ser atacado y determinar aquellos lugares más idóneos por la alta concentración de oficinas, comercios o público.

Cuando se inicia una agresión terrorista, indiscriminada, a unas instalaciones, entre los modelos de repuesta más consolidados a nivel internacional destacan tres: el modelo «Stay Safe» (Mantente a Salvo), de la National Counter Terrorism Security Office, que se resume en tres acciones: «Corre, escóndete, enfréntate». El modelo Stratfor: «Ser consciente de los riesgos, análisis del entorno y evacuación». Finalmente, el modelo asumido por el Ministerio del Interior español, una adaptación de los anteriores, que se resumen en: «Ser consciente de los riesgos (y preparar una serie de acciones), análisis del entorno (estar alerta para identificar una amenaza), corre (ante un ataque indiscriminado y muy violento), escóndete (para buscar protección si no es posible correr), alerta (si es posible, llamar a la Policía), enfréntate (de la manera más contundente posible, si no se consigue huir o esconderse) y actuación de las FFSSEE».

En relación con el último punto de la respuesta ante una acción terrorista, «Amok» en su jerga, el Ministerio del Interior convocó en julio de 2016 a los directores de Seguridad para trasladarles una serie de consejos de gran utilidad:

–Especial atención a la vestimenta (muy abrigado), así como a cuello, muñecas, manos y piernas.

–Congruencia, oportunidad y proporcionalidad en las intervenciones de los vigilantes de seguridad.

–Tener siempre presente la importancia del Jefe de Sala del 091 o Coordinador del 112.

–No colocar vehículos de la seguridad del recinto en los accesos al mismo.

–En caso necesario, protegerse utilizando el motor de los vehículos.

–Con el acceso de la Policía al lugar asaltado, policías y vigilantes nunca deberán retroceder, sino dirigirse hacia el lugar donde se encuentren los terroristas. Estos grupos no atenderán a los heridos, de los cuales se encargarán el personal adecuado.

–En caso de que en el transcurso de los disparos resulte herido un terrorista que lleve incorporado un chaleco con explosivos, no aproximarse por el riesgo de que se inmole.

–El estudio de los efectos de una explosión es valorado como uno de los medios más adecuados para minimizar los daños, por lo que será de gran ayuda determinar qué zonas pueden verse afectadas en función de los distintos tipos de cargas explosivas.

El riesgo de atentado yihadista en España siempre está presente a raíz de las declaraciones efectuadas tras las detenciones realizadas en los últimos meses por la Policía y Guardia Civil. Por ello, la sociedad española y europea deben ofrecerles la capacidad para hacer frente a cualquier acción terrorista mediante medidas efectivas de larga duración, que faciliten la por otro lado excelente labor realizada en la última década.

Fotos: Archivo.

Diccionario de Urgencia

- YIHADISMO: neologismo occidental utilizado para denominar las ramas más violentas y radicales del Islam político o islamismo.
- YIHAD: Lucha por Dios (también Guerra Santa).
- SALAFISMO: legitima la violencia contra los infieles. Interpretan con dureza el Corán y la Suna.
- SUNA: Código de comportamiento, la segunda fuente de la ley musulmana después del Corán.
- HADICES: Dichos y acciones de Mahoma, pilar fundamental de la Sunna.
- SHARÍA: Cuerpo de Derecho islámico (código detallado de conducta).
- JANNAH: Paraíso, lugar al que van los que se inmolan en las acciones terroristas.
- PRIMER GRAN ATENTADO: Líbano (241 militares norteamericano y 58 franceses, muertos).

FRANCISCO GUERRERO. DIRECTOR DE SEGURIDAD DE UNICAJA BANCO

Validaciones provisionales

Ley de Seguridad Privada. Ley 5/2014, de 4 de abril.

PARECE que es muy reciente, pero la nueva Ley de Seguridad Privada, Ley 5/2014, de 4 de abril, acaba de cumplir 3 años. Esta Ley sustituye a la 23/1992, que tras 22 años había quedado obsoleta, pero además de sustituirla da un giro importante a la normativa de seguridad privada, publicándose una norma más completa que la anterior, más extensa, con más detalle, y que regula nuevas situaciones.

Dentro de las novedades, llama la atención lo que la norma define como validaciones provisionales, o dicho de otra manera, la capacidad de validar provisionalmente hasta la inspección policial, otorgada a jefes y directores de Seguridad.

Al aparecer por primera vez en la Ley de 2014 podríamos pensar que estamos ante una función totalmente nueva, sin embargo estamos ante una idea antigua. Ya en agosto de 2003, en un artículo publicado en esta misma revista, expresaba que:

«… y en el caso de las entidades financieras, podríamos pensar que en un futuro, las autorizaciones de apertura y/o reforma de sucursales podrían realizarse con un certificado del director de Seguridad, como personal homologado por el Ministerio del Interior. Esto es, bastaría una notificación del director de Seguridad a la Subdelegación del Gobierno u organismo que se acuerde, de la intención de abrir una nueva oficina, y que se adjunte un certificado de que se ha procedido a la revisión de la sucursal, siendo las instalaciones de seguridad de éstas conformes a la normativa vigente. Las autoridades policiales inspeccionarán aquellas que entiendan interesante hacerlo, pero no como requisito imprescindible para poder aperturar y/o trasladar el centro …»

Once años después, esto es una realidad.

Sin embargo no se trata de una realidad pacífica ya que la norma contiene pasajes que necesitan ser aclarados. En este sentido, la norma diferencia la capacidad de validar dependiendo de si se es director de Seguridad o si se es jefe de Seguridad, y así, en el art. 36.1.e) se recoge como función del director de Seguridad:

«La validación provisional, hasta la comprobación, en su caso, por parte de la Administración, de las medidas de seguridad en lo referente a su adecuación a la normativa de seguridad privada».

Y en el art. 35.1.c) al referirse a los jefes de Seguridad expresa que es una de sus funciones:

«La propuesta de los sistemas de seguridad que resulten pertinentes, y el control de su funcionamiento y mantenimiento, pudiendo validarlos provisionalmente hasta tanto se produzca la inspección y autorización, en su caso, por parte de la Administración».

Esta distinción en el tratamiento debería ser aclarada. En una primera lectura y ateniéndonos al literal de la disposición, parecería una función obligatoria para los directores de Seguridad y potestativa para los jefes de Seguridad. En el primer caso no parece haber alternativa, y en el segundo se utiliza el término «pudiendo».

Igualmente, parece desprenderse de ambas redacciones que el director de Seguridad valida medidas de seguridad y el jefe de Seguridad valida sistemas de seguridad.

No queda claro cuál es la diferencia entre medidas de seguridad y sistemas de seguridad. La norma, sí realiza la definición de lo que hay que entender por medidas de seguridad. Concretamente su art. 2.5 define las medidas de seguridad como:

«las disposiciones adoptadas para el cumplimiento de los fines de prevención o protección pretendidos».

Y en su art. 52, diferencia entre los distintos tipos de medidas que se pueden adoptar:

– De seguridad física.
– De seguridad electrónica.
– De seguridad informática.
– De seguridad organizativa.
– De seguridad personal.

Sin embargo no aparece definido qué hay que entender por sistemas de seguridad; la norma hace muchas referencias: sistema de alarma, sistema de videovigilancia, sistema de cámaras, sistema de protección contra incendios, sistema de información, sistema de seguridad, y por último sistemas de recepción, verificación y, en su caso, respuesta y transmisión de alarmas, pareciendo desprenderse que se trata de un conjunto de elementos de seguridad individuales.

Así, por ejemplo, se podría concluir que un director de Seguridad podría validar provisionalmente la prestación de un servicio de escolta, y un jefe de Seguridad no, lo que no deja de llamar la atención ya que solo pueden prestar servicios de escoltas las empresas de seguridad homologadas en la actividad de protección personal, y sin embargo no están obligadas a contar con un director de Seguridad, restringiéndose su obligación a contar con un jefe de Seguridad.

> «La norma diferencia la capacidad de validar dependiendo de si se es director de Seguridad o si se es jefe de Seguridad»

Y hay más dudas de interesante resolución. ¿Puede un director de Seguridad autorizar la apertura de una empresa de seguridad de vigilancia, por ejemplo? Entedemos que la respuesta deber resultar negativa por imposibilidad de comprobación, es decir, para un director de Seguridad resulta imposible verificar determinados requisitos como los antecedentes penales de los administradores, o de la mercantil en su caso, o la existencia de uniformes que guarden similitud con el propuesto por la nueva empresa.

La Unidad Central de Seguridad Privada, a principios de marzo de este año, emitió un Informe al respecto de las validaciones provisionales, que incluía aspectos positivos como la elaboración de formularios con tal fin, con

instrucciones sobre su cumplimentación y entrega, y excepciones a las validaciones, concretamente se excepcionaban de ser susceptibe de validación provisional los servicios recogidos en los arts. 40.1.c) (servicios prestados en buques mercantes) y 41.2 (servicios que se prestan de forma coordinada con las Fuerzas y Cuerpos de Seguridad).

Sin embargo, incluye ciertos pasajes que generan dudas que antes del Informe no se tenían. De su literal, parece indicarse que hay que presentar formulario de validación provisional cumplimentado en los casos de adopción de medidas no obligatorias o reformas de establecimientos ya autorizados, cuando hasta la fecha del referido informe en estos casos solo se comunicaba la actuación a la unidad provincial de seguridad privada correspondiente, de conformidad con el art. 136 del Reglamento de Seguridad Privada.

Esta parte es la más relevante para los departamentos de Seguridad de entidades financieras, ya que donde antes solo había un trámite inocuo, comunicar las obras de reforma con afectación de medidas no esenciales, o la sustitución de un cajero automático ya autorizado por otro, ahora hay una subsunción de responsabilidades para el director de Seguridad que tendría que validar lo realizado, pudiendo incurrir en responsabilidades (sanciones) él personalmente y no la entidad, como ocurría anteriormente.

Desde un punto de vista práctico, sin entrar a valorar la validez jurídica de este cambio, un informe no puede cambiar una disposición legal, y sobre las premisas de que la validación provisional no es una función delegable por imperativo del art. 99 del Reglamento de Seguridad Privada, y que prácticamente todas las entidades estamos inmersas en migraciones masivas a grado III de los sistemas de seguridad de las sucursales, así como en la renovación de dispositivos sujetos a inspección como recicladores y cajeros automáticos, sería positivo que pudiera aclararse la actuación correcta por parte de los directores de Seguridad que nos podríamos encontrar en una situación de difícil salida.

Por un lado estaríamos obligados a validar todas estas actuaciones, que en el presente ejercicio y en los próximos pueden suponer cientos de validaciones, por otro lado no es una función delegable por lo que solo una persona por cada entidad puede realizarlas, y por otro es imposible hacer las validaciones mediante comprobación personal de los cambios, lo que obligaría a tener que validar a distancia, o lo que es lo mismo responsabilizarnos de una comprobación que no podemos realizar.

Alternativas hay, entiendo que para las nuevas aperturas, traslados de sucursales a otros locales o nuevas instalaciones de cajeros automáticos, las validaciones tal como están configuradas pueden ser una herramienta últil, pero para el resto de situaciones, si no puede seguir el régimen legal actual de primera y segunda comunicación, que es lo óptimo y nada hay que lo impida, se debería buscar una fórmula alternativa como que la validación sea solo de la documentación a aportar: certificado de instalación, certificado de anclaje en su caso, certificado de conexión con CRA, certificado de las pruebas con la CRA, homologaciones necesarias, etc., y no implique una validación a distancia.

Hay una buena sintonía entre la Unidad de Seguridad Privada y el sector, que seguro facilita una solución válida para todos los implicados, y es probable y deseable que el nuevo y futuro Reglamento de Seguridad Privada arroje más luz sobre procedimiento y requisitos de las validaciones provisionales, pero mientras tanto sería positivo tener claro qué podemos hacer en cada situación.

Recuerdo que finalicé mi artículo de 2003 con una cita de D'Alambert, permítanme finalizar este con una de Oscar Wilde apropiada para el presente «No existe una mejor prueba del progreso de la civilización que la del progreso de la cooperación». ●

SEGURIDAD

OPERADOR DE RPAS

DRONES

VIDEOVIGILANCIA

CONTROL DE ACCESOS

CENTRAL RECEPTORA DE ALARMAS

PROTECCIÓN CONTRA INCENDIOS

INSTALACIÓN Y MANTENIMIENTO DE SISTEMAS DE SEGURIDAD

CENTRO DE FORMACION DE SEGURIDAD

SISTEMAS INTEGRALES DE SEGURIDAD

SERVICIO DE ACUDAS Y CUSTODIA DE LLAVES

VIGILANTES DE SEGURIDAD

BUREAU VERITAS Certification

CYRASA

D.G.P. 3625

902 194 749 / C.R.A. 902 033 222
www.cyrasa.com / cyrasa@cyrasa.com

DEPARTAMENTO TÉCNICO DE HIKVISION

Videovigilancia inteligente, gana la banca y el cliente

EL sector financiero es probablemente el más vulnerable a amenazas en materia de seguridad. Por esta razón, fabricantes como Hikvision procuran adaptarse a sus necesidades especiales y ofrecerle soluciones completas y de confianza. La tecnología actual nos permite integrar funcionalidades inteligentes y, gracias a nuestros avanzados desarrollos, podemos cubrir con las mejores garantías todas las áreas de la sucursal bancaria, a pesar de las diferentes dificultades que presenta cada una de ellas.

La zona en la que se sitúan los cajeros automáticos cuenta con alto riesgo de robo. El sistema debe permitir una vigilancia discreta y ajustarse al entorno en el que se instalan. En el caso de las cabinas, situadas en el interior de la oficina bancaria, es aconsejable instalar una única cámara con gran angular que cubra todo el espacio. Para otro tipo de cajeros, los situados en el exterior, una óptica pinhole permite mayor discreción sin renunciar a una buena imagen. Por otra parte, los NVRs especiales para cajeros automáticos admiten la superposición de información de las transacciones para facilitar la identificación de eventos.

En la entrada de la oficina bancaria, nos encontramos con otros dos grandes retos en lo que a la seguridad se refiere: el tránsito de clientes y los grandes contrastes de luz que suelen producirse. A pesar de lo adversas que puedan resultar las condiciones, es importante contar con imágenes detalladas de los rostros. Para lograr la máxima nitidez se emplean cámaras con mayor amplitud de rango dinámico (hasta 140dB). En cuanto a calidad de imagen, según las características del proyecto y las preferencias del usuario, es posible contar con equipos de

Esquema de seguridad oficina bancaria

Entrada y vestíbulo

videovigilancia de hasta 4K. Además, es posible incorporar a estos equipos funciones inteligentes como la detección facial, intrusión en una zona, el cruce de una línea, detección de objetos abandonados, etc.

La actividad que se realiza habitualmente en una oficina bancaria supone un gran número de transacciones que incluyen desde la firma de documentos, retirada de efectivo, aprobación de préstamos… El área de ventanilla o mesas de atención al público donde se llevan a cabo todas estas operaciones también es un punto de interés cuando se trata de videovigilancia. Para captar las mejores imágenes, de ambos lados y en alta definición se emplean cámaras duales, con ajustes de lente independientes.

Tan importante como recoger toda esta información a través de las cámaras adecuadas en los diferentes puntos del establecimiento, es gestionarla y almacenarla de la forma más fiable y eficiente posible. Las plataformas, como nuestro software iVMS-5200, nos permiten visualizar, reproducir y controlar la totalidad de las operaciones diarias. Además del cliente de control, con todas las funciones de la plataforma (visualización en directo y reproducción, mapa electrónico, centro de alarmas, búsqueda por registros, etc.), estas plataformas ofrecen un cliente web y un cliente móvil para que todas aquellas personas autorizadas que lo precisen puedan acceder a determinadas funciones de control y seguimiento del sistema de CCTV: visualización en directo, reproducción, control de PTZ o configuración local. ●

Superposición de imágenes en cajero

Detección de intrusión.

Detección cruce de línea.

Detección objeto abandonado.

Detección objeto sustraído.

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

La combinación **ideal para la seguridad bancaria**

Plataformas de seguridad en cloud y detectores profesionales en Grado 3

EL sector bancario es uno de los que más riesgo asume en materia de seguridad, por ello exige unas medidas de cumplimiento obligatorio. Según la normativa del Ministerio del Interior del Gobierno de España, en cada entidad bancaria y demás entidades de crédito, tiene que existir un departamento de Seguridad que se encargue de la organización y administración de la seguridad de las mismas.

Dicha normativa obliga a que las entidades estén conectadas con una central de alarmas propia o ajena a los sistemas de seguridad implementados en los establecimientos y oficinas. Si por dificultades técnicas no se pudiese realizar la conexión, deberá situar en el lugar un servicio de vigilantes con personal perteneciente a empresas de seguridad.

Este sector se encuentra en una constante búsqueda de las soluciones más innovadoras del mercado. La normativa indica que no pueden ser sistemas estándar, ya que no son suficientes para todos los requisitos que demandan estas instituciones. Estos espacios precisan equipos especializados en seguridad integrada de Grado 3.

Para el sector bancario lo ideal es contar con una avanzada solución de seguridad de Grado 3 basada en la nube. Dicho sistema es recomendable que disponga de vídeo verificación con cámaras IP, que puedan ser controladas de forma remota a través de una aplicación para dispositivos móviles y a través de la interfaz web, proporcionando armar y desarmar el sistema, control de los distintos dispositivos de la instalación, y poder tener un control visual inmediato, así como recibir notificaciones.

Es recomendable también, que tenga una única plataforma hardware y que sea flexible y escalable en cuanto al número de zonas, es decir, que las empresas especializadas lo implementen en los espacios que sean necesarios y se pueda ir añadiendo según se vaya requiriendo.

Por otra parte, resulta indispensable tener instalados detectores específicos. Se debe contar con dispositivos sísmicos de alta seguridad que controlen las 24 horas la vibración y temperatura de la superficie protegida, detectando así cualquier tipo de ataque o intrusión.

En este tipo de instalaciones de máxima seguridad es importante implementar distintos tipos de tecnología para ampliar la cobertura de pro-

tección y tipologías de los equipos, utilizando detectores de movimiento, combinándolos con los de techo, que deben tener una lente gran angular de 110°, ya que así se puede cubrir un patrón de detección de campo visual de 360°, además de los pulsadores de emergencia. También es importante que todos los detectores de movimiento sean inteligentes, es decir, que incluyan las tecnologías de anti-enmascaramiento y anti-camuflaje, para que puedan percibir cualquier intento de manipulación por parte de los intrusos.

Todo ello es conveniente que esté instalado a través de una arquitectura súper híbrida que ofrezca cableado convencional, transmisión inalámbrica bidireccional y tecnología bus. Esta última, consiste en una arquitectura de cableado multipunto de 4 hilos para llegar a toda la instalación del sistema. Esta forma de instalación bus, hará que el cableado sea menor, que la instalación sea más rápida, y pudiendo realizar configuraciones y diagnósticos remotos, todo ello hace un importante ahorro en costes.

Además de todo esto, no hay que olvidar a la hora de seleccionar un equipo de seguridad, asesorarse por expertos que tengan experiencia en la implantación de sistemas idóneos para estos entornos y que respondan a las firmes exigencias del sector, ya que al más mínimo descuido los daños y repercusión que se pueden ocasionar son difíciles de restablecer.

En definitiva, bajo mi punto de vista, la mejor opción a la hora de adoptar medidas, en un sector donde la confianza y la seguridad de los bienes y las personas es tan importante, es poder disponer de la combinación de soluciones basadas en la nube junto con detectores profesionales específicos certificados según norma en Grado 3 de seguridad. ●

> «Para el sector bancario lo ideal es contar con una avanzada solución de seguridad de Grado 3 basada en la nube»

Fotos: Risco Group

ALFONSO MATA. DIRECTOR COMERCIAL DE SCATI

Viviendo el **futuro** de la seguridad bancaria

YA quedan lejos los días en los que el sector financiero en España, formado por decenas de bancos, cajas de ahorro, cooperativas de crédito y otras entidades, se limitaban a cumplir únicamente los mínimos exigidos por la reglamentación de seguridad.

Salvo grandes excepciones, estas entidades no reparaban demasiado ni en Seguridad Bancaria ni en tomar medidas en materia de seguridad electrónica. Tan sólo eran unas pocas las que implantaban medidas de seguridad y lo hacían sin la necesidad de explotar, supervisar y mantener el funcionamiento correcto de sus sistemas de seguridad.

Desde aquellos días, los riesgos, la normativa, la tecnología de sistemas y de comunicaciones, e incluso los procesos organizativos y estructurales de las empresas, han evolucionado y no siempre de forma sincronizada. Esta evolución también ha afectado a la figura del director de Seguridad que con el tiempo ha conseguido un posicionamiento fuerte dentro de su organización gracias a la combinación y la eficiencia en la gestión de personas, la operativa de la seguridad y el uso de la tecnología.

En cuanto a la evolución de los sistemas de seguridad hemos ido superando los distintos cambios de tecnologías, pasando de tener sistemas stand-alone, analógicos y sin comunicaciones o con comunicaciones basadas en la red telefónica tradicional, cuya transmisión de la información hoy vemos ineficiente; hasta tener una visión completamente distinta de la seguridad.

Una necesidad básica

Hoy, la seguridad es una necesidad básica. Un proceso transversal en el funcionamiento de cualquier entidad financiera en el que, la combinación y el uso eficiente de las tecnologías disponibles, la convierten en la herramienta más potente de optimización en la explotación y operativa con la que los responsables pueden agregar valor a sus organizaciones, facilitando información a otras áreas que jamás imaginaron.

En el momento actual, el director de Seguridad cuenta con multitud de sistemas, tecnologías y fabricantes que le aportan las piezas necesarias para abordar sus problemáticas, usando dispositivos en red que por tanto deben incorporarse de manera controlada en las infraestructuras de comunicaciones corporativas con el amparo de las áreas de TI.

Además no podemos olvidar cómo el factor económico influye actualmente en todos los procesos de decisión. En ocasiones las negociaciones de contra-

tación se desnaturalizan y se transforman en subastas que impiden tomar las decisiones más acertadas sin que el departamento de Seguridad pueda tomar parte.

Sin embargo, este hecho no es tan trágico cuando se cuenta con un sistema de seguridad profesional que garantiza un rápido retorno de la inversión; argumento imprescindible para que el director de Seguridad pueda liderar proyectos de inversión dentro de la entidad financiera.

Este sistema de seguridad debe tener la capacidad para ser flexible y adaptable; y debe permitir obtener economías de escala, optimización de procesos en el uso de las herramientas, reducción de tiempos de administración y ofrecer un valor añadido a otras áreas organizativas de las entidades.

Evolución de los sistemas de videovigilancia

Concretamente y entre todos los sistemas, merece la pena analizar cómo los sistemas de video vigilancia han evolucionado, hasta tener la vocación de ser una herramienta de valor y optimización de otros procesos dentro de la organización.

En cualquier oficina bancaria encontramos cámaras en los accesos, en el patio de público, en las ventanillas de atención, controlando los depósitos de efectivo, la caja fuerte, etc.

En todas esas ubicaciones la tecnología Megapíxel se ha impuesto y proporciona una calidad de imagen muy superior a su predecesora. Incluso en el acceso donde la pelea entre analógico e IP ha sido más larga y dura, ya vence con claridad las nuevas tecnologías y se protegen los accesos con cámaras de alta resolución, FullHD.

Estas cámaras son capaces de proporcionar una imagen nítida e identificativa incluso en las condiciones más adversas de iluminación. Pero en el enfoque que hoy necesita la Seguridad Bancaria, no es suficiente, se necesitan más justificaciones y la tecnología ofrece más alternativas.

«El director de Seguridad cuenta con multitud de sistemas, tecnologías y fabricantes que le aportan las piezas necesarias para abordar sus problemáticas»

Ya no sólo vale ver qué ocurre, grabar las escenas y poder recuperarlas con velocidad de descarga a través de la red en los centros de control de videovigilancia o las CRAs, ahora los dispositivos son capaces de se-

leccionar únicamente los rostros de las personas o contar los clientes que entran.

Para ello es imprescindible contar con un sistema de gestión de video capaz de gestionar esa información y de agregarla y presentarla de la manera más adecuada. Gracias a esta gestión eficiente del sistema, la inversión en seguridad ya no es vista únicamente como una obligación normativa sino que, bien explicada y consensuada con las áreas receptoras de estos nuevos beneficios, genera valor a las áreas comerciales y de negocio.

a las imágenes las transacciones que se efectúan en un cajero y reducir el tiempo de administración de una reclamación de un cliente, es un punto que el director de Seguridad debe poner en valor, ya que aquellos sistemas que tengan la capacidad de adaptarse a los requisitos de la entidad y, en este caso, sintonicen bien con las áreas de Seguridad Lógica y Medios de Pago, serán la apuesta ganadora.

En el caso específico de los cajeros, nuestros hermanos latinoamericanos nos llevan ventaja. Es tal el uso que se hace de ellos y existe tal diferencia en los riesgos en estos países, que las entidades financieras no han tardado en entender cómo la combinación e integración del video con el cajero o con herramientas de monitorización transaccional para la Prevención del Fraude, «se venden mejor» internamente y son las que generan el mayor valor a la organización.

El análisis de las imágenes para detectar situaciones y avisar de forma proactiva, el conteo de personas, los avisos real-time a los encargados del mantenimiento, la integración bidireccional de los sistemas de alarma y de video para la video verificación, el enlace del video y el cajero y con los sistemas de monitorización del fraude, son estrategias eficaces y a la vez imposibles sin el colaborador adecuado.

> «Los sistemas de video vigilancia han evolucionado, hasta tener la vocación de ser una herramienta de valor y optimización de otros procesos dentro de la organización»

Optimizar la inversión

Si nos fijamos en los cajeros automáticos, encontramos aplicaciones diferentes que tienen una filosofía similar, «optimizar la inversión». Poder asociar


shutterstock/jamesteohart

Solución End to End

El director de Seguridad de hoy sabe que la implantación de medidas de éxito en el ámbito de la videovigilancia, no es sólo seleccionar una serie de productos y colocarlos uno al lado del otro, sino que se utilice una solución «end-to-end» donde la responsabilidad en el diseño y la explotación del sistema esté claramente definida y tenga una visión de conjunto.

Si bien es cierto que no todos los sistemas disponibles tienen esa flexibilidad, es labor de los departamentos de Seguridad identificar aquellos que se adapten mejor a su realidad, que vayan a ser capaces de responder a la funcionalidad obligatoria y a la deseable, a la normativa de Seguridad y a la política corporativa.

Por ello es imprescindible contar con profesionales y partners que comprendan la singularidad de la Seguridad Bancaria frente a otras «seguridades». Empresas que tengan una clara orientación a «estos clientes» y que piensen en la maximización de la inversión y en las adaptaciones futuras. Porque todo puede volver a cambiar y ya está ocurriendo. ●

Fotos: Scati

Contactos de empresas, p. 7.

safire

HDTVI - HDCVI - AHD - CVBS

4N1

NUEVAS CÁMARAS ULTRA

- HD 1080P (1920x1080)
- WDR (12 FPS)
- 3D-NR, SenseUp, ATR
- Visión nocturna Starlight
- Menú OSD remoto

Encuentra tu distribuidor oficial en:

SAFIRE
www.safirecctv.com
info@safirecctv.com

safire

EL PROVEEDOR INTERNACIONAL DE PRODUCTOS DE VIDEOVIGILANCIA ESTÁ EQUIPANDO SUCURSALES BANCARIAS

Dahua lanza soluciones integradas de seguridad de vídeo para banca y finanzas

EN el sector bancario y financiero, donde millones de transacciones se procesan todos los días, la seguridad integral es esencial para protegerse contra el acceso no autorizado y las actividades delictivas. Es especialmente importante proteger las sucursales de los bancos contra los robos, los ataques y los intentos de fraude. Dahua, proveedor de soluciones en la industria global de vídeo vigilancia, ahora ofrece una gama de soluciones que satisface las exigencias bancarias y financieras con seguridad integrada de extremo a extremo en todos los escenarios de implementación, ya sea en el ATM, en el área de entrada o en el switch. La variedad tecnológica de Dahua abarca desde cámaras de vídeo para condiciones de recepción exigentes en la oscuridad o de alto contraste hasta centrales de seguridad, grabadores redundantes de vídeo y diversos mecanismos de alarma.

Protección integral

Dahua ofrece productos de seguridad para todas las áreas de una sucursal bancaria. Ya sea mantener una visión general de un vestíbulo bullicioso, supervisar zonas exteriores y el aparcamiento, o proteger mostradores y cajeros automáticos. La Solución Dahua para el sector bancario ofrece imágenes nítidas de alta resolución que garantizan una protección fiable. Una innovación tecnológica para destacar es, por ejemplo, la serie Starlight de cámaras Dahua, con un sensor más grande y capaces de proporcionar una detección muy clara, incluso con poca luz. **(Figura 1)**

Figura 1

Visualizar cada detalle en situaciones con una iluminación de alto contraste: 140db WDR

Dahua también tiene la respuesta perfecta a otras condiciones de luz difíciles. Un problema muy frecuente es, por ejemplo, un entorno con iluminación de alto contraste, en el que la cámara debe mostrar puntos muy brillantes y muy oscuros al mismo tiempo. La tecnología Dahua cumple estos requisitos para un rango dinámico extremadamente amplio a través de True WDR (Wide Dynamic Range) con hasta 140db. Gracias a 140dB WDR, las cámaras Dahua son capaces de proporcionar imágenes perfectas incluso desde el interior hacia afuera, alineadas a un acceso iluminado. Dahua utiliza una tecnología que toma dos imágenes con diferentes tiempos de exposición con el fin de superponerlas posteriormente. Por lo tanto, todos los elementos de la imagen siempre son perfectamente reconocibles, a pesar de la luz de fondo.

Centro de alta seguridad

Los expertos de Dahua también implementarán un moderno y confiable centro de seguridad en la sucursal bancaria, con un servidor central que asegura una completa seguridad de los datos. Los empleados del banco pueden rastrear, verificar y activar alarmas en caso de una emergencia. Si se de-

tecta una anomalía de red, Dahua garantiza una grabación adicional. En el caso de una desconexión de red, la señal de vídeo ya no se graba en los grabadores NVR centrales, sino en una tarjeta SD local. Además, varios grupos de grabadores NVR se pueden configurar de tal manera que uno esté siempre en modo standby. De esta manera, los registros no pueden perderse. **(Figura 2)**

Clara identificación de las personas

Las cámaras 4K y Ultra-Smart de Dahua tienen características de reconocimiento facial para asegurarse que cualquier individuo sospechoso y sus acciones sean claramente visibles. Así se pueden evitar incidentes. Al mismo tiempo, es posible pixelizar las caras de los clientes con el fin de proteger su privacidad.

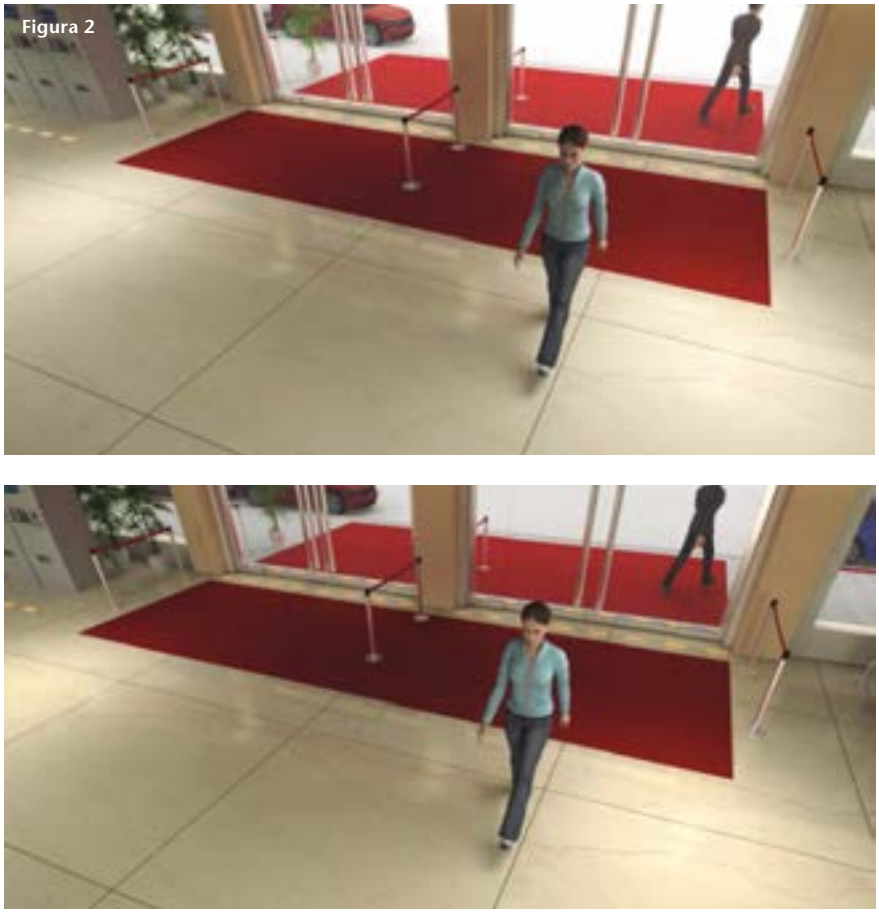
Detección VIP para una mejor experiencia del cliente

Para permitir que los bancos evalúen con mayor perfección el tráfico de sus clientes, y para que puedan proporcionarles un servicio correcto, Dahua también ofrece soluciones que incluyen posibilidad de conteo y de reconocimiento VIP basados en una plataforma DSS. Esto no sólo garantiza un aumento de la seguridad, sino que además, asegura una gestión más eficiente de la sucursal - el banco puede cumplir con los requisitos específicos del cliente de manera más específica y rápida. **(Figura 3)**

Instalación rápida y rentable

Las soluciones Dahua no sólo se caracterizan por la alta calidad de imagen y seguridad de los datos, también porque su instalación es muy asequible por su fácil manejo para usar en la infraestructura de red existente de la sucursal. Los productos Dahua pueden conectarse rápida y fácilmente a la antigua infraestructura, ya sean analógicos o digitales. Además, las soluciones Dahua se pueden combinar con una amplia variedad de otros sistemas. ●

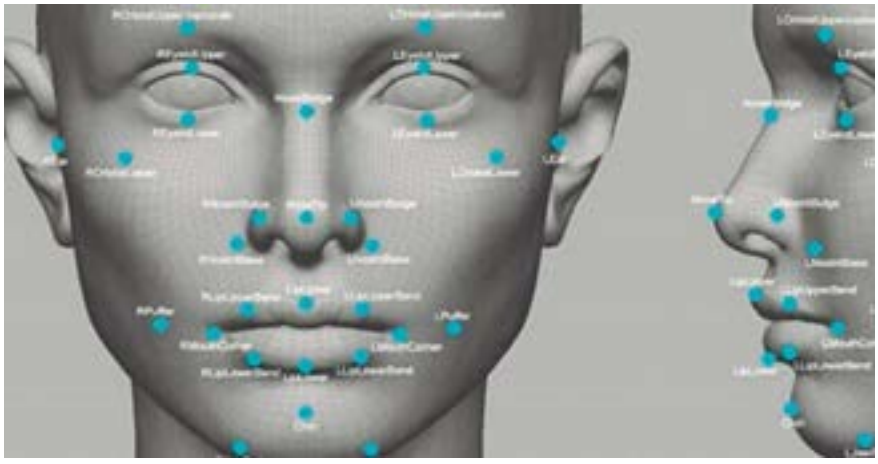
Figura 2



Fotos: Dahua

«Dahua ofrece productos de seguridad para todas las áreas de una sucursal bancaria»

Figura 3



Contactos de empresas, p. 7.

ESTUDIO «FINANCIAL INSTITUTIONS SECURITY RISK», DE KASPERSKY Y B2B INTERNATIONAL

La banca invierte tres veces más en seguridad que el resto de entidades no financieras

El 46% de los bancos reconoce que sus clientes son víctimas de intentos de phishing

LA inversión en seguridad es una prioridad fundamental para bancos e instituciones financieras, según se desprende del estudio Financial Institutions Security Risks de Kaspersky Lab y B2B International. Objetivo de ataques tanto su propia infraestructura como sus clientes, la banca invierte en seguridad TI hasta tres veces más que las empresas no financieras con una dimensión parecida. Más aún, el 64% de los bancos admite que invertirán en mejorar su seguridad TI sin tener en cuenta la rentabilidad, con objeto de satisfacer la creciente exigencia de organismos reguladores, alta dirección y también sus clientes.

A pesar de los importantes esfuerzos y elevados presupuestos invertidos en proteger sus perímetros ante ciberataques, proteger la infraestructura TI en toda su amplitud, ATMs y terminales de punto de venta, es bastante difícil. La enorme extensión y permanente evolución del panorama de ciberamenazas, unido al reto de mejorar los hábitos de seguridad de los clientes, supone para los cibercriminales poder contar con todavía más puntos débiles que poder aprovechar.

Riesgos emergentes: los ataques de ingeniería social a las cuentas bancarias

Los riesgos emergentes relacionados con la banca móvil aparecen destacados en el informe, como una tendencia que puede exponer a los bancos a nuevos ciberataques. El 42% de los bancos esperan que, en apenas tres años, una sobrecogedora mayoría de sus clientes usará la banca móvil, pero lamentan que los usuarios sean muy poco cuidadosos en su conducta online. La mayoría de los bancos entrevistados admite (46%) que sus clientes se ven muy frecuentemente atacados con intentos de phishing y el 70% de los bancos también reconoce que los intentos de fraude financiero terminan en pérdidas monetarias.

El creciente número de ataques de phishing e ingeniería social ha forzado a los bancos a reconsiderar sus esfuerzos de seguridad en esta área. El 61% de las respuestas ve en la mejora de la seguridad de aplicaciones y páginas web que sus clientes usan una de las principales prioridades en seguridad, seguida muy de cerca (52%) por la implementación de sistemas más complejos de autenticación y verificación de la información de acceso.

A pesar de su preocupación frente al phishing y otras herramientas usadas contra sus clientes, los bancos están mucho más preocupados por otro

«viejo enemigo», como son los ataques dirigidos. Razón no les falta, pues los ataques dirigidos se están convirtiendo en algo demasiado frecuente gracias a la creciente utilización de las plataformas de malware-como-servicio para atacarles.

Ataques dirigidos: amenazas permanentes

La experiencia alcanzada en incidentes reales nos muestra que la inversión en seguridad en el sector financiero, en la mayoría de las ocasiones, merece bien la pena. Las entidades financieras informan de menos incidentes de seguridad que compañías de tamaño parecido en otros sectores, con la única salvedad en ataques dirigidos y malware. La detención de actividad anormal y potencialmente maliciosa, que tiene lugar mediante la conjugación de herramientas legítimas con malware sin archivos, exige utilizar una combinación de avanzadas soluciones anti ataques dirigidos y una amplia información de seguridad. Aún así, el 59% de las empresas financieras todavía no ha implementado soluciones de información de amenazas de terceros.

Compartir información sobre amenazas ayuda a los bancos a identificar con rapidez todo tipo de nuevas y emergentes amenazas, un punto importante a tener en cuenta considerando los bajos niveles de preocupación de los bancos acerca algunos de sus dispositivos más vulnerables, como son los cajeros automáticos (ATM). Compartir más información de terceros, puede ayudar a los bancos a prepararse mejor ante las amenazas que no pueden prever.

Protección de los ATM: Bajo nivel de preocupación, alta vulnerabilidad

Los bancos muestran niveles de preocupación por las pérdidas financieras debidas a los ataques a cajeros electrónicos (ATM) muy bajos, a pesar de su alta vulnerabilidad frente a este tipo de ataques. Sólo el 19% de los bancos muestra su inquietud ante los ataques a estos equipos, y eso que su número es creciente (En el estudio de amenazas de 2016 encontramos un crecimiento en el malware de ATM de un 20% sobre 2015).

Alfonso Ramírez, director general de Kaspersky Lab Iberia: «Combatir la permanente evolución de las amenazas que se dirigen contra su infraestructura TI y las cuentas de sus clientes es un reto para las instituciones financieras. Ser capaces de poner en marcha una respuesta efectiva que proteja todos los puntos débiles, exige que las instituciones financieras cuenten con varios elementos clave: construir una protección altamente integrada frente ataques dirigidos, disponer de una seguridad antifraude multicanal, así como de información procesable sobre la evolución de las amenazas». ●

Fotos: Kaspersky Lab

TOM GANGOITI MEDINA. TECHNOLOGY ADVISOR. VISIOTECH

HD sobre coaxial en CCTV

Hace ya unos años que el HD, alta definición a partir de 720p, sobre cable coaxial es una realidad en el día a día de la videovigilancia; esperándose para 2018 que el 90% de las cámaras sobre coaxial sean HD.

COMENZÓ como una alternativa asequible y sencilla a las cámaras y videograbadores IP, permitiendo reutilizar las tiradas de cable coaxial del vídeo analógico convencional o CVBS, actualmente en extinción, e incorporando ventajas como la telemetría, control PTZ y acceso a menú, sobre el mismo cable coaxial. Todo ello con longitudes muy por encima de los

100 m del estándar en Ethernet con cable UTP para IP y sin latencia apreciable.

Evolucionando y adaptando estándares del mundo de la producción de vídeo como HD-SDI, en la actualidad las tecnologías HD principales son tres:

- HDCVI (High Definition Composite Video Interface), uno de los primeros en aparecer, pero exclusivo inicialmente del fabricante Dahua, con amplia presencia en Europa y América.
- HDTVI (High Definition Transport Video Interface), nacido algo después, mejorando lo existente y con el apoyo y la experiencia de más de 100 fabricantes, con líderes como Hikvision, TVT o Safire, con presencia mundial, especialmente en Europa.
- AHD (Analog High Definition), de posterior creación y normalmente con calidades menos depuradas, más extendido en algunas zonas de Asia.

El HD sobre coaxial se afianzó con los sensores de 2 megapíxeles y 1080p, la resolución FullHD, considerada básica en todo televisor y la ampliación de las distancias de trasmisión por encima de los 500 m, permitiendo el uso de baluns, transceptores de coaxial a UTP, específicos para HD.

Sin aún definirse el estándar que se mantendrá en tiempo, similar a lo que ocurrió en los regrabadores de DVD, que hubo DVD+R y DVR-R y que finalmente todos fueron DVD±R; en el HD sobre coaxial primero han sido las cámaras las que han adquirido la capacidad 4 en 1, es decir HDTVI, HDCVI, AHD y CVBS en una misma cámara. Pudiendo conmutar a la tecnología del videograbador, DVR, al instalarla, sin incremento de coste, facilitando el reemplazo y almacenaje de stock de cámaras.

Y desde hace unos meses, los videograbadores 5 en 1, a los que se pueden conectar cámaras HDCVI, HDTVI, AHD y CVBS sobre coaxial y cámaras IP, permitiendo usar básicamente cualquier cámara ya existente o las últimas y potentes novedades.

Esta capacidad 5 en 1 ha venido de la mano de la versión 3.0 de las tecnologías de HD sobre coaxial, que han aumentado la longitud de cable hasta los 1000 m para vídeo, permitiendo la alimentación sobre cable coaxial (PoC, Power Over Coaxial) y la trasmisión de las resoluciones de sensores de 3, 4 y 5 megapíxeles, superando el FullHD, por encima de muchas cámaras IP.

Por último, se puede afirmar que el futuro ya es presente, con las versiones 4.0 de HDTVI y HDCVI, ya en pruebas y disponibles en otoño de este año, que coincidiendo con el 4K (4 veces 1080p), cada vez más común y asequible en pantallas y monitores, permiten transportar resoluciones de 8 Mpx, aumentando las distancias de transmisión de vídeo sobre coaxial por encima del kilómetro.

Sin duda el HD sobre coaxial ha significado la revolución del CCTV y aún está en marcha, permitiendo actualizar instalaciones existentes, dotando de la más moderna tecnología a todas, distancias de cable antes inimaginables, sin preocupaciones sobre qué tecnología escoger gracias a los dispositivos con todos los estándares en uno y sobre todo con la sencillez que implica el uso profesional del cable coaxial. ●

Fotos: Visiotech

«El HD sobre coaxial ha significado la revolución del CCTV y aún está en marcha, permitiendo actualizar instalaciones existentes»

Contactos de empresas, p.7.

Técnicas de compresión en CCTV

Ahorro en Ancho de Banda

La tecnología Smart Compression de Pelco reduce el ancho de banda, y los requerimientos de almacenamiento hasta en un 70%, mientras que mantiene la calidad de imagen y la información crítica para un posterior análisis forense. Entre sus beneficios se incluyen los siguientes: menor capacidad de almacenamiento necesaria y alta resolución. Todo ello por medio de una simple actualización de firmware, lo que le ayudará a proteger su inversión sin sacrificar la calidad.

Reducción en el coste del almacenamiento

Pongamos un ejemplo, si usted tiene un pequeño negocio como una tienda o una oficina bancaria, con algunas cámaras de 3Mpx que requieren almacenamiento 24/7 durante 30 días a 15 IPS, sin Smart Compression necesitará hacer una inversión sustancial en almacenamiento.
Con Smart Compression todo cambia; las cámaras analizarán de manera dinámica y en tiempo real la cantidad de movimiento que hay en la escena, y comprimirán de manera inteligente la información que usted no necesita, mientras que mantendrán un gran nivel de detalle en las partes de la escena que más interesan.

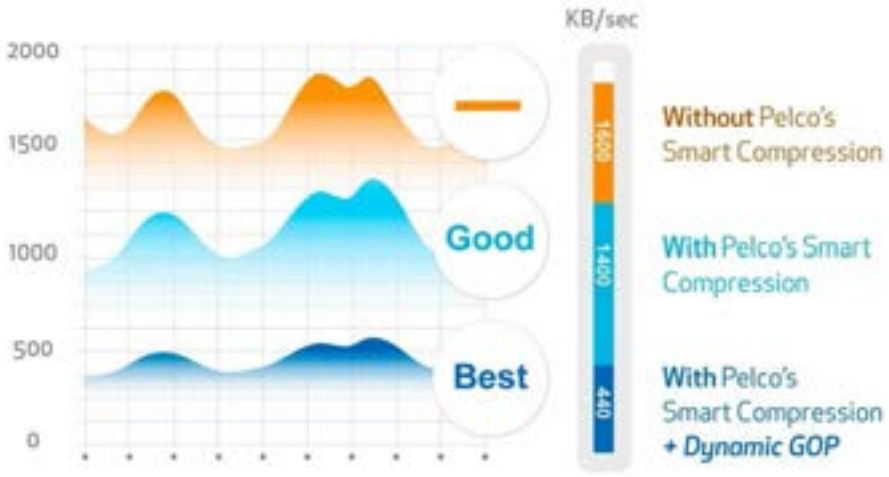
PELCO
by Schneider Electric

Choose with Confidence.

¿Cómo funciona?

La tecnología Smart Compression H.264 de Pelco identifica de manera dinámica el movimiento que se produce en las escenas qu está capturando la cámara, y mantiene los detalles de la escena con alta calidad para que no haya ningún tipo de degradación en el video recibido por parte de la cámara.

Las áreas de la escena en las que no hay movimiento reciben mayores niveles de compresión, reduciendo así el ancho de banda mientras que se mantiene la información crítica.



Cuando se activa la opción “Dynamic GOP Length” (Longitud del Grupo de Imágenes Dinámica), el número de I-Frames será variable, reduciéndose en los intervalos en los que el movimiento en la escena sea menor (como por ejemplo en el interior de un almacén), obteniendo como resultado un ancho de banda todavía menor.

En función de la complejidad de las escenas y del movimiento que se produzca en ellas, se puede conseguir una reducción aproximada de entre el 30% y el 70% en el ancho de banda.

Beneficios de Smart Compression

- Compresión Inteligente = Requerimientos de Almacenamiento Reducidos
  - Comprime más el fondo estático, menos las áreas con más movimiento.
  - El Intervalo de Imágenes I aumenta en las escenas con poco movimiento. Sin degradación del video con movimiento.
- Configuración Intuitiva = Mantiene la Experiencia del Usuario.
  - Se configura de manera intuitiva y sencilla en la interfaz web de la cámara
- Coste de Almacenamiento Reducido = ROI mejorado.
- Compatible con Pelco Video Xpert y con las plataformas VMS de otros fabricantes líderes del mercado
- Disponible en las series de cámaras Spectra Enhanced, Sarix Enhanced, Sarix Professional y Optera a través de una actualización de firmware sencilla y gratuita.

Spectra Enhanced

Sarix Professional / Enhanced

Optera

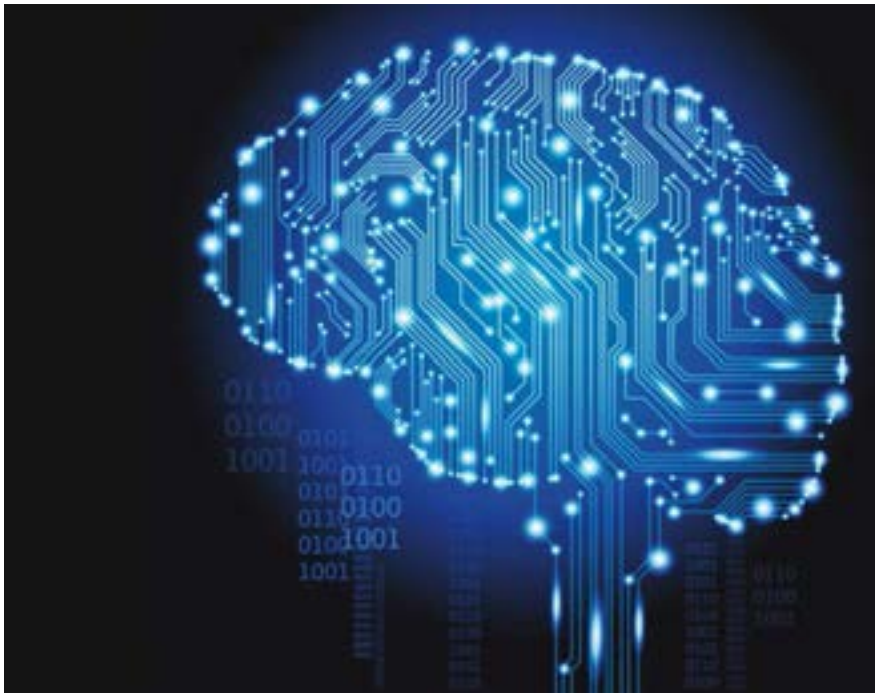
Contáctenos en pelco.iberia@schneider-electric.com
y visite pelco.com para descargar la documentación técnica.

JORDI ALONSO. JEFE DE PRODUCTO DE CCTV. CASMAR

«Deep Learning», un gran salto cualitativo

Últimamente mi teléfono móvil me sorprende prediciendo hacia dónde voy cuando me subo al coche, no sé si me gusta o me da miedo..., salgo de la oficina, me subo al coche e inmediatamente mi teléfono me lanza un mensaje diciéndome a dónde voy, cómo está el tráfico en mi ruta habitual y estimando el tiempo restante hasta llegar a casa. ¿Cómo sabe dónde vivo? Yo no se lo he dicho. Es más, ¿cómo sabe que me acabo de subir al coche?

LA Inteligencia Artificial, programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, hace tiempo que está entre nosotros y nos facilita la vida sin que en muchas ocasiones lo lleguemos a apreciar. Google o Facebook utilizan algoritmos que aprenden qué temas te interesan para incluir más tarde publicidad que pueda ser de tu interés. Todos hemos sido «víctimas» de este hecho y es posible que alguna vez te hayas preguntado cómo lo hacen.



Hoy en día, las aplicaciones que utilizamos recopilan datos sobre los usuarios para darnos una experiencia más satisfactoria. Los avances actuales han sido posibles gracias a unos algoritmos cada vez más sofisticados, a la mayor capacidad de proceso y a la presencia del Big Data, es decir, a la cantidad tremenda de información recopilada gracias a internet.

Netflix, por ejemplo, me recomienda películas que efectivamente me interesa ver, y lo hace gracias a esa capacidad de «aprender» qué tipo de películas me interesan. Las aplicaciones cuentan con inteligencia para reconocer los gustos y costumbres de sus usuarios: qué les gusta ver o escuchar, qué lugares frecuenta con regularidad, qué comida le gusta o cuál es la ruta frecuente para ir al trabajo.

Por otro lado, está el desarrollo de Deep Learning basado en sistemas de redes neuronales artificiales, que son capaces de emular la forma de aprendizaje de los niños.

Las aplicaciones que tiene la Inteligencia Artificial son infinitas: desde

funciones simples que ya conocemos hoy día, como el reconocimiento de huella digital, facial o de voz, hasta la posibilidad de hacer diagnósticos médicos asistidos a través de máquinas que sean capaces de interpretar radiografías o cualquier otra prueba médica. No es que Skynet de la famosa saga Terminator sea ya una realidad, pero vamos camino de conseguir algo parecido.

Todas las empresas de tecnología e innovación tienen previsto integrar la Inteligencia Artificial en sus desarrollos y el mundo de la seguridad no es distinto en este aspecto. La principal aplicación en nuestro sector será el video-análisis, permitiendo mejorar de forma muy sustancial la fiabilidad y rendimiento de estos sistemas. Detección de Intrusos y Reconocimiento Facial mucho más precisos o Sistemas LPR capaces de reconocer marca, modelo y color del vehículo, son solo algunas de las aplicaciones en las que ya se está trabajando con esta nueva tecnología y para las que se esperan importantes avances en los próximos meses.

Jirsak / Shutterstock

Aún habrá que esperar algún tiempo para poder ver el resultado final del trabajo de los desarrolladores, pero promete resultados nunca vistos hasta ahora.

Fotos: Casmar

JOSÉ LUIS ROMERO. DIRECTOR GENERAL PARA ESPAÑA DE HANWHA TECHWIN EUROPE

La nueva tecnología de videovigilancia

Un retorno mucho mayor de la inversión para el usuario final.

Los chipsets DSP integrados en las cámaras de videovigilancia de alta definición para redes IP, de última tecnología, ofrecen un nivel de funcionalidad inimaginable hasta hace solo unos pocos años. Esto se debe en parte a los importantes avances en tecnología que han dado como resultado la fabricación de chipsets «superpotentes». También se debe a que los fabricantes de primera línea como nuestra compañía han comprendido el valor que conlleva estar cerca de los clientes para garantizar la cobertura permanente de sus necesidades y los requisitos cambiantes del mercado. Veamos las principales tecnologías y los beneficios que aportan.

El núcleo con un rendimiento excepcionalmente elevado de los chipsets más recientes funcionan al doble de velocidad que las antiguas generaciones de chipsets. Esto les permite procesar vídeo de manera mucho más rápida, e igualmente importante, tienen la posibilidad de ejecutar aplicaciones de analítica especializada de terceros integrada en la cámara como, por ejemplo, ANPR, analítica de audio y gestión de colas. En determinados mercados verticales, como el comercio minorista, los usuarios le pueden sacar mucho más partido de sus cámaras, más allá de la función tradicional y habitual de disuadir y detectar actividades delictivas. Las dos principales son mapas de calor y conteo de personas.

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

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

Analíticas más diversas

Los nuevos chipsets superpotentes también incluyen una función de análisis de audio que reconoce sonidos críticos como, por ejemplo, disparos de pistolas, explosiones, gritos y cristales rotos, e inmediatamente produce una alarma.

Memoria RAM de 512 GB

Algunas cámaras disponen de dos ranuras para tarjetas de memoria SD. Estas ofrecen una capacidad de memoria de hasta medio Terabyte (512 Gbytes) de almacenamiento de grabación continua en la propia cámara. Opcionalmente, la segunda ranura podría utilizarse para reproducir mensajes promocionales, que han sido previamente cargados en una tarjeta de memoria SD.

WDR avanzado y compensación de luces puntuales (HLC)

Las cámaras de última generación funcionan con una relación de contraste de aproximadamente 150 dB respecto al WDR (amplio rango dinámico), lo que garantiza que todo lo que aparece

en la escena pueda verse claramente, incluso cuando ésta incluye zonas muy brillantes y muy oscuras.

Normalmente una imagen de amplio rango dinámico (WDR) se forma combinando 2 capturas con distintas exposiciones. La nueva tecnología WDR de 150 dB, que utiliza 4 capturas para crear una imagen más natural, ha sido desarrollada para eliminar el desenfoque, que es una debilidad crítica del WDR existente, proporcionando así imágenes claras y vistosas.

Junto con la tecnología de compensación de luces puntuales (HLC), que identifica y neutraliza zonas excesivamente brillantes de la imagen, el WDR avanzado elimina los problemas de contraluces. La compensación de luces puntuales (HLC) es una función particularmente valiosa para la lectura de números de matrículas de vehículos por la noche.

Sensor giroscópico mejorado para estabilizar las imágenes

La estabilización de las imágenes ha mejorado sensiblemente con la introducción de los sensores giroscópicos. Esto mejora el rendimiento de la cámara al negar el efecto de las vibraciones producidas por máquinas, vehículos en movimiento y condiciones meteorológicas adversas como viento fuerte.

Una tecnología de compresión complementaria

La última generación de cámaras Full HD y 4K puede convertirse en una solución cara cuando el usuario final necesita almacenar vídeos de alta resolución con fines operativos o como prueba pericial. Esto se debe a que las imágenes multipíxel de alta definición pueden llegar a consumir demasiado rápido el espacio de almacenamiento disponible en un NVR o servidor cuando se graban a una resolución y frecuencia de cuadro completas.

El coste de un sistema de videovigilancia puede aumentar considerablemente si la instalación cuenta con un gran número de cámaras de alta definición. Además de la inversión que hay que hacer en NVR y servidores de almacenamiento, los costes recurrentes del consumo energético de los discos duros, las unidades de aire acondicionado de apoyo y el mantenimiento continuo pueden ser importantes.

Asimismo, a las empresas con políticas respetuosas con el medio ambiente les preocupa el impacto medioambiental y la sostenibilidad de los sistemas que consumen grandes cantidades de energía.

Costes operativos

La reciente tecnología de compresión complementaria disponible controla de forma dinámica la codificación, equilibrando la calidad y la compresión de acuerdo al movimiento en la imagen. Cuando esto se combina con la compresión H.265, la eficiencia del ancho de banda puede mejorar hasta en un 99 %, en comparación con la actual tecnología H.264, garantizando que las cámaras no consuman excesivamente el ancho de banda disponible.

Al reducir los requisitos de almacenamiento de vídeo con la ayuda de las cámaras con compresión H.265, los usuarios también reducen la inversión de capital y los costes operativos de los dispositivos de grabación y almacenamiento necesarios para sacar el máximo provecho a las excepcionales imágenes que capturan las cámaras de alta definición.

Máximo retorno de la inversión

Es una situación en la que todas las partes salen ganando y, sobre todo, los fabricantes de cámaras y dispositivos de grabación, como Hanwha Techwin, que han comprendido la necesidad de incorporar las técnicas de compresión más recientes a sus productos y que, al hacerlo, permiten que los usuarios obtengan el máximo retorno de sus inversiones en soluciones de videovigilancia.

Con el integrador de sistemas en mente

Es probable que la última generación de cámaras reciba una gran acogida por parte de los instaladores, así como de los usuarios. Utilizando un puerto USB integrado, podrán conectarse a dispositivos móviles vía WiFi, para permitir la inmediata revisión de los ángulos de visionado durante la instalación de las cámaras. ●

Fotos: ***Hanwha Techwin***

Contactos de empresas, p. 7.

DEPARTAMENTO DE MARKETING. LSB, S.L.

Tecnologías y funcionalidades adicionales de las cámaras IP

Las cámaras de video vigilancia IP, presentes en el mercado desde hace aproximadamente 17 años, han sufrido una notable evolución, principalmente en lo relativo a resolución de los sensores, desde las resoluciones de 320x240 ó 640x480 (0,07 Mp ó 0,3 Mp) en las que hoy día como estándar se manejan los 1920x1080 (Full HD) o cámaras de 3, 5, e incluso 12 Mp.

LAS tecnologías han ido mejorando y progresando añadiendo algunas innovadoras para dar unos resultados de mayor calidad de imagen, a la vez que tratan de aprovechar de la mejor manera posible los recursos disponibles en la red, que también han ido creciendo con el tiempo.

Además las tecnologías de compresión de imagen o video que han ido surgiendo MJPEG, MPEG-4, H.264, y actualmente H.265, siempre han tratado de que los resultados del video suministrado sea de igual o superior calidad pero ocupando un ancho de banda inferior que el sistema precedente, y reduciendo notablemente las necesidades de almacenamiento.

En el presente artículo vamos a esbozar algunas tecnologías que junto a lo ya expuesto son actualmente básicas en el desarrollo IP.

Algunas de las tecnologías implementadas en las cámaras IP son:

- Sistema de Enfoque Inteligente.
- Tecnología WDR.
- Suprema Visibilidad Nocturna (SNV).

Sistema de Enfoque Inteligente (Smart Focus System)

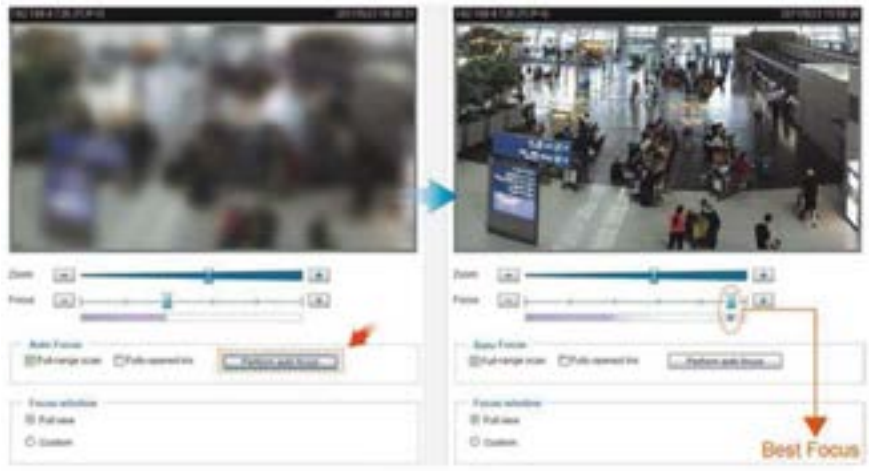
En muchas aplicaciones, las cámaras de vigilancia deben instalarse en lugares poco accesibles muy por encima del suelo, a fin de evitar manipulaciones y asegurar que tengan una visión amplia y sin obstrucciones del área a monitorizar. A menudo es difícil y requiere mucho tiempo realizar la instalación, porque las cámaras utilizadas normalmente para tales aplicaciones también requieren que el enfoque se establezca manualmente, un proceso que introduce la posibilidad de error y que requerirá acceso físico a la cámara para la ronda de configuración de enfoque.

Naturalmente, cualquier mantenimiento que se realice en tales cámaras después de su instalación requiere tiempo y mano de obra experta. Esto puede ser un problema particular para las cámaras al aire libre, como las utilizadas para luchar contra el vandalismo o el robo, debido a su exposición a grandes y rápidas fluctuaciones de temperatura.

Estos extremos en la temperatura hacen que los componentes de la cámara construidos con diferentes materiales se expandan y compriman de forma desigual, lo que provoca una pérdida de enfoque, que debe reajustarse manualmente en el caso de cámaras de vigilancia convencionales. En algunas situaciones, puede ocurrir en cuestión de días un deterioro notable en el enfoque.

Cuando una instalación tiene un gran número de cámaras desplegadas al aire libre, el mantenimiento de un enfoque óptimo para asegurar una vigilancia eficaz puede suponer que los gastos generales sean muy significativos en términos del tiempo adicional

Imagen 1



y de recursos de mano de obra necesarios.

Para superar estos inconvenientes, el fabricante Vivotek de sistemas IP, ha desarrollado un sistema de enfoque inteligente. Un sistema de enfoque inteligente puede consistir en varios elementos. El centro de este sistema es una utilidad de enfoque remoto, que permite a los usuarios ajustar el enfoque de la cámara de forma remota. Con la ayuda de una lente con motor paso a paso, un usuario puede hacer ajustes para enfocar sin acceso físico a la cámara.

Esta funcionalidad básica se puede aumentar para proporcionar características adicionales o mejorar las utilidades para el usuario. Por ejemplo, una capacidad avanzada de enfoque remoto proporciona la flexibilidad para mantener automáticamente el enfoque adecuado al acercar o alejarse, garantizando una calidad de imagen adecuada a medida que se cambia la longitud focal o cuando se requiere un campo de visión específico. Además de reducir la sobrecarga de mantenimiento de las cámaras de vigilancia, el enfoque remoto ofrece una forma muy eficaz de ajustar la vista de una ubicación monitorizada mientras cumple con los requisitos de resolución específicos.

La flexibilidad de un sistema de enfoque inteligente también permite disponer de algunas potentes funcionalidades adicionales. Por ejemplo, se podría proporcionar una característica para permitir a los usuarios definir una región de interés en el campo de visión de la cámara al establecer una ventana de enfoque en la interfaz. A petición del usuario, el sistema puede calcular un valor de enfoque basado en las dimensiones de la ventana de enfoque, proporcionando automáticamente la mejor calidad de imagen posible.

Es posible un tipo diferente de optimización con ayuda de enfoque integrado en un sistema de enfoque inteligente. Una función de asistencia de enfoque en el que se agrega un indicador gráfico y numérico del valor de enfoque actual, lo que facilita el ajuste fino del enfoque. Esta capacidad es especialmente valiosa en cámaras de megapíxeles de alta resolución, debido a que su amplio campo de visión y alto nivel de detalle hacen difícil distinguir en una pequeña pantalla de monitorización si un objeto o persona de interés está completamente enfocado o no.

Imagen 2

Un ejemplo de fabricante que se mueve agresivamente para adoptar sistemas de enfoque inteligente en sus cámaras es la compañía mencionada líneas más arriba. La implementación de esta compañía de un sistema de enfoque inteligente incluye todos los elementos descritos anteriormente: enfoque remoto, ventanas de enfoque y asistencia de enfoque.

Enfoque remoto - Lente con motor de paso Iris

La capacidad de enfoque remoto de la citda compañía está disponible a través de una interfaz de navegador

Imagen 3

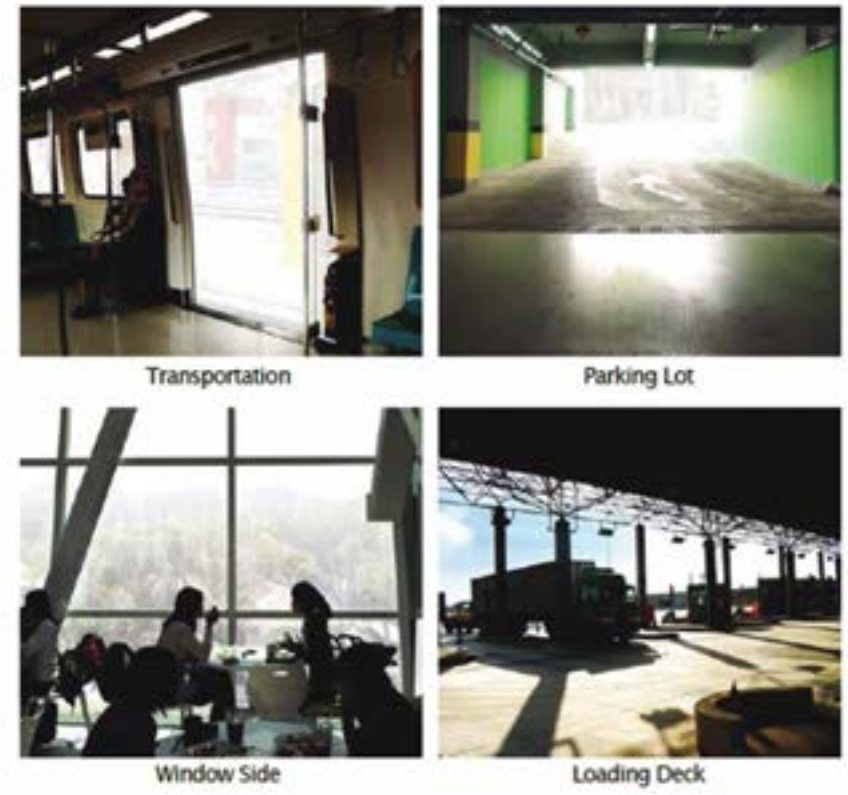
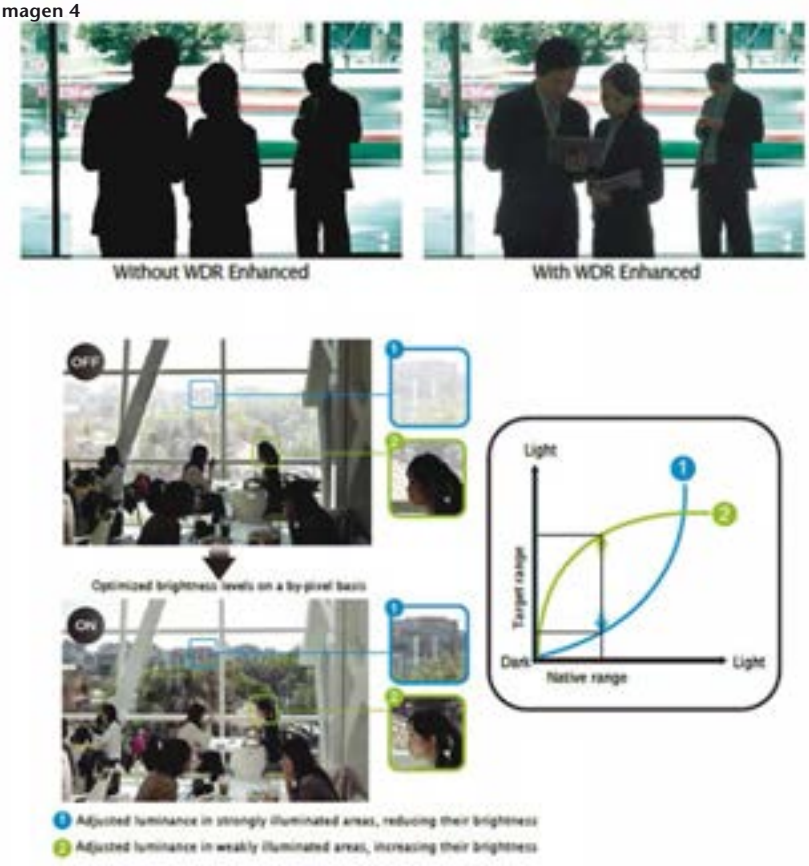


Imagen 4



«La funcionalidad WDR proporciona imágenes de alta calidad incluso cuando hay simultáneamente áreas muy brillantes y muy oscuras»

web. Los usuarios pueden manipular un control deslizante para ajustar el enfoque, con las opciones de enfoque automático también accesibles en la misma ventana. La capacidad de cambiar la configuración de zoom se controla para mayor comodidad con otro control deslizante situado justo por encima del control deslizante de enfoque, ya que los ajustes en los dos se realizan de forma consecutiva.

Se recomienda ajustar primero el zoom múltiple al valor deseado, lo que determinará la distancia focal. A continuación, haga clic en el botón «Realizar el enfoque automático» y el valor de enfoque óptimo se establecerá automáticamente, con la barra deslizante de enfoque reflejando cualquier cambio realizado dinámicamente. **(Imagen 1)**

Enfoque remoto: definición de una región de interés en la ventana de enfoque

Los usuarios pueden establecer un valor de enfoque explorando todo el campo de visión o definiendo una región de interés. Si se elige esta última opción, la región se puede establecer arrastrando un rectángulo o introduciendo el número de píxeles de ancho y altura en los campos proporcionados en la interfaz del navegador web. El primero proporciona una manera intuitiva y rápida de definir la región de interés, mientras que el segundo es particularmente útil cuando se desea una resolución específica.**(Imagen 2)**

Tecnología WDR

La visión humana tiene un rango dinámico muy alto *, lo que nos permite ver tanto con la luz de las estrellas como con el sol brillante. Aunque es difícil alcanzar el rango dinámico completo experimentado por los seres humanos con la tecnología de imagen en equipos electrónicos, tales como cámaras de video, se han desarrollado varios enfoques conocidos colectivamente como tecnología de rango dinámico amplio (WDR), en el caso de cámaras permiten representaciones más exactas de la gama de niveles de luminancia que se encuentran en los entornos del mundo real.

La funcionalidad WDR proporciona imágenes de alta calidad incluso cuando hay simultáneamente áreas muy brillantes y muy oscuras en el campo de visión de la cámara.

La tecnología WDR permite a la cámara capturar escenas de alto contraste de modo que los detalles sean claramente visibles a lo largo del fotograma en la imagen fija final o en el video.

La tecnología WDR está comúnmente incorporada en cámaras usadas para aplicaciones de vigilancia. La tecnología permite a una cámara capturar claramente las características detalladas, incluso cuando una persona o un objeto de interés aparecen en lugares donde hay una iluminación a contraluz fuerte, como al aire libre durante el día o frente a la iluminación artificial por la noche. La funcionalidad WDR está especialmente recomendada para las cámaras que se utilizan en la monitorización de lugares donde la luz entra

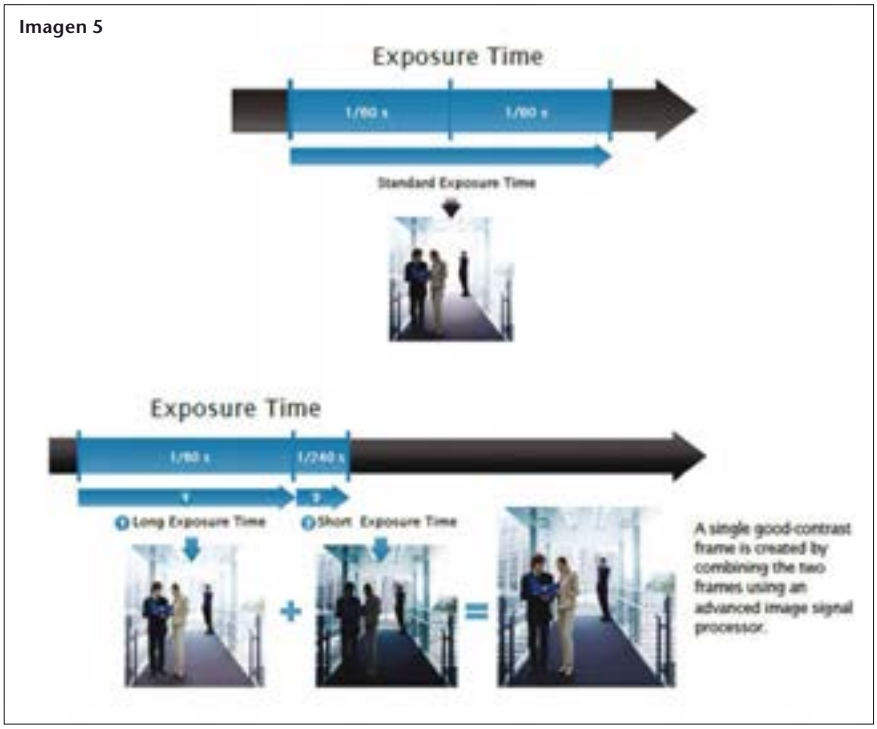
Techco security

Solutions beyond Security

900 77 77 80

Inscripción Registro D.S.E. Nº2979

Imagen 5



desde múltiples direcciones, asegurando que en cualquier ángulo de la cámara aparezca una persona u objeto de interés, se puedan obtener suficientes detalles para una identificación fiable. Ejemplos de lugares donde normalmente prevalecen las condiciones de iluminación de alto contraste son entradas de edificios, cajeros automáticos, instalaciones de transporte y cualquier espacio interior con ventanas. **(Imagen 3)**

El proveedor de soluciones de vigilancia Vivotek ha implementado una amplia gama de tecnologías WDR basadas en el mapeo de tonos y la generación de imágenes multi-frame para sus cámaras.

WDR Enhanced (WDR Mejorado) es la marca de esta compañía para su tecnología de mapeo de tono, reduciendo el rango dinámico de toda la imagen, manteniendo el contraste de la imagen. WDR Enhanced se basa en la investigación sobre cómo el ojo humano y la corteza visual realmente perciben una escena para lograr un resultado final que imita de cerca lo que la gente realmente puede ver.

La mejora de WDR produce resultados superiores en comparación con la compensación de retroiluminación convencional (BLC), porque BLC se basa en la evaluación automática del brillo en el centro del campo de visión. Si los niveles de iluminación son demasiado bajos, se eleva el brillo de todo el cuadro de video. La desventaja de este enfoque es que las áreas en el campo de visión que originalmente estaban bien iluminadas pueden quedar sobreexpuestas.

La mejora de WDR rectifica esta deficiencia de BLC ajustando la curva de tono uniformemente basada en los niveles de brillo en diferentes áreas del campo de visión, iluminando zonas oscuras y atenuando áreas excesivamente iluminadas para aumentar la visibilidad en todo el campo de visión.**(Imagen 4)**

Esta empresa también ofrece WDR Pro, que se basa en su implementación de imágenes multi-frame. WDR Pro funciona al capturar simultáneamente dos o tres imágenes del campo de visión a diferentes niveles de exposición. Una imagen con un tiempo de exposición más largo puede capturar más detalle en las áreas menos iluminadas en el campo de visión, aunque las áreas más brillantes pueden estar sobreexpuestas. Una imagen con un tiempo de exposición más corto, por otro lado, capturará con mayor precisión las áreas más brillantes, pero puede dejar las áreas menos iluminadas bajo exposición.

Un procesador de señales de imagen utiliza un algoritmo sofisticado para combinar sin problemas las imágenes «largas» y «cortas» en un solo marco de video que preserva el detalle en áreas más oscuras y brillantes del campo de visión. Además, debido a que el rango dinámico efectivo del video se amplía, la relación de contraste se mejora, acentuando aún más la claridad de detalle. **(Imagen 5)**

WDR Pro II es la próxima generación de WDR Pro, llevando la tecnología un paso más allá al capturar cuatro imágenes a cuatro niveles de exposición distintos. Este avance permite que las cámaras que incorporan WDR Pro II optimicen la calidad de imagen incluso para diferencias relativamente modestas en los niveles de iluminación. El resultado final es aún más detallado, en todo el campo de visión. **(Imagen 6)**

Debido a estos atributos, WDR Pro es una tecnología extremadamente valiosa para cualquier entorno de vigilancia.

WDR Pro II, en particular, asegura que cualquiera que sean las condiciones de iluminación presentes en un lugar monitorizado, o cómo un objeto o persona de interés se encuentra en relación con la cámara y las fuentes de luz, puede ser capturado un alto nivel de detalle y compuesta una imagen para una identificación positiva, un seguimiento preciso y otras aplicaciones exigentes. **(Imagen 7)**

Reducción de ruidos 2D/3D

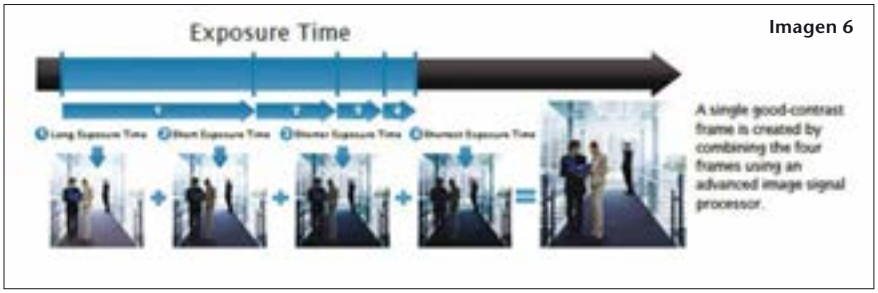


Imagen 6

En el contexto del vídeo, la distorsión de la señal -conocida más coloquialmente como «ruido» -puede adoptar la forma de un patrón aleatorio de píxeles que no representan características visuales en la escena que se captura, o ruido coherente producido por las características de un dispositivo particular. Un cierto grado de ruido es inevitable en cualquier dispositivo electrónico que transmita o reciba una señal, y en las cámaras de vídeo, el ruido es un subproducto de la captura de imágenes.

En pocas palabras, los píxeles individuales tienen tanto el color como el brillo -de aquí en adelante referidos conjuntamente como el «valor» del píxel por simplicidad-, que en el caso del ruido difiere del valor que transportarían si representaran con precisión la apariencia del área en el campo de visión al que corresponden. Un pixel ruidoso puede representar así un color incorrecto (ruido de crominancia) o un nivel de brillo (ruido de luminancia).

Dado que la presencia de niveles significativos de ruido afecta negativamente a la calidad de la imagen, la reducción del ruido al mismo tiempo que se preservan los detalles sobresalientes es naturalmente una alta prioridad para los fabricantes. En los últimos años se han desarrollado varios métodos basados en hardware y software para reducir el ruido en el video digital capturado por los sensores ópticos CMOS y CCD. Estos métodos pueden clasificarse ampliamente en dos tipos basados en su tecnología subyacente: espacial y temporal.

La reducción del ruido espacial se basa en el análisis de cuadros individuales de vídeo. Para reducir realmente el ruido, el enfoque más común es aplicar filtros que incorporen algoritmos diseñados para mitigar los efectos del ruido. Por ejemplo, un algoritmo de reducción de ruido puede asignar un píxel dado al valor mediano de los píxeles circundantes, o un promedio de su propio valor más los de los píxeles adyacentes a él. Por lo tanto, incluso si el píxel era ruido, su carácter «ruidoso» se diluiría, tomando un valor más alineado con los de los píxeles circundantes. Un efecto secundario de este enfoque es que, a menos que se usen algoritmos especiales para identificar los bordes de los objetos e impedir el promedio de píxeles a lo largo de la interfaz entre el objeto y el área circundante, puede ocurrir una pérdida de un borde limpio.

En un esquema de reducción de ruido temporal, el promedio se aplica no al valor de píxeles en la misma trama, sino a los valores de un píxel en la misma posición sobre marcos consecutivos. Debido a que se examinan cuadros consecutivos, el valor de un píxel en la misma posición a lo largo del tiempo puede compararse fácilmente, haciendo que el enfoque sea más efectivo que la reducción espacial del ruido para diferenciar y reducir los efectos del ruido en áreas estáticas que no cambian de marco a marco. Un efecto secundario de este enfoque, sin embargo, es la producción de desenfoque de movimiento si un objeto se mueve en el área procesada. En este caso, después de aplicar los algoritmos de reducción de ruido, un píxel en una posición en el marco en el que un objeto había aparecido en marcos anteriores, pero donde ya no aparece seguirá teniendo su valor parcialmente determinado por su valor anterior: Imagen visible del objeto en su posición anterior.

Debido a las deficiencias respectivas de las tecnologías espaciales y temporales de reducción del ruido, se desean sistemas que combinen ambos de una manera inteligente, ya que ofrecen una manera de compensar estas deficiencias. Algunos sistemas que ofrecen ambos no se pueden aplicar simultáneamente a los marcos de video individual, sino simplemente ofrecer una opción de uno u otro. Es importante tener en cuenta que simplemente ofreciendo una opción para cambiar entre los dos tipos de reducción de ruido es menos de lo ideal, ya que un solo cuadro de vídeo puede abarcar áreas estáticas, así como las zonas donde el movimiento se lleva a cabo.

La capacidad de procesar aquellas áreas del campo de visión donde ocurre el movimiento usando la reducción espacial del ruido y aquéllas con sólo contenido estático usando reducción de ruido temporal es la implementación ideal de un enfoque integrado. Este es el tipo de enfoque que la citada compañía ha adoptado en sus cámaras. Su reducción de ruido dinámico 2D (2DNR) es una versión optimizada de la tecnología de reducción de ruido espacial temporal, mientras que su reducción dinámica de ruido 3D (3DNR) combina tecnologías de reducción de ruido espaciales y temporales.

En comparación con 3DNR, 2DNR tiende a producir resultados superiores para objetos en movimiento, se aplica a tales objetos en el campo de visión.

Imagen 7

Mientras tanto, 3DNR se aplica en áreas estáticas del campo de visión. De esta manera, las cámaras de esta compañía son capaces de obtener las ventajas de cada tipo de enfoque de reducción de ruido mientras se evitan sus defectos. Además, la implementación de estos equipos incorpora rutinas para definir el movimiento dentro del área procesada, suprimiendo el desenfoque de movimiento distinguiendo entre los fotogramas en los que un píxel dado representa un estado anterior y aquellos en los que el píxel representa el estado actual.

• Calidad de video mejorada para una mejor identificación de objetos.

• Reducción del tamaño del archivo de vídeo para menores requisitos de ancho de banda y almacenamiento.

• Menos alarmas falsas para disminuir la vigilancia.

El ruido puede ser nada más que una molestia en el video que vemos por placer, pero obviamente puede ser un problema grave en video capturado para aplicaciones de seguridad. El ruido puede comprometer seriamente la efectividad de aplicaciones tales como la identificación de personas de interés o números de placa de matrícula del vehículo por la noche, o el monitoreo de áreas débilmente iluminadas en una oficina o espacio comercial. Si el ruido es particularmente extenso, la aplicación puede ser simplemente imposible.

El ruido de video es un problema frecuentemente encontrado con el video de vigilancia, ya que a menudo es capturado bajo esas condiciones, es decir, bajos niveles de luz, lo que fácilmente conduce a la aparición de ruido. Tales condiciones no sólo son propensas a producir ruido, sino que el ruido presente en el video disparado bajo condiciones de poca luz, como por ejemplo la noche, es particularmente difícil de tratar, ya que cualquier intento de aumentar la amplitud de la señal para mejorar la visibilidad aumentará generalmente el nivel de ruido también.

Además de mejorar la calidad de video, 2DNR de la mencionada compañía y 3DNR proporcionan otros beneficios importantes. Por un lado, reducen el tamaño de los archivos de vídeo capturados eliminando el ruido que añade complejidad y, por lo tanto, datos extraños a las áreas del campo de visión que en realidad son en gran medida uniformes en apariencia. Esta eliminación del ruido reduce el consumo de ancho de banda cuando se transmite vídeo desde la cámara a un NVR u otros nodos del sistema. Además, el reducido tamaño del archivo disminuye las necesidades de almacenamiento, permitiendo que más imágenes se archiven en equipos existentes o ahorren en los costos de compra de almacenamiento adicional.

Un segundo beneficio adicional de la reducción de ruido es que hace mucho menos probable que las alarmas de detección de movimiento se activen falsamente por la aparición de artefactos de vídeo que no reflejan el movimiento real en el entorno supervisado. Menos falsos positivos ahorran personal de tiempo perdido y distracciones, al tiempo que reducen la posibilidad de disminución de la vigilancia debido a frecuentes falsas alarmas.

Las cámaras con tecnologías robustas de reducción del ruido son la opción óptima para la vigilancia en interiores y exteriores en condiciones de poca luz. La capacidad de identificar y eliminar con precisión el ruido del video hace posible aplicaciones tan exigentes como la identificación de personas y números de matrículas de vehículos incluso por la noche. Como tal, las cámaras con fuertes capacidades de reducción de ruido son particularmente adecuadas para monitorear ambientes como parques de estacionamiento, instalaciones mal iluminadas como almacenes o ubicaciones que no están en uso activo por la noche, como oficinas

Suprema Visibilidad Nocturna (SNV)

Los bajos niveles de luz siempre han sido un desafío para las cámaras de vigilancia, y el rendimiento bajo tales

condiciones es considerado una métrica importante de las capacidades de una cámara. La cuestión del rendimiento en baja luz es particularmente crítico en las cámaras de seguridad, ya que a menudo tienen la tarea de capturar vídeo claro en la noche o en ambientes donde las condiciones iluminación son pobres.

La adición de capacidades de infrarrojos marcó un avance de las cámaras de vigilancia, lo que permite ser capturado cuando hay poca o incluso ninguna luz visible presente. Sin embargo, el uso de infrarrojos sigue siendo inferior a una solución ideal, ya que sólo son posibles las imágenes monocromáticas. El color, después de todo, puede ser un factor crítico en el éxito de muchas aplicaciones de seguridad sofisticadas. Para citar sólo un ejemplo, la capacidad de discernir del color de una persona de interés, pelo, ojos, piel y ropa puede significar la diferencia entre éxito y fracaso al realizar una identificación. Las cámaras con tecnologías robustas de reducción del ruido son la opción óptima para la vigilancia en interiores y exteriores en condiciones de poca luz. La capacidad de identificar y eliminar con precisión el ruido del video hace posible aplicaciones tan exigentes como la identificación de personas.

Esta compañía desarrolló la tecnología de Visibilidad Nocturna Suprema (SNV) con el fin de ofrecer la mejor calidad de imagen incluso a niveles extremadamente bajos de luz, logrando un nivel de señal de 30 IRE a una velocidad de obturación de 1 / 30s e Iluminación de 0,1 lux.

El esfuerzo se hizo no sólo para mejorar la claridad y reducir el ruido con Iluminación, sino también para preservar la capacidad de captar Incluso a niveles de lux donde las cámaras nocturnas convencionales se ven obligadas a confiar en la captura con infrarrojos.

Imagen 8

La Tecnología SNV representa un enfoque integral del problema, y es el resultado de los esfuerzos de esta compañía para identificar todas mejoras en el rendimiento en escenas con poca luz, y hacerlas realidad.

El enfoque de la citada compañía con SNV combina hardware optimizado y software. En el lado del hardware, SNV aprovecha sensores ópticos extremadamente sensibles que capturan en color de alta calidad incluso cuando prácticamente no hay luz visible disponible. Estos sensores están integrados con chips de procesamiento de señal de imagen de vanguardia para asegurar un contraste y una reproducción fiel del color. Los mejores componentes de hardware son Integrados con software avanzado diseñado para reducir el ruido, realzar el contraste, detalles nítidos, y sacar color.

Un ejemplo de la voluntad de esta compañía de ir más allá, es su tecnología de reducción de ruido 3DNR, que combina análisis algorítmico de las imágenes individuales y las imágenes sucesivas con el fin de eliminar los defectos visuales y dar más detalle. **(Imagen 8)**

Las cámaras reforzadas por la tecnología Supreme Night Visibility son particularmente adecuadas para monitorizar ambientes con condiciones de poca luz, y especialmente cuando son deseables imágenes en color para permitir o mejorar la capacidad de identificar personas u objetos de interés.

A diferencia de lo convencional en las cámaras de vigilancia día / noche, que cambian a blanco y negro incluso a niveles de luz en los que el ojo humano puede ver el color, las cámaras equipadas con tecnología SNV pueden capturar colores incluso en condiciones muy oscuras. En vista de estas ventajas, las cámaras que incorporan tecnología SNV son ideales para monitorizar entornos de baja iluminación en interiores, como almacenes y espacios comerciales en horas de oficina, así como áreas al aire libre como escuelas, campus, estacionamientos, carreteras y obras de construcción donde la vigilancia nocturna eficaz puede ser tan importante, si no más, que la monitorización diurna.

Además, debido a la excelente calidad de imagen del video capturado por las cámaras SNV, hacen que aplicaciones sofisticadas que requieren detalles claros y se beneficien del color (como las aplicaciones de lectura de matrícula y el reconocimiento facial), incluso bajo condiciones difíciles de poca luz.

Excepcionalmente para videos de alta calidad con un color preciso y detalles claramente capturados a niveles de lux extremadamente bajos, (las capturas con infrarrojos quedan reservadas únicamente a los escenarios donde no hay ninguna luz visible), Suprema Visibilidad Nocturna de la compañía es la tecnología número uno. ●

* La visión humana tiene un rango dinámico general de alrededor de 200dB, pero sólo una parte de la gama completa se puede percibir en un momento dado.

Fotos: LSB

Contactos de empresas, p. 7.

ALFREDO GUTIÉRREZ. BUSINESS DEVELOPMENT MANAGER PARA IBERIA DE MOBOTIX AG

La prevención es el futuro

Más seguridad gracias a la tecnología de vídeo IP y térmica

Como señalan las estadísticas actuales de la GDV (Asociación General de Aseguradoras de Alemania), en Alemania se incendia una empresa cada cinco minutos y los daños que estos causan en la economía nacional ascienden a varios miles de millones de euros anuales. Cabe destacar, además, el aumento de más de un 30% en cinco años de los allanamientos de morada y que las tasas de esclarecimiento para los allanamientos en comercios y empresas no alcanzan el 20%. Estas cifras ponen de manifiesto la importancia de la prevención en lo que respecta a robos e incendios.

LAS soluciones de seguridad inteligentes con tecnología de vídeo y térmica no solo sirven para el esclarecimiento del caso cuando se producen daños, sino que ayudan también a prevenir riesgos antes de que se materialicen.

Ante el aumento de las cifras de allanamientos de morada, se multiplican las soluciones rentables y efectivas de seguridad. Cada vez más empresas se decantan por el uso de la tecnología de vídeo para vigilar sus edificios, instalaciones y recintos empresariales.

Los daños económicos producidos por robos, vandalismo o incendios pueden ser muy importantes para una empresa, especialmente cuando no se trata únicamente de daños materiales directos, sino cuando causan también una parada de la producción. El objetivo, por tanto, debe ser prevenir riesgos y evitar daños. Pero, ¿qué prevención aporta la tecnología de vídeo?

Limitaciones de los sistemas de vídeo convencionales

Las cámaras de vídeo convencionales, con una calidad de imagen lo suficientemente buena y una grabación fiable, permiten obtener material de vídeo que facilita el esclarecimiento. No obstante, ni siquiera estos requisitos mínimos del usuario se alcanzan con muchos de los sistemas de vídeo instalados y comercializados actualmente, a veces, la calidad de la imagen no es suficiente para obtener grabaciones nítidas.

Una gran parte de las cámaras que se venden hoy en día siguen teniendo una resolución máxima de 3 megapíxeles (según el estudio de mercado

IHS Research de agosto de 2016). Otra limitación es la escasa sensibilidad a la luz de muchos sensores de imagen, de modo que, en condiciones de mala iluminación, el movimiento se desenfoca.

No obstante, la calidad de un sistema de cámaras no se mide únicamente por la claridad de las imágenes en movimiento durante el día y la noche, sino también por su fiabilidad. En este sentido, varios factores resultan decisivos: la resistencia y la disponibilidad de la cámara, así como la posibilidad de grabar en la propia cámara en caso de averías en la red para que no se pierdan imágenes decisivas para el esclarecimiento del caso.

Desde el punto de vista de la seguridad técnica, un sistema es perfecto si cada cámara es inteligente por sí misma y no depende de un servidor centralizado para el procesamiento y el análisis de las imágenes.

Los sistemas de vídeo inteligentes ofrecen soluciones de seguridad preventivas

Si la cámara está equipada con un potente ordenador y aplicaciones de software inteligentes, es posible utilizar el sistema de vídeo de forma más eficiente, sobre todo, puede ayudar a prevenir riesgos y evitar daños.

Una cámara inteligente entra en acción cuando realmente se necesita. Está equipada con un software de detección de movimiento y posibilita una gestión de alarmas fiable. Por ejemplo, si alguien entra en el recinto durante un horario definido, la cámara activa automáticamente un mensaje por megafonía y conecta una iluminación adicional para intimidar a visitantes no deseados. Además, la cámara puede informar por telefonía VoIP o correo electrónico a determinados empleados o a un servicio de seguridad.

Para que una moderna solución de videovigilancia IP de este tipo resulte rentable y práctica, es indispensable que las interferencias, como árboles o mástiles de las cámaras movidos por el viento, no provoquen falsas alarmas.

Aquí también suele fracasar la tecnología de seguridad convencional, muchos de los sistemas de vídeo disponibles en el mercado ofrecen posibilidades muy limitadas. Los sistemas más avanzados utilizan un software inteligente para la cámara que permite distinguir objetos en movimiento por su tamaño en función de su posición en la imagen. Con una detección de movimiento inteligente en 3D como la de MxActivitySensor 2.0, se reduce el número de falsas alarmas causadas por pájaros u otros animales.

La combinación de tecnología térmica y de vídeo proporciona una protección perimétrica y de la propiedad eficiente

Gracias a la inteligencia del sistema de cámaras, el software inteligente para la detección de movimiento y una gestión de alarmas activa, es posible diseñar una solución de seguridad preventiva potente, disponer de notificaciones puntuales y evitar los casos de robo y las situaciones de peligro.

En ocasiones, la videovigilancia se limita a una simple captación visual. La combinación de una solución de videovigilancia inteligente como la descrita con tecnología térmica aporta otras ventajas decisivas. Las cámaras duales, equipadas con un sensor óptico y un sensor térmico, pueden detectar de forma fiable objetos en movimiento por su radiación térmica, incluso en condiciones de absoluta oscuridad y a larga distancia. Mientras que el sensor térmico detecta de forma fiable los movimientos, el sensor de imagen óptico de 6 MP proporciona grabaciones de vídeo excelentes en las que pueden reconocerse perfectamente personas y acciones; un aspecto decisivo en la persecución de delitos. Para que suceda lo mismo de noche, el sistema de cámaras inteligentes conecta una fuente lumínica cuando el «ojo térmico» detecta un movimiento.

> «Las soluciones de seguridad inteligentes con tecnología de vídeo y térmica ayudan también a prevenir riesgos antes de que se materialicen»

Una cámara dual con sensor óptico y térmico permite una protección perimétrica y de la propiedad efectiva. Además, es de gran ayuda

en ámbitos en los que la protección de zonas privadas juega un papel importante, especialmente en áreas públicas como piscinas, instalaciones deportivas u hospitales.

La imagen térmica muestra un perfil de temperatura que no permite identificar a las personas con detalle. Con la configuración correspondiente, el sistema de cámaras duales cambia automáticamente de imagen térmica a sensor óptico, y graba una secuencia de vídeo de alta resolución en cuanto una persona se mueve dentro del área de vigilancia en cuestión.

Prevención mediante la supervisión de procesos inteligente

Las empresas utilizan también la tecnología de vídeo y térmica para detectar situaciones de peligro en el proceso de producción. En la industria alimentaria, por ejemplo, las cámaras de vídeo supervisan los procesos en el marco del control de calidad. En estos casos, suelen utilizarse cámaras hemisféricas de alta resolución con vista omnidireccional de 360 grados y zoom digital como equipamiento opcional. Para las áreas de producción se requieren cámaras de exteriores resistentes y de calidad, que puedan soportar las variaciones de temperatura y la humedad y que, por su diseño sin piezas móviles, prácticamente no precisen mantenimiento.

Las cámaras duales, equipadas con un sensor especial de radiometría térmica calibrado, además del sensor óptico, pueden supervisar también procesos en los que la temperatura es un factor crítico. Gracias a la inteligencia del sistema de cámaras, se puede también utilizar para prevenir daños por sobrecalentamiento o incendio: Si se sobrepasa el límite máximo o mínimo de temperatura definido, o se produce un súbito aumento de la temperatura, se genera una alarma automática.

Con la integración en un sistema SCADA para la supervisión y el control del proceso de producción, es posible detener el proceso o iniciar un procedimiento de enfriado, antes de que se produzcan daños. La cámara dual permite superponer imágenes visuales y térmicas. De esta forma, se pueden localizar por ejemplo rápidamente los «hotspots» o puntos con temperatura crítica en una sala de máquinas.

Los sistemas inteligentes son también rentables

La inversión en una solución de videovigilancia con cámaras resistentes y fiables controladas por software inteligente es una apuesta segura. En primer lugar, por la inteligencia de la cámara que, además de ofrecer imágenes excelentes, analiza los datos obtenidos, detecta riesgos e inicia acciones automáticas para neutralizar el peligro y evitar los daños económicos por robo, vandalismo o incendio. Un sistema de cámaras inteligentes y de calidad

aporta una ventaja adicional decisiva: genera un coste total reducido, al igual que una solución de vídeo convencional, y se amortiza en poco tiempo.

En segundo lugar, dado que el procesamiento y el análisis de imágenes se realiza en la misma cámara y no en el almacenamiento en red de forma permanente, sino activados por eventos, las exigencias en cuanto al ancho de banda y al resto de la infraestructura de TI son también menores.

Por norma general, un sistema de cámaras de este tipo con arquitectura descentralizada puede integrarse de forma sencilla en la infraestructura de red existente. El uso de la tecnología térmica, por su parte, reduce el número de cámaras necesarias para la protección de grandes áreas, precisa de una menor iluminación y requiere menos potencia en la instalación.

Según estudios de mercado actuales (IHS Research, agosto de 2016), se encargan mayoritariamente cámaras IP económicas con unas posibilidades, no obstante, limitadas. Si asumimos que «la prevención es el futuro», la decisión de compra no debería ser el precio sino las ventajas que ofrece una solución de videovigilancia inteligente. ●

Fotos: ***Mobotix***

La nueva línea de cámara Mx6 crea más posibilidades.

Más imágenes, en cualquier condición de luz, en cada estándar.

Más inteligencia esta en camino.

El nuevo sistema de cámaras Mx6 de 6 MP de MOBOTIX le ofrece un mayor rendimiento. Gracias a una frecuencia de vídeo hasta dos veces mayor, registra mucho mejor movimientos rápidos y ofrece imágenes más brillantes tanto en MxPEG y MJPEG como, por primera vez, en el estándar industrial H.264. La innovadora línea de cámaras Mx6 es más rápida, flexible y potente y le ofrece nuevas posibilidades de uso e integración para todas sus necesidades.

MOBOTIX AG • Langmeil, Germany • www.mobotix.com

MOBOTIX

DEPARTAMENTO PANOMERA MULTIFOCAL SENSOR SYSTEMS. DALLMEIER

Menos cámaras para **más seguridad**

Un sistema pionero en la videovigilancia del espacio público en Colonia

Teniendo en cuenta la creciente inseguridad en la población, todo el arco parlamentario alza la voz reclamando un incremento de la videovigilancia y el aumento del número de cámaras en las áreas públicas. Pero, ¿realmente garantizan más cámaras o cámaras con cada vez más resolución más seguridad? El fabricante germano con sede en Ratisbona, uno de los proveedores destacado a nivel mundial de sistemas de videoseguridad basados en red, lo niega. Y muestra en Colonia cómo debe ser un uso razonable que aumente la seguridad pública.

HASTA ahora, el montaje de grandes sistemas con la máxima cantidad de cámaras posible parecía ser la única vía lógica para poder proteger ampliamente áreas extensas e inabarcables. Sin embargo, en la mayoría de los casos, resultó que tal procedimiento, por una parte, quedaba fuera de los límites del presupuesto. Y por otra parte, simplemente no era posible técnicamente crear soluciones satisfactorias. «Por esa razón, en el pasado, al menos entre un 30 y un 40% de este tipo de proyectos ni siquiera se realizaron», dice Dieter Dallmeier, fundador y CEO del fabricante bávaro de vídeo, con una exitosa actividad desde hace más de 30 años en el ámbito internacional.

Sistema de sensores multifocal - un enfoque completamente nuevo

Gracias a las posibilidades técnicas únicas de la patentada tecnología de sensores multifocal y sus componentes de sistema de apoyo, también desarrollados por el experto alemán en CCTV/IP, es posible un enfoque completamente nuevo y pionero de la prevención de crimen. El sistema de sensores multifocal ha sido desarrollado especialmente para la protección completa de amplias áreas. Con él se visualizan, con una calidad de resolución no vista hasta ahora, espacios de grandes anchuras y superficies de gran profundidad, todo ello en tiempo real y con una tasa de imágenes de hasta 30 ips. Así es posible abarcar con la vista desde un solo lugar un área inmensa –y la resolución es escalable casi a voluntad, dependiendo de la tarea de vigilancia requerida. De modo que un sistema con ocho sensores puede sustituir aproximadamente 35 cámaras megapíxel convencionales.

Objetivo: Colonia

Los acontecimientos de la Nochevieja 2015 en Colonia aún están presentes en la conciencia de sus habitantes. La policía local reconoció la necesidad de examinar el concepto de seguridad existente, sobre todo en cuanto a la protección de grandes plazas públicas, y retocarlo donde fuera necesario. Empujados por los delitos que sucedieron en aquella Nochevieja alrededor de la Catedral de Colonia, eligieron esta zona del centro urbano para realizar planes nuevos de seguridad. En la primavera de 2016, presentaron los primeros conceptos de cómo se podría mejorar la vista general para la policía y la gestión del personal de intervención en el amplia área Bahnhofsvorplatz/Domplatte (la explanada de la estación y la catedral) mediante el empleo de sistemas de vídeo, especialmente cuando la concentración de personas fuera mayor. Ya en esta temprana fase de planificación se vieron enfrentados a un problema considerable: el uso de tecnología de vídeo convencional no

permitiría captar plenamente la superficie a cubrir de 8800 m². Asimismo, no encontraron ninguna tecnología de cámara que pudiera proporcionar la resolución requerida de toda el área para las investigaciones policiales. Finalmente, se reconoció también que un sistema de vídeo convencional con muchas cámaras individuales llevaría a una avalancha de imágenes poco inabarcable y que, por tanto, dificultaría esencialmente la observación proactiva y reacción rápida por los funcionarios en el centro de control.

Menos es más

Los ingenieros de proyecto del experto bávaro en vídeo se pusieron manos a la obra y, tras una breve introducción en la tarea, fueron capaces de idear un sistema que no sólo cumpliría los requerimientos definidos, sino que los superaría incluso. El encargo fue adjudicado al fabricante de Ratisbona, y así comenzó a mediados de diciembre de 2016 el montaje del sistema de sensores multifocal. En lugar de un sistema con innumerables cámaras de un solo sensor –lo que hubiera significado una instalación laboriosa, así como altos costes de infraestructura y mantenimiento–, el fabricante construyó una solución de vídeo que cubre el área de vigilancia completa y que, sin embargo, mantiene una presencia discreta. Únicamente fueron necesarios dos puntos de instalación, lo que por una parte hizo fácil el montaje y por otra, en comparación, dados los costes considerablemente inferiores en cuanto a infraestructura y mantenimiento del sistema, tendrá repercusiones financieras positivas para la ciudad.

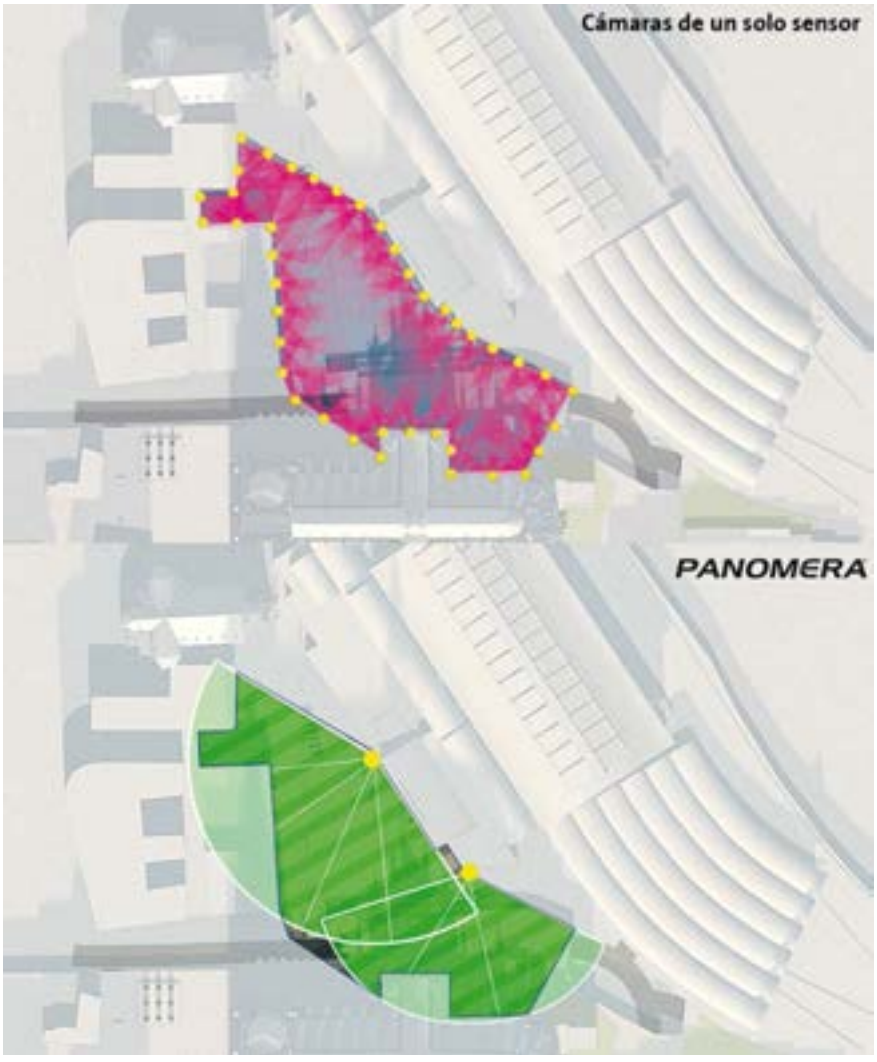
La protección de datos es cosa sabida

En Alemania, la protección de datos personales está reglamentada estrictamente por ley. Y también la policía de Colonia es absolutamente consciente de su responsabilidad con el tratamiento de datos de vídeo. El fabricante germano se ocupa mediante diferentes medidas de que los datos grabados cumplan las normas de protección de datos. Determinadas áreas de la imagen pueden ser ocultadas completamente de la captación por la cámara o caras y matrículas de vehículos pueden ser desfiguradas mediante pixelado. Adicionalmente, la conservación de los datos está limitada en el tiempo – sólo se guardan en casos de sospecha fundados y con fines probatorios ante los tribunales.

Observación activa vs. vigilancia pasiva

En vez de tener que fiarse de que un gran número de cámaras de vigilancia instaladas lleve a una disminución del índice de delincuencia, ahora la policía de Colonia puede sustituir una vigilancia pasiva inefectiva por una observación activa por vídeo. Esto significa que situaciones potenciales de peligro son detectadas antes de que puedan convertirse en acontecimientos en la estadística policial. El personal de intervención es avisado rápidamente y dirigido al lugar de los hechos. Y en el caso de que ante los «ojos» de los funcionarios se cometiera un delito, existirían, gracias a la tecnología de sensores multifocal, datos relevantes y admisibles ante los tribunales para el seguimiento penal.

Fotos: Dallmeier



Contactos de empresas, p. 7.

MARÍA JOSÉ DE LA CALLE*. DIRECTORA DE COMUNICACIÓN & ANALISTA SENIOR DE ITTI.

¿Sociedad de la información o **sociedad inundada** de información?

El uso de las tecnologías de la información con su capacidad de comunicación y producción de datos e información, ha conducido a una inundación de los mismos, inundación que está produciendo una incapacidad para leer, comprender, juzgar e interpretarlos, debidamente. Una consecuencia de esto, es la propagación de noticias falsas en las redes, a veces por desconocimiento, a veces con intenciones aviesas.

El vocablo «inundar» proviene de la palabra latina inundare, que significa llenar de agua. Así lo expresa el Diccionario de la Real Academia de la Lengua Española (DRAE), en su primera acepción es «Dicho del agua: Cubrir un lugar determinado». A lo que se añade una tercera «Dicho especialmente de un gran número de personas o cosas: Llenar un lugar».

Así mismo, el DRAE en la entrada de «informar», nos informa que viene del latín informare: «dar forma», «describir».

Así pues se puede afirmar que la información proporciona descripción de fenómenos, situaciones, actividades, personas, cosas, etc.

Los datos y la información no sólo los generamos los humanos, también los generan las máquinas. El V informe de INCAPSULA[1] del tráfico producido en la red proporciona el siguiente dato: el 51,8% es creado por máquinas, no por personas.

Wichy/shutterstock

La información se vierte -o vomita- en la red en forma de texto o imágenes sobre lo que sucede a nuestro alrededor. La inmediatez con que llegan las noticias colocadas en la web por cualquier testigo presente con un dispositivo móvil, ha producido que ya no se necesite tener a un periodista presente para contarlas. De hecho no es infrecuente ver vídeos o fotos tomadas por «aficionados» en las páginas web de periódicos, o un artículo-noticia «veteado» con «tweets» recientes de testigos de la noticia.

Unido a esto, hay aplicaciones o bots[2] que la generan automáticamente, como el caso de los que utiliza la BBC[3] . En Twitter, detrás de entre el 9% y el 15% de las cuentas no hay personas[4]. Son utilizadas para generar visitas a web poco visitadas –por personas–, generar spam, crear tendencias; o –por proporcionar ejemplos más positivos–, para atención al cliente o como asistentes.

Tal abundancia se puede llevar por delante y dañar la calidad de la propia información. Cuando se habla de la seguridad de la información, se está haciendo referencia a la confidencialidad (C), integridad (I) y disponibilidad (D). Quizás a la seguridad de la infor-

mación, para que ésta sirva para «dar forma» adecuada a hechos y cosas en general, habría que dotarla de otra cualidad, que es la veracidad, que a diferencia de la tríada C-I-D, no es un tema técnico, sino más bien de conocimiento de la disciplina relacionada con la propia información.

Las inundaciones constituyen, en la mayoría de los casos, fenómenos adversos que destruyen el «lugar que llenan», llegando a producir daños al medio ambiente, a propiedades e, incluso, a las personas. Se lo llevan todo por delante, allá por donde pasan.

De igual manera, la inundación de datos e información hace que éstos se tornen inútiles. Trae una mezcla de datos veraces y otros no tanto, de datos útiles e inútiles, de información publicada con una intención de informar o de desinformar. Hay que tener la capacidad de saber separar aquello necesario de lo que no lo es, y lo que es cierto de lo que no, de intuir el propósito que subyace a ella. Hay que saber elegir e interpretar aquello que sea útil para el propósito que se busca, en un tiempo razonable. Esto es lo que se denomina pertinencia.

La información no adecuada o falsa puede causar daños ya que puede confundir, dañar la imagen de una persona u organización, o manipular una toma de decisiones.

Por ejemplo, en unas elecciones la manipulación de hechos dirigidos a la «opinión pública», con el fin de conseguir votantes. Este fue el caso de las últimas elecciones presidenciales en EEUU, según la publicación de la Universidad de Stanford «Social Media and Fake News in the 2016 Election»[5], en que se puede leer la preocupación por los efectos que las falsas noticias que circularon por las redes sociales, la mayoría de las cuales favorecían al presidente electo, y cómo dichas noticias podían haber inclinado la balanza hacia él.

PIxxart/Shutterstock

«Se habla de la sociedad de la información, de la información como la energía del siglo XXI, de la revolución de la información»

La importancia de la información y su control no es un tema nuevo.

Así, el profesor Josep Fontana en su libro «La historia de los hombres»[6], explica «la aparición de una 'opinión pública' a partir de mediados del s. xvii. Un fenómeno ligado al surgimiento de una auténtica "industria de la información" que multiplicó las impresiones de cartas, folletos, gacetas y, en general, de textos breves y accesibles a un público extenso, que se ocupaban de crítica política o reproducían todo tipo de noticias del momento». Y añade «la importancia que tuvo en Italia y Francia esta revolución de la información que llevaba a los propios historiadores a decir que vivían en un tiempo "lleno de noticias" y que obligó a los gobiernos a tomar historiadores a su servicio para combatir los efectos de la crítica (Luís XIV de Francia tenía en nómina a 19 historiadores)».

El adjetivar el tiempo en que vivían como «lleno de noticias» nos hace sonreír. Con el apoyo de las Tecnologías de la Información, la cantidad de información que se genera y distribuye en el mundo hoy día es enorme. Para medirla, y tomando como base el byte[7], se ha pasado desde el comienzo de estas nuevas tecnologías, de kilobytes (Kb = 103 bytes), a megabytes (Mb 106 bytes), gigabyte (Gb = 109 bytes), terabyte (Tb = 1012 bytes), petabyte (Pb = 1015 bytes), exabyte (Eb = 1018 bytes), zettabyte (Zb = 1021 bytes).

Un artículo[8] de hace un año de la «Northeastern University» ya decía que al día se producían 2,5 Eb, equivalentes a 90 años de grabación de vídeo en alta definición, o a 150 billones de canciones o a 250.000 veces el contenido en digital de la biblioteca del Congreso de EEUU.

Se habla de la sociedad de la información, de la información como la energía del siglo XXI, de la revolución

de la información. Pero para que ésta constituya un bien para todos y riqueza para la sociedad, es necesario aprender a utilizarla, a producirla y a distribuirla. Hay que cuidarla y mantenerla adecuada para el consumo, al igual que el agua. La información contaminada, puede causar muchos daños.

¿Qué es la información?

La información es el resultado de la interpretación de unos datos: primero hay que conocer la bondad de dichos datos, y segundo, fijar un contexto para interpretar dichos datos.

Por tanto, con el fin de poder hacer uso de una información, hay que tener la capacidad para analizar ambas cosas: los datos y el contexto utilizado para interpretarlos. Así, se podrá distinguir lo verdadero de lo falso, o la intención que pueda subyacer a la información.

¿Pero hay tiempo de reflexión suficiente o criterios claros a la hora de retwittear o dar un click en a «me gusta»? ¿Hay capacidad para una adecuada selección de datos a la hora de utilizarlos?

Desde luego nos podemos servir de herramientas que ayuden a esta tarea, pero dichas herramientas están basadas en criterios de selección, clasificación y extracción que también se deberían conocer, ya que podrían estar creados para dar unos resultados no acordes con los fines buscados. Recordemos además que todo filtro supone falsos positivos y falsos negativos.


ESB Professional/Shutterstock

Para esto, la educación tiene mucho que decir. Sin ir más lejos, en la plataforma de cursos gratuitos en-línea (moocs) «edx» hay un curso «Fake News, Facts, and Alternative Facts»[9], «para aprender a distinguir fuentes de noticias fiables e identificar los sesgos de la información para llegar a ser un consumidor crítico de la información».

Cómo decidir si una información es falsa

En una reciente infografía[10] de «Futurism.com» se puede leer lo siguiente: «Las noticias falsas son un serio problema en EEUU a día de hoy por varias razones: está influenciando las acciones de las personas, y éstas están teniendo dificultades para entender qué noticia es verdadera y cuál es falsa».

La existencia de tantos datos e informaciones falsas, parece que ha empezado a preocupar. A juzgar por las noticias publicadas, lo que ha disparado dicha preocupación han sido las últimas elecciones en los EEUU –como el ya comentado documento de la Universidad de Stanford o la infografía de Futurism– en las que se ha hecho una utilización masiva de las redes sociales, y en las que se podía saber minuto a minuto todo lo que decían los candidatos y lo que se comentaba de ellos, fuera cierto o no.

En la infografía se proponen tres soluciones: que quien edita la noticia se asegure de que es cierta –solución que ya en publicaciones de cierto rigor se viene haciendo–; que sean los usuarios/lectores quienes juzguen, marcándolas en un sentido u otro; algoritmos que las marquen, solución que ya se ha puesto en marcha en algunas redes.

Tanto la primera solución como la segunda dependen del «buen hacer» de las personas, y el proceso a veces es lento para la velocidad de comunicación en la web. En cuanto a las soluciones automatizadas, se pone en manos de unos pocos -las empresas dueñas de dichas soluciones- la importante tarea de marcar datos e información como no falsos.

Según el artículo de «The New York Times», «Google and Facebook Take Aim at Fake News Sites»[11], las redes sociales no se libraron de las críticas por permitir las noticias falsas. Tanto es así, que tomaron cartas en el asunto: Google prohibiría las webs que difundieran noticias falsas, y Facebook no mostraría publicidad de páginas –sites– que incluyan noticias falsas;

Posteriormente, Facebook, según un artículo[12] de Vox del pasado 27 de marzo, obligaría a dar dos click para poder compartir una noticia que según sus algoritmos considerara falsa, marcándola con una etiqueta «disputed» (controvertida).

Las medidas que implementan dichas empresas en sus herramientas, están basadas en algoritmos de los que hay que fiarse sin saber muy bien cómo funcionan.

Esto se complica más si dichos algoritmos pertenecen a la categoría de la «Inteligencia Artificial»; la cuestión de conocer cómo está funcionando un algoritmo concreto sería un tema difícil de resolver: el sistema adapta sus algoritmos dependiendo de los nuevos datos que trate. Citando un artículo[13] de la «MIT Technology Review», «Nadie realmente sabe cómo los más avanzados algoritmos hacen lo que hacen. Esto podría ser un problema».

Cualquiera de las tres soluciones parece tener sus problemas, quizás la solución no sea una u otra sino todas al unísono.

Pero hay una última de la que no habla la infografía, que ya he apuntado antes: la educación, es decir, aprender a tratar la información, contrastarla con diferentes fuentes, aprender cómo conseguir fuentes fiables. Y tomarse el tiempo suficiente –dependiendo de las consecuencias de la acción posterior– para tomar en consideración una información u otra. En definitiva, aprender a vivir en la sociedad de la información.

**** María José de la Calle.***
Cofundadora. Directora de Comunicación & Analista Senior de IttI.
Email: mjdelacalle@ittrendsinstitute

Referencias

1.-«Bot Traffic Report 2016». url [a 20170424] https://www.incapsula.com/blog/bot-traffic-report-2016.html

2.- «Un bot (aféresis de robot) es un programa informático, imitando el comportamiento de un humano», según la definición que ofrece Wikipedia. url [a 20170424] https://es.wikipedia.org/wiki/Bot

3.- «How can we leverage bot technologies to reach new audiences on messaging platforms and social media?» url [[a 20170424] http://bbcnewslabs.co.uk/projects/bots/

4.- O. Varol, E. Ferrara, C. A. Davis,F. Menczer, A. Flammini (20170327) «Online Human-Bot Interactions: Detection, Estimation, and Characterization». url [a 20170424] https://arxiv.org/pdf/1703.03107.pdf

5.- H. Allcott, M. Gentzkow (201703). «Social Media and Fake News in the 2016 Election». url [a 20170424] https://web.stanford.edu/~gentzkow/research/fakenews.pdf

6.- «La historia de los hombres» Pag. 84. Josep Fontana. Ed. Crítica, 2001.

7.- url [a 20170424] https://es.wikipedia.org/wiki/Byte

8.- M. Khoso (20160513) «How Much Data is Produced Every Day?». Northeastern University. url [a 20170424] http://www.northeastern.edu/level-blog/2016/05/13/how-much-data-produced-every-day/

9.- «Learn how to distinguish between credible news sources and identify information biases to become a critical consumer of information». edx. url [a 20170424] https://www.edx.org/course/fake-news-facts-alternative-facts-michiganx-teachout-2x

10.- «Fake news is a serious problem in the U.S. right now, for several reasons: it is influencing the actions of real people, and people are having difficulty undestanding which news is real and which news is fake» Futurism.com. url [a 20170424] https://futurism.com/images/fighting-fake-news-can-technology-stem-the-tide/

11.- N. Wingfield, M. Isaac, K. Benner (20161114) «Google and Facebook Take Aim at Fake News Sites» The New York Times. url [a 20170424] https://www.nytimes.com/2016/11/15/technology/google-will-ban-websites-that-host-fake-news-from-using-its-ad-service.html?_r=0

12.- A. Romano (20170324) «Facebook is fighting fake news by making it harder — or at least more annoying — to share» Vox. url [a 20170424] http://www.vox.com/culture/2017/3/24/15020806/facebook-fake-news-alert-fact-checking

13.- «No one really knows how the most advanced algorithms do what they do. That could be a problem.» W. Knight (20170411) "The Dark Secret at the Heart of AI". MIT Technology Review. url [a 20170424] https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/?utm_source=MIT+Technology+Review&utm_campaign=40d49ebf11-weekly_roundup_2017-04-20_edit&utm_medium=email&utm_term=0_997ed6f472-40d49ebf11-153813777&goal=0_997ed6f472-40d49ebf11-153813777&mc_cid=40d49ebf11&mc_eid=f684c51e62.

IGOR RODRÍGUEZ. DIRECTOR DE EXPORTACIÓN EN DORLET

Normativa de **Sistemas de Control de Accesos EN 60839**

La norma EN 60839-11-1 establece unas funcionalidades y rendimiento mínimas para los sistemas electrónicos de control de accesos. Esta norma suple a las normas anteriores EN 50133-1 y EN 50133-2-1, quedando definida en ella todos los requisitos generales del sistema y particulares de sus componentes. Esta norma tiene como particularidad la clasificación de los grados de seguridad en función del tipo de negocio y de los riesgos asociados a la instalación que se va a asegurar.

LOS grados de seguridad están clasificados del 1 al 4, siendo grado 1 el de menor riesgo y 4 el mayor riesgo. En la **Tabla 1** se puede observar la clasificación íntegra.

Esta clasificación sirve de ayuda a la hora de definir un pliego de características técnicas y permite comparar dos o más sistemas de seguridad sin entrar de lleno a investigar los cientos de funcionalidades que cada sistema de control de acceso pueda llegar a tener.

¿Dónde aplica?

La norma EN 60839 tiene su homóloga como estándar internacional en la IEC 60839, por lo que es considerada una norma internacional. A día de hoy, la EN 60839 es de obligado cumplimiento en los países integrantes de la Unión Europea.

Cada país se basa en la norma para identificar qué grado es necesario en cada edificio o instalación. Por ejemplo, el país «A» puede legislar de tal modo que los bancos deban instalar obligatoriamente sistemas de control de accesos de grado 3, mientras que el país «B» requiera para sus bancos grado 4.

En el caso de Latinoamérica, la EN 60839 no es de obligado cumplimiento. A pesar de ello, la norma aporta una garantía de calidad y seguridad por lo que se recomienda su uso en proyectos de control de accesos, especialmente aquellos de carácter crítico. Tampoco se desecha que en un futuro, países latinoamericanos puedan adoptar esta norma e imponer su uso, por lo que conviene conocerla y familiarizarse con ella.

Esta norma se usa igualmente en proyectos privados donde el propietario u organización, pese a no estar obligado por ley, desea asegurar sus instalaciones con unas garantías de calidad y seguridad.

Aplicación en España

La norma europea EN 60839 tiene su transposición en la norma española UNE-EN 60839 que es la de obligado cumplimiento en aquellas infraestructuras establecidas por el Ministerio del Interior y CNPIC según la tabla de grados referida.

La orden ministerial INT/316/2011 sobre el funcionamiento de los sistemas de alarmas en el ámbito de la seguridad privada especifica en su artículo 3, que todos los sistemas de control de accesos han de ser certificados, en cualquiera de sus grados, por la norma UNE-EN 50133, reemplazada por la UNE-EN 60839 en la orden INT/1504/2013.

Para nuevas instalaciones a partir de la fecha de publicación de la orden ministerial (18 febrero 2011) todos los sistemas de control de accesos han de estar certificados en EN 60839 en su grado correspondiente.

Para instalaciones existentes que cuentan con sistemas de control de accesos existe una prórroga de 10 años (2021), a partir de la cual deberán adaptar sus sistemas a la nueva normativa EN 60839 en su grado correspondiente.

¿Qué se certifica?

Según la norma EN 60839 los elementos de control de accesos que de-

ben certificarse son las Unidades de Control de Accesos (UCAs), los lectores (proximidad, biométricos, etc.), y el software de control de accesos.

Otros elementos como cerraduras, tornos, barreras, magnéticos, etc., estarían fuera del ámbito de aplicación de la norma.

¿Quién certifica?

La entidad certificadora nacional es la única que puede expedir la certificación de producto, en cualquiera de los grados de la norma EN 60839, basada en los resultados de los ensayos realizados por un laboratorio acreditado por dicha entidad.

En los casos donde la norma es de obligado cumplimiento por un gobierno, cada país puede añadir requerimientos. Recordemos que la norma EN 60839 es de mínimos, y cada país es soberano para poder incrementar los requerimientos de la norma.

En el caso de España, la UCSP (Unidad Central de Seguridad Privada) dependiente del CNP (Cuerpo Nacional de Policía), para la obtención del certificado EN 60839, exige al fabricante una «evaluación del proceso de producción» adicional, que implica:

-Ensayos sobre muestras tomadas en producción.
-Inspección del proceso de producción.
-Auditoría del sistema de calidad del fabricante.

Ventajas / objetivos

El principal objetivo de la norma EN 60839 es la de dotar de mayor seguridad a los sistemas de control de acceso, a la vez que se unifican criterios y categorizan sus funcionalidades. En los últimos años, los avances tecnológicos han inundado el mercado de nuevos productos que requieren de una normalización y adaptación a los requisitos de seguridad actuales.

Aumento del grado de fiabilidad de los sistemas. Este aumento de fiabilidad beneficia a los usuarios de seguridad de la instalación, así como en la comunicación de incidencia a los Cuerpos de Seguridad del Estado.

Adaptación de los sistemas de control de acceso al riesgo de la instalación. A mayor riesgo, el sistema de control de acceso ha de ser más avanzado.

Ejemplos de grados

–Grado 1 (bajo riesgo)

Una cerradura autónoma (código PIN o tarjeta) u offline, instalada en un área pública para situaciones de bajo riesgo.

Ejemplo de tecnología de tarjeta: 125 Khz y Mifare Classic, lectura CSN.

Ejemplos típicos: Puertas internas o áreas en las que se desea restringir la circulación del público.

GRADO	1	2	3	4
Nivel de Riesgo	Bajo	Entre bajo y medio	Entre medio y alto	Alto
Aplicación	Aspectos organizativos, protección de los activos de escaso valor	Aspectos organizativos, protección de los activos de un valor entre medio y bajo	Menos aspectos organizativos, protección de los activos comerciales de un valor entre medio y alto	Principalmente protección de infraestructura crítica o comercial de gran valor
Alcance	Para sistemas de seguridad dotados de señalización acústica, que no se vayan a conectar a una central de alarmas o centro de control.	Dedicado a viviendas y pequeños establecimientos, comercios e industrias en general, que pretendan conectarse a una central de alarmas o a un centro de control.	Destinado a establecimientos obligados a disponer de medidas de seguridad, así como otras instalaciones comerciales o industriales a las que por su actividad u otras circunstancias se les exija disponer de conexión a central de alarmas o a un centro de control.	Destinado a las denominadas infraestructuras críticas, instalaciones militares, establecimientos que almacenen material explosivo reglamentado y empresas de seguridad de depósito de efectivo, valores o metales preciosos, materias peligrosas o explosivos, requeridas, o no, de conexión a una central de alarmas o a centros de control.
Capacidad/conocimiento de adversarios/atacantes	Escasa capacitación, escaso conocimiento de ACS, desconocimiento del identificador y tecnologías de TI. Medios financieros escasos para los ataques	Capacidad y conocimiento medio de ACS, escaso conocimiento del identificador y tecnologías de TI. Medios financieros entre bajos y medios para los ataques	Gran capacidad y conocimiento de ACS, conocimiento medio del identificador y tecnologías de TI. Medios financieros de ataque medios	Capacidad y conocimiento de ACS de muy alto nivel, elevador conocimiento del identificador y tecnologías de TI. Medios financieros de ataque importantes
Ejemplos típicos	Hotel	Oficinas comerciales y pequeñas empresas	Industrial, administración, financiero	Zonas altamente sensibles (instalaciones militares, gobierno, I+D, zonas de producción críticas

Tabla 1

–Grado 2 (riesgo bajo a medio)

Un sistema on-line que utiliza tarjetas o códigos PIN para restringir el acceso. Los eventos se reciben en tiempo real en el software de gestión de accesos.

Ejemplo de tecnología de tarjeta: Se debe utilizar la tecnología Mifare PLUS SL3 o superior, o Mifare Classic con escritura del número de serie en sectores.

Ejemplos típicos: Oficinas comerciales y pequeñas empresas.

–Grado 3 (riesgo medio a alto)

Un sistema on-line que utiliza autenticación de dos factores o biometría de factor único para restringir el acceso. Los eventos se reciben en tiempo real en el software de gestión de accesos.

Ejemplo de tecnología de tarjeta: DESfire lectura CSN, o Mifare Classic con escritura del número de serie en sectores.

Ejemplos típicos: áreas seguras de negocios comerciales como salas de servidores, centros de datos.

–Grado 4 (Alto riesgo)

Un sistema on-line que utiliza dos, o más, factores de autenticación, uno de los cuales debe ser biométrico o de verificación de la imagen, para restringir el acceso. Los eventos se reciben en tiempo real en el software de gestión de accesos. Cuando se utiliza biometría la tasa de error ha de ser menor al 0,1%

Ejemplo de tecnología de tarjeta: Mifare DESfire con escritura del número de serie en sectores.

Ejemplos típicos: Infraestructuras críticas.

Infraestructuras criticas

El Grado 4 está especialmente orientado a la protección de Infraestructuras Críticas. Se entiende por Infraestructuras Críticas aquellas que son necesarias para el funcionamiento normal de los servicios básicos y sistemas de producción de cualquier sociedad. De tal manera que cualquier interrupción no deseada, ya sea debida a causas naturales, técnicas o por ataques deliberados, tendría graves consecuencias en los flujos de suministros vitales o en el funcionamiento de los servicios esenciales, aparte de ser una fuente de perturbaciones graves en materia de seguridad. **Tabla 2**.

Fotos: Dorlet

Tabla 2. Ejemplos de Infraestructuras Críticas.

Sectores estratégicos donde se ubican las Infraestructuras Críticas	
Administración del Estado	Industria Nuclear
Agua	Instalaciones de Investigación
Alimentación	Sistema Sanitario y de Salud
Industria de la Energía	Sistema Financiero y Tributario
Industria Aeroespacial	Tecnologías de la Información y las Comunicaciones (TIC)
Industria Química	Transportes

CAJAS FUERTES

PUERTAS Y CÁMARAS ACORAZADAS

SISTEMAS DE ANCLAJE Y RAMPAS

VALIJAS Y SUBMOSTRADORES

SISTEMAS DE INGRESOS Y CONSIGNAS

FERRIMAX
WORLDWIDE SECURITY SERVICES
www.ferrimax.com

Armarios de Seguridad, Armeros, Blindajes de Vehículos, Bases ATM, Buzones Electrónicos, Cajón Anti-atraco, Cerraduras Electrónicas y Biométricas, Compartimentos de Alquiler, Instalaciones Bancarias, Placas de Anclaje, Porta Videos, Productos Ignífugos, Puertas Blindadas, Sistema Anti-gas, Submostradores, Vitrinas Blindadas.

Servicio Técnico y Mantenimiento.

ANA MARZO. SOCIA WHITAN ABOGADOS

La **cultura del riesgo** aplicada a la **protección de datos de carácter personal**

El Reglamento General de Protección de Datos (RGPD) que entró en vigor el pasado mes de mayo de 2016 y será plenamente aplicable a partir de mayo de 2018, ha introducido en la normativa sobre protección de datos de carácter personal la necesidad de dar cumplimiento a las obligaciones legales, utilizando metodologías y herramientas de análisis y gestión de riesgos, pero no sólo en relación con los aspectos de seguridad, sino también y fundamentalmente, en relación con los aspectos organizativos y estrictamente jurídicos.

EL análisis y la gestión de riesgos será parte esencial del proceso de cumplimiento de la normativa sobre protección de datos y permitirá el mantenimiento de un entorno de cumplimiento controlado, minimizando los riesgos de vulneración de derechos y deberes de las personas, hasta niveles aceptables.

La reducción de los niveles de riesgo, se deberá realizar mediante el despliegue de medidas legales, que establezcan un equilibrio entre las categorías de personas afectadas, la naturaleza de los datos tratados, los fines de tratamiento y los riesgos de vulneración de derechos y libertades a los que estén expuestos.

Parece una tarea sencilla, pero no lo es. Y no lo es fundamentalmente porque, pese a que en el ámbito de la seguridad los técnicos están habituados a trabajar con este tipo de metodologías, en el ámbito legal la costumbre es seguir los dictámenes de las leyes, la doctrina y la jurisprudencia. Y en este tema, no tenemos ni doctrina ni jurisprudencia.

Además, el RGPD es una norma directamente aplicable, que no requiere de normas internas de trasposición (generalmente tampoco de normas de desarrollo o aplicación) y, pese a que contiene muchos conceptos, principios y mecanismos similares a los establecidos por la Directiva 95/46/CE, otros tantos son conceptos, principios y mecanismos nuevos, en un entorno donde la evolución tecnológica y de negocio, es de verdadero vértigo.

Añadido a lo anterior, el RGPD modifica algunos aspectos del régimen actual y contiene nuevas obligaciones que deben ser analizadas y aplicadas por cada organización teniendo en cuenta sus propias circunstancias.

Así que, veamos cómo podemos empezar.

El RGPD parte de la necesidad de que el responsable del tratamiento sea capaz de demostrar el cumplimiento de sus obligaciones («responsabilidad proactiva») e implantar medidas que tengan en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas. Es decir, no sirve cualquier medida.

En todo caso, con carácter general, conviene diferenciar dos cuestiones. Por un lado, los principios de protección de datos contenidos en el RGPD y por otro, las medidas.

Los principios están declarados en el RGPD y deben aplicarse a toda persona física, identificada e identificable. Y las medidas a implantar están definidas (en mayor o menor medida) en el propio reglamento, pero estas deben ser moduladas en función de determinados criterios. Estos criterios serán el resultado de llevar a cabo un análisis de riegos en la organización.

Así, podríamos decir que, los principios recogidos y regulados en el RGPD deben ser inexorablemente cumplidos por cualquier organización y sin embargo, las medidas que el RGPD establece se aplicarán y modularán en función del nivel y tipo de riesgo que los tratamientos presenten.

La aplicación de las medidas previstas por el RGPD debe, por tanto, adaptarse a las características de las organizaciones.

Cualquier organización que se enfrente al cumplimiento del RGPD, deberá llevar a cabo con carácter previo un análisis y tratamiento de los riesgos a los que están expuestos los derechos y libertades de los interesados.

Y cuando el resultado de este análisis suponga la existencia de un «alto riesgo» para los derechos y libertades de las personas, la organización, con carácter previo a llevar a cabo el tratamiento, deberá además realizar una Evaluación de Impacto en la Protección de Datos (EIPD).

En el caso del análisis inicial de riesgos, la probabilidad y la gravedad del riesgo para los derechos y libertades del interesado, deberá determinarse con referencia a la naturaleza, el alcance o número de interesados afectados, el contexto, los tipos y fines del tratamiento de datos y la cantidad y variedad de tratamientos que una misma organización lleve a cabo. El riesgo debe ponderarse sobre la base de una evaluación objetiva, mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto (en cuyo caso deberíamos llevara a cabo una EIPD). Según indica la Guía del Reglamento General de Protección de Datos[1] , en «grandes organizaciones», como regla general, el análisis deberá llevarse a cabo utilizando alguna de las metodologías de análisis de riesgo existentes y en «organizaciones de menor tamaño y con tratamientos de poca complejidad», el análisis será el resultado de una reflexión, mínimamente documentada, sobre las implicaciones de los tratamientos en los derechos y libertades de los interesados.

En pequeñas organizaciones, seguramente bastará un análisis informal, en lenguaje natural, que (a) identifique los tratamientos en los términos indicados, (b) las amenazas más probables; (c) las salvaguardas o medidas que protejan de dichas amenazas; y (d) la identificación de los riesgos residuales.

«El RGPD es una norma directamente aplicable, que no requiere de normas internas de trasposición»

En el caso de la EIPD, la finalidad será valorar la particular gravedad y probabilidad del «alto riesgo», teniendo en cuenta el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo, así como la naturaleza, ámbito, contexto y fines del tratamiento. Dicha evaluación de impacto debe incluir, en particular, las medidas, garantías y mecanismos previstos para mitigar el riesgo, garantizar la protección de los datos personales y demostrar la conformidad con el RGPD.

Y después del análisis ...

Después del análisis de riesgos, cada organización deberá desarrollar e implantar su propio sistema de gestión de riesgos (prevención, detección y reacción), así como adoptar medidas para mitigar o suprimir los riesgos, las cuales por tanto, deberán estar plenamente justificadas, existiendo en todo caso una proporcionalidad entre las medidas adoptadas y los riesgos identificados.

Y de cualquier manera, tanto en uno como en otro caso es preciso que el análisis y gestión de los riesgos no sean una cuestión puntual, sino que, deberán mantenerse permanentemente actualizados, en tanto el responsable mantenga en vigor los tratamientos.

En definitiva, una buena gestión de la protección de datos para dar cumplimiento al RGPD significa tener procesos y metodologías eficaces para mantener el cumplimiento de todos los principios contenidos en el RGPD. ●

1-Fuente: https://www.agpd.es/portalwebAGPD/temas/reglamento/index-ides-idphp.php estado de sus sistemas.

Contactos de empresas, p. 7.

JOSÉ IGNACIO OLMOS CASADO. DIRECTOR DE SEGURIDAD. FORMADOR AVSEC Y TÉCNICO EN FORMACIÓN

La formación específica del personal de seguridad privada en España

Cuando hablamos de garantizar a los ciudadanos un derecho fundamental como es la seguridad, recogido en el artículo 17 de nuestra Constitución, en un Nivel de Alerta 4 en el Plan de Prevención y Protección Antiterrorista, y teniendo en cuenta que en nuestro país contamos con casi 80.000 vigilantes de seguridad en activo prestando servicio (más efectivos que los cuerpos de seguridad pública), la formación de este personal se convierte en elemento fundamental para contribuir a cumplir la misión que la Ley 5/2014, de Seguridad Privada le encomienda a ésta como complementaria de la Seguridad Pública.

DESDE el año 2012, al aparecer la Resolución de 12 de noviembre, de la Secretaría de Estado de Seguridad, por la que se determinan los programas de formación del personal de seguridad privada, se desarrollan los contenidos de los cursos de formación específica que, como antecedente, aparecieron en la Orden INT 318/2011, de personal.

La idea de la formación específica es muy buena; la especialización es fundamental en este ámbito. Sin embargo, la forma en la que se ha llevado a término es, a mi juicio, bastante desafortunada, y debe ser objeto de una severa crítica en los siguientes términos:

– En primer lugar es criticable que una formación específica sea válida a efectos de formación permanente, pues ésta ha de ser una formación destinada a reciclarse, es decir, a refrescar los conocimientos adquiridos en la formación básica.

– Es llamativo que en los catorce tipos de servicios establecidos en la norma falten algunos tan básicos y tan importantes en la actividad económica de nuestro país como puedan ser los hoteles o infraestructuras turísticas, parques de ocio y diversión, centros de control y otros.

Shutterstock / Africa Studio

Duración mínima establecida

– La duración mínima establecida es claramente insuficiente; si bien es cierto que la administración deja a juicio de los organizadores de la formación la duración que se considere conveniente más allá de esas diez horas, la experiencia nos dice que por costes económicos no se realizan más que diez horas presenciales con carácter general, lo cual limita los conocimientos a unas pocas pinceladas básicas.

– Los contenidos de bastantes de los cursos son manifiestamente inadecua-

dos, apareciendo temas poco importantes y faltando otros indispensables. Es reseñable por ejemplo en el curso de rayos x la ausencia en el temario de lo relativo a máquinas detectoras de trazas o de líquidos, equipos que se vienen manejando hace años.

– En el análisis de esos contenidos encontramos en bastantes de los cursos materias que se dan en la formación básica como la protección contra incendios o los primeros auxilios (cuando no un curso entero como el de transporte de fondos o el de vigilancia con aparatos de rayos x que se estudia en el tema «medios de detección» del área instrumental), que no deberían impartirse en una formación específica; así mismo, no tiene sentido, por ejemplo, que al personal de un centro comercial se le pida que sepa sobre primeros auxilios y al de un museo no.

– Otra cuestión siempre importante son las prácticas; el ámbito práctico es siempre interesante, pero sobre todo en algunos cursos concretos es imprescindible: servicios de vigilancia con perros y aparatos de rayos x. Bien, pues en España con la normativa en la mano uno puede hacer estos cursos y no conocer al perro o tocado una radioscopia, es decir, con 10 horas teóricas y un manual, ya he recibido la formación específica en la materia.

Shutterstock / Pressmaster

«Los contenidos de bastantes de los cursos son manifiestamente inadecuados, apareciendo temas poco importantes y faltando otros indispensables»

– Así mismo representa una problemática la impartición de los cursos específicos a personal aún no habilitado y su sellado en cartilla; es un mero problema de entendimiento legal: la formación específica es para vigilantes, cosa que un aspirante aún no es.

Shutterstock / Matej Kastelic

Conclusiones

Después de lo visto no nos queda más que afirmar que la formación específica del personal de seguridad privada es insuficiente e inadecuada.

Los órganos de control de la Administración deben ser dotados de más medios para un mayor cumplimiento de la legislación vigente, y el legislador debe tomar conciencia de que debe realizar su labor competentemente.

Espero que esta problemática se solucione en un futuro próximo. ●

Fotos: Archivo

JORNADA ORGANIZADA POR LA GUARDIA CIVIL, BAJO LA COORDINACIÓN DEL SERVICIO DE PROTECCIÓN Y SEGURIDAD (SEPROSE)

III Jornada sobre «Situación de la amenaza terrorista yihadista»

En el marco del programa COOPERA y PLUS ULTRA, la Guardia Civil convocó a más de un centenar de profesionales el pasado 26 de abril en el salón de actos de la Asociación de Huérfanos de la Guardia Civil en Madrid. Bajo la coordinación del Servicio de Protección y Seguridad (SEPROSE), la III Jornada sobre la «Situación de la amenaza terrorista yihadista» sirvió de punto de encuentro profesional para conocer la situación actual y evolución de la amenaza terrorista yihadista, así como reforzar la colaboración público privada en esta materia.

La jornada fue inaugurada por Pedro Díaz, General de la Jefatura de Unidades y de Reserva de la Guardia Civil, acompañado de Andrés Sanz, Coronel jefe del SEPROSE.

Situación Geopolítica y Geoestratégica en Zonas de Implantación de Organizaciones Yihadistas

La primera ponencia fue impartida por Miguel Ángel Ballesteros, General de Brigada de Artillería y Director del Instituto Español de Estudios Estratégicos, exponiendo de forma exhaustiva las claves geopolíticas y los intereses estratégicos de cada uno de los actores de las diferentes zonas de conflicto, dejando una clara conclusión: Aquellas zonas donde exista riesgo de un estado fallido y no controlado, es una zona potencial para el establecimiento de organizaciones yihadistas y un claro riesgo para la seguridad.

Situación y evolución de la amenaza terrorista yihadista

El Capitán Rafael Navarro, de la Jefatura de Información de la Guardia Civil, realizó un análisis de valoración de la amenaza basándose en acciones recientes en Europa y explicando los motivos por los cuales se ha incrementado las acciones terroristas en territorio europeo, y cómo las Fuerzas y Cuerpos de Seguridad establecen procedimientos para prevenir y detectar este tipo de amenazas, en especial el control y seguimiento de los combatientes extranjeros y su retorno a sus países de origen.

Respuesta Operativa ante actuación yihadista

Después tuvo lugar una ponencia sobre la respuesta operativa ante una actuación terrorista, impartida por el Teniente del Centro de Adiestramientos Especiales de la Unidad de Acción Rural de la Guardia Civil, Antonio Perchín, quien expuso las características principales de los últimos ataques perpetrados por terroristas yihadistas en Europa, así como las principales amenazas y recomendaciones para el establecimiento de protocolos de actuación, destacando el protocolo americano RUN-HIDE-FIGHT.

Medidas de autoprotección

Para finalizar, Alberto Tovar, director de seguridad de CEPSA y José Manuel Parejo, responsable de Seguridad Internacional de CEPSA, expusieron un caso práctico de medidas de autoprotección en su corporación, destacando la implicación del departamento de Seguridad en la protección de todo su personal, especialmente el expatriado, y de la necesidad de contar con un procedimiento de evaluación de amenaza y análisis de riesgos continuo, basado en modelos de inteligencia corporativa y protocolos de actuación actualizados para poder ofrecer una respuesta inmediata frente a estas y otras amenazas.

Texto y Fotos: Redacción.

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**.

SPIDER
Full Control Included

VdS

www.baussa.com

BAUSSA
INDUSTRIAS DE SEGURIDAD

TECNOLOGÍA DIGITAL Y CIBERDELINCUENCIA CENTRAN EL DEBATE

X Jornada «Seguridad en Casinos de Juego»

Al amparo de la Asociación Española de Casinos de Juego y el Cuerpo Nacional de Policía, y con el patrocinio de Heitel, Arquero, Axis y Xtralis, se celebró los pasado días 8 y 9 de marzo en Badajoz, la X Jornada de Seguridad en Casinos de Juego, siendo esta convocatoria la que mayor representación de Responsables de Seguridad en Casinos ha tenido. Durante los dos días se impartieron diferentes ponencias y se analizaron las amenazas actuales y futuras que afectan a la seguridad de los casinos de juego.

La jornada fue inaugurada por Mª Cristina Herrera Santa-Cecilia, Delegada del Gobierno en Extremadura, y por el Vicepresidente de la Asociación de Casinos, Ángel María Escolano, y con la presencia de altos cargos policiales y del Servicio de Control de Juegos de Azar.

La primera ponencia técnica de la jornada fue impartida por Serafín Román, Director General de Heitel, bajo el título: «Nuevas tecnologías para reforzar la Seguridad en los Casinos». Durante la ponencia, se expuso que las nuevas tecnologías están basadas en la mejora de la tecnología digital al servicio de la Seguridad. Desde cámaras IP que controlan unas grabaciones precisas que son almacenadas en discos duros, hasta cámaras con lecturas de matrículas, lectores de huellas y por supuesto, reconocimiento facial, técnicas que permiten reconocer a una persona antes de identificarse. Así mismo destacó la importancia de los sistemas integrales de controles de acceso, que constituyen una alternativa vital en aras de proteger los activos de los establecimientos de juego y, en caso de que se produzcan, poder desvelar la identidad de los responsables.

Bajo el título «Fraude mediante medios de pago», Miguel Martín Martín, Inspector Jefe de la Brigada de Delincuencia Financiera de la UDEF del Cuerpo Nacional de Policía, realizó una presentación basada en la investigación sobre el fraude con tarjetas de crédito y travel cheques. Este último sistema prácticamente desaparecido, actualmente todo está basado en las tarjetas de crédito y sus distintas formas de co-

piar, clonar o falsificar. Entre estos sistemas destacó un lector que se introduce dentro de los cajeros que copia la tarjeta, sin que su propietario se percate de nada. Una vez copiada o clonadas, son usadas en compras a través de internet y habitualmente en otros países para que los cargos tarden en llegar al propietario.

Para hacer frente a esta amenaza, la sección de medios de pago del Cuerpo Nacional de Policía tiene encuentros y reuniones con los procesadores de los medios de pago y departamentos de Seguridad de entidades bancarias, además de coordinación con Interpol, Europol, Eurojust, etc. De igual forma las entidades proveedoras de medios de pago y los comercios tratan de diseñar mejores procedimientos para evitar el fraude.

«Ciberseguridad en el juego» fue el título de la ponencia impartida por Marta Fernández, Inspectora del Grupo de Redes Abiertas de la Unidad de Investigación Tecnológica del Cuerpo Nacional de Policía. Destacó que la delincuencia especializada está pasándose a los robos por internet que son más rápidos, más seguros y el rastro que dejan es mínimo por lo que la investigación se hace más ardua. Desde robarte imágenes a través de la cámara de nuestros PC para luego proceder al chantaje hasta acceder a cuentas bancarias para vaciarlas. Lo que busca la Ciberseguridad es proteger la información digital en los sistemas interconectados (Redes). Para ello, las recomendaciones más importantes son utilizar unos buenos sistemas antivirus, anti spam y conectarse siempre con páginas seguras (https). Las empresas tienen mucho margen de mejora para protegerse ante los ciberataques ya que todavía consideran un gasto superfluo dichas protecciones. Se hizo especial énfasis en la importancia de denunciar estos casos lo antes posible y de disponer el mayor número de pruebas posible para facilitar la investigación. Además las empresas deben valorar qué activos son los más vulnerables y planificar la Seguridad de acuerdo con esas valoraciones. Las barreras que protegen de los delitos informáticos son débiles frente a los ciberdelicuentes, cada vez más sofisticados.

«Durante dos días se analizaron las amenazas actuales y futuras que afectan a la seguridad de los casinos de juego»

A continuación se celebró una mesa debate donde el Jefe del Servicio de Control de Juegos de Azar, Jesús Fuentes Sastre, analizó casos ocurridos en el resto del mundo a través de las informaciones recibidas tanto por Europol como por Interpol. Ángel Pérez Alcarria, Director de Seguridad del Grupo Gran Madrid, hizo un análisis de la evolución de la delincuencia en los Casinos durante 2016 y las previsiones para 2017, y Pablo González Salcines, Director de Seguridad del Casino de Badajoz, habló de los clientes portugueses, ya que en ese casino y por la proximidad con Portugal, tienen muchas visitas de esa nacionalidad, así como de su idiosincrasia en el juego. Por último, el Jefe de Seguridad del Casino de Castellón, Gregorio Abril Doñate, anunció su próxima jubilación, no sin antes hacer una comparativa entre la Seguridad Pública y la Seguridad Privada.

A la finalización del acto y antes de la clausura, se entregó una placa conmemorativa al Director de Seguridad del Casino de Badajoz como agradecimiento a su buena labor para la preparación y desarrollo de este evento.

Tras el almuerzo, los asistentes tuvieron la oportunidad de desplazarse al Casino de Estoril, siendo recibidos por su Director de Juego, Manuel Ho, y por el Director de Seguridad, Rui Melo, quienes mostraron a los presentes las instalaciones y relataron su trabajo habitual, brindando la posibilidad de establecer nuevos campos de colaboración con el país vecino. Tras la cena ofrecida por ese Casino, los asistentes regresaron a Badajoz para dar por concluida la X Jornada de Seguridad en Casinos de Juego. ●

ASOCIACIÓN ESPAÑOLA DE EMPRESAS DE SEGURIDAD. AES

12 Encuentro Seguridad Pública & Seguridad Privada

La Asociación Española de Empresas de Seguridad, AES, celebró el pasado día 27 de abril en Madrid el 12 Encuentro Seguridad Pública & Seguridad Privada, en el que se abordaron los diferentes planes estratégicos de las Fuerzas y Cuerpos de Seguridad en el ámbito de la Seguridad Privada, así como se profundizó en el Manifiesto de AES y el documento de Recomendaciones para el Diseño de Medidas en la Protección de Instalaciones Estratégicas SRC 915 765 225.

TRAS unas palabras de bienvenida a cargo de Antonio Pérez, presidente de AES, comenzó el turno de intervenciones con la ponencia de Manuel Yanguas, Comisario Jefe de la Brigada Central de Empresas, de la UCSP, donde anunció, dentro de las acciones del Plan quinquenal de la UCSP, la reestructuración de la unidad, la apuesta por una mayor colaboración, así como nuevas líneas de actuación. «Potenciaremos nuestra presencia en encuentros profesionales, el control e inspección de los centros de formación, así como la lucha contra el intrusismo y el fraude», apuntó.

Andrés Sanz, Coronel Jefe del Servicio de Protección y Seguridad (SEPROSE) de la Guardia Civil, anunció la puesta en marcha de planes anuales de inspección «sólidos y serios» en los que están involucradas las unidades territoriales y provinciales del servicio, con el objetivo de luchar también contra el intrusismo. Además, Sanz apostó por incrementar la integración funcional de las capacidades de ambas seguridades, a través de planes de cooperación y colaboración.

Montserrat Martínez, jefe de la Sección de Legislación y Estudios del Servicio de Normativa y Coordinación del CNPIC, analizó el estado actual de la implantación del Sistema PIC, que se encuentra en su cuarta fase, y del que explicó que conlleva un proceso muy dinámico, así como del trabajo que desarrolla el organismo en cuanto a esquemas de normalización y certificación, enmarcado dentro de la Normativa NIS.

Francisco Llaneza, Jefe de la Unidad de Seguridad Privada de la Ertzaintza, señaló que a lo largo del año pasado se habían llevado a cabo cerca de 1.400 inspecciones a empresas, acción que se llevará a cabo también este año, además de potenciar la lucha contra el intrusismo. Llaneza destacó la apuesta de la unidad porque todo se tramite por sede electrónica.

Carles Castellano, Jefe de la Unidad de Seguridad Privada de los Mossos d´Esquadra, anunció el establecimiento de Planes de Seguridad donde «se recoge el eje estratégico de colaboración con el sector de la seguridad privada», la inspección y control de los centros de formación «para que todo se realice de forma correcta».

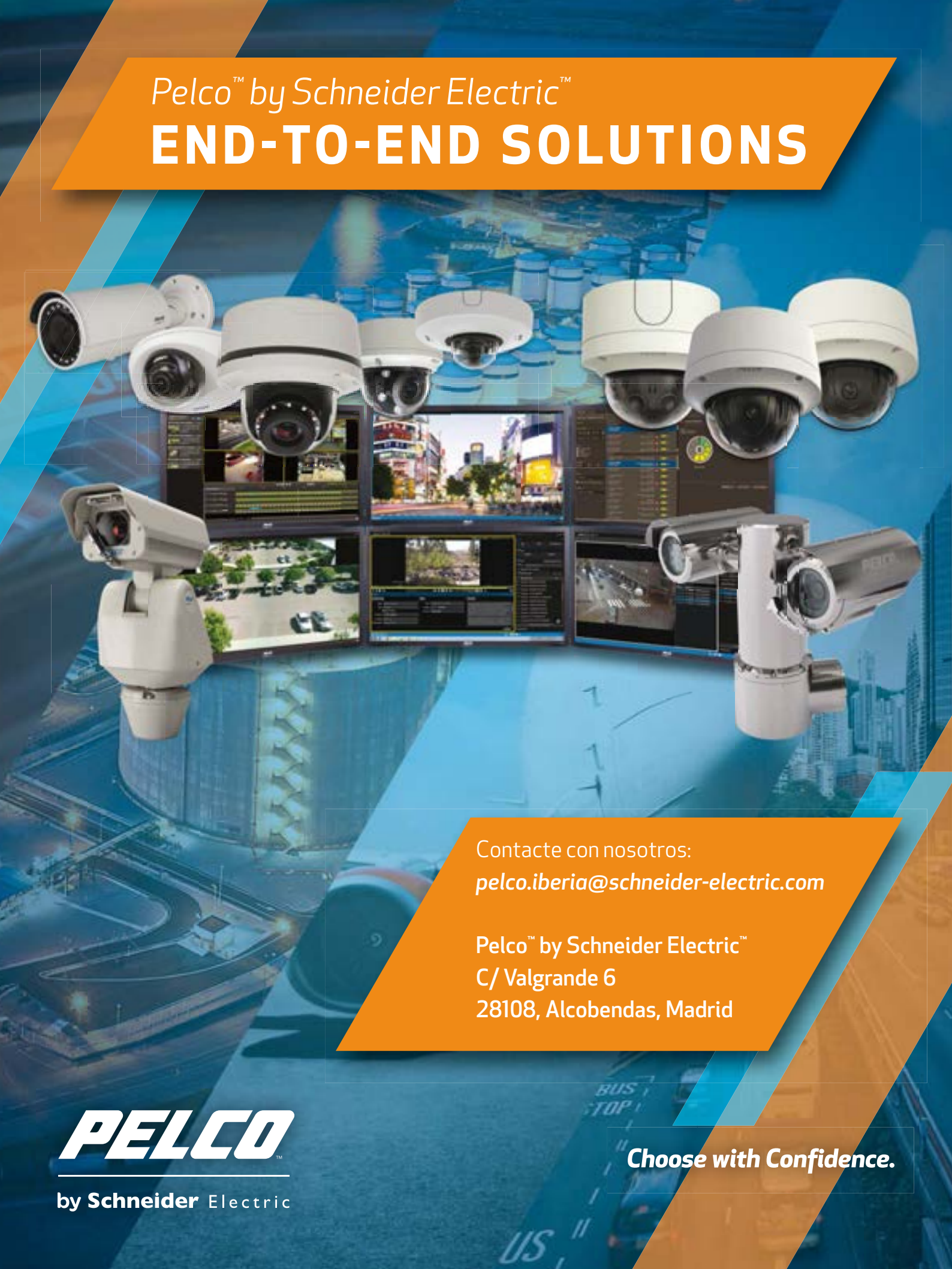
Antonio Escamilla, vicepresidente de AES, explicó el Manifiesto AES «Por una España y Europa Segura» y el propósito de la asociación de llevar a cabo una «ronda de evangelización con el sector».

Julio Pérez, de AES, llevó a cabo un análisis del personal acreditado según la Ley de Seguridad Privada, donde destacó la problemática en la definición de funciones, su formación y proceso de acreditación, al tiempo que hizo hincapié en la potenciación de la formación continua acorde a las nuevas tecnologías.

Manuel Sánchez Gómez Melero, vocal de la AES, explicó el documento elaborado por la AES sobre «Recomendaciones para el diseño de medidas en la Protección de Instalaciones estratégicas».

Pelco™ by Schneider Electric™

END-TO-END SOLUTIONS



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

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

PELCO™
by Schneider Electric

Choose with Confidence.

TYCO INTEGRATED FIRE & SECURITY PRESENTA LAS ÚLTIMAS TENDENCIAS EN SOLUCIONES DE SEGURIDAD Y PROTECCIÓN CONTRA INCENDIOS

«Making Progress Together»: Industrias y edificios más inteligentes, seguros y sostenibles

Tyco Integrated Fire & Security, empresa mundial en soluciones de seguridad y protección contra incendios, ha celebrado el evento «Making Progress Together: Industrias y edificios más inteligentes, seguros y sostenibles», donde se mostraron las últimas tendencias en soluciones de seguridad y protección contra incendio en sus dos showroom móviles. El evento, que se realizó en el Circuito del Jarama de Madrid, dio a conocer de un modo práctico, el amplio portfolio de soluciones de la compañía.

Entre las soluciones presentadas:

– Showroom móvil con soluciones de seguridad de Tyco Security Products: Desde la gestión de alertas hasta la prevención de riesgos y pérdidas, las plataformas de integración pueden ayudar a gestionar mejor la seguridad, y a aumentar el rendimiento del negocio gracias a su facilidad de uso y el acceso rápido a la información. La implantación de sistemas PSIM (Physical Security Information Management) permite unificar la gestión de diferentes plataformas en una sola, simplificando los diversos procesos. Mediante este workshop se mostró de modo muy práctico la tecnología más avanzada y las soluciones más adecuadas para cada sector y cómo integrarlas. En él se expuso toda la gama de productos Tyco: American Dynamics, Kantech, Software House, DSC, Visonic, Bentel Security y Exacq.

– Showroom móvil con soluciones de detección y extinción de incendios de Tyco Fire Protection Products: Los incendios son uno de los mayores riesgos a los que nos enfrentamos pero gracias a las nuevas tecnologías se ha conseguido alcanzar nuevos niveles de protección que garantizan una detección de incendios más rápida. Minimizar así, los diversos daños que pudieran producirse. En este showroom se mostró el nuevo panel de detección de incendios Profife y sus complementos, además de sus detectores de llamas FLAMEVision. Los asistentes pudieron comprobar su funcionamiento mediante tests de pruebas de los elementos de detección.

Esta muestra forma parte de una campaña para la formación y demostración de soluciones de seguridad de Tyco Security Products por Europa Occidental, que recalará en Irlanda, Bélgica, Holanda, Finlandia, Alemania, Inglaterra e Italia.

La visión de Tyco sobre el futuro de la seguridad se traduce en una estrategia basada en la integración de los diferentes sistemas de seguridad con plataformas de software que gestionen la información de seguridad física, las plataformas PSIM (Physical Security Information Management). ●

Texto y Fotos: Tyco

Contactos de empresas, p. 7.

DOCUMENTO ELABORADO POR TECNIFUEGO-AESPI

Se presenta la I Guía de **Sistemas de Protección Pasiva contra Incendios**

Madrid fue escenario de la presentación de la primera Guía de «Sistemas de Protección Pasiva contra Incendios en la edificación. Conceptos generales y clasificación». Se trata de un documento elaborado, tras años de trabajo, por el grupo de expertos del Comité de Productos de Protección Pasiva de TECNIFUEGO-AESPI.

La presentación, guiada por Vicente Mans y Jordi Bolea, responsables del Área de Protección Pasiva y del Comité, respectivamente, tuvo lugar en el Auditorio de UNESPA ante un público interesado en las novedades y facilidades que introduce este documento para la protección pasiva de un edificio frente a un incendio.

Durante el acto, Vicente Mans informó de la actividad de la Asociación y de los avances que se están promoviendo para profesionalizar y normalizar el área de la Protección Pasiva contra Incendios (PPCI), especialmente en la aplicación e instalación de productos. «Estamos trabajando en el Registro de Instalador de Protección Pasiva, un avance necesario para regular una profesión que necesita de profesionales bien formados y acreditados», adelantó Mans.

Regulado, pero no se cumple siempre

Por su parte, Jordi Bolea insistió en que «El sector de la Protección Pasiva contra Incendios está regulado, pero no se cumple siempre. Si bien los productos aplicables deben disponer de los correspondientes certificados de calidad y de prestaciones, la realidad es muy diferente para otros intervinientes en el proceso como son: los prescriptores, los instaladores, los técnicos de las entidades de control y los de las compañías de seguros para quienes existe poca información técnica para poder desarrollar su trabajo».

Trece sistemas de protección pasiva

Esta Guía viene a contribuir a la información y formación en el campo de aplicación de los productos de PPCI. En el texto se describen 13 sistemas de protección pasiva, y para cada uno de ellos se hace una descripción genérica, y se desarrollan sus diferentes tipologías, se indica la normativa aplicable, y en algunos casos se identifican particularidades relativas al uso, o la instalación, riesgos laborales o para la salud, etc.

El documento impreso está disponible en TECNIFUEGO-AESPI y tiene un precio especial y simbólico de 5 euros para asociados y 10 euros para empresas y profesionales no asociados. ●

Tyco y By Demes Group, acuerdo de distribución de productos DSC

La marca de sistemas anti-intrusión DSC cuenta con una nueva alianza en España y Portugal. By Demes Group se ha convertido en el nuevo distribuidor oficial de los sistemas de seguridad DSC, firma perteneciente a la multinacional de alarmas y seguridad Tyco.

El nuevo acuerdo alcanzado permitirá a los clientes de By Demes Group tener acceso directo con stock permanente a los productos DSC, los cuales incluyen las gamas de productos DSC NEO y DSC WIRELESS.

Los productos ya están disponibles para todos los clientes de By Demes Group y son comercializados a través de su extensa red comercial en el territorio de Iberia, con todo el excelente soporte técnico-comercial que caracteriza a la distribuidora especializada de material electrónico de seguridad.

DSC, como una de las marcas destacadas en la industria del diseño y fabricación de alarmas y productos de seguridad electrónica, es reconocida por su alta calidad y superior desempeño en más de 140 países. Se caracteriza por ofrecer productos innovadores y fáciles de instalar, programar, mantener y usar, además de disponer del mejor y más extenso Vía Radio del mercado gracias a la tecnología POWERG heredada de la adquisición de Visonic por el Grupo Tyco.

Los puntos fuertes del nuevo catálogo DSC para By Demes Group son las nuevas centrales compactas DSC WIRELESS fabricadas con el corazón de VISONIC - POWERMASTER bajo el nombre DSC, así como la más extensa y potente gama de productos Vía Radio del mercado con protocolo POWERG. Además, esta gama Vía Radio POWERG puede ser utilizada tanto para las centrales compactas DSC WIRELESS como para las centrales POWER NEO, facilitando stockajes y referencias adicionales.

Aprobado el Reglamento de Instalaciones de Protección contra Incendios

Según anticipó TECNIFUEGO-AESPI hace unos días, el Consejo de Ministros aprobó el 19 de mayo, mediante un Real Decreto, el Reglamento de instalaciones de protección contra incendios (RIPCI). El objeto del mismo es determinar las condiciones y los requisitos exigibles al diseño, instalación, mantenimiento e inspección de los equipos, sistemas y componentes que conforman las instalaciones de protección activa contra incendios.

El RIPCI es fundamental para la seguridad contra incendios ya que incorpora tanto las exigencias derivadas de la implantación de la legislación europea, como la regulación de los sectores que no estaban contemplados y los productos que no se encontraban amparados por normas armonizadas.

En la publicación que hace La Moncloa se concretan los siguientes aspectos:

- Las condiciones y requisitos que deben cumplir los equipos, sistemas y componentes de protección contra incendios.
- Las condiciones de habilitación y funcionamiento de las empresas instaladoras y mantenedoras.
- Las condiciones para la instalación, puesta en servicio, mantenimiento mínimo e inspecciones periódicas de estas instalaciones.
- El régimen sancionador.

Las instalaciones de protección contra incendios se rigen actualmente por un Reglamento del 5 de noviembre de 1993. No obstante, la evolución, tanto de la técnica como del marco normativo, hace imprescindible actualizar y revisar los requisitos establecidos en el citado Reglamento. En concreto, pueden citarse dos Reglamentos comunitarios de 2008 y 2011.

Por otro lado, el Reglamento de seguridad contra incendios en los establecimientos industriales, de 2004, y el Código Técnico de la Edificación, de 2006, establecen que el diseño, la ejecución, la puesta en funcionamiento y el mantenimiento de las instalaciones de protección contra incendios, así como sus materiales, componentes y equipos, deben cumplir lo establecido en su reglamentación específica. Se hace necesario, en consecuencia, establecer las condiciones que deben reunir los equipos y sistemas que conforman las instalaciones de protección contra incendios para lograr que su funcionamiento, en caso de incendio, sea eficaz.

Tecnifuego-Aespi: Marta Peraza, nueva secretaria general

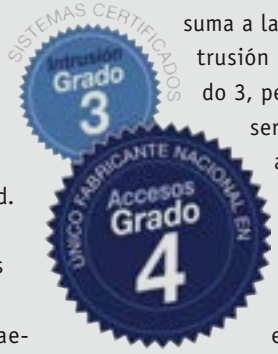
LA Junta Directiva de Tecnifuego-Aespi ha ratificado el nombramiento de la nueva secretaria general de la Asociación, Marta Peraza Parga.

Peraza tiene una dilatada experiencia en la organización y gestión de certámenes, proyectos y organismos. Conoce, el papel fundamental de las asociaciones sectoriales en la dinamización, desarrollo y tecnificación del sector al que sirve y su capacidad de interlocución ante las administraciones y las instituciones.

Marta Peraza es licenciada en Derecho y ha desarrollado gran parte de su carrera profesional en IFEMA, desde diversos cargos de responsabilidad, y como directora de las ferias relacionadas con automoción. Además, en el ámbito del asociacionismo ha sido gerente de una federación del sector de la salud y ha participado en proyectos de potenciación y promoción de la imagen de España en el exterior, en colaboración con Marca España. En su periodo profesional más reciente, ha retomado su formación jurídica, ejerciendo como analista de protección internacional en el Ministerio del Interior.

Dorlet, primer fabricante nacional en obtener la certificación de control de accesos EN 60839 (Grado 4)

Dorlet, dentro de su compromiso con sus clientes, de suministrar los más avanzados sistemas de control de accesos e integración de sistemas de seguridad, ha certificado sus sistemas dentro de la nueva norma de Control de Accesos EN 60839, concretamente en el Grado 4, el más alto posible, de esta forma sus clientes pueden acometer instalaciones con las más altas exigencias de seguridad. Proyectos como edificios gubernamentales, instalaciones de I+D, zonas de producción críticas, industria nuclear o aeroespacial... pueden ser realizadas con completa solvencia técnica y cumpliendo la nueva normativa gracias a nuestros sistemas de control de acceso (UCAs y lectores) y a la plataforma de software Dorlet DASSnet. Esta certificación se suma a la ya obtenida en Intrusión EN 50131 para Grado 3, permitiendo a Dorlet ser la opción más aconsejable para instalaciones con un sistema de seguridad integral. Más información en www.dorlet.com.



Visiotech: Cursos de Certificación en CCTV Safire

CONTINUANDO con su proceso de implantación en el mercado europeo, la marca de CCTV Safire organiza cursos de certificación a través de sus distribuidores españoles.

Estos cursos, orientados a instaladores profesionales de seguridad, tratan de formar técnicamente a los asistentes en la instalación, configuración y uso cotidiano de los equipos Safire. Se cubre fundamentalmente la configuración de videograbadores y de NVR IP, aunque también se trata directamente de cámaras IP, cámaras analógicas 720p, 1080p y las nuevas cámaras analógicas de 3 Mpx y 5 Mpx.

Las ventajas para los asistentes son importantes. En primer lugar, son cursos gratuitos. En segundo lugar, la formación es dada por personal español altamente cualificado. Tras la formación, se pasa un test a los asistentes y al cumplimentarlo, los instaladores reciben el certificado CCTV Safire, una ampliación de la garantía en productos Safire de 3 a 5 años, apoyo técnico directo del fabricante y un kit CCTV de regalo (grabador 1080p y cámara).

En el mes de junio, los cursos de certificación serán los siguientes:

- En Málaga, Mercasat (www.mercasat.es), el 22 de junio.
- En Valencia, JM Systems (www.jmsystems.es) el 29 de junio.

Para apuntarse a cualquiera de estos cursos, únicamente es necesario contactar con cualquiera de estas empresas distribuidoras.

Reunión de primavera del blog Potluckforum

Desde que se puso en marcha el blog de seguridad bancaria Potluckforum, han celebrado tres reuniones presenciales con ponentes nacionales e internacionales, expertos en esta materia: Directores de Seguridad de Entidades Financieras e integrantes de la Seguridad Privada y Pública. En el caso de estos últimos, han contado no solo con la presencia de responsables del control de la regulación administrativa, sino también de las Unidades de Investigación de esta nueva delincuencia, violenta y lógica. Dichas jornadas terminaron con intensos y productivos debates de los que extraer conclusiones para mejorar esta específica seguridad.

La última reunión tuvo lugar el pasado 26 de abril en el Club Financiero Génova. El interés que habían suscitado las distintas publicaciones del Blog sobre Cajeros Automáticos marcó la pauta para celebrar una jornada monográfica sobre Cajeros Automáticos, en la que estuvo como ponente Leonel Martínez, Ejecutivo de Diebold Nixdorf, que bajo el título genérico de «Visión y experiencia desde la perspectiva del fabricante», disertó sobre las tendencias de fraude contra los ATMs en LATAM: ataques con malware, cash trapping, skimming... Abundó también en la mejora de la seguridad en los cajeros, Self Service Trusted Computing y HW lectura encriptados, así como la mejora de las operaciones en los ATMs, con soluciones como el Sistema Active Guard TM o el control inteligente de fraude en unidades y errores de seguridad lógica del disco duro. Terminó ofreciendo algunos datos de interés sobre la nueva tecnología para la lectura de las tarjetas (Sistema ActiveEdge).

Posteriormente dos representantes de la banca española pusieron de manifiesto las distintas formas de ataques a cajeros automáticos en nuestro país, las medidas empleadas para evitarlo y lo que esperan de la regulación administrativa de estas máquinas en el nuevo Reglamento de Seguridad Privada.

Cerró la fase de ponencias el representante de la Administración, Comisario Jefe de la U.C.S.P., Esteban Gándara,-cargo que ocupaba al cierre de esta edición- dando a los asistentes un anticipo de cómo ven ellos las medidas de seguridad que deben cumplir los cajeros para prevenir los delitos, impedir los robos y consecuentemente evitar la alarma social que estos actos generan.

En el posterior debate con el que se cerró la jornada, participaron miembros de la Judicatura, CC y FF de Seguridad, Estatales y Autonómicos, y los Directores de Seguridad de los principales bancos del país. «Sin duda, este tipo de foros resultan de gran utilidad para intercambiar experiencias y conocimientos en la lucha contra esa nueva forma de delincuencia, máxime cuando las entidades financieras siguen siendo oscuro objeto del deseo de los delincuentes y está mutando de los tradicionales ataques físicos, a los más modernos y sofisticados, lógicos», señalan desde la organización

Para finalizar, dejar constancia de que el Blog: www.potluckforum.es ha alcanzado un alto nivel de interés que, «esperamos seguir manteniendo con nuestras publicaciones, y pensando ya en la jornada presencial del otoño».

Hommax comprometida con sus clientes

HOMMAX cumple con el compromiso adquirido con sus clientes y amplía su plantilla; incrementar un 20% la facturación permite a Hommax crecer como empresa, reforzando sus áreas más sensibles, técnica, almacén y comercial.

Después de haber sido la primera empresa de distribución de aplicaciones electrónicas de seguridad en certificarse en el modelo de calidad ISO, «solo nos queda por cumplir con nuestros compromisos adquiridos durante los más de 37 años de experiencia acumulada, haciendo que las cosas siempre estén bien hechas y a la primera».

«Hacemos caso a la demanda de nuestros clientes - señalan desde la compañía- y aportamos mayor valor añadido, personas que creen en lo que están haciendo y en el compromiso que adquiere Hommax con ellos, mejorando nuestra respuesta en la consultoría técnica, mejorando en el envío de nuestra paquetería, mejorando en la preventa y la postventa».

En palabras de su Director General, José Torner, «En Hommax, siempre hemos creído que el valor de las personas es el valor de nuestra empresa, por ello nos sentimos muy orgullosos de poder crecer no solo en resultados, sino en medios y personas».

Contactos de empresas, p. 7.

Detnov: Detnov Explorer, telemantenimiento y control remoto de las instalaciones de detección de incendios

Detnov Explorer es la solución que muchos estaban esperando en el sector de la seguridad contra incendios ya que permite monitorizar y controlar remotamente cualquier central de detección de incendios de Detnov.

La tarjeta de comunicación TCP/IP con referencia TED-151WS, se instala en el interior de la gama de centrales convencionales CCD-100 o de las centrales analógicas CAD-150, la cual nos permite la conexión a Internet de nuestras centrales a través del puerto Ethernet que viene en la placa de la tarjeta.

TED-151WS dispone de un Web Server integrado que nos permite interactuar a distancia mediante Detnov Explorer a través de iconos visualizados en el navegador web (Google Chrome, Firefox, Internet Explorer, Safari, etc.) de cualquier dispositivo (Smartphone, Tablet o PC) siempre que disponga de acceso a Internet.

Detnov Explorer nos permite visualizar el estado de la instalación de detección de incendios en tiempo real, así como ver un histórico de todo lo sucedido gracias a su memoria interna. Permite el envío de correos electrónicos para recibir alarmas o averías de la instalación.

El acceso a Detnov Explorer es mediante contraseña para proteger el acceso no autorizado. Las acciones remotas que se pueden realizar son: Activar sirenas, parar sirenas, silenciar zumbador, rearme de la central. Además podemos cambiar el estado de las zonas de detección (reposo, anulado o test).

Mobotix: Las cámaras duales Mx6 abren las puertas a nuevas posibilidades

Mobotix, fabricante mundial de sistemas en red de videovigilancia de cámaras megapíxel, ha comenzado la fabricación en serie de su nueva línea de cámaras Mx6 de 6 MP, con las cámaras duales para exteriores M16, D16, S16 y V16. Por fuera, y en comparación con los modelos todavía disponibles de cámaras x15, estos modelos no varían, puesto que las innovaciones se encuentran en la placa base y el software de la cámara.

Más rendimiento e inteligencia

La Mx6 utiliza una nueva y potente CPU que, con la misma resolución, aporta hasta dos veces más imágenes por segundo. Por ejemplo, en Full HD se alcanzan hasta 34 imágenes por segundo. Esto permite un mejor registro de los movimientos rápidos. La nueva línea de cámaras no sólo es más rápida, sino que también tiene una mayor capacidad para aplicaciones de software como, por ejemplo, el análisis de movimiento en 3D y el reconocimiento de matrículas en la propia cámara.

Imágenes brillantes en MxPEG y H.264

Mx6 proporciona datos de vídeo simultáneos en hasta tres formatos distintos: MxPEG, MJPEG y, por primera vez, también en H.264. De esta forma, los usuarios de Mobotix pueden elegir el códec adecuado para su uso y, por ejemplo, cumplir el requisito de una elevada calidad de imagen con MxPEG o la compatibilidad con un estándar industrial con H.264. Además, las cámaras Mx6 ofrecen ahora una serie de funciones clásicas de ONVIF, un estándar de interfaz global y abierto. La compatibilidad total con ONVIF (www.onvif.org) se alcanzará con una de las próximas actualizaciones del firmware.

En un primer paso, se introducirán los modelos de cámaras duales D16, M16, S16 y V16. Estas ofrecen el mayor número de funciones y, gracias a su diseño robusto, son especialmente adecuadas para su uso en el exterior. Gracias al sistema modular con diversas opciones de lentes y sensores, las cámaras duales de Mobotix se pueden configurar de forma individual.

Visiotech: Safire presenta la nueva cámara IP para lectura de matrículas

La marca de CCTV Safire trae al mercado europeo una cámara IP innovadora, la SF-IPCV788ZW-2LPR, capaz de reconocer vehículos y leer las matrículas de los mismos hasta una velocidad de 120 km/h. Con esta nueva incorporación al catálogo de Safire, la marca se asienta en el sector, siendo sus principales puntos fuertes la fiabilidad, el diseño y la innovación.

Además del reconocimiento de matrículas, cuenta con la tecnología Ultra Low Light. Este sistema permite a la cámara ver en las condiciones más adversas; con la luz de las estrellas es suficiente para sacar una imagen nocturna de la calidad que se exige a una marca como Safire.

La SF-IPCV788ZW-2LPR tiene un sensor 1/1.8" Progressive Scan CMOS capaz de grabar a una resolución de 1080p @ 60 fps, que sumado a su WDR Real 120dB y 3DNR, entradas y salidas de audio, alimentación a través de PoE, compresión H265 y compatibilidad ONVIF convirtiéndola en una de las cámaras de referencia en el mercado.

A esta cámara le acompañan varios software a su altura, Safire Control Center, disponible tanto para Windows como para Android o iOS. Se trata de un sistema profesional que engloba multitud de parámetros configurables, administración de equipos, configuración de vistas tanto en grabaciones como visión en directo y realización de mapas de seguridad.

Safire Easyview, también multiplataforma, caracterizada por la sencillez de uso y fiabilidad, siendo útil tanto a profesionales como a usuarios finales. Así como SAFIRE SADP, aplicación de escritorio que permite encontrar e identificar cualquier dispositivo de red de la marca.

www.safirecctv.com

Vivotek: robusta cámara tipo domo esquinera anti-ligadura para ambientes en correcionales

Vivotek, fabricante mundial de soluciones de vigilancia IP, presenta sus dos nuevas cámaras de red tipo domo anti-ligaduras de montaje en esquina con lente fijo CD8371-HNVF2 y lente varifocal CD8371-HNTV. Ambas cámaras de red tipo domo esquineras de 3 megapíxeles cuentan con un diseño anti-agarre, una cubierta robusta IK10 e iluminadores IR de 940nm invisibles al ojo humano. Las cámaras esquineras de domo Vivotek están especialmente diseñadas para entornos de alta seguridad, tales como prisiones, celdas de detención, salas psiquiátricas, hospitales mentales e instituciones correccionales, ya que permiten reducir la posibilidad de autolesiones y simultáneamente proteger la seguridad del personal institucional.

Conscientes de la creciente necesidad de vigilancia al interior de ambientes críticos, Vivotek ha desarrollado los modelos CD8371 HNVF2 y CD8371-HNTV para afrontar los retos de este exigente campo. Sus bordes anti-agarre tienen el objetivo de prevenir autolesiones e incluso suicidios. Diseñadas para instalarse en la esquina superior de una celda, las cámaras de domo esquineras también permiten a los vigilantes de seguridad ver cualquier evento en las celdas, gracias al gran angular horizontal FOV (hasta 108°) y vertical FOV (hasta 79°).

Bosch: soluciones de grabación en red e híbridas DIVAR

Bosch ha presentado una gama totalmente nueva de soluciones de grabación en red e híbridas DIVAR.

Se ha diseñado específicamente para funcionar las 24 horas del día y ofrece la posibilidad de crear soluciones de videovigilancia con características de seguridad profesionales, fáciles de instalar y de utilizar. Soluciones que se pueden ajustar a la medida de las necesidades crecientes de pequeñas y medianas empresas.

Híbridos

Los modelos híbridos DIVAR 3000 y 5000 son dispositivos de grabación rentables para empresas que tengan una solución de videovigilancia analógica que deseen actualizar a IP gradualmente. Es posible sustituir todas las cámaras analógicas con el tiempo, ya que los 32 canales pueden estar equipados con cámaras IP en red. Es posible conectar 16 cámaras analógicas como máximo a un grabador híbrido. Los dos modelos híbridos ofrecen la misma interfaz y la misma experiencia para el usuario que la bien conocida familia de grabadores analógicos de vídeo DIVAR AN, basada en una selección de menús y comandos de operador sencillos.

Red

Para las pequeñas y medianas empresas que ya utilizan dispositivos digitales, las series DIVAR network 2000 (16 canales), 3000 y 5000 (ambas con 32 canales) son formas rentables de invertir en un sistema de vigilancia IP preparado para el futuro que se puede escalar a medida que la empresa crece.

Gracias a un conmutador integrado Power over Ethernet (PoE), conectar las cámaras IP a estos videograbadores de red no requiere adaptadores de alimentación aparte, lo cual hace que la instalación sea rápida y fácil.

Las series DIVAR hybrid 3000 y DIVAR network 2000 y 3000 son, esencialmente, soluciones independientes para negocios con una sola ubicación, como pequeños comercios, supermercados u hoteles de tamaño mediano. DIVAR hybrid 5000 y DIVAR network 5000 se han diseñado para montarlos fácilmente en rack de 19", lo cual los hace adecuados para empresas medianas y cadenas de tiendas que prefieren una instalación oculta debajo del mostrador, en una sala de servidores separada u otra ubicación adecuada.

Con los grabadores DIVAR, resulta sencillo ver imágenes en directo, reproducir contenido grabado o reconfigurar los ajustes de una unidad local en cualquier momento y desde cualquier lugar. Esto se puede hacer mediante la aplicación DIVAR Mobile Viewer, disponible para smartphones (iOS y Android) y mediante navegador web.

Prodextec amplía su catálogo con los equipos de la marca CIAS

Como continuación al desarrollo de la marca y su catálogo de productos orientados a dar soluciones a los proyectos de seguridad perimetral, Prodextec ha incorporado recientemente la marca CIAS Elettronica a su repertorio.

De este modo, la oferta de Prodextec a sus clientes se amplía, cubriendo un amplio rango de tecnologías y productos: infrarrojos, microondas, cable microfónico, cable sensor, fibra óptica, todo ello de la mano de los principales fabricantes y marcas de referencia del sector, como son Optex, Takex, FiberSensys, Redwall, Bunker y ahora CIAS.

En breve estará disponible para nuestros clientes la lista de precios actualizada con estos productos junto con las últimas novedades como son el Redscan RLS-2020I/S, las barreras de infrarrojos para montaje en columna SL-BT o la serie más económica de barreras vía radio SL-100/200TNR de OPTEX. Más información en www.prodextec.es.

Contactos de empresas, p. 7.

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

ALARMA Y CONTROL

PYRONIX

C/Almazara, 9
28760 Tres Cantos Madrid
Tel. 91 737 16 55
marketing@pyronix.com
www.pyronix.com

Techco Security
C/ Barbadillo 7
28042 Madrid
+34 91 312 77 77
www.techcosecurity.com
tcs@techcosecurity.com

GAROTECNIA
Valdelaguna, 4 local 3
28909 Getafe (Madrid)
Tel.: 916 847 767 - Fax: 916 847 769
garotecnia@garotecnia.com
www.garotecnia.com
Autorizada por la D.G.P. con el nº 2.276

Tyco Integrated Fire & Security

Edificio Ecu-I
Ctra. de La Coruña, km 23,500
28290 Las Rozas (Madrid)
Tel.: 902 444 440 - Fax: 91 631 39 78
www.tyco.es

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

MADRID: Calidad 48, Polígono Industrial Los Olivos
28906 Getafe • Tel.: 917 544 804
CANARIAS: Ctra. del Norte 113 - 35013 Las Palmas
de Gran Canaria • Tel.: 928 426 323
Fax: 928 417 077
PORTUGAL: Rua Fernando Namora 33, 2º-I
4425-651 Maia (Porto) • Tel.: (+351) 932 220 421
bydemes@bydemes.com
www.bydemes.com

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

Central Receptora de Alarmas/Videovigilancia
Autorizada por la D.G.P. con el nº. 729
Avda de Olivares 17 – Plg. Industrial PIBO
41110 Bollullos de la Mitación (Sevilla)
Tlfno. 902194814 – 954108887
Fax. 954002319
gerencia@gruporomade.com
SERVICIOS EN TODA ESPAÑA

Accesos CCTV Incendio Intrusión
Oficina Central:
Maresme, 71-79 · 08019 Barcelona
Fax 933 518 554
902 202 206 www.casmar.es

CONTROL DE ACCESOS ACTIVO

TALLERES DE ESCORIAZA, S. A. U.
Barrio de Ventas, 35
E-20305 Irún • SPAIN
Tel.: +34 943 669 100
Fax: +34 943 633 221
tesalocks@tesa.es • www.tesa.es

GRUPO SPEC
Líderes en Gestión de Horarios y Accesos desde 1978
C/ Caballero, 81
08014 Barcelona
Tel. 93 247 88 00 • Fax 93 247 88 11
spec@grupospec.com
www.grupospec.com

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: Calidad 48, Polígono Industrial Los Olivos
28906 Getafe • Tel.: 917 544 804
CANARIAS: Ctra. del Norte 113 - 35013 Las Palmas
de Gran Canaria • Tel.: 928 426 323
Fax: 928 417 077
PORTUGAL: Rua Fernando Namora 33, 2º-I
4425-651 Maia (Porto) • Tel.: (+351) 932 220 421
bydemes@bydemes.com
www.bydemes.com

Avda. Roma, 97
08029 BARCELONA
Tel.: 93 439 92 44 • Fax: 93 419 76 73

Delegación Zona Centro:
Sebastián Elcano, 32
28012 Madrid
Tel.: 902 92 93 84

Soluciones integrales en control de Accesos y seguridad

Carrer Esperança, 5
08500 Vic (Barcelona)
Tel.: 902 447 442
Fax.: 938 864 500

info@accesor.com
www.accesor.com

DORLET S. A. U.
Parque Tecnológico de Álava
C/Albert Einstein, 34
01510 Miñano Mayor - ALAVA - Spain
Tel. 945 29 87 90 • Fax. 945 29 81 33

e-mail: comercial@dorlet.com
web: http://www.dorlet.com

SETELSA
Polígono Industrial de Guarnizo - Parcela 48-C Naves "La Canaluca" 2 y 4
39611 GUARNIZO-CANTABRIA. ESPAÑA
Tel.: 942 54 43 54
www.setelsa.net

¿No cree...
... que debería estar aquí?

El directorio es la zona más consultada de nuestra revista.

Módulo: 660€/año*

Más información:
Tel.: 91 476 80 00
e-mail: publi-seguridad@epeldano.com
* Tarifa vigente 2017

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

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

TECOSA
Telecomunicación, Electrónica y Conmutación
Grupo Siemens
Infraestructure & Cities Sector
División Building Technologies
Ronda de Europa, 5
28760 Tres Cantos - Madrid
Tel.: +34 91 514 75 00
Asistencia Técnica: 902 199 029
www.tecosa.es

TARGET TECNOLOGIA, 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

PROTECCIÓN CONTRA INCENDIOS. ACTIVA

detnov

C/ Alguer nº8 08830 Sant Boi de Llobregat (Barcelona)

Tel: +34 93 371 60 25
Fax:+34 93 640 10 84

www.detnov.com
info@detnov.com

bydemes

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

MADRID: Calidad 48, Polígono Industrial Los Olivos 28906 Getafe • Tel.: 917 544 804
CANARIAS: Ctra. del Norte 113 - 35013 Las Palmas de Gran Canaria • Tel.: 928 426 323
Fax: 928 417 077
PORTUGAL: Rua Fernando Namora 33, 2º-I 4425-651 Maia (Porto) • Tel.: (+351) 932 220 421
bydemes@bydemes.com
www.bydemes.com

aguilera

GRUPO AGUILERA

FABRICANTES DE SOLUCIONES PCI DETECCIÓN Y EXTINCIÓN DE INCENDIOS

SEDE CENTRAL
C/ Julián Camarillo, 26 28037 MADRID
Tel. 91 754 55 11 • Fax: 91 754 50 98
www.aguilera.es

Delegaciones en:
Galicia: Tel. 98 114 02 42 • Fax: 98 114 24 62
Cataluña: Tel. 93 381 08 04 • Fax: 93 381 07 58
Levante: Tel. 96 119 96 06 • Fax: 96 119 96 01
Andalucía:Tel. 95 465 65 88 • Fax: 95 465 71 71
Canarias: Tel. 928 24 45 80 • Fax: 928 24 65 72

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 • IG-55 • NOVECTM • SAFEGUARD • Hfc-227ea • Co_2

pefipresa

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

PROTECCIÓN CONTRA INCENDIOS. PASIVA

solexin

Calle Alberto Alcocer, 28, 1º A
28036 Madrid

Tel. 913 685 120

info@solexin.es
www.solexin.es

DICTATOR Española

DICTATOR ESPAÑOLA
Mogoda, 20-24 • P. I. Can Salvatella
08210 Barberá del Vallés (Barcelona)
Tel.: 937 191 314 • Fax: 937 182 509
www.dictator.es
dictator@dictator.es

PROTECCIÓN CONTRA INTRUSIÓN. ACTIVA

bydemes

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

MADRID: Calidad 48, Polígono Industrial Los Olivos 28906 Getafe • Tel.: 917 544 804
CANARIAS: Ctra. del Norte 113 - 35013 Las Palmas de Gran Canaria • Tel.: 928 426 323
Fax: 928 417 077
PORTUGAL: Rua Fernando Namora 33, 2º-I 4425-651 Maia (Porto) • Tel.: (+351) 932 220 421
bydemes@bydemes.com
www.bydemes.com

RISCO GROUP
Creating Security Solutions

RISCO Group Iberia
San Rafael, 1
28108 Alcobendas (Madrid)
Tel.: +34 914 902 133
Fax: +34 914 902 134
sales-es@riscogroup.com
www.riscogroup.es

Tecnoalarm
Hi-Tech Security Systems

TECNOALARM ESPAÑA

C/ Vapor, 18 • 08850 Gavà (Barcelona)
Tel.: +34 936 62 24 17
Fax: +34 936 62 24 38
www.tecnoalarm.com
tecnoalarm@tecnoalarm.es

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

PROTECCIÓN CONTRA ROBO Y ATRACO. PASIVA

TELECOMUNICACIONES

La solución de seguridad M2M definitiva para las comunicaciones de su CRA

Condesa de Venadito 1, planta 11
28027 Madrid
T. 902.095.196 • F. 902.095.196

comercial@alai.es • www.alaisecure.com

VIGILANCIA POR TELEVISIÓN

HIKVISION SPAIN
C/ Almazara 9
28760- Tres Cantos (Madrid)
Tel. 917 371 655
info.es@hikvision.com
www.hikvision.com

Hanwha Techwin Europe Ltd

Avda. De Barajas, 24, Planta Baja, Oficina 1
28108 Alcobendas (Madrid)España(Spain)
Tel.: +34 916 517 507

www.hanwha-security.eu
hte.spain@hanwha.com

Tel. 902 502 035 - Fax 902 502 036
iptecno@iptecno.com - www.iptecno.com

SEDE BARCELONA
IPTECNO Videovigilancia S.L.
C/ del Besos, 12 - P. I. Can Buscarons de Baix
08170 Montornés del Vallés

SEDE MADRID
IPTECNO Seguridad S.L.
Avda. Tenerife, 2 - Blq. 2, Pta. 3
28703 S. S. de los Reyes

DAHUA IBERIA, S.L.
C/ Juan Esplandiú 15 1-B. 28007 Madrid

Tel: +34 917649862
sales.iberia@global.dahuatech.com
www.dahuasecurity.com

Visiotech
Avenida del Sol, 22
28850, Torrejón de Ardoz (Madrid)
Tel.: 911 826 285 • Fax: 917 273 341
info@visiotechsecurity.com
www.visiotechsecurity.com

Expertos en VIDEOVIGILANCIA

LSB, S.L.
C./ Enero, 11 28022 Madrid
Tf: +34 913294835
info@lsb.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: Calidad 48, Polígono Industrial Los Olivos
28906 Getafe • Tel.: 917 544 804
CANARIAS: Ctra. del Norte 113 - 35013 Las Palmas de Gran Canaria • Tel.: 928 426 323
Fax: 928 417 077
PORTUGAL: Rua Fernando Namora 33, 2°-I
4425-651 Maia (Porto) • Tel.: (+351) 932 220 421
bydemes@bydemes.com
www.bydemes.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

WD ESPAÑA
4 boulevard des Iles
92130 Issy les Moulineaux · Francia
florence.perrin@wdc.com
Tel.: 615 235 013
www.wdc.com

BOSCH SECURITY SYSTEMS SAU
C/ Hermanos García Noblejas, 19
Edificio Robert Bosch
28037 Madrid • Tel.: 902 121 497
Delegación Este:
Plaça Francesc Macià, 14-19
08902 L'Hospitalet de Llobregat (Barcelona)
Tel.: 93 508 26 52 • Fax: 93 508 26 21
Delegación Norte: Tel.: 676 600 612
es.securitysystems@bosch.com
www.boschsecurity.es

AXIS COMMUNICATIONS
Vía de los Poblados 3, Edificio 3,
Planta 1 – 28033 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

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

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

HOMMAX
Alquería de Moret, 9
46210Picanya - Valencia
+34 (96) 159 46 46
www.hommaxsistemas.com

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

C/ Albarracín, 58, Local 10, Planta 1ª
28037 Madrid
Tel 91 055 97 50
www.aecra.org

anpasp

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

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

INGRAM MICRO

Viladecans Business Park
Edificio Australia. C/ Antonio Machado 78-80, 1ª y 2ª planta
08840 Viladecans (Barcelona)
Web: www.ingrammicro.es
Teléfono: 902 50 62 10
Fax: 93 474 90 00
Marcas destacadas: Axis y D-Link.

AEINSE
Asociación Española de Ingenieros de Seguridad

ASOCIACIÓN ESPAÑOLA DE INGENIEROS DE SEGURIDAD

C/ San Delfín 4 (local 4 calle)
28019 MADRID
aeinse@aeinse.org
www.aeinse.org

ADSI

ADSI - Asociación de Directivos de Seguridad Integral
Gran Via de Les Corts Catalanes, 373 - 385
4ª planta (local B2)
Centro Comercial **Arenas de Barcelona**
08015 Barcelona
info@adsi.pro • www.adsi.pro

ASEPAL

ASOCIACIÓN DE EMPRESAS DE EQUIPOS DE PROTECCION PERSONAL
Alcalá, 119 - 4º izda.
28009 Madrid
Tel.: 914 316 298 - Fax: 914 351 640
www.asepal.es

PELCO
by Schneider Electric

PELCO by Schneider Electric
C/ Valgrande 6
28108, Alcobendas, Madrid
Tel.: +34 911 234 206
pelco.iberia@schneider-electric.com
www.pelco.com

ACAES

C/ Viladomat 174
08015 Barcelona
Tel.: 93 454 48 11
Fax: 93 453 62 10
acaes@acaes.net
www.acaes.net

AES

ASOCIACION ESPAÑOLA DE EMPRESAS DE SEGURIDAD
Alcalá, 99
28009 Madrid
Tel.: 915 765 225
Fax: 915 766 094

ASIS INTERNATIONAL
Advancing Security Worldwide™
CAPITULO 143 – ESPAÑA
143 CHAPTER - SPAIN

ASIS-ESPAÑA
C/ Velázquez 53, 2º Izquierda
28001 Madrid
Tel.: 911 310 619
Fax: 915 777 190

ASOCIACIONES

tecnifuego AESPI

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

aproser

ASOCIACIÓN PROFESIONAL DE COMPAÑÍAS PRIVADAS DE SERVICIOS DE SEGURIDAD
Marqués de Urquijo, 5 - 2ºA
28008 Madrid
Tel.: 914 540 000 - Fax: 915 411 090
www.aproser.org

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

UAS

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

Asociación Española de Lucha Contra el Fuego
ASELF

ASOCIACION ESPAÑOLA DE LUCHA CONTRA EL FUEGO
Calle Escalona nº 61 - Planta 1
Puerta 13-14 28024 Madrid
Tel.: 915 216 964
Fax: 911 791 859

FES

FEDERACIÓN ESPAÑOLA DE SEGURIDAD
Embajadores, 81
28012 Madrid
Tel.: 915 542 115 - Fax: 915 538 929
fes@fes.es
C/C: comunicacion@fes.es

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

ASOCIACIÓN DE JEFES DE SEGURIDAD DE ESPAÑA

Avd. Meridiana 358. 4ºA.
08027 Barcelona
Tel. 93-3459682 Fax. 93-3453395
www.ajse.es presidente@ajse.es

ASOCIACIÓN VASCA DE PROFESIONALES DE SEGURIDAD
Parque tecnológico de Bizkaia
Ibaizabal Kalea, 101
sae@sae-avps.com
www.sae-avps.com

ASOCIACIÓN NACIONAL DE TASADORES Y PERITOS JUDICIALES INFORMÁTICOS (ANTPJI)

C/ Juan de Mariana, 5
28045 Madrid
Tlf 91 / 469.76.44
www.antpji.com
contacto@antpji.com

FORMACIÓN DE SEGURIDAD

Homologado por el Ministerio del Interior y la Junta de Andalucía.

Avda de Olivares 17 • Plg. Industrial PIBO.
41110 Bollullos de la Mitación (Sevilla).
Tlfno. 902194814 – 954108887
Fax. 954002319
gerencia@gruporomade.com

CENTRALES DE RECEPCIÓN Y CONTROL

ALARMAS SPITZ S. A.
Gran Vía, 493 - 08015 Barcelona
Tel.: 934 517 500 - Fax: 934 511 443
Central Receptora de alarmas
Tel.: 902 117 100 - Fax: 934 536 946
www.alarmasspitz.com

INSTALACIÓN Y MANTENIMIENTO

Techco Security
C/ Barbadillo 7
28042 Madrid
+34 91 312 77 77
www.techcosecurity.com
tcs@techcosecurity.com

FUNDADA EN 1966

INSTALACIONES A SU MEDIDA

Antoñita Jiménez, 25
28019 Madrid
Tel.: 91 565 54 20 - Fax: 91 565 53 23
seguridad@grupoaguero.com
www.grupoaguero.com

ISO 9001

MATERIAL POLICIAL

SABORIT INTERNATIONAL

Avda. Somosierra, 22 Nave 4D
28709 S. Sebastián de los Reyes (Madrid)
Tel.: 913 831 920
Fax: 916 638 205
www.saborit.com

VIGILANCIA Y CONTROL

SECURITAS SEGURIDAD ESPAÑA
C/ Entrepeñas, 27
28051 Madrid
Tel.: 912 776 000
email: info@securitas.es
www.securitas.es

Grupo RMD
Autorizada por la D.G.P. con el nº. 729
Avda de Olivares 17 – Plg. Industrial PIBO
41110 Bollullos de la Mitación (Sevilla)
Tlfno. 902194814 – 954108887
Fax. 954002319
gerencia@gruporomade.com
SERVICIOS EN TODA ESPAÑA

¿No cree... ... que debería estar aquí?

El directorio es la zona más consultada de nuestra revista.

Módulo: 660€/año*

Más información:
Tel.: 91 476 80 00
e-mail: publi-seguridad@epeldano.com
* Tarifa vigente 2017

TRANSPORTE Y GESTIÓN DE EFECTIVO

LOOMIS SPAIN S. A.
C/ Ahumaos, 35-37
Polígono Industrial La Dehesa de Vicálvaro
28052 Madrid
Tlf: 917438900
Fax: 914 685 241
www.loomis.com

Bilbao

COMPROMISO CON LAS PERSONAS

EUSKO JAURLARITZA GOBIERNO VASCO

ERTZAINTZA

III Congreso de Seguridad Privada EUSKADI

Segurtasun Pribatuko Batzarra

Seguridad: un trabajo **de todos**

Bilbao Bizkaia Aretoa

5OCT2017

CUADERNOS DE SEGURIDAD

Peldaño

www.congresoseguridadeuskadi.com | congreso@congresoseguridadeuskadi.com | 914 768 000

HIKVISION

UN PARTNER SÓLIDO, COMPROMETIDO, INNOVADOR, FIABLE, PRESENTE.

El valor de un partner tecnológico se mide por su capacidad de generar ventaja competitiva, así como por su actitud y el poder de transmitir determinación, entusiasmo, y motivaciones siempre nuevas. Hikvision garantiza profesionalidad, solidez empresarial, compromiso, fiabilidad tecnológica, innovación continua y un alcance global con presencia local.

Hikvision Spain
C/ Almazara, 9
28760 Tres Cantos (Madrid)
T +34 91 7371655
info.es@hikvision.com