CUADERNOS DE SEGURIDAD

Núm. 316 • NOVIEMBRE 2016 • 10 euros

PUNTOSEGURIDAD.com

Seguridad en entidades bancarias

Vigilancia por CCTV

Ciberseguridad: el dinero como datos

Eco-savvy 3.0

Evolución tecnológica 3.0

- ☑ Mayor Resolución
- ☑ Codificación H.265
- ☑ Mayor Rendimiento
- ☑ Mejor Calidad de Imagen

- Mejora en la resolución, capacidad 4K, 4MP/2MP en tiempo real.
- Tecnología de codificación de alta eficiencia H.265, con ahorro del 50% de almacenaje y ancho de banda.
- Mejor rendimiento, 4K@15fps, 4MP@30fps, 2MP@60fps.
- Incremento en la calidad de imagen, tecnología Starlight para visualización clara incluso en la oscuridad.

HF5830/5431/5231E

HFW5830/5431/5231E-Z

HDBW5830/5431/5231E-Z

HDW4830/4431/4231EM-AS

HDBW4431/4231F-AS

ISO 9001:2000

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

Lejanía sin límites

Superando todo lo imaginable

Solución Dahua de total fiabilidad con Domo laser y NVR

500m IR

±25% tolerancia de voltaje de entrada

IVS Auto tracking

-40～70 amplio rango de temperatura de trabajo

PoE

Hi-PoE

IP67

Wiper

8KV protección lumínica

-20°～90°rango de inclinación

España

Portugal

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

¿ESTÁS PREPARADO?

CCIB
Centro de Convenciones
Internacional de Barcelona

17 y 18 de mayo
BCN**2017**

www.securityforum.es

Security FORUM
International Security Conference & Exhibition

SECURITY FORUM 2017 SE CELEBRARÁ LOS DÍAS 17 Y 18 DE MAYO EN BARCELONA

Cinco años al lado del sector

Por y para el sector de la seguridad fue el pilar sobre el que se gestó Security Forum, evento anual que en 2017 cumple su quinto año consecutivo de celebración. Un encuentro, completamente consolidado, que volverá a reunir, los días 17 y 18 de mayo en Barcelona, a todos los profesionales del sector de la seguridad en nuestro país. Es entonces cuando este evento, ya asentado como un gran foro de debate y análisis que promueve la generación de ideas, el conocimiento y el networking, volverá a caminar de la mano de un sector, en continuo desarrollo, convirtiendose en escenario y testigo excepcional de los numerosos cambios y avances que se han producido en el ámbito de la seguridad.

Security Forum, que ha contado desde sus orígenes con el apoyo de todo un sector, ha sido el reflejo del espíritu emprendedor e innovador de las empresas y profesionales que forman la gran familia de la Seguridad. Así quedó patente en la pasada edición donde se superaron con creces todas las expectativas de asistencia y convocatoria de la organización: más de 6.000 visitantes profesionales, 59 expositores, con más de 200 marcas representadas, y 452 congresistas.

Datos que confirmaron el avance de un sector, que apuesta por la innovación y desarrollo, y que al margen de la coyuntura económica, afronta esta situación con perspectivas de un futuro prometedor, apoyándose y siendo partícipe y protagonista de iniciativas novedosas como Security Forum.

La quinta edición de Security Forum volverá a mostrar la oferta más selecta de servicios, equipos y sistemas de seguridad en CCTV, integración de sistemas, seguridad física, seguridad lógica, control de accesos, IP/redes… Y de forma paralela a la zona expositora, de nuevo se desarrollará el Congreso Security Forum, que desglosado en dos sesiones diferenciadas –Global Day y Ciber Day–, se convertirá en punto de reflexión donde reconocidos expertos debatirán y analizarán los nuevos riesgos y amenazas de un entorno global.

Además, un año más, Security Forum ya ha abierto la convocatoria de los Premios Security Forum, que pretenden promover y potenciar la investigación, el desarrollo y la innovación de la industria de la seguridad en España, a través del reconocimiento a los responsables de proyectos actuales de investigación en materia de seguridad, y a aquellos proyectos de carácter significativo ejecutados, que puedan ser modelo y escaparate internacional del amplio potencial de nuestra industria. La convocatoria se desglosa en dos modalidades: Mejor Proyecto de I+D+i y Mejor Proyecto de Seguridad en España. Las memorias deben ser recibidas antes del 31 de marzo de 2017 y el fallo del jurado se producirá antes del 30 de abril.

De nuevo, y cinco años después, Security Forum 2017 servirá para confirmar que el sector de la Seguridad Privada sigue creciendo y avanzando. En la nueva web de Security Forum (www.securityforum.es) está disponible toda la información actualizada sobre la próxima edición.

CUADERNOS DE SEGURIDAD

www.puntoseguridad.com

Nº 316 • NOVIEMBRE 2016

Peldaño

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

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

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

Suscripciones y distribución:
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

Nota de la redacción:

El artículo publicado en el número de septiembre «Las auditorías...también en seguridad», fue atribuido a Alfonso Bilbao, cuando su autor era Enrique Bilbao Lázaro.

ÍNDICE DE EMPRESAS CITADAS EN ESTA EDICIÓN

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

ÍNDICE DE ANUNCIANTES

EMPRESA	PAG.	TELÉFONO	WEB
Avitom	83,86	925516797	www.avitom.es
Axis Communications	74	918034643	www.axis.com
Baussa	43	946749099	www.baussa.com
Bosch Security Systems	49,83	902121497	www.boschsecurity.es
Buguroo	62	912294349	www.buguroo.com
Casmar	69,78	902202206	www.casmar.es
CCN-CERT	3ª Cub		www.ccn-cert.cni.es
Cuevavaliente Ingenieros	80	918047364	www.cuevavaliente.com
Dahua	2ª Cub,107	865718768883	www.dahuasecurity.com
Dallmeier	89, 106	915902287	www.dallmeier-electronic.com
Diid	21	902565733	www.diid.es
Dormakaba	51, 100	917362480	www.dormakaba.com
Ferrimax	46,53	934601696	www.ferrimax.com
FF Videosistemas	27	902998440	www.ffvideosistemas.com
Fujinon	23	4921150898921	www.fujifilm.eu/fujinon
GMV	31,58	918072100	www.gmv.com
Grupo Aguilera	107	917545511	www.aguilera.es
Grupo Álava	60	915679700	www.alava-ing.es
Gunnebo	72	902100076	www.gunnebo.es
Hanwha Techwin	54,57	916517507	www.hanwha-security.eu
Hikvision	4ª Cub, 9, 44, 105	917371655	www.hikvision.com
Hommax Sistemas	95	961594646	www.hommaxsistemas.com
Iptecno	65	902502035	www.iptecno.com
Iseo Ibérica	29	918843200	www.iseo-iberica.eu
LSB	25	913294835	www.lsb.es
Mobotix	84	911115824	www.mobotix.com
Morse Watchmans	17	1159671567	www.morsewatchmans.com
Pyronix	11	917371655	www.pyronix.com
Realsec	70	914490330	www.realsec.com
Risco Group	50	914902133	www.riscogroup.es
Saborit	85	913831920	www.saborit.com
Salvador Tarazona Correduría	63,102	902884059	www.starazona.com
Security Forum	4	914768000	www.securityforum.es
Setelsa	7	942544354	www.setelsa.net
Vanderbilt	66	911799770	www.vanderbiltindustries.como
Visiotech	41	911836285	www.visiotech.com
WD	77	615235013	www.wdc.com

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

LOS PREMIOS SE ENTREGARÁN LA NOCHE DEL 17 DE MAYO EN BARCELONA

Convocada la V edición de los **Premios Security Forum**

La convocatoria se desglosa en las dos modalidades ya consolidadas: Mejor Proyecto de I+D+i y Mejor Proyecto de Seguridad en España

Security Forum 2017 ya ha abierto la convocatoria, continuando con la trayectoria ya marcada desde hace cuatro años, de los premios Security Forum, que pretenden promover y potenciar la investigación, el desarrollo y la innovación de la industria de la seguridad en España, a través del reconocimiento a los responsables de proyectos actuales de investigación en materia de seguridad, y a aquellos proyectos de carácter significativo ejecutados, que puedan ser modelo y escaparate internacional del amplio potencial de nuestra industria.

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

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

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

La dotación de los premios será:

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

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

Fotos: Xavi Gómez

Detector Volumétrico de Exteriores de Triple Tecnología y Anti-masking

Pyronix
HIKVISION

XDH10TT-AM

Características

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

Para recibir más información, regístrese aquí

ENRIQUE RUBIO-MANZANARES ÁLVAREZ. CHIEF INFORMATION SECURITY OFFICER (CISO). EVO BANCO

«*La tecnología es la protagonista de las corporaciones bancarias y con ella la ciberseguridad*»

LA protección de la información, el robo de información y las normativas son los grandes retos a los que se enfrenta hoy en día el sector bancario ante internet», así lo asegura Enrique Rubio-Manzanares Álvarez, CISO de EVO Banco, quien además analiza, entre otros aspectos, cómo han cambiado los riesgos y amenazas en cuanto a aspectos de ciberseguridad.

—El CISO es una figura profesional relativamente reciente dentro del organigrama de las empresas, incluido el sector bancario. ¿Podría indicarnos su trayectoria hasta su incorporación en Evo Banco?

—Llevo más de 15 años trabajando en Comunicaciones y Seguridad. Empecé en Ibermática, pasando después por Indra, Everis… He estado en varias empresas en estos años. En 2010 estuve trabajando para Yoigo y después dí el salto a una empresa de ciberseguridad como S21sec. No llevaba mucho tiempo en ella cuando surgió la oportunidad en EVO que para mí fue irrechazable.

—¿Cuáles son las funciones concretas que desempeña un CISO dentro de una entidad financiera como es el caso de EVO Banco?

—El abanico de funciones es muy amplio, quizás las más relevantes sean:

- Identificar las necesidades del negocio en materia de seguridad.
- Trasladar la necesidad del negocio en materia de seguridad hacia tecnología.
- Establecer criterios mínimos de seguridad, de forma uniforme a toda la organización.
- Revisar que las implantaciones están acordes con los criterios mínimos de seguridad.
- Velar por el cumplimiento de la Seguridad de la Información.
- Identificar y tratar los GAPs de la Seguridad de la Información.
- Gestión de la Continuidad del Negocio.

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

—Sobre todo, conseguir justificar la inversión que hay que realizar para conseguir un entorno con una seguridad de ciertas garantías. Creo que este punto es el principal reto. Actualmente es complicado conseguir todo el presupuesto que querríamos para seguridad. Después la normativa y la regulación. Conseguir que toda la organización cumpla con la normativa es muy complicado y más aún negocio. Adaptar la normativa al negocio es a veces complejo, digo esto sobre todo por el gran volumen de proyectos de negocio que tenemos en el

grupo. Como explico es muy difícil encontrar el equilibrio negocio-seguridad, aunque también tengo que decir que nosotros hasta ahora lo vamos encontrando. La clave está en la colaboración y la comunicación entre áreas.

—Con una visión profesional, ¿cuál cree que es actualmente el nivel de seguridad en el ámbito TI de las entidades financieras de nuestro país, en relación con Europa?

—Creo que hay entidades muy potentes en materia de seguridad y otras que lo son menos. Ya sea por recursos, presupuesto, tiempo, etc. Pero en general el nivel de las entidades de este país es bastante alto.

Si nos comparamos con Europa, no creo que estemos lejos. Sobre todo los grandes bancos.

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

—Han cambiado una barbaridad, ahora gran parte del negocio está en las Webs o las APPs. Además, todas las oficinas tienen conexiones a Internet, a los servicios centrales. La tecnología es la protagonista y con ella la ciberseguridad.

Cuando quieren atacar a tu entidad, cualquier cliente puede ser utilizado para ello, sin su consentimiento obviamente, el phishing, el malware, la ingeniería social…, son técnicas que están a la orden del día y que gran parte de la población no las conocen lo suficiente como para detectarlas. Hay phishing que son realmente buenos.

—Entrando en aspectos de normativa, ¿qué valoración haría a cerca de la Directiva sobre la Seguridad de las Redes y de la Información (Directiva NIS)? ¿Cómo afectará al sector empresarial en el que usted trabaja?

—A mí no me disgusta la Directiva, creo incluso que es necesaria. Al final es necesario marcar unos mínimos en materia de seguridad y que todo el mundo los conozca. Creo que es pronto, pero mi sensación es que va a venir bien.

Al sector financiero, creo que le va a afectar en bastantes aspectos. Pero como decía antes, va a venir bien.

—¿Cuáles son los grandes retos a los que se enfrenta hoy en día el sector bancario ante Internet?

—La protección de la información, el robo de información y las normativas. La información que manejamos es muy sensible y hay que protegerla y cumplir con la normativa en cada uno de los procesos que interviene en nuestro día a día.

—Hoy en día se apuesta por la convergencia de la seguridad –física y lógica– como un concepto integral, ¿cree que las grandes corporaciones financieras están preparadas para asumir este concepto?

«La seguridad física y la lógica buscan y tienen los mismos objetivos: la protección de la información»

—Yo creo que sí, además es una convergencia natural. Es más, ya son varias compañías las que han pasado esa convergencia y trabajan perfectamente. Pero al final la seguridad física y la lógica buscan y tienen los mismos objetivos, que es la protección de la información.

Texto y Fotos: Gemma G. Juanes/EvoBanco

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

«La **información es poder**, un punto crucial para entender la **seguridad financiera contemporánea**»

LA seguridad bancaria está en continua evolución y ello obliga a sus integrantes a una continua actualización en materia tanto de prevención, como innovación, planificación o formación». Así lo asegura Eduardo J. Álvarez Blázquez, Security Director Spain. CSIS Spain Citibank, quien a lo largo de la entrevista explica además cuáles son los pilares sobre los que debe asentarse una adecuada seguridad bancaria.

—¿Qué objetivos se ha planteado tras asumir el cargo de Security Director Spain de Citibank? ¿Qué líneas estratégicas marcarán su actividad?

—Citibank, como parte de una entidad de origen norteamericano y vocación internacional, tiene objetivos de marcado carácter global, por lo que uno de los objetivos que me planteé al ingresar en Citi fue el tratar de implementar las políticas globales de Seguridad de Citi en España. Esta es una labor que, si bien se venía realizando anteriormente a mi incorporación, requería de una revisión tanto de los procedimientos como de los diferentes objetivos a cubrir. Tratar de engarzar ambos campos de seguridad, el local o español por un lado, y el corporativo o global de Citi, por otro, es siempre complicado.

Otro de los objetivos prioritarios fue la concienciación a todos los estamentos del Staff del valor añadido que la seguridad ofrece a toda la corporación, en un doble aspecto:

Por un lado, la pura seguridad física, tratando de sensibilizar a la plantilla en la necesidad de unos controles de accesos adecuados y con la suficiente flexibilidad para no entorpecer las labores cotidianas de la Corporación. Es cierto que a esta labor ha contribuido en gran medida los diferentes atentados que venimos sufriendo en suelo europeo últimamente, y la posterior psicosis que generan. Dentro de este aspecto, creo que un departamento de Seguridad profesional es capaz de gestionar y minimizar esta psicosis a través de unas correctas políticas y medidas de seguridad, donde la información correcta distribuida por los canales adecuados de la propia Corporación es vital.

Por otro lado, asegurar el cumplimiento de las políticas de privacidad interdepartamental y corporativa de la Compañía, aspecto básico de la organización, y en la cual el departamento de Seguridad juega un papel clave, al gestionar los accesos a los que personal clave de la Corporación tiene derecho en función de su cargo, y a los que no, en función de este mismo cargo. Tenemos un potente departamento de Compliance que está enfocado en estos aspectos al 100%.

El mantener contacto fluido con Fuerzas y Cuerpos de Seguridad del Estado debe ser un pilar fundamental sobre el que sustentar la actividad de cualquier

departamento de Seguridad Bancaria. Asistir a los diferentes foros y reuniones especializadas aporta un feedback constante entre la entidad y los diferentes Cuerpos de Seguridad, tanto estatales como autonómicos o locales en nuestro ámbito de actuación, que no hacen más que redundar en beneficio de ambas partes.

—¿Cuál es la estructura e infraestructura actual del departamento de Seguridad de Citibank?

—Nuestro departamento de Seguridad se encuentra enmarcado, dentro de la organización de Citi en CSIS (Citi Security and Investigative Services), departamento de Citi que provee de seguridad, tanto física como en prevención y detección de fraude a todos los negocios de Citi a nivel global. Este tipo de organización nos permite un grado de cobertura de las diferentes amenazas muy superior al que ofrecen otras compañías que operan en el sector, dado que nos beneficiamos de la información recogida por CSIS en los países de nuestra región en la que opera Citi, por lo que nuestra perspectiva tanto de la amenaza como de su neutralización se analiza no tanto a nivel local sino desde un prisma global.

CSIS España se compone de un departamento de Seguridad, cuyas funciones se encuentran definidas por ley, y que gestiona principalmente todo los elementos relacionados con la seguridad física, tanto de los inmuebles como de los trabajadores, usuarios y directivos de la entidad, así como las relaciones con Fuerzas y Cuerpos de Seguridad del Estado. En el caso de Citi, dado su carácter de entidad norteamericana, debe cultivar otra serie de relaciones, tales como la Embajada de los EEUU en España, Servicio Secreto, por citar las más importantes.

Es el responsable del cumplimiento de las políticas de seguridad establecidas por Citi, tanto a nivel local como regional y global. También debe gestionar la implementación de las medidas y los medios de seguridad adecuados para garantizar la seguridad y protección de bienes y personas responsabilidad de Citi.

Además del citado departamento de Seguridad, existe un departamento de Prevención del Fraude, que gestiona todo el fraude tanto interno como externo que afecta a la compañía. Este departamento es un departamento muy potente, con una cobertura global y con una enorme especialización, compuesto en su gran mayoría por profesionales del sector de la Prevención del Fraude, muchos de ellos antiguos miembros de cuerpos policiales con unas capacidades investigativas muy notables.

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

—La mayor diferencia que en mi opinión se ha producido es en la gestión y la protección de la información. Mientras que antes un 90% de los esfuerzos de seguridad y protección se veían encaminados a asegurar el efectivo, el dinero para ser claro, sea cual sea su forma, actualmente estos mismos esfuerzos se dirigen a asegurar la trazabilidad de la información, tanto de las propias operaciones de la Compañía, como la información de los usuarios, tanto externos como interno, de la misma.

La información es poder, como reza el viejo adagio, y éste es un punto en mi opinión crucial para entender la seguridad financiera y bancaria contemporánea. No hay ninguna entidad financiera que pueda afrontar una fuga de información, y por ello se están impulsando tanto la creación como el desarrollo de departamentos específicos de Seguridad de la Información (los BISO, CISO, etc.) que gestionan, neutralizan o minimizan este tipo de riesgos.

Nuevas formas de delincuencia relacionada con entidades bancarias y que se apoyan en las nuevas tecnologías (phishing, hacking, ingeniería social, etc.) sustituyen a los antiguos delitos contra nuestras entidades, dado que la recompensa al delito es mucho mayor, y el riesgo asumido por los ciberdeli-

cuentes es mínimo. Tanto el auge de las nuevas tecnologías como la creciente globalización de nuestro entorno, si bien favorece el establecimiento de nuevos vínculos y relaciones laborales, también favorece este tipo de delincuencia transnacional.

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

—Desde mi punto de vista una adecuada seguridad bancaria se sustentaría en los siguientes pilares:

-Proactividad: La seguridad bancaria está en continua evolución y ello obliga a sus integrantes a una continua actualización en materia tanto de prevención, como innovación, planificación o formación. Deben estar en constante aprendizaje, tratando de marchar de la mano de los tiempos que vivimos.

-Profesionalidad: En un ámbito con una responsabilidad tan enorme como es el ámbito, no sólo de la seguridad, sino además bancaria, los miembros que componemos este sector deben preocuparse de cada uno de los extremos que abarca su trabajo, desde la seguridad corporativa, al cumplimiento normativo, por citar algunos.

-Multidisciplinar: Se deben considerar todas y cada una de las disciplinas que entraña la seguridad bancaria. Seguridad física, medios técnicos, protección ejecutiva, relación con Fuerzas y Cuerpos de Seguridad del Estado…, sin enfocarse en una sola actividad y desatendiendo el resto. Se trata de trabajar la seguridad bancaria de forma integral.

—Hoy en día el sector apuesta por la convergencia de la seguridad como un concepto integral, ¿están preparadas las compañías financieras para asumir los cambios que esto conlleva?

—Con toda sinceridad, sí. Dado que la mayoría de las grandes compañías financieras operan a nivel global, con una enorme diversidad tanto de empresas como de productos, mercados y países, se encuentran en un entorno que favorece en gran medida este concepto de seguridad integral, donde diferentes negocios se respaldan entre sí, generando una sinergia que les ayuda a liderar su sector y alcanzar el objetivo deseado.

De este modo, en este tipo de corporaciones resulta mucho más natural y sencillo que el departamento de Seguridad opere en conjunto con otros departamentos, tales como Cumplimiento, Tecnología o Relaciones Públicas, por citar sólo algunos. Estas Corporaciones tienen muy presente que «la parte representa al todo», de tal forma que una actuación del departamento de Seguridad no se considera una acción exclusiva de este departamento, sino que afecta a otros sectores, hay que analizar si se ha actuado conforme a normativas, tanto interna de la propia corporación como externa, involucra cuestiones de seguridad de la información, tales como datos personales de trabajadores o clientes, y así un largo etcétera.

—¿Cuál cree que es el nivel de seguridad de las entidades financieras de nuestro país en relación con Europa?

> «Nuevas formas de delincuencia relacionadas con entidades bancarias y que se apoyan en las nuevas tecnologías sustituyen a los antiguos delitos contra nuestras entidades»

—Muy alto, de los más altos de nuestro entorno, y no lo digo yo, podemos ver por distintas auditorías que el nivel de competencia en el sector seguridad se encuentra entre los más reconocidos y profesionales de la UE. En esta valoración entiendo que tiene mucho que ver tanto el perfil del profesional de Se-

guridad que ocupa puestos directivos de seguridad en las distintas entidades financieras, como la propia regulación que existe en España sobre los requisitos para ser director de Seguridad o, en el ámbito de las empresas de Seguridad Privada, del jefe de Seguridad.

La gran mayoría de estos profesionales tiene un bagaje muy amplio en cuestiones de seguridad, muchos de ellos provienen del Sector Público, de Fuerzas y Cuerpos de Seguridad del Estado. Debemos tener en consideración, que en muchos países de nuestro entorno, y me estoy refiriendo a países de la UE, no es necesaria ninguna habilitación o titulación profesional para desempeñar funciones de seguridad privada, siendo un sector tan delicado como es. Además, debemos también tener en cuenta que las entidades financieras españolas se encuentran entre las más punteras del mundo y, evidentemente, este volumen de negocio requiere de un departamento de Seguridad acorde al mismo.

—Entrando en temas legislativos, ¿qué aspectos le gustaría que recogiese el Reglamento de Seguridad Privada?

—Me gustaría que le diera mayor trascendencia a la seguridad bancaria como tal, creo que su consideración dentro de la nueva ley es escasa para la entidad que tiene. Esto viene muy al hilo de lo que hemos hablado anteriormente. En mi opinión, la seguridad bancaria se sigue enfocando prácticamente en su totalidad a la protección del efectivo, así como de las oficinas y sus trabajadores, pero desde un punto de vista meramente físico, descuidando la tipología de los ataques que sufren actualmente las corporaciones financieras. Muy poco acerca de los ataques a la Seguridad de la Información. Muy poco en relación a la ingeniería social. Muy poco acerca de los ciberataques. La lista es grande. Lamentablemente, una vez más, la Ley se adecua a los tiempos con cierto retraso. Cierto es que cada vez se acortan más los tiempos de adecuación, pero todavía queda camino por recorrer.

En un aspecto tal vez más «egoísta», creo que se debería cuidar y dotar de mayores atribuciones al director de Seguridad. En justa compensación por la carga tanto jurídica como administrativa que soporta el puesto del director de Seguridad, y más aún en entidades bancarias, debería tener una capacidad de actuación muy superior a la que la ley le atribuye actualmente. Mayor capacidad es sinónimo de mayor eficacia en el cumplimiento de las funciones legalmente encomendadas.

*Texto y Fotos: **Gemma G. Juanes/Freepik.***

JUAN SOLÍS CÉSPEDES. DIRECTOR DE SEGURIDAD INFORMÁTICA. UNICAJA BANCO

«El enfoque de la **seguridad** debe ser **integral**, abordando de igual forma la seguridad **física**, **lógica** y **organizativa**»

La mayoría de las entidades financieras han reccionado a la evolución de las amenazas y han desplegado mecanismos que las neutralizan con una gran efectividad», asegura Juan Solís Céspedes, director de Seguridad Informática de Unicaja Banco, durante esta entrevista en la que analiza los retos que debe asumir un CISO a la hora de implantar una estrategia de seguridad o la repercusión de la normativa NIS en el ámbito bancario.

—El CISO es una figura profesional relativamente reciente dentro del organigrama de las empresas, incluido el sector bancario. ¿Podría indicarnos su trayectoria hasta su incorporación en Unicaja Banco?

—Ciertamente, la colección de acrónimos referidos a las distintas responsabilidades no para de ampliarse con nuevas denominaciones… Aunque los perfiles específicos del puesto asociado a las siglas CISO pueden diferir en función de las organizaciones, mi función actual como responsable de la Seguridad Informática de Unicaja Banco responde a ese cargo.

He desarrollado toda mi carrera profesional en el departamento de Informática, desde el año 1980, en diversas funciones y responsabilidades, como técnico de Sistemas, primero; posteriormente, como responsable de Sistemas Centrales, luego, jefe de Infraestructuras Tecnológicas y, en la actualidad, asumo la coordinación de las actividades en el marco de la Seguridad Informática, función que vengo ejerciendo desde diciembre de 2015.

Quiero hacer hincapié en que la seguridad ha sido siempre básica y prioritaria dentro del departamento de Informática. Existe una unidad dedicada a dicha función de forma expresa desde los años 90. Por tanto, mi misión actual da continuidad a las actividades y proyectos que ya se vienen realizando de forma habitual en dicha unidad desde que se constituyó.

—¿Cuáles son las funciones concretas que desempeña un CISO dentro de una entidad financiera como es el caso de Unicaja Banco?

—En mi caso concreto, las funciones que desarrollo son:

- Colaborar en la planificación y en la fijación de los objetivos de la Dirección de Informática, estableciendo la planificación de proyectos y actividades en relación con la seguridad informática, de acuerdo con las prioridades marcadas y velando por su cumplimiento.
- Proponer y elaborar las políticas de seguridad de la información, redactando, en consecuencia, dichas políticas, los procedimientos, normas, reglas y estándares encaminados a garantizar un adecuado nivel de seguridad dentro del departamento.

• Definir y ejecutar proyectos y estudios relativos a la Seguridad de la Información, ya sean exclusivos del ámbito de la unidad o, en el caso de proyectos multidisciplinares, en colaboración con otras unidades del departamento.
• Proponer y participar en la realización de planes y actuaciones orientados al cumplimiento normativo, fundamentalmente en relación con aquellas normativas que afecten a la seguridad de los datos y servicios informatizados.
• Colaborar con otros equipos internos y externos a Informática en el establecimiento y supervisión de los planes de recuperación de desastres informáticos y de continuidad del negocio de la entidad.
• Realizar el seguimiento de la operación del Sistema de Gestión de Seguridad de la Información (SGSI), que Unicaja Banco tiene implantado y certificado desde el año 2007 para el ámbito de Banca Electrónica y Autoservicio.
• Supervisar la administración de identidades y acceso.

maneja ha estado siempre muy restringido y controlado. En los últimos tiempos, la ciberseguridad ha atraído casi toda la atención y se han hecho grandes esfuerzos en seguridad lógica para blindar los sistemas de información frente a ataques, tanto procedentes del exterior como del interior.

> «Hasta el ataque menos sofisticado podría tener éxito ante un usuario poco informado o confiado, si no fuera por las contramedidas que se han desarrollado»

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

—En una entidad financiera la seguridad ha sido siempre una preocupación de máxima importancia. Tradicionalmente, se han hecho grandes inversiones en seguridad física, tanto en las oficinas de cara al público como en las instalaciones de proceso de información, donde el acceso físico al host y a toda la información que se

Actualmente, el enfoque de la seguridad debe ser integral, abordando de igual forma y coordinadamente los aspectos de seguridad física, la seguridad lógica y la seguridad organizativa, entendiendo por esto último la asignación clara de funciones y responsabilidades a los actores que directamente tratan aspectos de seguridad, así como a todo el personal en lo que respecta al manejo de información y sistemas, y a los procedimientos de actuación para que todas las operaciones sean seguras. A todo esto se une la necesidad de cumplir con las múltiples normativas de seguridad que le son aplicables a la actividad de una entidad financiera, tanto las impuestas por leyes, por los supervisores (Banco de España y BCE), por otros agentes, como las marcas de medios de pago, y las autoimpuestas para seguir las mejores prácticas de seguridad reconocidas en el mercado. Un reto principal en el enfoque de la estrategia de seguridad es la implantación de unos mecanismos de gestión, que permitan controlar el despliegue y mantenimiento de todas las medidas de seguridad derivadas de todas las normativas aplicables, de forma que se unifiquen los esfuerzos, ya que existe cierto solapamiento entre ellas, y se pueda verificar el cumplimiento conjunto de todas ellas con un esfuerzo razonable. La forma en la que se aborde esa gestión integrada va a marcar en gran medida la eficacia y la eficiencia del trabajo del CISO.

—Con una visión profesional, ¿cuál cree que es, actualmente, el nivel de seguridad en el ámbito TI de las entidades financieras de nuestro país en relación con Europa?

—La seguridad de la banca española es similar a la de las entidades del resto de Europa. Tanto en el ámbito de la Unión

Europea como dentro de la zona euro existen directrices de seguridad dictadas por la Autoridad Bancaria Europea y el Banco Central Europeo (BCE), que hacen que el nivel de seguridad sea bastante homogéneo en el sector. Por otra parte, otras normativas de seguridad que afectan al sector, tales como PCI-DSS, contribuyen a la mencionada homogeneidad.

Obviamente, hay diferencias en las medidas de seguridad que se implantan en unos bancos y otros, o en sus mecanismos de gestión, pero el nivel final de seguridad alcanzado es bastante equivalente.

En el siempre difícil equilibrio entre seguridad y usabilidad sí que se observan algunas diferencias entre la banca española y la de otros países. Así, por ejemplo, en España no están extendidos los sistemas de autenticación de usuarios por medio de tokens que generan claves de un solo uso, mientras que en algunos países sí se ven estos sistemas. Por el contrario, la mayoría de bancos españoles admiten como mecanismo de autenticación el DNI electrónico y eso no es habitual en otros países.

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

—Las amenazas a las que se enfrentan los bancos, en cuanto a ciberseguridad, se han multiplicado enormemente en los últimos años. Desde hace tiempo hay una especie de carrera entre los ciberdelincuentes y los bancos; los primeros, inventando cada vez más sofisticados ataques, y los segundos, diseñando soluciones de seguridad más robustas. Esta carrera ha podido ser percibida por los usuarios, que han ido viendo cómo para realizar sus operaciones han necesitado más elementos de confirmación: dobles claves, tarjetas de coordenadas, verificación de las transacciones a través del móvil y otros muchos elementos que están ahí pero que el usuario no los percibe.

Actualmente, la seguridad de todas las infraestructuras que dan soporte a las operaciones de un banco por Internet es muy alta, y la parte más vulnerable es (en realidad lo ha sido siempre) el usuario final. Los ciberdelincuentes centran casi todo su esfuerzo en dicho usuario final y le lanzan ataques que pueden ser muy burdos (como la mayoría de los ataques de phishing) hasta otros muy sofisticados, instalando troyanos en el equipo del usuario. Hasta el ataque menos sofisticado podría tener éxito ante un usuario poco informado o confiado, si no fuera por las contramedidas que se han desarrollado.

La mayoría de las entidades financieras han reaccionado a la evolución de las amenazas y han desplegado mecanismos que las neutralizan con una gran efectividad. Esto es algo objetivo, demostrable, ya que el nivel de fraude al usuario debido a ciberataques es bajo. Y los pocos casos de fraude que se han dado se han debido a la falta de aplicación por los afectados de las más elementales normas de seguridad. Las entidades financieras tratan de informar de esas elementales medidas a sus clientes, mediante el envío de comunicados o mediante la publicación de consejos y advertencias en sus sitios web.

Pero, incluso, en los casos más adversos, la seguridad de las transacciones es actualmente muy elevada. Y aun así, cuando una determinada transacción muestra un patrón de comportamiento que no es habitual (por la cantidad, por el lugar desde donde se realiza, por la forma en la que se ha pretendido realizar, etc.) se lleva a cabo una verificación de que la operación es legítima.

En un futuro próximo, la mayor actividad de los usuarios en las redes sociales y la tendencia a estar siempre conectados a través de los smartphones puede hacer que los ciberdelincuentes encuentren la forma de conocer suficientes detalles de la vida de las personas, de modo que diseñen fraudes basados en la extorsión, que pueden suponer un verdadero desafío para ser combatidos, ya que, en ese caso, el usuario que realizaría transacciones sería el legítimo.

—Entrando en aspectos de normativa, ¿qué valoración haría

acerca de la Directiva sobre la Seguridad de las Redes y de la Información (Directiva NIS)? ¿Cómo afectará al sector empresarial en el que usted trabaja?

—La Directiva NIS trata de establecer un nivel mínimo, pero suficiente y elevado, de seguridad en todos los sectores que tienen relación con el funcionamiento de la sociedad actual, y homogéneo en todos los países de la Unión Europea.

Un aspecto muy importante que introduce la directiva es la necesidad de que las organizaciones de los sectores afectados comuniquen los incidentes de seguridad que puedan sufrir. Efectivamente, la compartición de información sobre incidentes de seguridad se identificó hace ya mucho tiempo como un elemento muy importante para mejorar la seguridad. Si a mi vecino le roban en su casa y me informa de ello, y me dice por dónde le entraron, seguramente yo tomaré unas medidas preventivas que no habría tomado de no haberlo sabido. Esta comunicación de incidentes puede ser un punto muy delicado, ya que a las organizaciones no les gusta tener que revelar ese tipo de información porque puede afectar a su imagen pública.

En el caso del sector banca, la directiva es de aplicación total, pero no supone un cambio significativo, ya que el sector está ya fuertemente regulado, con unos requisitos de seguridad que superan al exigido por la directiva, y que hacen, además, que haya bastante uniformidad entre todas las entidades. Por otra parte, el requisito de comunicar incidentes de seguridad ya estaba establecido en las prácticas de supervisión del BCE, por lo que la directiva no introduce en realidad cambios significativos respecto a lo que se venía haciendo ya en la banca. Sí que puede suponer una novedad el hecho de que las autoridades de seguridad, o los CSIRT (Equipos de Respuesta ante Incidencias de Seguridad Informática), informen a las entidades financieras sobre determinados incidentes y haya que desplegar ciertos mecanismos de coordinación y de respuesta a dichos incidentes, aunque esos mecanismos se integrarán seguramente en los ya existentes actualmente.

—¿Cuáles son los grandes retos a los que se enfrenta hoy en día el sector bancario ante Internet?

—Podríamos decir que hay tres líneas de trabajo que suponen un reto: la funcionalidad, la seguridad-usabilidad y el cumplimiento normativo.

En un banco como Unicaja Banco, ha existido tradicionalmente un gran número de clientes que, por su perfil,

estaban habituados a acudir físicamente a las oficinas. Pero esto está cambiando. Las transacciones por Internet están creciendo exponencialmente y son cada vez más los clientes que prefieren no tener que acudir a la oficina para cualquier gestión. Ante la nueva situación, el canal Internet tiene que ser capaz de permitir las mismas operaciones que las que se pueden realizar físicamente en una oficina. Lo anterior implica un reto en muchas ocasiones, debido al dinamismo en los productos ofertados, la multitud de dispositivos desde los que puede acceder un cliente y la necesidad, para ciertas operaciones, de mover documentación, requerir firmas, etc.

Respecto a la seguridad, ya hemos comentado antes la carrera existente entre los ciberdelincuentes y las entidades financieras. La seguridad en la banca por Internet es muy elevada, pero mantenerla a ese nivel requiere un continuo esfuerzo, desplegando nuevas medidas de seguridad, mejorando las ya existentes, pero, sobre todo, gestionando toda esa seguridad. Para ello, es preciso desplegar y operar un sistema de gestión que permita medir: a) el grado de seguridad que se tiene; b) la eficacia de las medidas de seguridad implantadas, y c) identificar en qué aspectos habría que reforzar algún mecanismo de seguridad. Y, todo ello, en un proceso de revisión y mejora continuas, ya que las amenazas exteriores cambian y evolucionan.

Pero elevar la seguridad en el lado del usuario, que, obviamente, juega un papel clave en el proceso, requiere siempre llegar a un compromiso entre la seguridad y la usabilidad, frecuentemente reñidas entre sí. Para combatir el fraude, lo más eficaz es garantizar la autenticidad de la identidad del cliente, conocer quién realmente está operando al otro lado. Existe tecnología para ello, pero no siempre se utiliza por la incomodidad que puede suponer para el usuario. Así, por ejemplo, la autenticación basada en el DNI electrónico es muy fidedigna, pero, al menos hoy por hoy, requiere que el usuario disponga de lector y se complica enormemente si el dispositivo desde el que accede es un móvil o una tableta. Siguiendo con este ejemplo, casi todas las entidades admiten el DNI electrónico como un medio de autenticación, pero su uso es opcional, no obligatorio.

En cuanto al cumplimiento normativo, la necesidad de cumplir un gran número de normas y poder verificar ese cumplimiento requiere un gran esfuerzo si no se aborda una estrategia de gestión adecuada. Todas estas normas exigen el despliegue de unas ciertas medidas de seguridad, precisan del mantenimiento de una gran cantidad de documentación, de un conjunto de indicadores, de unos registros de evidencias, de auditorías internas y de otros muchos elementos que pueden llegar a tener cierto impacto en la organización. Es, por ello, importante poder realizar una gestión de forma integrada de todas las normativas, de forma que se simplifique su mantenimiento.

—Hoy en día se apuesta por la convergencia de la seguridad -física y lógica- como un concepto integral, ¿cree que las grandes corporaciones financieras están preparadas para asumir este concepto?

—Es cierto que, tradicionalmente, la seguridad física y la seguridad lógica han llevado caminos separados. Típicamente, cada una de ellas recaía en un departamento diferente de la organización y existía poca o nula coordinación entre ellos. Pero esto está cambiando. Todas las normativas de seguridad que afectan al sector exigen un enfoque integral de la seguridad, dentro del que se coordinen los aspectos de seguridad física, lógica y de los recursos humanos. Y no sólo eso, sino que se piense en la seguridad desde el momento mismo en que se concibe un nuevo producto o solución. Es, por tanto, una necesidad el establecimiento de comités de seguridad donde estén representadas las partes de la organización que tienen que decir algo respecto a la seguridad , y en los que se analicen conjuntamente los incidentes que se hayan podido producir; el enfoque de seguridad de nuevos productos, o el acceso físico al lugar donde se encuentran los sistemas. Éste es un camino que se está recorriendo, no sin esfuerzo en ocasiones, ya que hay que vencer inercias organizativas.

FUJIFILM
Value from Innovation

Una nueva dimensión de la Seguridad:

4K

Primeras lentes Vari Focales 4K de Fujinon

Day Night

Nuevo DV2.2x4.1SR4A-SA2L de Fujifilm

Rendimiento óptico avanzado para capturar imágenes de seguridad en alta resolución 4K. Detalles más finos durante el día y la noche gracias a la tecnología Día/Noche incorporada. Escanea para más información o visita www.fujifilm.eu/fujinon

Fujinon. Para ver más. Para saber más.

FUJINON

CÉSAR BILBAO DELGADO. DIRECTOR DE SEGURIDAD BANCARIA CORPORATIVA. MEX & ADS. BBVA

«Nuestros **objetivos estratégicos** son mejorar **la calidad del servicio, aumentar la satisfacción del cliente,...»**

CADA vez más, la preparación técnica de los directores de Seguridad que asumen responsabilidades en las grandes compañías, incluye formación en seguridad integral, física, tecnológica, de la información, continuidad de negocio, riesgos laborales y, en las corporaciones en que todavía no está integrada, existe, o debe de existir una estrecha colaboración e interacción entre las áreas», explica César Bilbao Delgado, director de Seguridad Bancaria Corporativa. MEX & ADS. BBVA, quien además analiza para Cuadernos de Seguridad los medios y medidas de seguridad a implantar en una entidad BBVA y los riesgos a los que hace frente un director de Seguridad en una entida bancaria.

—¿Cuál ha sido su trayectoria profesional en el ámbito de la Seguridad Bancaria? ¿Qué aspectos más importantes destacaría de ella?

—Comencé hace 38 años en Bilbao (Grupo BBVA), tras pasar por la Dirección Territorial de Cataluña me incorpore al departamento Central de Seguridad en Madrid, donde he desempeñado funciones en la Prevención del Fraude y la Seguridad Bancaria; en la actualidad mi ámbito de actuación es la Seguridad Bancaria Corporativa en el perímetro de América Latina.

Todo en mi trayectoria profesional ha sido destacado, los primeros años de Bilbao, conociendo el funcionamiento de la casa, la escasa e inicial legislación en su vertiente de la Seguridad Privada, Real Decreto 554/1.974, que permitía la creación de empresas y entidades de seguridad privada, y obligaba a las entidades de crédito a implantar medidas de seguridad y disponer de departamento de Seguridad.

Una segunda etapa, interesantísima, en la Dirección Territorial de Catalunya, allá por los años 80, periodo de tiempo que coincidió, creo, con el mayor número de atracos sufridos a las entidades de crédito, lo que nos obligó a plantearnos si las medidas de seguridad instaladas en las oficinas bancarias eran lo suficientemente válidas para combatir esa lacra; fue en esa época cuando comenzamos con las instalaciones de cámaras de 35 mm y arcos detectores de metales.

La primera fase de mi desempeño en Madrid, después de 10 años en Cataluña, fue excepcional, comenzamos en el departamento, con lo que denominamos «Seguridad Operativa», para tratar de aglutinar y minimizar el fraude que comenzábamos a padecer, disposiciones de efectivo por caja, falsificación de cheques en todas sus modalidades, pero muy especialmente en fraude con la tarjeta de crédito, robo y utilización, falsificación integral, etc.

Posteriormente y ya en la función de Seguridad Bancaria, fue apasionante recorrer, prácticamente toda la geografía de España, y parte de Europa, impartiendo formación de Seguridad, realizando visitas a oficinas, a fin de informar y mejorar las actuaciones de nuestros compañeros en evitación de actos delictivos, ayuda en los posteriores momentos de los incidentes producidos (atracos, robos, hurtos,

etc.), visitas de obras con el objetivo de realizar las obligadas instalaciones de elementos de seguridad.

No me puedo olvidar de lo que aprendí asistiendo a seminarios, reuniones en la AEB, CCI, etc., a fin de compartir información, unificar criterios en cuanto a cumplimientos normativos, instalaciones, etc.

Otro aspecto destacado en todas las funciones que he desempeñado ha sido y sigue siendo, la colaboración con las Fuerzas y Cuerpos de Seguridad del Estado, Policías Autonómicas, entidades de crédito, etc.

Otras etapas inolvidables han sido la participación en la remodelación del Centro de Gestión de Alarmas y la colaboración en la ejecución y puesta en marcha de la aplicación FARO.

Para finalizar, entre los aspectos más importantes en mí paso por el departamento de Seguridad de BBVA, resalto la

inestimable colaboración que he disfrutado de todos mis compañeros y la cercanía y saber hacer de mis superiores.

Creo, queda claro, como decía al principio, que todo lo que he desarrollado en el departamento de Seguridad ha sido, para mí, muy importante.

—¿Cuáles son sus funciones en el área de Seguridad Bancaria, integrado dentro del departamento de Seguridad Corporativa?

—Como comentaba en uno de los puntos de la pregunta anterior, en la actualidad mi función es la de apoyar y coordinar todo lo referido a la Seguridad Bancaria (Oficinas /Centros de Gestión de Alarmas), al objeto de conseguir homogeneizar aplicaciones, proveedores, siempre que la particularidad del país lo permita, minimizar costes, distribución de alertas tempranas, modus operandi de los distintos incidentes que se producen, para lo que contamos

con la herramienta FARO, en definitiva transmitir las políticas y estrategias corporativas de seguridad.

—¿Qué medios y medidas de seguridad cree que son necesarias hoy en día en las entidades de BBVA?

—Como mínimo lo exigible por las distintas legislaciones que les afecte, no obstante, creo que todas las entidades superan ese mínimo, y lo deseable, dado la época que vivimos, sería implementar equipamientos de corte digital, tanto en las Centrales Receptoras de Alarmas como en las oficinas, al objeto de conseguir una más ágil transmisión de señales, encaminadas al control y gestión de mantenimientos, servicios de vigilancia y muy especialmente lo referido a imágenes, que permitirá mejorar la comunicación con las distintas policías, pudiendo recibir éstas en directo durante la comisión de hechos delictivos, con la posibilidad de ahorro de costes en la gestión y almacenamiento.

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

—Los riesgos a los que en Seguridad Bancaria nos enfrentamos son los que afectan a las personas (clientes/empleados), al patrimonio y a la información. Hacemos frente a este tipo de contingencias, organizando, planificando, identificando riesgos, impartiendo formación, instalando medidas de Seguridad eficientes (físicas/electrónicas), para protegernos de lo que busca la delincuencia. Todo lo anterior con las mejores prácticas y cumpliendo la normativa en materia de seguridad privada, tanto la interna como la externa.

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

—Cada vez más, la preparación técnica de los directores de Seguridad que asumen responsabilidades en las grandes compañías, incluye formación en seguridad integral, física, tecnológica, de la información, continuidad de negocio, riesgos laborales y, en las corporaciones en que todavía no está integrada, existe, o debe de existir, una estrecha colaboración e interacción entre las áreas detalladas, por lo que no creo que sea complejo asumir este patrón de la gestión de la seguridad por las grandes corporaciones.

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

—En este tema me gustaría comenzar felicitando tanto a la Unidad Central de Seguridad Privada como al Servicio de Protección y Seguridad de la Guardia Civil por la excelente labor realizada en los últimos años, lo que ha dado paso a la nueva Ley de Seguridad Privada que culminará con la aprobación del anhelado Reglamento.

En cuanto a qué me gustaría que recogiese, creo que es mejor esperar a su publicación, analizarlo con el mayor detalle posible y, si es el caso, comentar con las autoridades competentes la posible adaptación a las realidades del momento.

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

—En nuestro caso, los pilares sobre los que trabajamos y nos sentimos cómodos, por no decir seguros, son los que tenemos como objetivos estratégicos para toda el área Corporativa de Seguridad, incluida la Bancaria, que bajo el acrónimo de MAR, detallamos:

- Mejorar la calidad del servicio.
- Aumentar la satisfacción el cliente (Interno / Externo).
- Rentabilidad en todas nuestras gestiones.

Si a lo anterior unimos, nuestras señas de identidad y el modelo de gestión corporativa, creo tenemos un adecuado y sólido soporte para gestionar las responsabilidades asignadas a cada una de las personas que conformamos el departamento. ●

Texto: Gemma G. Juanes.
Fotos: BBVA

GEUTEBRÜCK
Excellence in Video Security

G-SIM de GEUTEBRÜCK

Optimizando la seguridad de las Entidades Bancarias

NO MÁS ÁNGULOS MUERTOS

No pierda el más mínimo detalle de lo que sucede en todas las áreas de su instalación. Gracias a cámaras de resolución hasta 48 MP y 360º podrá ver lo que sucede con todo lujo de detalles.

CONTROL TOTAL DE LA INSTALACIÓN

Desde el centro de control será capaz de visualizar todo lo que está ocurriendo, el estado de salud de los equipos, enviar tareas y alarmas y mantener conversaciones entre usuarios.

INFORMES - DOCUMENTACIÓN DETALLADA

Realice auditorias de la forma más completa. Con ayuda de un filtro ajustable es fácil realizarlo.¿Desea imprimir el informe? ¿Enviarlo por correo electrónico? ¿Guardarlo en otros formatos?

ALTA DISPONIBILIDAD

Equipos con sistemas avanzados de protección.
Configuración RAID interna para S.O. y Base de Datos.
Fuente de alimentación redundante.

F.F. Videosistemas
www.ffvideosistemas.com
Tel. 902 99 84 40
ffvideo@ffvideosistemas.com

F.F. Videosistemas
GEUTEBRÜCK

JUAN CARLOS ROBLEDO HERNÁNDEZ. DIRECTOR DE SEGURIDAD INTEGRAL. CAJA RURAL DE SALAMANCA

«En **España** somos un referente en materia de **Seguridad Pública y Seguridad Privada**»

EL sector financiero español es un sector de referencia no solo a nivel europeo sino mundial. Grandes entidades de nuestro país desarrollan su actividad en otros continentes, con lo que en materia de seguridad supone, distintas normativas, riesgos muy distintos, culturas, religiones e incluso conflictos bélicos, dejando a nuestro sistema de seguridad financiero en la más alta consideración». Son palabras de Juan Carlos Robledo Hernández, director de Seguridad Integral de Caja Rural de Salamanca, quien a lo largo de la entrevista explica, entre otros aspectos, cuáles son los pilares sobre los debería asentarse una adecuada seguridad bancaria.

—¿Podría describirnos las particularidades sobre la gestión de seguridad en Caja Rural de Salamanca?

—En Caja Rural de Salamanca gestionamos una red de oficinas repartidas entre las provincias de Salamanca, Ávila y Valladolid. El 70% de las sucursales se encuentran ubicadas en demarcación rural, muchas de ellas en poblaciones muy descentralizadas, con problemas de fácil accesibilidad por carretera y núcleos de baja población. Esto hace que nos tengamos que enfrentar en ocasiones a retos añadidos al resto de la entidades financieras focalizadas en grandes núcleos urbanos, a la vez que asumimos los propios de estos núcleos urbanos donde mantenemos el 30% restante de nuestra red comercial.

Incidencias básicas como enviar acuda a una oficina, o emitir una señal de alarma a los servicios de seguridad pública suponen todo un reto, ya que debemos valorar su eficacia ante largos desplazamientos y tiempos de respuesta. Si además te encuentras que a estas poblaciones rurales se puede acceder por varias vías, muchas de ellas incluso forestales, hace que ante siniestros delictivos estemos ante un grave problema de desprotección. Las dificultades, en este sentido, son lo que nos ha hecho ser muy perfeccionistas con nuestros sistemas y medidas de seguridad, a la vez que favorecen la implantación de una correcta cultura de seguridad en las personas que trabajan en nuestra organización, asumiendo en estas obligaciones y conductas disciplinarias, un beneficio hacia su propia integridad física.

—¿Cuál es la estructura e infraestructura actual del departamento de Seguridad en la Entidad?

—En Caja Rural de Salamanca, como en otras muchas pequeñas o medianas entidades de crédito, un mismo área agrupa a varios departamentos y este es nuestro caso, el departamento de Seguridad está integrado en el Área de Servicios Generales. Al frente me encuentro como director de Seguridad

desde hace dieciocho años, siendo además director del Área de Servicios Generales y director del Área de Organización e Informática.

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

—Nos enfrentamos a los mismos riesgos que el resto del sector financiero, con la salvedad en alguno de ellos sobre la problemática que comentaba anteriormente debido a la dispersión geográfica que perjudica o dificulta en cierta medida. Por clasificar los riesgos nosotros tenemos catalogados tres grupos diferenciados, donde por un lado tenemos los riesgos comunes o históricos por su perduración en el tiempo, como son atracos, falsificaciones, robos de todo tipo, etc; otro grupo de riesgos derivados del correcto cumplimiento normativo como es prevención de blanqueo de capitales y financiación del terrorismo, trasparencia financiera, continuidad de negocio, etc, y por último los riesgos emergentes, casi siempre como no puede ser de otro modo, relacionados con las nuevas tecnologías de comunicación, debido a que estos son los más novedosos canales para operar en banca, siendo estos riesgos el mayor reto para los profesionales de la seguridad.

—Desde una visión profesional, ¿cuál cree que es actualmente el nivel de seguridad de las entidades financieras de nuestro país en relación a Europa?

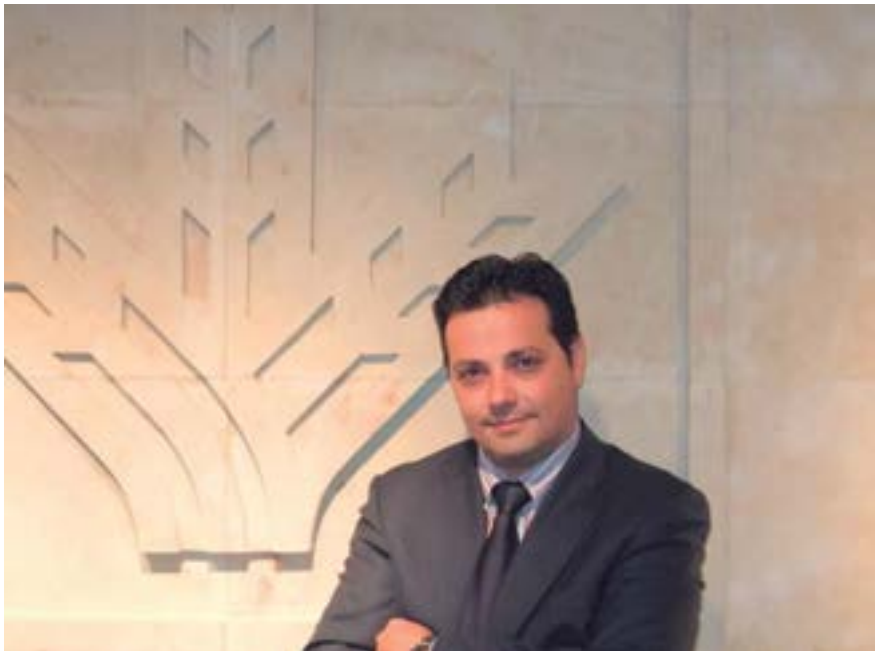
—El sector financiero español es un sector de referencia no sólo a nivel europeo sino mundial. Grandes entidades de nuestro país desarrollan su actividad en otros continentes, con lo que en materia de seguridad supone distintas normativas, riesgos muy distintos, culturas, religiones e incluso conflictos bélicos, dejando a nuestro sistema de seguridad financiero en la más alta consideración.

Por otro lado y centrándonos en la gestión de seguridad financiera dentro de nuestro país, partimos de una Ley de Seguridad Privada que ha sido un referente a nivel europeo. Esto lo que ha hecho es que tengamos un punto de partida avanzado, mientras en otros países miembros el sector de la seguridad privada no cuenta con regulación ni con criterios homogéneos.

No quiero decir con ello que nos encontremos en una posición inmejorable, porque las normas y leyes deben evolucionar de la mano de los nuevos tiempos, pero podemos decir que con ciertos matices nos podemos sentir satisfechos, contamos con certificaciones de sistemas, grados de medidas catalogadas, formación reglada, habilitaciones profesionales, unidades policiales encargadas de la supervisión, control y cooperación, etc., en definitiva creo que en España y muy a nuestro pesar, precedidos por altos índices de siniestros en los años ochenta y la lacra del terrorismo, somos un referente en materia tanto de seguridad pública como privada.

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

—No creo que hayan cambiado los riesgos lo que si tengo claro es que han aparecido nuevos y con ellos las prioridades de protección. Por poner un ejemplo siempre estaremos expuestos a robos, pero la pérdida que nos pueda suponer un robo no es comparable a los daños que pueda provocar en una entidad financiera un sabotaje a sus sistemas de comunicaciones, fuga de datos en servidores, phishing masivo a clientes, etc. Estos riesgos además de novedosos,



suponen un gran reto para los profesionales de la seguridad ya que su canal de ejecución es la tecnología, y luchar para frenar los avances tecnológicos muchas veces no está en manos de los profesionales de seguridad, y es por ello que de estos incidentes nunca puedes tener la garantía de estar exento; en este campo el objetivo actual es minimizar los riesgos y la probabilidad de sufrirlos.

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

—Estoy totalmente convencido, en Caja Rural este modelo es el que mantenemos implantado y de otro modo podría provocar dispersión y lagunas de seguridad graves. Lo que si hay que tener muy en cuenta es que un directivo de Seguridad dentro de una entidad financiera es un cargo ejecutivo, cuya misión entre otras, es servir como enlace con los Cuerpos y Fuerzas de Seguridad del Estado, que tiene que velar por el cumplimiento normativo, analizar y planificar las medidas y políticas de seguridad para asegurar los intereses de la Entidad, a la vez que evita se convierta en un canal para la comisión de cualquier suceso delictivo. Si bien, se precisa adquirir unos conocimientos amplios en relación a todos los riesgos, sin la necesidad de ser experto cualificado en todas y cada una de las materias, dando mucho más valor a la gestión de los equipos humanos a su disposición, especialistas que bajo su coordinación, trabajando en equipo y bajo una única finalidad, formarán parte muy importante del éxito de la política de seguridad.

—¿Qué aspectos le gustaría que recogiese el Reglamento de Seguridad Privada?

—Son muchas las propuestas que los profesionales del sector podemos hacer, pero por centrarnos en algunos aspectos concretos, bajo mi opinión, deberíamos ser capaces de no ser tan generalistas a la hora de dotar la adopción de medidas de seguridad en oficinas financieras ya que no todas están expuestas a los mismos riesgos. Hasta ahora la única diferencia entre ellas está basada en el número de habitantes del municipio donde se ubica y esto es insuficiente, se deben tener en cuenta criterios básicos como número de trabajadores, ubicación, encajes de efectivo, y todo ello plasmado en un plan de seguridad de la propia sucursal donde en función de los riegos se destinen medidas para enfrentarnos a ellos. Es complejo pero seríamos capaces de ajustar más la protección a las necesidades reales.

Por otro lado, es necesario que el Reglamento regule la gestión de seguridad en otro tipo de actividades de alto riesgo, donde en la actualidad y en gran número de ellas, las medidas y protecciones de seguridad están en manos de personas no expertas. Me refiero a complejos hospitalarios, museos, grandes centros comerciales, etc., en definitiva lugares de alto riesgo, donde en la actualidad no existe ninguna obligación sobre la gestión en seguridad más lejos de prevención de incendios o riesgos laborales.

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

—Bajo mi apreciación, y es algo de lo que además estoy convencido por la trayectoria y experiencia, una correcta política de seguridad necesita de una participación plena por parte de todos los intervinientes, siendo básico el conocimiento sobre los riesgos, sus consecuencias y su forma de evitarlos. Por ello la formación a toda la cadena humana es fundamental. No sirve de nada implantar planes y medidas muy correctas o incluso hacer fuertes inversiones, si todo ello está sujeto al desconocimiento para el personal operativo. ●

Texto: Gemma G. Juanes.
Fotos: Caja Rural de Salamanca

TE AYUDAMOS A DAR EL

SALTO DIGITAL

Desde hace más de 30 años, GMV lleva sumergiéndose en la más alta tecnología para ayudar a empresas e instituciones a llegar a lo más alto del pódium en sus negocios.

Liderazgo tecnológico, capacidad de innovación, calidad, eficiencia y flexibilidad son el trampolín perfecto que GMV proporciona a sus clientes para acompañarles a dar el salto al mundo digital.

GMV, CONSEGUIR TUS RETOS ES NUESTRA MEDALLA

GMV
www.gmv.es marketing.TIC@gmv.es

www.facebook.com/infoGMV

@infoGMV_es

gmv®
INNOVATING SOLUTIONS

AERONÁUTICA I ESPACIO I DEFENSA I SANIDAD I CIBERSEGURIDAD I TRANSPORTE I TELECOMUNICACIONES I TECNOLOGÍAS DE LA INFORMACIÓN

EDUARD ZAMORA. DIRECCIÓN DE SEGURIDAD PERSONAL Y PROTECCIÓN. GRUPO BANCO SABADELL

*«Abogo por que exista en cada entidad una **Dirección de Seguridad, integral, única y potente»***

PARECE como si la ciberseguridad hubiera eclipsado o borrado del mapa a la delincuencia «tradicional», cuando lo cierto es que todavía, en la mayoría de entidades financieras, la ciberdelincuencia no llega a los importes de perjuicio económico real que causa el resto de delincuencia, la de los delitos paradigmáticos de la banca durante toda su existencia y que hoy, aunque parezca que muchos lo hayan olvidado, centrándose tan sólo en hablar de la ciberdelincuencia, sigue existiendo y haciendo daño a las cuentas de resultados de la banca», asegura Eduard Zamora, Dirección de Seguridad Personal y Protección. Grupo Banco Sabadell, quien a lo largo de la entrevista aborda entre otros aspectos cómo han cambiado las amenazas en las entidades bancarias, o cuáles son los grandes retos a los que se enfrenta el sector bancario.

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

—Hemos debido adaptar nuestras estructuras, recursos económicos y mentalidad a los nuevos tiempos que nos han tocado vivir en el sector financiero, al igual que en el resto de actividades económicas y productivas del país. En base a ello, nos ha tocado remodelar diversos aspectos de estos apartados:

•**Estructuras**: ha sido preciso simplificar las mismas, haciéndolas más prácticas y operativas. Debe decidirse entre las posiciones que estrictamente sea preciso e indispensable mantener en nuestra empresa y cuáles otras pueden ser externalizadas, sin dejar de mantener un estricto control de su funcionamiento y perfecta coordinación con nuestra Dirección, pero sin que vengan a engrosar las plantillas efectivas de la entidad. Esto nos permite una mayor capacidad de adaptación a las necesidades de cada momento, tanto en cantidad como en especialidad, pero es muy importante aquí contar con la complicidad de las empresas de seguridad en quienes deleguemos las funciones y tareas externalizables.

•**Recursos económicos:** ha habido que valorar si las partidas presupuestarias de gastos e inversiones debían mantenerse en los niveles anteriores, o bien podían reducirse en sus importes, sin que se afecten los riesgos básicos a cubrir. En todo caso, con la conformidad inequívoca de la Dirección máxima de la entidad, nunca por nuestra cuenta y riesgo, puesto que las políticas de seguridad deben adaptarse a dos aspectos indispensables: la regulación normativa obligatoria y, en paralelo y sin afectar a ella, la definición del nivel de coberturas que quiera aplicar nuestra entidad, en base a los riesgos reales que se evidencien por nuestra capacidad analítica y directivas.

Superadas ya las épocas de presupuestos ingentes y hasta, quizás, muy poco controlados por las direcciones financieras de nuestras entidades, llega el momento de replantearse toda partida

y definir cuáles deben seguir vigentes y en qué medida. Todo ello en pro de la mayor eficiencia y control presupuestario que se exige a todos los ámbitos de nuestras entidades, a la seguridad también, como no puede ser menos.

•**Mentalidad:** hemos debido de olvidarnos de épocas en las que parecía que la Dirección de Seguridad pudiera ser un mundo aparte dentro de las entidades dotadas de este departamento, importante, eso sí, pero no en menor grado que las direcciones vitales para la compañía.

Superar los momentos en los que argumentando el simple concepto de «en pro de la seguridad» todo parecía ser aceptable por los diversos estamentos de la empresa no ha sido tarea fácil para muchos de nosotros. Ahora, en cambio, se nos exige, como al resto de direcciones, la mayor contribución al negocio y a la eficiencia de nuestras empresas. Hemos dejado de «comer aparte» y hay que asimilar, por lógica y por necesidad, que hemos de adaptarnos a los mismos requerimientos y exigencias que se definen para los demás.

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

—Parece como si la ciberseguridad hubiera eclipsado o borrado del mapa a la delincuencia «tradicional», cuando lo cierto es que todavía, en la mayoría de entidades financieras, la ciberdelincuencia no llega a los importes de perjuicio económico real que causa el resto de delincuencia, la de los delitos paradigmáticos de la banca durante toda su existencia y que hoy, aunque parezca que muchos lo hayan olvidado, centrándose tan sólo en hablar de la ciberdelincuencia, sigue existiendo y haciendo daño a las cuentas de resultados de la banca.

Otra cosa diferenciada es si hablamos de riesgos potenciales, entonces ya si que hemos de manejar y evaluar riesgos de otra manera, puesto que la potencial criticidad de la ciberdelincuencia puede superar ampliamente la capacidad de daño económico de los modus operando más clásicos.

No debemos diferenciar algunos tipos delictivos de la ciberdelincuencia (robo, hurto, suplantación de identidad, fraude, etc.) de los delitos de la delincuencia tradicional, puesto que los mismos delitos son perfectamente encajables en ambos mundos delincuenciales. Se diferencian dichos universos delictivos, el ciber y el tradicional, tan sólo en los medios empleados, pero no en la base definitoria y características que configura el ordenamiento jurídico para la definición de cada uno de dichos delitos.

Y como el riesgo potencial y la criticidad del perjuicio no somos todavía capaces de definir si pueden acotarse claramente, o bien si los ciberdelincuentes pudieran causar un perjuicio astronómico si son lo suficientemente hábiles en el ataque, parece lógico que las prevenciones se centren en este tipo de delitos, que pueden estar eclipsando a los delitos tradicionales de manera errónea, cuando lo lógico y coherente debería ser que se trabajasen en común y conjuntamente las coberturas y minimización de sus correspondientes impactos monetarios. Por ello, a mi modo de ver, no estoy conforme con el «boom» que se está dando a la gestión de la ciberdelincuencia en todos los medios y entornos de gestión de la seguridad, en parte provocado por las empresas de seguridad que han visto un nicho de negocio importantísimo y se vuelcan en ofrecer medios, sistemas y procedimientos preventivos, y por otra, por las entidades usuarias que se han dejado obnubilar por el alto potencial de perjuicio de los ciberdelitos. El justo equilibrio en la gestión y prevención de ambos espectros, que los dos son realmente importantes, en perjuicio directo y/o potencial, sería la posición ideal.

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

—La entiendo contestada en el contenido de mi respuesta a la primera pregunta, donde he expuesto que las Direcciones de Seguridad han debido

reconducir sus estructuras, presupuestos y mentalidad anteriores a la crisis económico-social en que se han visto envueltas nuestras entidades.

—En entrevistas anteriores usted aseguraba que había llegado el momento de pensar en nuevos organigramas de las Direcciones de Seguridad, ¿cómo artícularía la estructura de esos departamentos?

—Sigo defendiendo, años después, la bondad de los planteamientos que durante tantos años he manifestado al respecto: las estructuras de seguridad debieran integrarse en una sóla Dirección, un macrodepartamento que trate, con los expertos precisos en cada caso, en cada una de sus especialidades o ámbitos de trabajo, todo tipo de delitos y riesgos delincuenciales.

Considero un error que se estén adaptando estructuras, presupuestos y mentalidades para ir en la línea de mayor eficiencia y eficacia que hoy se exige a toda la empresa, en global, y que todavía sigan en ámbitos totalmente diferenciados las diversas gestiones de los múltiples riesgos delictivos a que se enfrenta una entidad financiera. Así, en muchos casos el fraude se trata en Medios de Pago, Operaciones o Cumplimiento Normativo. Los ciberdelitos en la Dirección Tecnológica; los robos y atracos en la Direccion de Seguridad Física, y la protección de la Alta Dirección en una Dirección de Seguridad Personal, dependientes, estas dos últimas, según la entidad, de Servicios Generales, Dirección General de Medios o, incluso, en el caso de la última, de la propia Presidencia.

Este amplio abanico de posibilidades diferenciadas de gestión de la seguridad por un abanico diverso de departamentos que trabajan sus múltiples aspectos resta, de manera notable, efectividad y eficiencia, conceptos que, como decía, hoy han de ser básicos en el funcionamiento de cada dirección de la entidad, incluida la que gestiona la seguridad. Por todo ello he defendido, y abogo todavía hoy, que exista en cada entidad una sola Dirección de Seguridad, integral, única y potente, que gestione, en común y bajo un mismo prisma, todos los riesgos delictivos y que, con esa integralidad, aproveche las múltiples sinergias, económicas, de gestión y de visión global y transversal, que el tratamiento unificado de las incidencias delictivas puede aportar en mayor grado.

—¿Cuáles considera que son hoy en día ante nuevos riesgos y amenazas los pilares sobre los que debe asentarse una adecuada seguridad bancaria?

—Creo que deben protegerse, en este mismo orden en que las enumero, las amenazas a las personas, a los bienes y a la eficiencia de la entidad.

Primero siempre ha de ser, muy por encima de todo, la protección de las personas, adaptada, claro está, al nivel de riesgo que conlleve no tan sólo el nivel jerárquico que se ocupe, aspecto que siempre influye notablemente en el riesgo específico de ciertos cargos, sino que debe proteger a toda persona (plantilla, subcontratas, clientes, etc.) en todo aquello que implique el desarrollo de una función determinada dentro de la entidad.

Hay tareas que, sin ser de Alta Dirección, conllevan un alto riesgo para las personas que las llevan a cabo. Por todo ello hay que partir de la base de una adecuada evaluación del riesgo de todas y cada una de las posiciones y funciones dentro de la entidad, adaptando las medidas preventivas y de protección a los riesgos definidos para aquellas.

En segundo lugar la protección de los bienes y hoy este concepto se ha ampliado, sumándose la reputación y la imagen de la empresa como un bien esencial a proteger. Hasta hace bien poco parecía que sólo nos debíamos encargar de proteger los bienes muebles e inmuebles de nuestra entidad. Hoy el catálogo de bienes se ha ampliado con aquellos otros, que pueden ser igual de críticos o más que los clásicos.

En tercer lugar la eficiencia. Aunque pareciera que con los dos primeros apartados este ya podría estar incluido, merece ser remarcado, por considerarlo un aspecto diferenciado de aquellos, en un punto aparte por ser un aspecto básico que hemos de proteger: la eficiencia de

todas y cada una de las funciones, procesos y procedimientos de la entidad. La minimización del impacto delictivo en todos ellos los hará, sin duda, más eficientes y contribuiremos así al mayor beneficio de la cuenta de resultados de la empresa.

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

—Una mayor flexibilidad en los actuales planteamientos que rigen en la determinación de las medidas obligatorias aplicables y en los sectores y actividades obligadas a disponer de dichas medidas.

En otros países prima el criterio particular, la voluntad de cada entidad en la definición de las medidas de protección y prevención aplicables en su actividad. Las aseguradoras y las certificadoras sirven de filtro para que el nivel de dichas medidas sea mayor o menor, debiéndose abonar mayores primas, en unos casos, o bien renunciar a la validación de la certificadora si no se disponen de unos mínimos exigibles en la gestión material y efectiva de la seguridad.

En nuestro país, quizás para evitar que la picaresca propia de los latinos pueda eludir ciertos niveles de cumplimiento, prima un modelo de obligatoriedad de unas medidas hoy, con toda seguridad, pudiera ser totalmente insuficientes para cubrir el amplio abanico delictivo que comentaba anteriormente. No se regulan hasta hoy medidas preventivas que no se refieran expresamente al robo o al atraco, cuando, estadísticamente, son los menos importantes y perjudiciales en la actividad bancaria.

No se atiende al fraude en general, sea ciber o tradicional. Tampoco se trata de cómo proteger a las personas de las amenazas o riesgos derivados de su función en las entidades, que antes comentaba. Por ello, como me habéis oído pronunciar en muchas ocasiones y sigo manteniendo firmemente, muchos aspectos del modelo de la gestión de la Prevención de Riesgos Laborales es para mí un modelo de gestión mucho más adaptado a las necesidades reales de nuestras entidades.

La normativa de seguridad privada debiera tomar de aquel modelo varias de sus premisas básicas y modernizar su regulación en lo necesario para favorecer que, mediante normas técnicas y mediante datos estadísticos reales de cada sector o entidad, se facilite la definición del modelo de gestión y medidas técnicas aplicables a cada caso.

No sirve el café para todos, ni tampoco la libertad absoluta de gestión. Lo válido, a mi parecer, sería una adaptación de cada entidad a las necesidades reales de sus riesgos y necesidades. Tan sólo así el sistema de gestión y medidas de seguridad, materiales y organizativas, que se le debe exigir a cada empresa, sin importar el sector en que desarrolle su actividad, lograría ser realmente justo y adaptable a cada momento, superando uno de los problemas que creo causa el sistema actual: que regula profundamente, quizás en exceso, un sector o actividad, y dentro de ella atendiendo a unos mínimos tipos delictivos (robo-atraco) y deja otros, de iguales o parecidos riesgos, pero de mayor número de incidencias y perjuicio económico real, a su libre albedrío.

—¿Cuáles son los grandes retos en cuanto a Seguridad a los que se enfrenta hoy en día el sector bancario?

—En los anteriores apartados creo que se han ido definiendo en su totalidad, pero intento resumirlos en estos tres apartados:

- Adaptación a las necesidades de eficiencia de las empresas actuales.
- Concentración de la gestión de los diversos riesgos delictivos en un solo ámbito, en una Dirección de Seguridad «integral», que trate, conjunta y unificadamente, la totalidad de las tipologías delictivas y los múltiples riesgos que pueden afectar a cada entidad, en función de su sector de actividad, visibilidad y tamaño.
- Reordenación de la normativa reguladora, ganando en objetividad y en la aplicación de criterios reguladores que permitan definir las medidas precisas que deben aplicarse en base a los riesgos reales de cada sector o entidad.

Texto: Gemma G. Juanes.
Fotos: Banco Sabadell/Xavi Gómez

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

La Banca ante su más difícil despegue

HACE tan solo ocho años los bancos europeos contaban en sus plantillas con casi 3.300.000 empleados, todo un récord jamás conocido en la historia de las entidades financieras del viejo continente. Según las últimas estadísticas de la UE, tras seis años de crisis, en 2014, esa cifra se había reducido en casi 400.000 personas. La estructura de oficinas también sufrió en su línea de flotación las terribles consecuencias de lo que originariamente se definió como unos tipos de interés irresistiblemente bajos, que lanzó a millones de personas a la adquisición sin control de viviendas gracias a hipotecas con tipos de interés de saldo por derribo, y a la insaciabilidad de algunas empresas sin escrúpulos que titularizaban por paquetes auténticos torpedos en las líneas de flotación de las entidades financieras compradoras. En España, la evolución de las estadísticas en número de empleados y sucursales no tuvo nada que envidiarle a las europeas y sí añadirles unos significativos ratios negativos: desde 2008 a 2015 el número de empleados se redujo en 76.000 personas y las sucursales pasaron de 46.167 a 30.853 en el espacio de ocho años (2008-marzo 2016). Los medios nacionales nos hacían temblar con sus balances demoledoramente deudores: «La banca española, a la cabeza del recorte de empleo en Europa». Todo un desastre que estaba pidiendo a gritos cambios trascendentales mediante nuevos estilos de liderazgo y procesos y estrategias más audaces que nunca.

Los primeros cambios ya apuntaban a un nuevo horizonte tecnológico con el diseño de un nuevo perfil de profesionales. Las entidades resumían en sus ofertas la nueva cancha de juego demandando especialistas de Big Data, Marketing Digital, Análisis Estratégico, y Regulación y Cumplimiento Normativo. Los titulares periodísticos siguen las nuevas pistas de los cambios emprendidos por las entidades del sector: «La Banca pone a directivos clave al frente de la revolución digital», «El Big Data, la última frontera de la Banca»… Mientras tanto, los bancos prosiguen en la consecución de sus nuevos objetivos de transformar sus plantillas, confirmando el cambio hacia los nuevos estilos de liderazgo anunciados, pero a cambio de conceder a las organizaciones una estructura plana y abierta, recíprocamente flexibles, y nuevas formas de contratación y trabajo: externalización, teletrabajo, nueva organización física del centro de trabajo…

La economía española

Por su parte, la economía general, en el caso español, mantiene la tónica expansiva, alejándose del negativo PIB registrado en 2013 (-1,7%) al esperanzador 3,1% de 2016 y al descenso controlado de una previsión de 2,5% en

2017 y 2,0% en 2018. En un confortable paralelismo, la creación de empleo, siempre según las estadísticas más formales, pasará en ese mismo periodo de tiempo (2013-2018) de un fatídico -233.000 afiliados a un +475.000 de 2016 y de un +635.000 entre 2017 y 2018.

Otro gran reto para los bancos será encontrar otros ingresos diferentes a los exiguos tipos de interés (por aplicarles un adjetivo muy optimista), que les permitan hacer frente a los cuantiosos presupuestos que se derivan de la implantación de los nuevos retos tecnológicos, porque la innovación no puede limitarse exclusivamente a un cambio en la gestión de personas, sino al compromiso de ganar en eficiencia y creación de valor. ¡Qué gran invento ese de las Fintech, un dominio que les permitirá a las empresas financieras utilizar la tecnología para crear y/o ofrecer servicios financieros más eficaces y menos costosos, con la invalorable colaboración de las startups!

En España, uno de los países con más avances en el uso de las nuevas tecnologías, los nuevos sistemas de pago ya permiten efectuar pagos con el móvil en más de 700.000 establecimientos, sin contar con que, por ejemplo, Inditex o el Corte Inglés han incorporado a sus terminales el pago de las compras de sus clientes desde el teléfono.

Las entidades financieras han percibido que una parte significativa de los clientes está cambiando (no hay más que preguntarles a los millenials), están demandando nuevos procedimientos de pago, nuevas relaciones con sus entidades financieras distinta a la mantenida con las sucursales tradicionales, sin que eso signifique ni mucho menos una tendencia a la desaparición de estas oficinas, que tenderán a la diversificación por especialidades.

Por si hubiera alguna duda sobre el futuro a medio plazo de nuestro país en el uso del rey de las comunicaciones y no tardando mucho de una parte de las operaciones bancarias, los smartphones, baste recordar que España es uno de los países en el podio de mayor número de estos dispositivos por habitante, lo que le ha conducido a un lugar de honor de los análisis que realizan las áreas de marketing y gabinetes de estudio de los bancos, así como a la puesta en marcha de plataformas que ofrecen la posibilidad de concentrar todas las cuentas en una única aplicación.

«La seguridad de las entidades financieras está involucrada en el mismo discreto pero imparable cambio que en el resto de otros muchos sectores»

¿Y la Seguridad?

La seguridad de las entidades financieras está involucrada en el mismo discreto pero imparable cambio que en el resto de muchos otros sectores, obligadas no sólo por sus propios cambios internos, sino sobre todo por los nuevos riesgos, los temibles riesgos tecnológicos, esos que han provocado, por ejemplo, un perjuicio en 2015 de 11.000 millones de dólares sólo en el fraude de datos y tarjetas de crédito, que algunas empresas usuarias achacan a la falta de tecnología, otros a la variedad de las amenazas y otros al elevado número de cajeros.

Sin embargo, el esfuerzo europeo por adelantarse a la previsible amenaza que se cernía sobre tarjetas, cajeros, terminales puntos de venta (TPV) y compras online, obtuvo sus frutos con la creación de las tarjetas con chip EMV, en parte contrarrestado por el incomprensible retraso de muchos países en la incorporación de este excelente medio de protección, por muy justificables que se estimaran los problemas económicos derivados de esta iniciativa.

Nuevos desarrollos espectaculares

Pero no sólo de tecnología EMV superviven las tarjetas de muchos países, lo último de lo último se está cocinando en algunos labs que han presentado en la segunda edición de la Ethereum Developer Conference (DEVCON2), celebrada en Malasia: el desarrollo de un sistema de identidad digital sobre blockchain, lo que vendría a asegurar du-

«Los ataques a empresas por sofisticadas estructuras de delincuentes ya empiezan a notarse»

rante un largo periodo de tiempo la identidad del titular de las operaciones.

Algunas de estas aplicaciones se están desarrollando sobre la base de uno de los pilares cada día más consolidados por las entidades financieras y que no es otra cosa que el conocimiento del cliente (Know Your Customer), principio de partida para un nuevo modelo de recepción y relaciones comerciales con los clientes, y de enorme y obligado interés para otras áreas como PBC.

Como es conocido, Blockchain (cadena de bloques) es el equivalente a la prueba de identidad en versión tecnológica, y representa un cuaderno de contabilidad que incluye el registro de todas las operaciones llevadas a cabo en el sistema en orden cronológico, garantizando la cohesión y coherencia del estado de cuentas de todos los usuarios. En el mundo financiero será una herramienta decisiva porque permite no sólo la difusión descentralizada, sino la gestión segura e inviolable de las transacciones financieras, lo que en primera y última instancia permite las muchas operaciones que las entidades financieras atienden en su calidad de intermediarias, así como los contratos inteligentes entre distintos sectores de la sociedad, incluyendo las máquinas. Esta es una tecnología todavía en desarrollo, pero cuya capacidad está llamada a soportar millones de transacciones prácticamente simultáneas.

Unas empresas muy singulares

Pero, entretanto, los ataques a empresas por sofisticadas estructuras de delincuentes ya empiezan a notarse. El término «estructura» no es gratuito porque incluso hay compañías con horarios laborales que tienen como objetivo hackear objetivos empresariales. No hace falta añadir que existen otros grupos a los que no les hace falta estar registrados en los órganos administrativos de sus países. Estos grupos son organizaciones mafiosas que harían palidecer a los más cualificados gánsteres italo-norteamericanos.

El diario «El País» publicaba a primeros del mes de octubre un excelente informe que bajo el título «La Era de la Inseguridad Cibernética», apuntaba que «el problema ya no está en saber si se producirá un ataque en la Red, sino cuándo y cómo». De su contenido, con-

fieso que una de las noticias que más me ha vuelto a inquietar (porque ya la conocía), es la referida a los hackeos de la cuenta de iCloud de Pippa Middleton, hermana de la Princesa de Gales, por la facilidad que supone tanto el acceso a la Nube como la divulgación de su contenido.

En el recorrido del informe, me detuve especialmente en los datos aportados por Miguel Rego, director del INCIBE, sobre el número de ataques que se sufren diariamente en España: «En España resolvimos unos 50.000 incidentes en 2015, y en 2016 tenemos previsión de superar…. ¡los 100.000!».

A los que trabajamos en las entidades financieras, Rego no nos sacó de dudas cuando describió el tipo de ataques más comunes, pero nos sacudió una vez más a golpe de cruda realidad: «Principalmente los intentos de estafa y fraudes electrónicos o por Internet. Suplantaciones de identidad, intento de robo de credenciales personales, (…) robos de cuentas de correo (...)». Y eso sin incluir los ataques de denegación de servicio, el back door Tyupkin, los black box, los botnets, Watering Hole, los macros como vector de ataque, los exploits y otra larga serie de malware que ha dejado a los skimmers casi en la prehistoria de los ataques a dispositivos de efectivo o a las empresas.

Paradójicamente, algunos pretenden combatir estos últimos ataques con medidas físicas (cámaras, detectores, sirenas, luces, alarmas…), que ya están instaladas en la abrumadora mayoría de los cajeros para impedir los accesos a las zonas de los medios informáticos que lo gestionan, sin percibir la reiterada dura realidad de la vía emprendida por los atacantes. Es evidente que la solución no viene sólo de la mano de la seguridad electrónica o física y que hace necesario insistir en el estudio de las vulnerabilidades tanto del software como del hardware, preferiblemente junto a los fabricantes, como ya se está realizando por muchas entidades.

> «Los delitos tecnológicos parecen dejar en una bruma los delitos que calificaríamos de "clásicos", atracos, robos, estafas documentales, falsificaciones, amenazas»

Los delitos «clásicos»

Los delitos tecnológicos parecen dejar en una bruma los delitos que calificaríamos de «clásicos», atracos, robos, estafas documentales, falsificaciones, amenazas. Aunque con un impacto económico muy inferior a los primeros, la repercusión que la mayoría de estos actos ilícitos tienen en las plantillas de las entidades nos recuerda que deben ser una prioridad en el establecimiento de las medidas de prevención. Si es importante el desarrollo de medidas destinadas a prevenir los ataques a las empresas consideradas como infraestructuras críticas, la protección de los empleados no debe bajar de la prioridad número uno.

En este sentido cabe aplaudir la sentencia dictada hace unas pocas semanas por un juzgado de Donostia contra tres atracadores, con condenas que suman treinta años de prisión.

Conclusión

Definitivamente, en un mundo tan complicado como el tecnológico, no sólo por su profundidad y diversidad, que requieren de un profundo conocimiento, sino por la multiplicidad de soluciones técnicas como es el caso de la autentificación mediante biometría, en la que cada cual defiende la supremacía de la suya (de voz, de huella, de iris…), se hace necesario un acuerdo de gran alcance entre Administración, usuarios y proveedores para desarrollar un I+D, ajustado a las vulnerabilidades derivadas de la ampliación a dimensiones desconocidas de la superficie de ataque del mundo digital: más tráfico en la red (casi 170 exabytes en 2019), más usuarios (4000 millones en 2019), más dispositivos conectados con IP (cerca de 25.000 millones en 2019) más conexiones de smartphones (6000 millones en 2019) y más datos (44 millones de zettabytes en 2020). Unos datos que simplemente nos colocan a todos en el disparadero. ●

Fotos: *Pixabay*

JOSÉ IGNACIO OLMOS CASADO. DIRECTOR DE SEGURIDAD, TÉCNICO DE FORMACIÓN Y EXPERTO EN PREVENCIÓN DE BLANQUEO DE CAPITALES

La **formación** del director de Seguridad

TODOS estamos de acuerdo a estas alturas en que la figura del director de Seguridad es clave como gestor de riesgos en el ámbito de una seguridad integral.

Aunque cada entidad puede ser un mundo en cuanto a organización y estructura, hay algunas cuestiones que sí pueden ser aceptadas de forma general derivado de lo que apuntábamos: el director de Seguridad es un profesional del ámbito directivo, que gestiona riesgos de forma multidisciplinar en un sector de actividad concreto.

Con estas premisas tenemos bastantes pistas para saber en qué materias debería formarse el director de Seguridad de las entidades de crédito.

La actual formación de los directores de Seguridad para su habilitación ha venido siendo la recogida en el Anexo III de la Orden INT 318/2011, de 1 de febrero, sobre personal de seguridad privada, en el mejor de los casos, cuando no un simple examen de habilitación. Es verdad que esta Orden Ministerial incluyó materias interesantes como gestión de equipos humanos o gestión de recursos materiales.

Por lo que se refiere a los cursos para la habilitación de los directores de Seguridad, actualmente son casi todas las universidades las que imparten dichos cursos, en muchos de los casos con una calidad notablemente mejorable. Uno puede habilitarse como director de Seguridad realizando un curso completamente on line en muy pocos meses y superando como prueba algunos test. Estos cursos se han convertido en un negocio puro y duro, y tanto empresas de seguridad como centros de formación independientes homologan los cursos con cualquier universidad (gran parte de las veces privadas), a las que les suele dar igual calidad y prestigio, ya que para ellas es un negocio muy cómodo facturar un buen porcentaje del precio de la matrícula del alumno tan solo por emitir un diploma. No deja de ser curioso el ínfimo número de alumnos que no superan los cursos… Cuando se vaya implantando el grado universitario que marca la Ley de Seguridad Privada de 2014 ya veremos cómo se enfoca y si esto cambia.

pressfoto/Freepik.com

Las materias objeto de estudio, como señalábamos, se encuentran recogidas en la Orden INT 318/2011, de 1 de febrero, sobre personal de seguridad privada. El devenir histórico de estos cursos de dirección de seguridad ha hecho que la calidad baje notablemente salvo contadas excepciones y que, en su mayor parte, hoy día se realicen primordialmente on line o, como mucho, de forma semipresencial. La duración prevista en la norma es de un mínimo de cuatrocientas horas. En la actualidad parece que ningún curso sigue lo apuntado en el artículo 6 de la Orden: «… pudiendo complementarse

safire

3.0

HD OVER COAX

- Grabadores 5n1
- Ultra HD 4Mpx
- H.264/H.264+
- Mayor distancia de transmisión

HD TVI HD CVI IP CVBS AHD

Distribuidores oficiales:

www.jmsystems.es

www.avantech.info

www.visiotech.es

SAFIRE
www.safirecctv.com
info@safirecctv.com

con otras relacionadas con las funciones y habilidades directivas y la seguridad en general»; lejos quedan ya los tiempos en que algunos de los cursos, los primeros (que también eran los de mayor calidad), impartían otras asignaturas relacionadas con el mundo de la empresa y muy necesarias, a nuestro juicio, para una adecuada gestión de un departamento de Seguridad, tales como recursos humanos, contabilidad de costes y otras.

¿Y qué decir de las acreditaciones de los docentes de los cursos de dirección de seguridad?. Pues no mucho, ya que no existe regulación específica, al ocuparse la ley únicamente de los centros de formación en los que se pretendan impartir enseñanzas de formación y actualización de personal de seguridad privada, que son los que se autorizan por Secretaría de Estado, puesto que para los cursos de dirección de seguridad lo que se autoriza es el propio curso y no el centro que lo imparte, aunque en todo caso se debe contar en tal curso con el respaldo de un centro universitario.

Con todo, los veinte módulos impuestos por la normativa son aceptables como una formación básica. Entre ellos se incluye, por cierto, uno sobre seguridad en entidades de crédito, es de suponer que motivado porque, inicialmente, era el único sector obligado por normativa a disponer de departamento de Seguridad. Este módulo, muy centrado en la normativa, obviamente no es suficiente para colmar las necesidades que comentábamos antes. Hablando en general de la formación de los directores de Seguridad, no sólo los del ámbito que nos ocupa, es imprescindible una especialización, la cual por cierto sí es obligatoria para el personal operativo en catorce tipos de servicios diferentes. En este sentido sí han existido algunas iniciativas concretas (hospitales, centros comerciales…) sin mucho éxito.

> «Todos estamos de acuerdo en que la figura del director de Seguridad es clave como gestor de riesgos en el ámbito de una seguridad integral»

javi_indy/Freepik.com

Sin querer extendernos más, y en base a lo que apuntábamos al inicio del artículo, la formación del director de Seguridad, además de esos veinte módulos iniciales, debería incluir al menos:

- Formación de nivel directivo y relacionada con gestión de departamentos empresariales: liderazgo, negociación, selección de recursos humanos…
- Formación específica relacionada con la actividad de las entidades de crédito y el sector financiero.
- Formación más extensa en gestión de riesgos y aseguramiento.
- Formación en mayor profundidad en el área de la autoprotección y emergencias.
- Normas sobre calidad y certificadoras (ISO, UNE).
- Formación en materias conexas como la prevención de blanqueo de capitales, fraude, cumplimiento normativo, etc.
- Formación en ciberseguridad, (clave de futuro inmediato si no de presente) imprescindible absolutamente en este sector.

Seguramente, algunas otras materias también podrían tener cabida en esta formación, como pudiera ser el ámbito de los eventos o el Patrimonio Histórico Artístico para entidades que disponen de fundaciones o realizan actividades culturales, exposiciones, etc.

En este punto estamos expectantes de lo que pudiera aportar el Grado en Seguridad previsto en la Ley de 2014, aunque, seguro que después seguiría existiendo necesidad de formación específica en nuestro ámbito. ●

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

ROCÍO CANO. KEY ACCOUNT MANAGER. HIKVISION

Seguridad en el sector bancario

LA banca ha sido uno de los sectores dentro de la seguridad que más ha evolucionado. No es de extrañar, ya que su propio modelo de negocio ha cambiado drásticamente. Las oficinas bancarias han cambiado su diseño y arquitectura con el objetivo principal de mejorar su accesibilidad al ciudadano y generar confianza en un ambiente de cercanía.

En este sentido, esta nueva arquitectura ha hecho que los elementos de vídeo que se estén instalando sigan la misma línea, no sólo teniendo como objetivo asegurar los bienes personales y materiales, sino también siendo lo más discretos posibles para conseguir la ansiada imagen de confianza.

Antes de entrar en detalle sobre las problemáticas fundamentales, me gustaría hacer un comentario sobre la migración de tecnología.

Hace no tanto tiempo, la tecnología que se utilizaba era analógica. Dadas las limitaciones en cuanto a resolución, WDR y flexibilidad que conlleva trabajar en analógico, los sistemas comenzaron a migrar a la tecnología IP, la cual nos permitiría solucionar aquellos problemas que otras tecnologías no eran capaces de resolver.

Pero ¿qué ocurría en aquellas instalaciones donde el cambio de cableado era realmente un problema tanto económico como de estructura? ¿Debíamos estar encadenados a la resolución analógica?

Aquí es donde ha irrumpido de manera importante la tecnología HD-TVI. Esta tecnología permitía transmitir calidad HD sobre coaxial y que, ahora con su nueva versión 3.0, nos permite trabajar con resoluciones de hasta 5 Mpx. Esto obviamente supone un incremento muy notable en la calidad de las instalaciones, pero ¿es suficiente?

Lo es, aunque se debe tener en cuenta que la flexibilidad que da una arquitectura IP no la tendremos con un sistema analógico.

Dicho esto, y considerando que la tecnología IP es la más adecuada, entremos a valorar los riesgos más comunes en este sector:

1. Fuerte nivel de contraluces en las cámaras de entrada.
2. Tamaño reducido y alto WDR en cámaras de cajero.
3. Visionado general sin dañar estética.
4. Sistema operativo Linux.

Para el primer caso, se aconseja cámaras con una tecnología similar a Lightfighter. Esto significa no sólo que la cámara tenga un WDR muy alto (+ 120 dB) sino que trabaje con triple exposición, de manera que entrelace la alta, baja y media exposición, obteniendo así una imagen más clara, tanto en las zonas oscuras como suavizando las zonas muy claras.

Cajeros. En este tipo de instalación, es prioritaria la dimensión de la lente, debiendo escoger un modelo reducido como el modelo Pinhole, con alto WDR de nuevo como en el caso anterior ya que el nivel de contraluces es extremo. Además deberá contar con funciones de vídeo análisis. Esta tecnología garantizaría que la cámara se active solo cuando detecte una persona. Este punto es muy importante para cumplir la LOPD.

Visionado General. No hace mucho tiempo, para tener una imagen general de la oficina, se utilizaban varios elementos de vídeo para poder cubrir la escena global.

Con el objetivo de cumplir uno de los requerimientos de estética comentados al principio del artículo y cubrir el área de interés, se tiende a utilizar las cámaras 360º, las cuales nos permiten tener un visionado general y diferentes sub PTZ virtuales del mismo stream, consiguiendo obtener una panorámica y su correspondiente nivel de detalle en aquellas escenas que interesen.

Algo que también es una ventaja, es que estas cámaras dispongan de IR y audio, garantizando así la opción de grabar audio y de un visionado nocturno sin necesidad de un apoyo de luz externo.

Hemos comentado los principales riesgos pero no me gustaría acabar sin hacer mención a la importancia del grabador.

El grabador tiene que estar preparado para trabajar con unos anchos de banda muy limitados y sobre todo que tenga un sistema operativo lo más seguro posible. Por ello se recomienda que se trabaje con Linux, bastante más robusto que otros sistemas más domésticos.

Confiamos en que haya sido de su interés nuestra visión del mercado, aunque es altamente probable que en poco tiempo podamos ofrecerles importantes novedades, ya que como proveedores de soluciones estamos en continua evolución. ●

Fotos: Hikvision/Pixabay

Contactos de empresas, p. 8.

RAMÓN RAMOS. JEFE DE VENTAS NACIONAL. FERRIMAX

Últimas tendencias en **cámaras acorazadas**

Compartimentos con apertura biométrica y control a distancia

CÁMARAS acorazadas existen desde hace siglos, cámaras que en algunos casos podían llegar a tener una capacidad de resistencia a la efracción incluso superior a alguna de las actuales, pero que, en la mayoría de ocasiones, era evidente que no ofrecían una mínima garantía de resistencia ante un ataque.

Es a partir de la Orden Ministerial de 23 de abril de 1997 donde se concretan determinados aspectos en materia de seguridad. Y concretamente en el artículo octavo del Capítulo II, donde se especifican las medidas de seguridad que debían tener las cámaras acorazadas de efectivo en entidades de crédito. Aquí se indicaban por primera vez el nivel de resistencia mínimo que debían tener los muros de las cámaras acorazadas, el de la puerta y el del trampón de seguridad (nivel C en las obsoletas normas UNE 108-111-87 y 108-113-87, que pronto se verían sustituidas por la actual norma europea UNE EN 1143-1). También indicaba la anchura máxima del pasillo de ronda, 60 centímetros, sin especificar el nivel de seguridad de las paredes exteriores del muro que delimita dicho pasillo de ronda.

No sería hasta la publicación de la Orden Ministerial 3171/2011, de 1 de febrero, sobre medidas de seguridad privada, cuando se complementaron esas características y donde se detalló, de forma obligatoria, también en el artículo octavo del Capítulo II, las medidas de seguridad específicas que deben tener las cámaras acorazadas:

– Habrán de estar delimitadas por una construcción de muros acorazados en paredes, techo y suelo; con acceso a su interior a través de la puerta y trampón, si lo hubiera, ambos acorazados. Deberán estar construidos de forma que, como mínimo, su grado de seguridad sea VII, según la norma UNE-EN 1143-1.

– El muro estará rodeado en todo su perímetro lateral por un pasillo de ronda con una anchura máxima de 60 centímetros, delimitado por un muro exterior con grado de seguridad II, también según la norma UNE-EN 1143-1

– Las puertas de las cámaras acorazadas contarán con un dispositivo de bloqueo y sistema de apertura retardada de, como mínimo, diez minutos. Quedan exceptuadas del sistema de apertura retardada aquellas que contengan compartimentos de alquiler.

Ambas Órdenes Ministeriales hacían referencia en sus artículos décimos del mismo Capítulo II, al nivel de seguridad que debían ostentar las cajas o compartimentos de alquiler que debían estar instalados en las cámaras de seguridad: Nivel A (en el caso de la Orden más reciente, según la Norma UNE 108115).

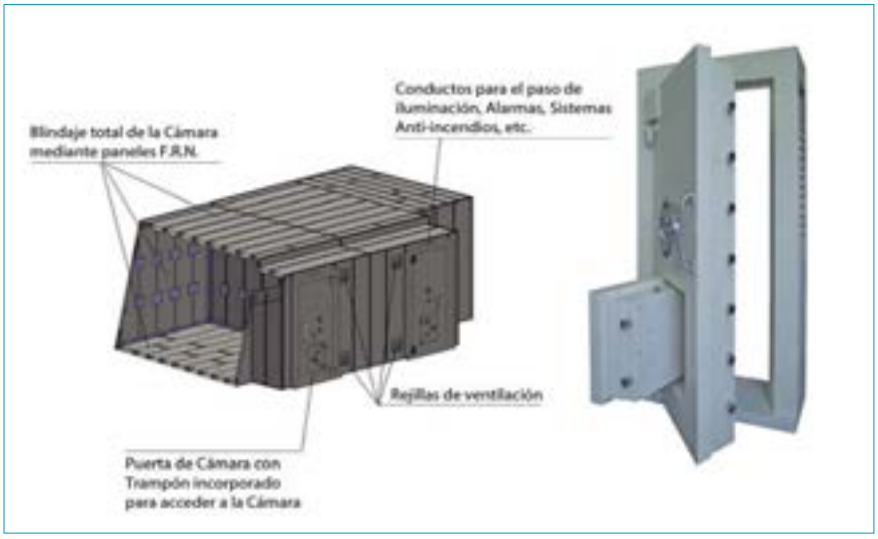
Pero aún más importante que esta información complementaria de obligado cumplimento, una de las novedades que supuso la Orden Ministerial 3171 de 2011, fue la Disposición Adicional sexta: Acreditación de elementos de seguridad física y electrónica, en la que se exigía a partir de la publicación de la orden, que «todos los elementos de seguridad física y electrónica, […], deberán contar con la evaluación y requisitos constructivos reglamentarios, que únicamente podrán ser garantizados mediante un certificado emitido por un Organismo de Control acreditado para tal fin.

Esta evaluación de la conformidad de los productos se llevará a cabo por Organismos de Control acreditados por la Entidad Nacional de Acreditación (ENAC), sobre la base de la Norma UNE-EN 45011.»

Así, las cámaras acorazadas y los pasillos de ronda construidos mediante paneles prefabricados, no sólo deben tener un nivel de seguridad mínimo, sino que hay que acreditarlo mediante el certificado del producto correspondiente. Del mismo modo, las cámaras y pasillos fabricados «in situ» con hormigón, también deben certificarse siguiendo un procedimiento preestablecido y documentado, utilizando hormigones y materiales también certificados.

Por último, en la Disposición transitoria única de la Orden Ministerial de 2011 se indica que «Los elementos de seguridad física y electrónica y los sistemas de alarma, instalados antes de la fecha de la entrada en vigor de la presente Orden, en establecimientos obligados y no obligados, se adecuarán a la misma en el plazo de 10 años. Los establecimientos a que hace referencia la Disposición adicional primera de esta Orden, dispondrán de un plazo de dos años para que cumplan lo previsto en ella, respecto a su conexión a central de alarmas y disponer de sistema de registro de imágenes.[…] Transcurrido el periodo de carencia de diez años establecido en el primer párrafo de esta Disposición, se deberá disponer del pertinente certificado emitido por un laboratorio acreditado para ello en la Unión Europea y exhibirse en caso de ser requerido.»

Últimamente se está viviendo un auge en la fabricación de las cámaras acorazadas con compartimentos de alquiler. De todos es conocido que los tipos de intereses tan bajos que estamos viviendo desde hace años, incluso negativos desde hace meses, está trasladando parte de los ahorros que los clientes de banca mantenían en depósitos, fondos de inversión, planes de ahorro, etc., a su custodia en efectivo. El incremento en las ventas de cajas fuertes en la Europa central y Japón no oculta un problema de seguridad adicional, y que también va en aumento desde hace años: Los robos con violencia en viviendas particulares. Sin embargo, el uso de los compartimentos de alquiler solventa la intranquilidad que pueda generar guardar dinero en efectivo en el domicilio en caso de atraco.



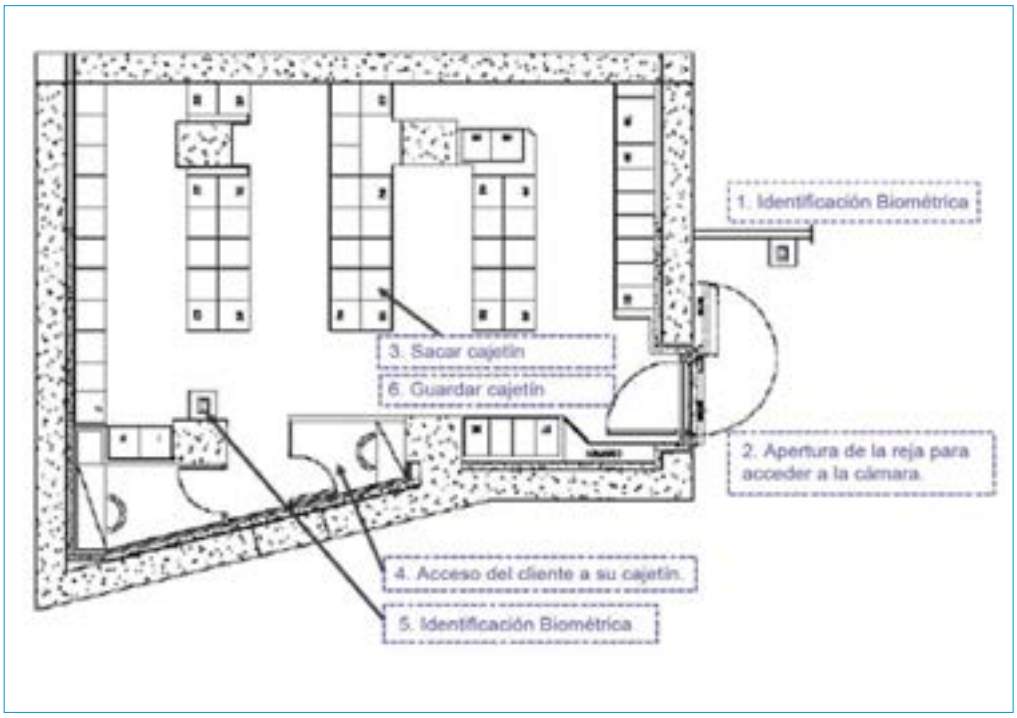
A partir de ahí, cada Entidad desarrolla nuevas estrategias para la construcción o adaptación de cámaras acorazadas y conseguir mayor control, menores costes de mantenimiento y más autonomía para el cliente. Todo esto se consigue con los compartimentos de apertura biométrica a distancia.

La apertura biométrica, aplicada a los compartimentos bancarios, hace posible la apertura remota del compartimento, lo que facilita al cliente un acceso más confidencial a sus efectos personales en la cámara acorazada.

El cliente sigue necesitando la llave de su compartimento para abrirlo, pero el acceso a la cámara acorazada y el desbloqueo del compartimento está controlado por el sistema de control de accesos.

Una sencilla modificación de los compartimentos permite monitorizarlos y controlar su apertura de forma sencilla y segura.

Todos los cajetines tienen una cerradura electromecánica conectada al servidor, lo que permite al banco no tener llave de control, facilitando también un



ne de una consola interactiva para controlar el acceso de los clientes a la cámara acorazada y su identificación con sistema biométrico. Una vez que el cliente efectúa su gestión, ha de volver a identificarse con una consola secundaria que se sitúa en el interior. El sistema de apertura biométrica y control a distancia, además realiza auditorías de apertura de los compartimentos, puede conectarse al sistema de alarmas para la detección de compartimentos abiertos durante un tiempo excesivo, y controla los cajetines a través de un bus de comunicaciones conectado a la consola central. Por supuesto, los compartimentos disponen de los mismos elementos de seguridad que hasta ahora, con la cerradura de llave prisionera para evitar la extracción de la llave con la puerta abierta. En caso de emergencia o fallo del sistema, los compartimentos mantienen igualmente la posibilidad de apertura sin necesidad de conexión al sistema de control.

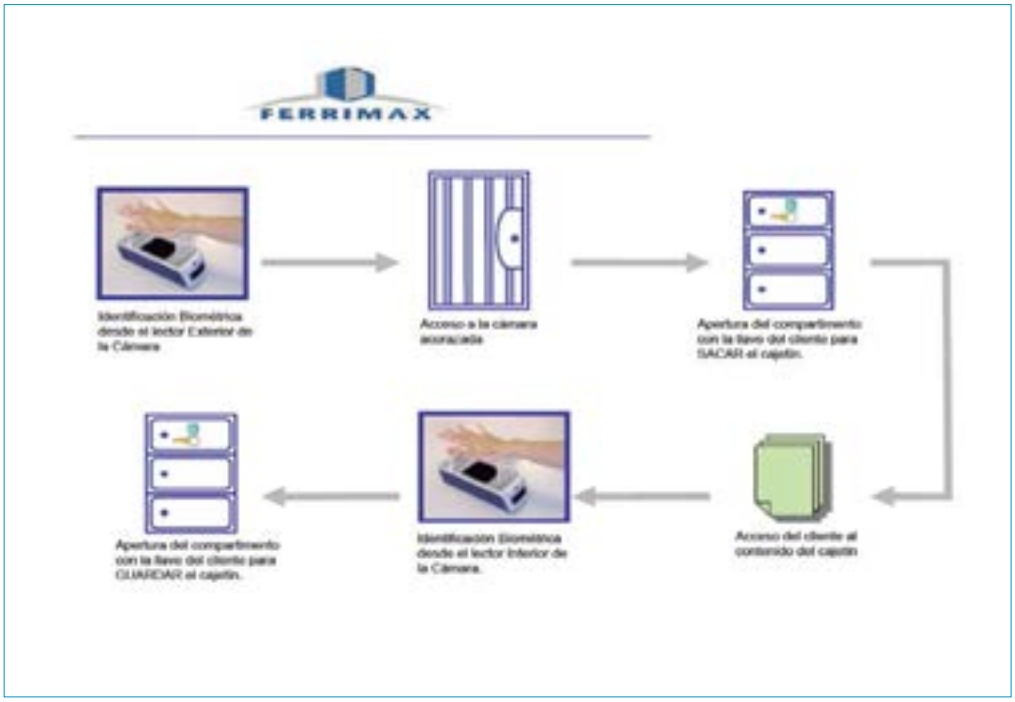
La identificación biométrica no sólo aumenta la seguridad por los aspectos señalados en el párrafo anterior. Además, la incrementa exponencialmente con los nuevos sistemas de reconocimiento de personas. Las

acceso más fácil y rápido al compartimento por parte del cliente.

¿Qué conseguimos? Una reducción de costes directa, ya que evita el personal de seguridad que hasta ahora acompañaba al cliente hasta su compartimento tradicional para poder abrirlo con las 2 llaves: la del cliente y la de control.

«La apertura biométrica, aplicada a compartimentos bancarios, hace posible la apertura remota del compartimento»

También se obtiene un aumento de la seguridad, ya que el sistema dispo-



nuevas tecnologías han desarrollado sistemas de reconocimiento que hacen prácticamente imposible su sabotaje. A los clásicos lectores de huellas dactilares y de reconocimiento facial u ocular, se añaden ahora lectores sin contacto que capturan una imagen del tramado de las venas de la palma de la mano a través de rayos infrarrojos. Un patrón de las venas que es único por cada individuo, diferente en la mano izquierda y la derecha, y que no cambia con el crecimiento.

Sólo falta añadir las múltiples posibilidades que otorga este sistema. La parametrización de las aperturas permite que un mismo compartimento pueda abrirse por varios usuarios, identificando a la persona que accede al compartimento, dando permisos individuales o mancomunados, etc. Es más, se pueden establecer horarios de acceso personalizados para que algunos usuarios puedan acceder a la cámara dentro del horario que se determine.

Un ejemplo de aplicación de esta parametrización podría ser el uso de un compartimento de seguridad por parte de una Notaría. El notario (o los notarios), tendrían privilegios máximos, con acceso individualizado y a cualquier hora, pero los oficiales, sólo tendrían acceso al compartimento en caso de identificación conjunta. Por ejemplo, los oficiales que trabajan por la tarde, no tendrían acceso por la mañana y a la inversa.

Otro caso típico sería el de una familia estándar. Se podrían parametrizar el acceso a la cámara acorazada de la misma forma que la disponibilidad de sus cuentas abiertas en esa entidad, con acceso a los compartimentos de forma independiente por parte de los padres, y de forma mancomunada en caso de acceso por parte de los hijos (titulares y autorizados).

Como se ha podido comprobar, la seguridad en una cámara acorazada ya no sólo depende de la resistencia física de sus paredes a las que obliga la normativa expuesta al inicio de este artículo. Esa seguridad se puede complementar mediante el uso de compartimentos de apertura biométrica y control a distancia. ●

Contactos de empresas, p. 8.

Fotos: Ferrimax

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

Las entidades bancarias requieren **sistemas de seguridad infalibles**

EL sector bancario se encuentra en una constante búsqueda de las soluciones más innovadoras en cuanto a su seguridad. Debido al inmenso riesgo que asumen, se les exige unas medidas, de cumplimiento obligatorio, capaces de prevenir cualquier suceso y de solventar aquellas situaciones que puedan perjudicar la estabilidad del negocio.

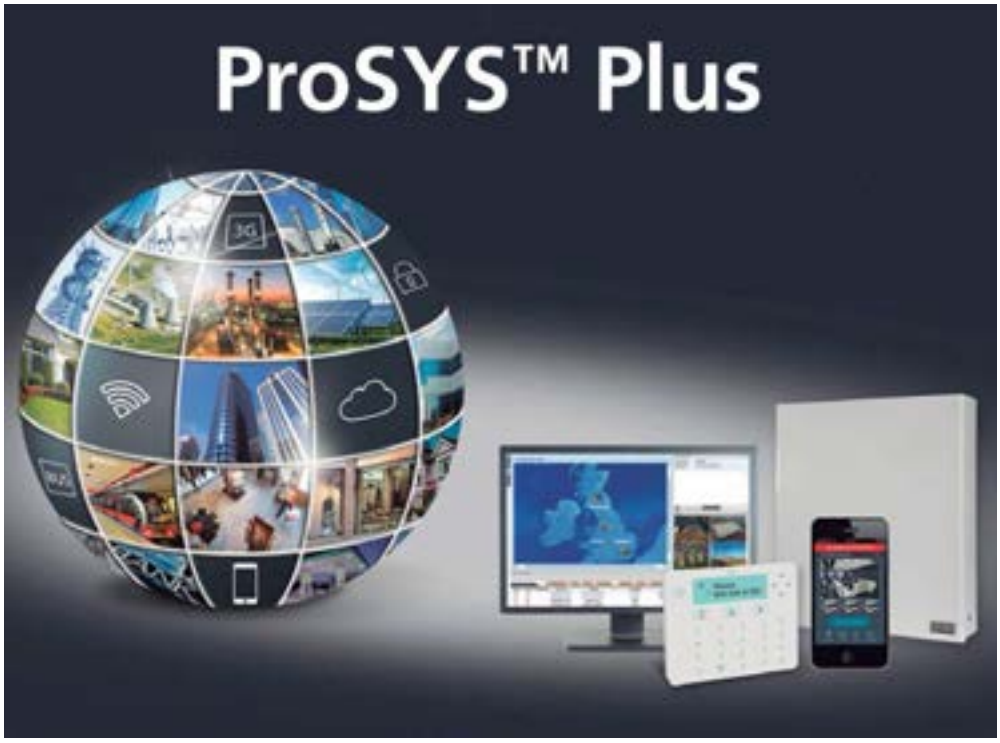
Para ello, en primer lugar, hay que recalcar la necesidad de trabajar con sistemas específicos, herramientas creadas expresamente para garantizar la seguridad en el entorno financiero.

La instalación de sistemas estándar, aunque resulten eficaces en otras áreas o negocios, no es suficiente para los requisitos que demandan estas instituciones. Es así, ya que estos espacios precisan equipos exclusivos y especializados en seguridad integrada de Grado 3.

Lo ideal es una solución flexible en cuanto a número de zonas/particiones, que esté diseñada para su uso por integradores de sistemas, e instalada por empresas especializadas en seguridad con un gran número de zonas y que disponga de vídeo verificación con cámaras IP integradas.

Estabilidad y fiabilidad en los sistemas

Es importante instalar detectores inteligentes que perciban intentos de camuflaje por parte del intruso (Anti-Cloak), que perciban si el detector está siendo manipulado (Anti-enmascaramiento) incluso con el detector desarmado, y que ofrezcan un alto nivel de rendimiento, hasta en espacios con altas temperaturas ambientales, detectores con la tecnología microondas, permitiendo reducir la penetración de las microondas a través de las paredes, y desactivándose cuando el sistema está desactivado para eliminar las emisiones de radiación excedentes según las directrices medioambientales



Asimismo, es aconsejable el uso de dispositivos sísmicos que controlen la vibración y la temperatura de la superficie protegida, con entrada de reducción remota de sensibilidad, y que permita su

El acceso inteligente

El socio de confianza que aporta soluciones de acceso innovadoras y seguras en todo el mundo

Le ofrecemos un servicio completo que incluye desde el asesoramiento en su proyecto hasta la implementación y el correspondiente servicio posventa.

dorma+kaba
María Tubau 4
28050 Madrid
España

T: +34 91 736 21 10

www.dormakaba.com

dormakaba

funcionamiento tanto en espacios de máxima seguridad como en cajeros automáticos.

Por otra parte, resulta indispensable tener un sistema de seguridad completo de alarmas y cámaras, que el mecanismo de videovigilancia y de control de accesos esté conectado a una única interfaz de usuario.

Por todo lo señalado, es conveniente que los directores de Seguridad acudan a compañías expertas en proporcionar tecnologías innovadoras de prevención y que cuenten con dispositivos que incrementen significativamente la capacidad de detección, a la vez que disminuyan la incidencia de falsas alarmas.

Sirve de gran ayuda que el sistema elegido puede integrarse con otros sistemas de CCTV, automatización y de gestión remota de edificios, ya que se podría hacer una gestión remotamente.

Del mismo modo, se recomienda que el responsable pueda tener el control del establecimiento de manera remota. Para ello, existen sistemas de control vía App que ayudan a gestionar y controlar la actividad de la entidad, permitiendo, incluso, visualizar en tiempo real, lo que ocurre en el interior del mismo.

Evidentemente gracias a la tecnología/instalación en bus se puede configurar y diagnosticar remotamente en los detectores de la instalación, de esta manera se ahorra mucho tiempo y costes.

En definitiva, es necesaria la adopción de sistemas de videovigilancia determinados para estas entidades. Asesorarse por productores que tengan experiencia en la implantación de sistemas idóneos para estos entornos y que respondan a las firmes exigencias del sector.

En este caso, podemos destacar nuestra experiencia en las entidades bancarias, la implantación de detectores de Grado 3 en entidades bancarias de nuestro país, así como en China, donde se instalaron miles de sistemas de seguridad con un éxito excepcional. Siguiendo el protocolo y las normas establecidas se procedió a la instalación de equipos de última tecnología que daban respuesta a las demandas del sector financiero chino.

> «El sector bancario se encuentra en constante búsqueda de las soluciones más innovadoras en cuanto a seguridad»

Disponer de estos sistemas es primordial cuando se trata de un sector donde la confianza y la seguridad de los bienes y de las personas es tan importante. Es necesario prestar atención a cada detalle, pues el más mínimo descuido puede ocasionar unos daños y repercusión difíciles de recuperar. ●

Fotos: Risco Group

Contactos de empresas, p. 8.

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.

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

La importancia de la compresión **en los sistemas de videovigilancia**

La videovigilancia ha sido utilizada durante muchos años por los bancos para ayudar a detectar, monitorear y registrar pruebas de actividades delictivas como el vandalismo, agresión dirigida a personal, dispositivos para clonar tarjetas y robo a mano armada, así como para controlar de forma remota los locales fuera de las horas de oficina.

La relativamente reciente disponibilidad de cámaras Full HD y 4K están transformando la forma en que los directores de Seguridad son capaces de hacer frente a estos problemas, pero también tiene coste. Esto se debe a que cantidad de píxeles de las imágenes de alta definición llenan con demasiada rapidez la capacidad de almacenamiento de un NVR o servidor, cuando se graban imágenes a plena resolución y a una velocidad de fotograma de 25 ips.

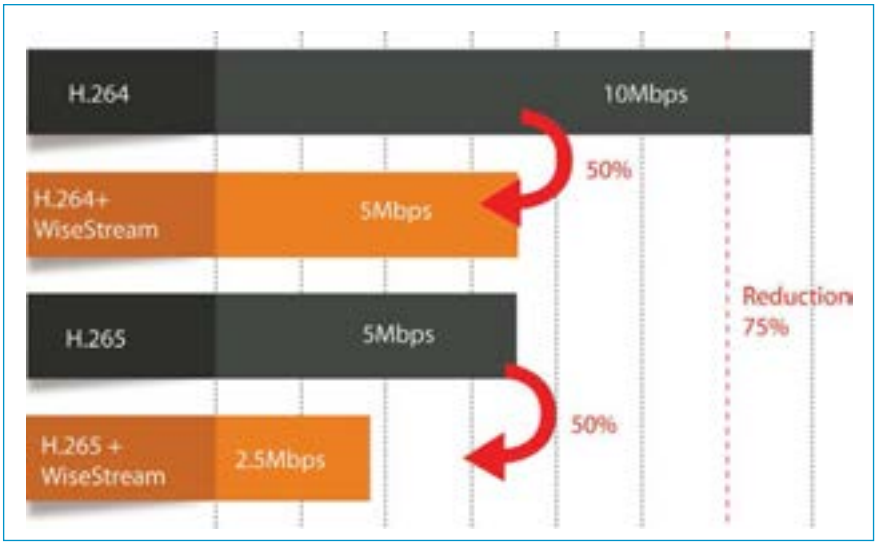
La necesidad es la madre de la creación

Es muy probable que dentro de un año, los que trabajamos en soluciones de videovigilancia echemos la vista atrás para preguntarnos cómo hemos podido sobrevivir sin esta tecnología. La compresión H.265 ya está aquí y no podía haber llegado en mejor momento.

Se dice que «la necesidad es la madre de la creación» y este ha sido el caso con la compresión H.265 y los beneficios que aporta a los sistemas de videovigilancia con cámaras Full HD y 4K. Lo mismo se puede decir de las tecnologías complementarias de compresión que están emergiendo, que al controlar de forma dinámica la codificación, la calidad de los balances y la compresión de acuerdo al movimiento en la imagen y trabajar de forma conjunta con la compresión H.265, reduce el uso del ancho de banda en hasta un 75 % en comparación con la actual tecnología H.264.

¿Por qué es necesaria una compresión más eficiente?

La última generación de cámaras Full HD y 4K puede resultar una solución costosa 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 ocupar demasiado rápido el espacio de almacenamiento disponible en un NVR o servidor cuando



se graban a una resolución e imágenes por segundo completas.

Los usuarios finales no paran de cuestionar el coste total de poseer un sistema de videovigilancia; un coste que puede incrementar considerablemente si la instalación cuenta con un gran número de cámaras de alta definición. Además de la inversión económica necesaria para los NVR y servidores de almacenamiento, los costes recurrentes del consumo energético de los discos duros, las unidades ventilación de apoyo y el mantenimiento continuo pueden ser importantes. Asimismo, a las empresas con políticas respetuosas con el medioambiente les preocupa el impacto medioambiental y la sostenibilidad de los sistemas que consumen grandes cantidades de energía.

Al reducir los requisitos de almacenamiento de vídeo con la ayuda de la compresión H.265 y otras tecnologías complementarias de compresión, 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.

En este sentido nosotros, que no somos el único fabricante con cámaras Full HD y 4K con compresión H.265, vamos un paso por delante en relación a las tecnologías complementarias de compresión, lo que permite conseguir importantes ventajas desde un punto de vista técnico.

H.265: ¿Qué es y cómo funciona?

El Grupo de Expertos en Imágenes en Movimiento (MPEG) y el Grupo de Expertos en Codificación de Vídeo (VCEG) definieron el estándar H.265, también conocido como Codificación de Vídeo de Alta Eficiencia (HEVC). Es

compatible con resoluciones de hasta 8192 x 4320. Esto es posible gracias a que duplica la tasa de compresión de datos en comparación con la compresión H.264, mientras que sigue ofreciendo la misma calidad de vídeo o consigue mejorar notablemente la calidad de vídeo a la misma velocidad de bits. Esto se traduce, básicamente, en una mayor eficiencia, pues los vídeos se graban, almacenan y transmiten con la misma calidad aunque consumiendo menos ancho de banda o manteniendo su consumo para obtener una calidad aún mayor.

La compresión H.265 es parecida a la H.264 en la medida en que compara distintos fragmentos de un fotograma de vídeo para encontrar áreas redundantes, tanto en un único fotograma como en los subsiguientes. Después se sustituyen estas áreas redundantes con una descripción breve y no con los píxeles originales. Los principales beneficios de la compresión H.265 en comparación con la H.264 son que se amplían las áreas de comparación de patrones y de distinta codificación: de 16 x 16 píxeles hasta 64 x 64. También mejora la segmentación variable-bloque-tamaño, la intra-predicción dentro de una misma imagen y la predicción del vector de movimiento. El uso efectivo de estas mejoras significa que la compresión de vídeo cuenta con una mayor capacidad de procesamiento de la señal y un menor impacto en los cálculos necesarios para la descompresión.

> «La videovigilancia ha sido utilizada durante muchos años por los bancos para ayudar a detectar, monitorear y registrar pruebas de actividades delictivas»

Puede que la compresión H.265 sea una tecnología emergente para el sector de la videovigilancia, pero en el sector de los medios audiovisuales es un estándar establecido. El sector de la videovigilancia siempre ha sabido aprender de los principales medios audiovisuales para hacer propias las mejores prácticas de estos, tal y como ocurrió

cuando se pasó de MPEG a H.264. Así que es totalmente natural que aprovechemos los últimos avances tecnológicos en beneficio de nuestros clientes.

Apoyo a la transición

Con el fin de ayudar a los usuarios finales en su transición a las tecnologías H.265, la última generación de cámaras Wisenet emplea un triple códec que permite reproducir simultáneamente en tres formatos: H.265, H.264 y MJPEG. Así, es posible grabar vídeos y visualizar sus contenidos en distintos formatos. También facilita la integración con sistemas de terceros que todavía no son compatibles con la compresión H.265, lo que permite que los usuarios instalen las mejores cámaras del mercado y migren a la compresión H.265 cuando se ofrezca compatibilidad con su VMS.

Tecnología de compresión complementaria de GOV dinámico

Tal y como ya he comentado, las tecnologías complementarias de compresión, controlan de forma dinámica la codificación, la calidad de los balances y la compresión de acuerdo al movimiento en la imagen. Tal vez sea interesante identificar y describir algunos de los factores y términos principales implicados.

GOV

Un GOV (Grupo de Vídeo) está formado por una I-frame con datos de vídeo completos y múltiples P-frames, con datos de vídeo modificados. El GOV dinámico es una tecnología que controla la longitud del GOV.

Si el GOV se alarga reduciendo la I-frame, se reduce también el ancho de banda, pero la calidad de vídeo será deficiente si contiene mucho movimiento. La configuración óptima es un GOV largo cuando hay poco movimiento y un GOV corto cuando hay mucho.

La tecnología de GOV dinámico calcula los movimientos o complejidad del vídeo para controlar después los intervalos entre I-frames.

- Menos movimiento / mayor complejidad, supone una reducción del consumo de ancho de banda al incrementar el intervalo I-frame.
- Más movimiento / menor complejidad, inserta más I-frames para mantener la integridad de la calidad de vídeo.

Región de interés (ROI)

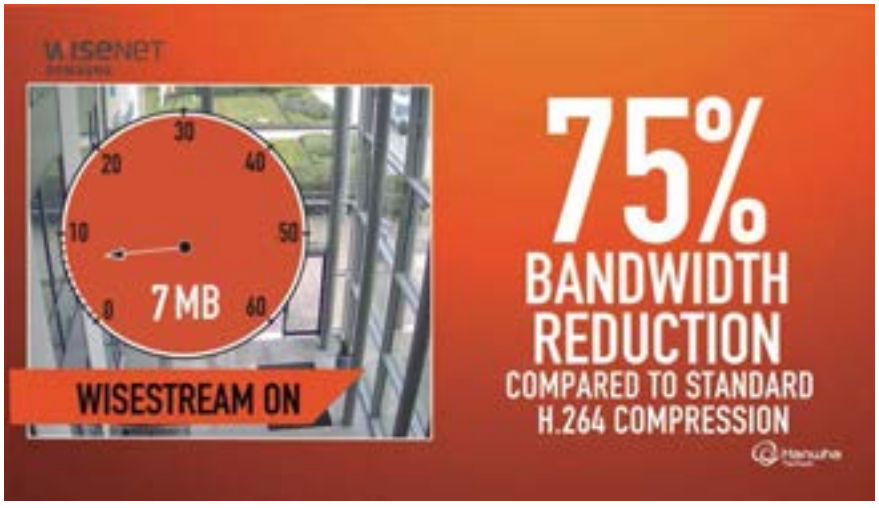
En vídeo, a los usuarios normalmente les interesa visualizar zonas estáticas que contengan poco movimiento y zonas dinámicas con mucho movimiento. La tecnología ROI analiza las zonas estáticas y dinámicas de un vídeo basándose en una analítica avanzada de vídeo. Después aplica distintas tasas de compresión en cada área para reducir la calidad de vídeo y el ancho de banda.

Control predictivo de la velocidad de bits

Los códecs H.264 y H.265 predicen y calculan la complejidad de una escena para su compresión, aunque por lo general se suele producir una mayor velocidad de bits cuando el códec realiza los cálculos por sí mismo. La tecnología de control predictivo de la velocidad de bits cuenta con una lógica de cálculo previo que predice la complejidad antes de realizar la compresión H.264 o H.265. Controla la velocidad de bits al predecir la escena (parámetro de cuantificación) y, como resultado, evita que la velocidad de bits incremente de forma innecesaria y optimiza el flujo de datos.

La oportunidad

La masiva capacidad de procesamiento de los chipsets DSP integrados en la última generación de cámaras de alta definición ofrece oportunidades para que los bancos y entidades financieras disfruten de un mayor valor añadido en sus sistemas de videovigilancia. Es una situación en la que todas las partes salen ganando y, sobre todo, los fabricantes de cámaras y dispositivos de grabación que han comprendido la necesidad de incorporar las técnicas de compresión más recientes a sus productos y que, al hacerlo, permiten que los bancos obtengan el máximo retorno de sus inversiones en soluciones de videovigilancia. ●



Fotos: Hanwha Techwin Europe

Contactos de empresas, p. 8.

¿NECESITA MÁS ESPACIO?

Nuestra tecnología WiseStream comprime sus datos en un 75 %

WiseStream

Hanwha Techwin presenta WiseStream, una tecnología complementaria de compresión que controla de forma dinámica la codificación, la calidad de los balances y la compresión de acuerdo al movimiento en la imagen.

En combinación con la compresión H.265, la eficiencia del ancho de banda puede mejorarse en hasta un 75 % en comparación con la tecnología H.264.

WiseStream está disponible en las cámaras de la nueva gama Wisenet Q y P, y todas las gamas H.265 futuras.

WISENET. WISESTREAM. WISE CHOICE.

hanwha-security.eu

Hanwha Techwin

GMV

BBVA, avanzado sistema de gestión global de la seguridad

¿Te imaginas poder gestionar toda la información de Seguridad de tu negocio desde una única aplicación?

A qué director de Seguridad no le gustaría conocer en tiempo real todos los incidentes que suceden en cualquiera de sus oficinas o sedes a nivel mundial, qué relación hay entre ellos y qué acciones debe realizar para evitar acciones similares en el futuro. Para el BBVA ya es una realidad, gracias a la implantación de la plataforma Faro Security es capaz de asegurar una gestión óptima de todos los aspectos relacionados con la seguridad física de su organización.

BBVA es capaz de monitorizar todos los incidentes de seguridad que suceden en sus oficinas y sedes corporativas del grupo a nivel mundial, obteniendo una visión global del estado de la seguridad de todo su negocio. Gracias al análisis de estos aspectos en tiempo real, el grupo financiero dispone de una gran ventaja a la hora de tomar decisiones futuras.

Inés Díaz Ochagavia, directora de Producción de Seguridad Corporativa de BBVA, destaca los beneficios que la visión global de la herramienta aporta a la organización: «Nuestros procesos son más ágiles y homogéneos, hemos conseguido automatizar el trabajo del día a día, siendo más flexibles según las necesidades de cada usuario obteniendo informes a medida. Faro Security nos ha permitido mejorar en la toma de decisiones y el control de la función de seguridad gracias a la visión global que nos proporciona.»

La implantación de Faro Security ha supuesto para BBVA un avance muy importante y fundamental en la gestión del fraude, según la directora de Prevención del Fraude Corporativo en BBVA, Pilar García Alcantarilla: «Con Faro Security podemos obtener, de forma ágil y rápida, datos comparativos de los incidentes y modus operandi que suceden en todos los países donde BBVA está implantado, así como informes de gestión, cuadros de mando y mapas de riesgo, que son de gran ayuda en la gestión del fraude.»

Pero esta herramienta, no es solo un repositorio de incidentes sino que va más allá, incluyendo una serie de funcionalidades que permiten llevar a cabo una gestión integral de la seguridad. Hagamos una breve revisión de las principales funcionalidades de Faro Security, y cómo contribuye a la eficiencia en la gestión la seguridad.

• **Gestión e Inventario de dispositivos de seguridad** instalados en las dependencias, tanto a nivel nacional como internacional. A través de un catálogo único de elementos o dispositivos de seguridad, Faro Security permite unificar tanto los nombres de los dispositivos como sus marcas y mode-

los homologados por la organización a nivel corporativo, o por los correspondientes organismos a nivel sectorial.

Los profesionales de la seguridad encargados de la gestión, también tienen acceso a libros de registro de seguridad, certificados, manuales internos, legislación, guías técnicas de los productos que están homologados, mantenimientos y revisiones realizadas y previstas, así como en qué dependencia concreta (instalaciones técnicas, oficinas, edificios, etc.) están instalados y ubicados los equipos.

• **Gestión de incidentes de seguridad.** Abarca el ciclo de vida completo de los incidentes, tales como sabotajes, vandalismo, atracos, robos, hurtos, fraude, y otras tipologías de incidencias, que la aplicación permite configurar.

• **Gestión de auditorías de seguridad** y evaluación de dependencias, en cuanto a las medidas de seguridad existentes, en concordancia con el entorno que las rodea, o frente a lo establecido por la organización o las normativas aplicables. Un mapa de riesgos detallado ayuda a tomar las medidas necesarias en cada caso.

• **Planificación y control de los servicios de vigilancia**, y gestión de contratos y facturación de las empresas proveedoras. Permite hacer un seguimiento y control de la información asociada a los servicios de vigilancia, y aporta una visión tanto a corto como a medio plazo, vital en la ayuda a la toma de decisiones.

• **Gestión de presupuestos** globales y detallados de los servicios relacionados con la seguridad, como los servicios de vigilancia, para realizar previsiones anuales. También realiza comparativas de presupuestos con años anteriores y facilita el seguimiento del presupuesto planificado frente al ejecutado.

• **Gestión de empresas proveedoras de seguridad**, incluyendo prestación de servicios, agenda de contactos y personal externo, detallado por dependencias y puestos. Realiza la gestión de contratos y tarifas de proveedores para los diferentes servicios, así como la valoración de estos y su personal, siendo de inestimable ayuda en el proceso de seguimiento y evaluación de proveedores.

• **Informes y Cuadros de mando.** Dispone de un potente sistema de búsquedas avanzadas e informes configurables, y aporta una visión general de la gestión de seguridad a través de la definición de indicadores o KPIs, que miden el nivel del desempeño, la evolución, y el estado de aspectos relevantes del negocio.

• **Existen otras funcionalidades** y herramientas generales de la aplicación que dan robustez y valor a Faro, tales como:

El concepto de la «Oficina sin papeles» se logra con la incorporación de un gestor documental en el que es posible almacenar todos los expedientes, fotos y vídeos relacionados con cada incidente, así como documentación asociada a cada activo, como certificados de instalación, registros de revisión, mapas, documentación normativa, legislación vigente, etc.

El soporte multipaís y multiempresa hace posible gestionar a través de una única aplicación la seguridad de todos los activos de grupos multinacionales.

Dada la naturaleza e importancia de la información que se necesita procesar, y para cumplir con los requisitos de algunas normativas específicas, la plataforma está provista de un cifrado integral de los datos.

Su motor de seguridad y perfilado y la gestión de ámbitos de actuación que incorpora, habilita el uso a todo el personal involucrado en la seguridad, desde los vigilantes hasta el responsable último del área de Seguridad Corporativa.

Hasta la fecha, BBVA ha desplegado la solución en 11 de los países en los que opera y su uso le reporta innumerables ventajas, habiendo racionalizado con ello el uso de los recursos de Seguridad Corporativa, una de las funciones críticas en la organización. En palabras de César Bilbao Delgado, Director de Seguridad Bancaria Corporativo BBVA «Faro Security ha supuesto multitud de beneficios para el Departamento de Seguridad de BBVA. Lo que más claro tengo es el importante ahorro que nos ha supuesto desde su puesta en servicio.» ●

Fotos: GMV

Contactos de empresas, p. 8.

ROBERTO MONTEJANO. DESARROLLO DE NEGOCIO. ÁREA DE SEGURIDAD. GRUPO ÁLAVA

Sistemas PSIM: Consolidación de la gestión de la seguridad

ESTAMOS en un punto donde la tecnología existente en seguridad, así como la normativa que rige la aplicación de la misma al entorno bancario, sitúa el concepto de seguridad bancaria con una percepción positiva, pero que todavía puede mejorar en lo relativo a su gestión y optimización.

Así pues, están resueltas las problemáticas de diversa índole para afrontar los retos propios de una oficina bancaria, desde la identificación de personas en el acceso a una oficina donde nos encontramos en una situación donde debemos utilizar sistemas de captación de imagen con un alto WDR (Wide Dynamic Range) que resuelvan el fuerte contraluz existente en la entrada, la grabación y transmisión de imágenes a la CRA, los diversos sistemas anti-atraco formados por pulsadores, pedales, pinzas de billetes, retardos de apertura; diferentes sistemas antirrobo, como volumétricos, contactos magnéticos, sistemas inerciales antibutrón, sistemas de escucha ambiente, conectados al panel de alarma, sistemas de esclusa, sistemas de control de acceso y cómo no, los sistemas de detección de incendio.

Es decir, en una entidad bancaria, la tecnología utilizada es fiable, madura y está avalada por la experiencia de años de aplicación de la misma, así como por la evolución de la tecnología que hoy día disfrutamos en sistemas de seguridad.

Nos encontramos en un escenario en el cual en un entorno muy pequeño, una oficina bancaria, aglutinamos todas las tecnologías típicas de seguridad como CCTV, sistemas anti-intrusión, y anti-atraco, control de accesos, sistema de detección de incendio, todos ellos sujetos a una normativa a cumplir, y además con el añadido que el fallo de alguno de los sistemas puede conllevar desde una interrupción del servicio hasta un sobrecoste económico, por la necesidad de tener que contar con vigilancia física en la propia sucursal.

Si además hablamos de entidades con cientos, incluso miles de oficinas, ya sea a nivel nacional, o incluso, a nivel internacional, nos encontramos con un gigantesco parque de dispositivos y sistemas de diferentes fabricantes que debemos gestionar y administrar tanto desde el punto de vista operativo estricto de seguridad, como desde el punto de vista de la optimización de todos esos recursos materiales sujetos a mantenimiento.

Con la presión que se genera ante las expectativas de hacer las operaciones más rentables, la mejora continua, la incorporación de nuevas tecnologías y la gestión en la supervisión del mantenimiento de esta ingente cantidad de datos, se incrementa notablemen-

te la cantidad de información a gestionar simultáneamente desde la Central Receptora de Alarmas.

Un sistema PSIM proporciona las herramientas necesarias para tratar cada aspecto del ciclo vital de la gestión del Centro de Control y Recepción de Alarmas de manera global, fusionando todos los datos en un cuadro de operaciones común. Se analiza y correlaciona toda esta información, para aplicar un operativo estándar de procedimientos y planes de respuesta en todos los ámbitos.

Un sistema PSIM integra y correlaciona la información de múltiples y diversos sistemas de seguridad como sistemas CCTV, CC.AA, intrusión, o de cualquier otra índole, como por ejemplo, sistemas BMS (Building Manager Sistems), a nivel global en toda la entidad en tiempo real. Al mismo tiempo, coordina las respuestas más efectivas, asegurándose de que todo el mundo en la cadena de operaciones sepa qué está sucediendo, dónde está sucediendo y cómo responder.

Respuesta más rápida y eficaz

Un PSIM correlaciona todos sus datos entrantes y analiza un evento en curso para tener conocimiento inmediato de la situación. Al presentar automáticamente toda la información relevante, los procedimientos y los flujos de trabajo, siempre se da la misma respuesta predefinida ante eventos iguales, mitigando el riesgo del error humano y habilitando una óptima gestión de la situación sin importar quién sea el operador responsable.

Solución abierta

Como solución abierta permite incorporar cualquier producto de cualquier fabricante y mantener las existentes potenciando funcionalidades de las mismas. Al mismo tiempo, está preparada para la implementación de nuevas tecnologías futuras facilitando la mejora continua.

Cumplimiento de normativas

En un entorno cada vez más regulado, el incumplimiento no solo es costoso, sino que puede incrementar el riesgo. Mediante flujos de trabajo e informes automatizados, un PSIM asegura que todas las políticas y procedimientos se siguen uniformemente, ayudando a las organizaciones a mantener el cumplimiento normativo en cualquier momento.

Informes y auditoría

Los informes también ocupan una gran cantidad de tiempo y pueden ser muy dañinos si se hacen inapropiadamente. Las capacidades de informes personalizables y automatizados ahorran tiempo y recursos, proporcionando explicaciones exactas y completas sobre cada acción tomada relacionada con un incidente. Además nos permiten establecer control sobre tareas externalizadas.

Panel de Operaciones

Permite una visualización eficaz y automática del evento en tiempo real de todos los sistemas integrados involucrados, permitiendo ver qué está sucediendo a través de las cámaras CCTV relacionadas, dónde está sucediendo, sistemas GIS, planos, mapas, modelos 3D, y cómo responder ante el evento mediante los procesos preestablecidos.

Automatización de procesos

Los administradores pueden desarrollar los procedimientos de respuesta ante las más complejas situaciones de emergencia como para tareas rutinarias. Cuando alguna tarea no ha sido gestionada adecuadamente o en una ventana temporal definida, se puede escalar reasignando automáticamente o de forma manual a otra persona o recurso predefinido.

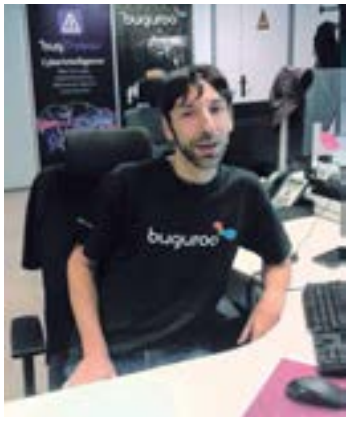
Un sistema PSIM permite «alimentar» y dar paso a la implementación de un módulo de Inteligencia de Negocio (BI), como herramienta en la gestión global, que puede incluir beneficios como, por ejemplo:

- Visualización de KPI´.
- Número de incidentes abiertos.
- Monitorización del status de los diferentes operadores.
- Monitorización de desempeño de distintos departamentos.
- Monitorización del cumplimiento de SLA.
- Análisis de tendencias.

La seguridad en entidades bancarias puede ganar en eficiencia y ahorrar costes que se derivan de la gestión de enormes cantidades de información generadas por la disparidad de sistemas y fabricantes, la criticidad de la gestión de alarmas, así como de la tarea de la gestión de las operaciones necesarias para el mantenimiento en estado operativo de todos ellos mediante sistemas PSIM y BI.

Fotos: Grupo Álava

Contactos de empresas, p. 8.



ÓSCAR GALLEGO. RESPONSABLE DE LABS DE BUGUROO OFFENSIVE SECURITY

Malware: Transferencias fraudulentas

LA incorporación a nuestras vidas cotidianas de las diferentes comodidades que la tecnología nos ofrece ha venido acompañada en todo momento por el abuso que los cibercriminales hacen de ella. La Banca Online, por supuesto, no ha sido una excepción. El auge de este tipo de servicios trajo consigo la proliferación de un nuevo tipo de amenaza destinada a vaciar las cuentas de los usuarios: el malware bancario, con uno de sus primeros exponentes –que más adelante se convertiría en una verdadera epidemia– el troyano Zeus.

Con su aparición en 2006, Zeus no era solo un troyano bancario, sino también un Kit que permitía a los cibercriminales crear sus propias campañas contra entidades y usuarios.

Desde entonces el malware bancario no ha cesado de evolucionar, y si bien podríamos escribir un vademécum sobre las tecnologías que emplean, sus métodos de distribución e infección, cómo se ocultan en el sistema, el salto a los dispositivos móviles u otras características, en esta ocasión nos vamos a centrar en los mecanismos que emplean para realizar transferencias fraudulentas desde los PC de los usuarios infectados.

El registro de las pulsaciones de teclado –Keylogger– o la captura del tráfico que el navegador web envía –Form Grabber– fueron los métodos elegidos por los cibercriminales en una primera aproximación. La utilización de teclados virtuales en la página web de la entidad, o el uso de una tarjeta de coordenadas fueron algunas de las protecciones que aparecieron para afrontar esta amenaza, y que obligaron a los creadores de Malware a emplear nuevos métodos de engaño.

Phishing automático

Los ataques de Phishing ya venían utilizándose desde mediados de los 90, y para entonces se habían convertido en un problema habitual para los servicios de Banca Online. Pronto se incorporó esta capacidad al Malware bancario, a fin de obtener las credenciales del usuario haciéndole creer que está visitando el sitio web original, cuando en realidad se encuentra en una copia del mismo bajo el control de los cibercriminales.

Originalmente estos ataques se realizaban a través del correo electrónico, simulando ser mensajes enviados por la propia entidad bancaria. El éxito del ataque dependía en exceso del usuario, al que debían engañar para hacerle confiar en el mensaje de correo, los enlaces que contenía o el sitio web al que finalmente conducía.

Los cibercriminales llevaron esta técnica un poco más lejos. En lugar de requerir la intervención del usuario, emplearían malware para engañar al propio sistema operativo, de manera que las visitas que se realicen a los servicios de Banca Online vayan a parar a un servidor web bajo su control.

Encontramos ejemplos de este tipo de ataque a lo largo de los años y en diferentes familias de Malware bancario. Las primeras versiones de Zeus modificaban el fichero Hosts de Windows para que la propia resolución de nombres llevará a sitios web maliciosos en lugar de a los originales.

Otro tipo de redirección de las visitas con este mismo propósito lo encontramos en troyanos como Retefe. En este caso el Malware modifica la configuración del Proxy del navegador, de manera que los cibercriminales consiguen controlar y redirigir el tráfico web hacia sus propios servidores.

Más adelante, ya en 2014, troyanos bancarios mucho más evolucionados y modernos como Dyre o Dridex extendieron esta misma idea, realizando la redirección durante la propia navegación del usuario, a la vez que anulaban ciertas características de seguridad que pidieran evidenciar el fraude, como la ausencia de un certificado válido durante una visita https.

Aunque estas técnicas presentan ciertas ventajas para los cibercriminales, como la facilidad en su implementación, se enfrentan también a un gran problema para ellos.

La constante y a veces frenética actividad en los CERT y SOC ha conseguido

que el tiempo de vida de los sitios web fraudulentos sea muy breve.

Tan pronto se detecta una nueva campaña, los expertos en análisis de Malware extraen su configuración para determinar la localización de estos sitios web maliciosos y se procede a su cierre.

Acceso remoto al sistema del usuario infectado

Algunas familias de Malware empezaron a incorporar módulos tipo VNC, que permitían a los cibercriminales acceder al sistema del usuario en remoto. De esta manera eran capaces de realizar transferencias fraudulentas aprovechando la sesión del propio usuario, mientras este hacia uso de los servicios de Banca Online.

El acceso a través de VNC se emplea actualmente durante ataques dirigidos, no masivos, en los que los cibercriminales quieren garantizar la operación contra un usuario concreto que resulta de especial interés para ellos.

Los principales problemas a la hora de realizar este ataque los encontraban en la necesidad de emplear un operador que realice la intrusión manualmente. La operación de transferencia deja evidencias visibles en el extracto, permitiendo al usuario detectar con cierta facilidad el fraude. Finalmente, el riesgo aumenta al requerir una conexión directa en tiempo real entre el criminal y la víctima.

Inyección de código en las páginas web

Modificar la página web de la entidad bancaria fue el siguiente paso en la

evolución de este tipo de fraude online. Para ello los cibercriminales crearon un Malware capaz de realizar ciertas modificaciones sobre el código Html de la página web antes de mostrársela al usuario infectado. De esta manera podrían modificar el formulario de acceso al servicio, por ejemplo, de manera que se enviaran las credenciales a un servidor bajo su control.

Esta técnica recibió el nombre de Webinject, y no solo permitía capturar las credenciales de acceso al servicio de Banca Online, algo que se podría haber conseguido empleando un Keylogger tradicional, sino que además ofrecía una gran flexibilidad a la hora de afrontar los diferentes mecanismos que las entidades bancarias ponían en marcha en respuesta a estos ataques.

Un ejemplo de esto lo encontramos en los Webinject que añadían campos al formulario de login, instando al usuario para introducir su firma electrónica o los números de su tarjeta de coordenadas, además de su identificación y contraseña. La utilidad de estos mecanismos de seguridad, ya de por si rudimentarios, se quedó muy atrás y fue necesario poner en marcha otras tecnologías tales como el segundo factor de autenticación a través de mensajes SMS.

El uso de Webinject permitía independizar la creación del Malware del diseño del código Html o Javascript específico que se inyectaría sobre las páginas web de cada entidad bancaria. Esto propició la aparición de servicios especializados en la creación de estos Webinject, que se volvieron mucho más complejos y potentes.

Transferencias automáticas

La sofisticación del código empleado en los Webinject aumentó drásticamente a fin de evitar la detección, dificultar el análisis y, finalmente, flexibilizar su explotación por parte de los diferentes grupos de cibercriminales que los emplean en su Malware. El propio código dejó de estar presente en las configuraciones, sustituyéndose por una simple referencia a un script remoto alojado en un panel de control adicional. El operador de dicho panel ganaba un mayor control sobre el código inyectado, así como la posibilidad de ofrecerlo como servicio.

El código inyectado en la página ya no se limitaba a añadir campos al formulario de acceso, o a la captura pasiva de credenciales. Ahora era capaz de realizar transferencias fraudulentas de manera automática en el contexto de la propia sesión del usuario durante su utilización del servicio de Banca Online.

Este tipo de Webinject se denominó ATS – acrónimo de Automatic Transfer System– y es el tipo de ataque que emplean las campañas de Malware con distribución masiva y más avanzadas en la actualidad.

Estado actual

En la actualidad nos encontramos con grupos de cibercriminales especializados en el fraude contra la Banca Online que operan a nivel mundial. Los Webinject que emplean presentan un altísimo grado de sofisticación: Capacidad para depuración remota, funcionamiento automático o asistido por el operador, selección manual de mulas para cuentas bancarias de especial interés, manipulación directa del DOM, abuso de CSS para crear capas u ocultar mensajes, etc. Durante su funcionamiento, este tipo de Webinject son capaces de realizar transferencias de manera automática, ocultar la operación en el extracto o ajustar el saldo, de manera que el usuario no se percata del fraude hasta x.

Las entidades no pueden proteger a los usuarios contra todas las amenazas, pero sí que está en su mano proporcionar al usuario la máxima protección durante el uso de su plataforma web de Banca Online, incorporando mecanismos que impidan y dificulten la actividad maliciosa en el contexto de la propia aplicación. ●

Fotos: Buguroo/ Archivo.

Contactos de empresas, p. 8.

iPTECNO

DISTRIBUIDOR OFICIAL DAHUA ESPAÑA

DEPARTAMENTO DE I+D

Desarrollamos soluciones a medida dirigidas a mejorar la competitividad de nuestros clientes: Apps para conexión a grabadores, pasarelas para Central Receptora de Alarmas, servidores DDNS y P2P propios para conexión con los grabadores, etc...

ASESORAMIENTO Y SERVICIO TÉCNICO

Contamos con especialistas que pueden solucionar tus problemas en las instalaciones o proyectos, mediante servicio telefónico, online y en la propia instalación. Además de un servicio de reparación en nuestro propio taller con técnicos certificados.

AMPLIO STOCK Y ENTREGAS EN 24H

Disponemos del mayor catálogo de productos Dahua en stock permanente, con las últimas novedades. Y una gestión logística con entregas en 24H y seguimiento de pedidos mediante web, esto permite al cliente conocer el estado del pedido en tiempo real.

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

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

IPTECNO BARCELONA - C. Pla del Ramassar, 52- 08402 Granollers (BCN)

JESÚS GARCÍA CUBILLO. RESPONSABLE DE PRODUCTO DE INTRUSIÓN. VANDERBILT INTERNATIONAL ESPAÑA

La nube

En el mercado de la seguridad electrónica, la nube está cobrando creciente importancia, debido a los estrechos lazos que nuestra actividad tiene con el mundo IT y el de las comunicaciones

ES imposible no haber oído hablar de ella. Nuestro tecnológico mundo no podría ya seguir subsistiendo sin este nuevo entorno al que cada vez más personas, empresas e instituciones confían no sólo sus datos, sino también importantes servicios.

La nube tiene un claro objetivo: Ahorrar recursos económicos, técnicos y espacio físico en base a hacer residir en entornos muy profesionales, caracterizados fundamentalmente por su alta disponibilidad (en teoría es muy difícil que se caiga el servicio), determinadas aplicaciones que, de otro modo, habrían de instalarse en la sede del usuario, obligándole a desplegar la adecuada infraestructura IT con el coste que ello conlleva.

La nube y la seguridad electrónica

En el mercado de la seguridad electrónica, la nube está cobrando creciente importancia, como era de esperar, debido a los estrechos lazos que nuestra actividad tiene con el mundo IT y el de las comunicaciones.

Por otra parte, no olvidemos que una nube puede ser propiedad de una empresa que proporciona servicio a diversos clientes, pero puede estar también destinada a un único cliente que, además, puede incluso ser su propietario. Podría suceder con una CRA de grandes dimensiones.

En ese sentido, y en cuanto a lo que la nube nos puede proporcionar, es necesario establecer 3 servicios o funcionalidades, que están bien diferenciadas:

- Servicios orientados exclusivamente al usuario.
- Ídem a la gestión técnica de los sistemas instalados.
- Ídem a la recepción y gestión de alarmas.

Acceso al usuario final

Los servicios dirigidos al usuario permiten que, desde su tablet, PC o Smartphone, pueda acceder a voluntad a su(s) sistema(s) para comprobar su estado e incluso manipularlo remotamente, emulando así todo lo que podría hacer si se encontrara personalmente ante el teclado del sistema. Incluso, si dispone de cámaras de TV, podrá visionar imágenes en vivo de las mismas.

¿Cómo se logra este servicio? Es fácil. Basta que se disponga de un servidor dotado de una determinada aplicación y una URL, con el que los equipos de los abonados establecerán comunicación permanente una vez configurados, además de hacerlo con la CRA. El usuario sólo efectuará la comunicación con su sistema a través de ese servidor, siendo de este modo indiferente que su router disponga de una dirección IP dinámica (el servidor siempre sabe cuál es ésta). Este servidor puede residir localmente en la sede del fabricante o proveedor de servicios (CRA, etc.), pero también puede estar en la nube y así externalizar este servicio.

Gestión técnica

Los servicios orientados a la gestión técnica están previstos tanto para el instalador como para el departamento técnico de la CRA. En este caso, el acceso al sistema de un abonado a través de un servidor, que puede ser

el mismo que el comentado en el párrafo anterior, presenta varias ventajas de las que hablaremos más adelante y, una de ellas, independientemente del sistema de que se trate, en que no se necesita abrir puerto alguno en el router del abonado para acceder directamente a la central desde el tradicional software bidireccional, o mediante un simple navegador, si la central posee página web embebida. La tarea de apertura de puertos del router, que es aparentemente sencilla considerándola desde un punto de vista individual, presenta importantes inconvenientes. Uno de ellos es la apertura de un punto de acceso desde el exterior que, en caso de filtración de datos, podría poner en peligro la integridad del sistema, haciéndolo susceptible de recibir un ciberataque. Otro, es la generación de costes cada vez que el usuario cambia de router o de operador, lo que exige la inmediata visita de un técnico para abrirle de nuevo el puerto o los puertos de acceso.

Recepción y gestión de alarmas

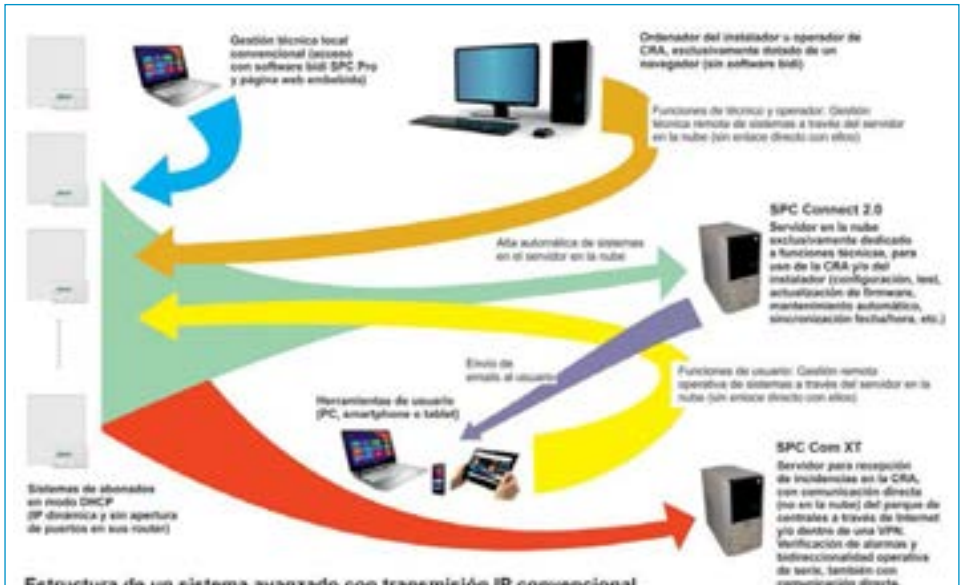
Los servicios destinados a la recepción de alarmas también arrojan claras ventajas, pero aquí haremos una reflexión previa.

En los dos servicios que acabamos de ver, su suspensión temporal debida a un problema técnico de cualquier tipo supondría un inconveniente. Impediría de forma transitoria la operativa al usuario o al servicio técnico, que no podría revisar su sistema o efectuar ninguna operación por control remoto pero, en general, no afectaría a la seguridad básica del sistema, el cual mantendría íntegra su funcionalidad de envío de incidencias a la CRA. Ésta continuaría recibiendo los «polling» y atendiendo posibles alarmas. Además, en cuanto al acceso remoto al sistema, tanto por parte del técnico como del usuario, nada se dice en la actual normativa.

Como ocurre desde siempre en una CRA, la implantación de un sistema de recepción de alarmas exige redundancia. Desde los tiempos en que la RTB era la base de las comunicaciones de seguridad (por llamarlo de alguna manera, pero entonces sin ninguna otra posibilidad), la CRA había de contar con una o más receptoras de repuesto, donde líneas telefónicas y puerto RS232 se conmutaban a mano. Aunque parezca mentira, muchos miles de sistemas continúan empleando todavía RTB en esas condiciones. Trabajo por delante el que tiene el sector para dar una solución a tanta precariedad.

Para IP existen equipos físicos capaces de atender las señales de sistemas de diversos fabricantes (al estilo de las clásicas RTB), que habrá que tener duplicados y, otros, generalmente basados en software y que sólo pueden trabajar con los sistemas de su misma marca, aunque varios puedan coexistir en una misma máquina. Esto origina que, en una CRA pública, que admite todo tipo de clientes, se multipliquen los equipos para atender sus señales y dotarles de las adecuadas medidas de seguridad que impidan un fallo, a los que sumar los backup correspondientes de las bases de datos, etc. Y a esto hay que añadir el software para la comunicación bidireccional, también específico de cada fabricante.

Con este escenario, es obvio que la nube resulte tentadora para la CRA. El caso más típico en cuanto a recepción de alarmas es el emplazamiento en ella de servidores con aplicaciones de diferentes fabricantes, de modo que, a la CRA, le bastará con su sistema de gestión, al que los citados servidores reenviarán todas las señales recibidas, y las aplicaciones clientes de estos, desde las que administrar los abonados (altas, bajas, modificaciones, etc.). No cabe duda de que la CRA se libera de un peso considerable. Y todavía puede simplificarse más: Hasta el servidor del sistema de gestión podría técnicamente estar en la nube e, igualmente, la CRA sólo tendría clientes de ese servidor en los puestos de operador. Una moderna CRA minimalista, pero que también



Estructura de un sistema avanzado con transmisión IP convencional de incidencias a CRA y gestión técnica remota en la nube

precisa de otra reflexión: Las comunicaciones entre los sistemas de los abonados y el servidor que atiende las señales están encriptadas, en ciertos casos hasta con protocolos AES de 256 bits, pero no lo está la señal que ese servidor envía al sistema de gestión, bastante simple, generalmente basada en un protocolo conocido como Surgard que emplea un formato SIA semejante al que se transmite por RTB.

Operativa y seguridad de funcionamiento

Los proveedores de «nubes» aseguran la casi indestructibilidad del sistema. Las aplicaciones comentadas y las bases de datos se instalan en potentes servidores dotados de todos los mecanismos de backup necesarios, que se mantienen continuamente actualizados para prevenir las vulnerabilidades que puedan aparecer. Estos servidores pueden estar desplegados geográficamente en cualquier sitio. Es un hecho que la red lo soporta todo, pero es necesario pensar en que un fallo, sabotaje, etc. puede producirse y, entonces, ¿quién se responsabiliza de sus consecuencias? Es necesario meditar sobre ello.

No obstante, la nube tiene una ventaja sobre la aplicación individualizada en la CRA, en la que ésta recibe en una dirección IP y en un puerto las señales procedentes de los abonados que emplean un determinado sistema. Ciertas aplicaciones son capaces de generar un tráfico masivo contra este socket y saturarlo (conocido como DoS/DDoS o Ataque/Distribuido de Denegación de Servicios) y podrían ser empleadas para bloquear la recepción de señales en una CRA. Los recursos tecnológicos a los que el proveedor de la nube tiene acceso, son capaces de hacer frente a este problema y salir inmunes, lo que en una CRA privada exigiría una considerable inversión y dedicación.

Además, es importante señalar que estos accesos a los servidores de la nube se realizan mediante conexiones seguras (https), lo cual garantiza que la información transferida no puede ser interceptada y utilizada por terceros.

Volviendo a la gestión técnica, la nube puede proporcionar grandes beneficios. Algunos sistemas ya no precisan de una aplicación bidireccional determinada, les basta con un navegador desde el que se accede al servidor, el cual muestra todos los abonados a los que se tiene acceso y, este acceso a cada uno de ellos, se efectúa a través de la propia página web embebida del equipo.

Ventajas adicionales para sistemas web

Pero las ventajas no se quedan ahí. Determinados sistemas ofrecen extraordinarias ventajas a la CRA y al servicio técnico para que la gestión del parque instalado sea más rápida, económica y eficiente.

Imaginemos un sistema donde las centrales poseen página web embebida para que el acceso técnico no exija del empleo de ninguna aplicación concreta y baste con un navegador. Ni siquiera será necesario mantener actualizada la base de datos, ya que de eso se encargará el servidor.

Por otra parte y el mundo en que ya nos movemos, es necesario mejorar la seguridad de los sistemas no sólo frente a ataques cibernéticos encriptando las comunicaciones, sino también frente a posibles manipulaciones malintencionadas desde el punto de vista técnico.

De forma remota y trabajando con un servidor de este tipo, entre otras funciones, se puede llevar a cabo:

• Actualizaciones de firmware por lotes. Tras definir un grupo de centrales, su firmware se actualiza automáticamente desde el servidor.

• Migración de CRA. Un grupo predefinido de abonados puede ser transferido automáticamente de una CRA a otra, evitando el engorroso trabajo que esto supone ahora. Gran ahorro de tiempo y ausencia de errores.

• Mantenimiento automático periódico pre-programado. Los sistemas, periódicamente, envían al servidor un conjunto de datos sobre su estado que quedarán almacenados en la base del servidor con el fin de elaborar informes, generar estadísticas, etc.

• Gestión de claves de acceso técnico (teclado, software bidi y página web) intrínsecamente segura. Tras una sesión técnica en el sistema (configuración inicial, mantenimiento, etc.), el servidor carga claves nuevas en ese sistema, que le serán comunicados al técnico en la siguiente visita. Imposible acceder de forma no autorizada previamente al evitar la habitual repetición de claves en múltiples sistemas que hoy en día se produce.

• Análisis de la configuración establecida y ya operativa en cada sistema, frente a posibles cambios malintencionados que pudieran poner en peligro su correcto funcionamiento.

• Posible alta automática de centrales en el servidor. Disponibilidad inmediata de acceso.

• Usuarios del sistema (servidor) con niveles de acceso configurables mediante la creación de perfiles.

En conclusión, la nube está aquí y ha venido para quedarse definitivamente, aunque sea necesario pensar seriamente que es positivo y que podría suponer un riesgo, incluso desde un enfoque legal.

Es necesario apostar por las nuevas tendencias ya que pueden aumentar la eficiencia del sector de la seguridad electrónica y, paralelamente, reducir costes, de lo que todo el mundo anda muy necesitado. Pensar de otro modo sería «estar en las nubes». ●

Fotos: *Vanderbilt/Freepik*

Contactos de empresas, p. 8.

Sistemas de Videoanálisis con Visión Térmica

DAVANTIS
YOUR VIDEO ANALYSIS PARTNER

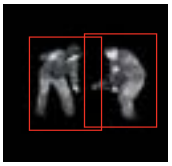
FLIR

SR7®

Vigilancia perimetral, la solución perfecta

Reducción de costes aumentando la eficacia

Detección con cámaras térmicas, mucho más eficaz que con cámaras convencionales.



Estabilizador de imagen: mayor precisión, menos falsos positivos.

Máxima estabilidad ante factores ambientales (iluminación, clima…).

Detección en más de 450 metros con cada cámara.

Reducción significativa en materiales y en mano de obra.

Detección automatizada de fuego

Máximo alcance, máxima seguridad

SR7Fire©, es un sistema que ha sido especialmente diseñado para la detección de fuegos generados en entornos industriales con capacidad de detección en un radio de hasta 2.500 metros.

Especialmente indicado para detección de incendios en exteriores, como puertos (deportivos o mercantes), refinerías, industrias químicas y petroquímicas, plantas de residuos, parques fotovoltaicos, centrales eléctricas, industrias madereras, etc.

casmar
sistemas de seguridad

www.casmar.es casmar@casmar.es
Tel: 933 406 408 / 902 202 206 • Maresme, 71-79 • 08019 Barcelona

JESÚS RODRÍGUEZ CABRERO. CEO DE REALSEC

Criptografía para la seguridad de los **medios de pago**

A FINALES del S.XX surgen las primeras tarjetas bancarias y, por lo tanto, el empleo de dinero no efectivo. Tarjetas bancarias que actualmente conviven como medios de pago con otros dispositivos móviles como las tablets o smartphones dentro de este nuevo paradigma de la banca on line, que desempeña un rol clave en la transformación digital en la que nos encontramos inmersos.

Los medios de pago evolucionan y su seguridad también, puesto que el comportamiento de los individuos a lo largo del tiempo para llevar a cabo sus transacciones dinerarias nunca ha estado exento de acarrear consigo medidas de seguridad que proporcionen esta confianza a la hora de usar los medios de pago.

Minimización de los riesgos en las transacciones financieras

El concepto de medios de pago es algo en constante evolución. En los últimos treinta años hemos visto un escenario de continua y proactiva mejora de seguridad, agilidad y ergonomía para el usuario.

En la década de los 80 nacen las primeras tarjetas bancarias, las que no contaban con criptografía, puesto que la comprobación de las transacciones se hacía de manera manual: el comercio telefoneaba en el momento de la transacción al centro de procesamiento de tarjetas donde atendía un operador, quien a su vez llamaba al banco emisor para verificar los datos de la transacción y solicitar su aprobación. Esta conversación era grabada y se asignaba una referencia a cada transacción que se escribía con bolígrafo sobre la boleta.

Quizá muchas veces nos hemos preguntado por qué en nuestras tarjetas bancarias, nuestros datos personales y el PAN (número de la cuenta personal) aparecen en relieve (algo que a día de hoy es prescindible) pero que en ese momento constituía el único elemento de seguridad, debido a que estos datos en relieve eran calcados con tinta en papel carbón, originando tres copias de una misma: boleta para el banco, el comercio y el cliente.

Esto únicamente se usaba para compras, no para la retirada de dinero en efectivo, porque tampoco existían los cajeros automáticos que hoy conocemos.

En una segunda fase, con la expansión y democratización del uso de las tarjetas, el proceso de la transacción financiera se automatiza, y es entonces cuando surge la banda magnética de estas tarjetas, lo que constituye el primer escenario de aplicación de la Criptografía en el mundo financiero.

En esta banda magnética encontramos información de valor del usuario de la tarjeta como límites de riesgos, modalidades de operaciones autorizadas…y, a su vez, surge el primer elemento de seguridad, el uso del PIN con conocimiento y posesión exclusiva del titular de la tarjeta.

El PIN tecleado por el titular viaja cifrado desde el propio terminal bancario (PINBlock) y es comprobado en el banco, que dispone del PINOffset (complemento algorítmico al PIN) y realiza así, en la memoria protegida de un hardware criptográfico, una operación que da como resultado el PAN, sirviendo éste de comprobación.

Se desarrollaron así las primeras transacciones electrónicas seguras, de forma telemática, a través de los terminales de compra en los puntos de venta (POS) y cajeros (ATMs).

Criptografía en los actuales Medios de Pago: Tarjetas Chip &Pin EMV y Smartphones

Después, la seguridad de las tarjetas bancarias se mejoró migrando de la banda magnética al chip, debido a que esta banda era muy fácilmente clonada, quedando como elemento único de autenticación el PIN, susceptible de ser capturado por diversos métodos.

Las tarjetas Chip&PIN EMV, cuya tecnología criptográfica (basada en algoritmos de claves simétricas y asimétricas) representa un importantísimo avance en la seguridad, puesto que se pasa a un siste-

ma de autenticación robusta basada en múltiples elementos. A través de la «cadena de certificación» (marca, emisor, titular) se comprueba in situ la bondad del origen de la tarjeta. Y ahora, el PIN sólo conocido por el titular es usado para utilizar una clave exclusiva que sólo ese titular posee para generar un criptograma de petición de aceptación al banco emisor.

Esta seguridad que proporciona la tecnología EMV a las tarjetas minimiza los riesgos de fraude, beneficiando al conjunto de participantes en el Sistema (marca, emisor, adquirente y merchant) al mantener la confianza de los usuarios en él.

Además, como medida de lucha contra el fraude y uso indebido de los datos, las propias empresas de medios de pago exigen a las empresas con las que se llevan a cabo las transacciones («merchants») contar con soluciones de cifrado capaces de custodiar los datos de los titulares de las tarjetas, en cumplimiento a los requerimientos de la Normativa PCI/DSS.

Actualmente, y en consonancia con la nueva banca digital y sus consecuentes prácticas de ciberseguridad, este chip criptográfico EMV se ha ampliado con complementos tecnológicos como contactless (cuyo chip con tecnología RFCI permite un diálogo NFC), permitiéndonos usar nuestras tarjetas bancarias a través de esta tecnología de proximidad o hacer uso de estas tarjetas a través de nuestro smathphone o tablet, en cuyos casos, desde su tarjeta SIM accede a los datos asociados a esa tarjeta financiera y las funciones pertinentes.

No obstante, aunque como usuarios el poder efectuar pagos con nuestros dispositivos móviles nos facilita la vida, no podemos obviar que, en términos criptográficos de securización, este proceso de validación es mucho más complicado, ya que cada operación de pago con un dispositivo móvil construye «ad hoc» unas claves criptográficas y datos de un solo uso.

> «La criptografía es imprescindible para la seguridad del ámbito bancario»

A medida que simplificamos el medio, nos vemos obligados a complicar más las medidas de seguridad y la protección robusta que nos da la criptografía. Medidas más complejas para no poner en riesgo la transacción al aumentar la ergonomía.

En la actualidad, en España, existen un 75% de comercios cuyos terminales aceptan el pago contact-less y, en base a los datos de la segunda edición del estudio de Ipsos, «Pagos por móvil en España. La perspectiva del consumidor – 2016» se desprende que «Más de la mitad de los usuarios de smartphones en España pagaría a través de su móvil en 2017». Lo que evidencia el aumento en el uso de esta tecnología, cuya confianza e implementación avanza acorde a la transformación digital que está experimentando nuestra sociedad.

Pero no podemos olvidar que para que esta nueva forma de pago sea segura debe estar basada en los estandartes de la criptografía. Ya que la red debe identificar, procesar y validar lo canalizado por otros dispositivos, ofreciendo así un entorno financiero seguro en el que efectuar transacciones.

Actualmente, las transacciones presenciales y las que se generan vía web a través de los medios de pago conviven. Ambas requieren integrarse en un entorno confiable tanto para los usuarios como para las entidades financieras, así como para las redes franquiciadoras de los medios de pago (VISA, MasterCard…) y, por ello, la criptografía es imprescindible para la seguridad del ámbito bancario.

Para generar este entorno de confianza y seguridad las entidades financieras cuentan con módulos hardware de seguridad con aplicaciones específicas para los medios de pago. ●

Fotos: Realsec

Contactos de empresas, p. 8.

ÁLVARO RODRÍGUEZ. DIRECTOR DE MERCADO. GUNNEBO ESPAÑA

La **tecnología** aplicada a los **compartimentos de alquiler**

Si nos preguntasen por un lugar seguro, muchos de nosotros incluiríamos a los bancos dentro de las dos o tres primeras respuestas. Me atrevería a decir que no existe otra institución tan presente en nuestro día a día que cuente con unos niveles de seguridad similares. Seguridad física, accesos, videovigilancia, cámaras acorazadas…, sus requisitos son muchos y requieren soluciones eficientes y exclusivas que, aparte de neutralizar los riesgos de seguridad, no resulten intimidatorios para los clientes.

Afortunadamente, el desarrollo que la tecnología aplicada a la seguridad ha vivido en los últimos años ha hecho posible que los niveles de seguridad de las entidades bancarias aumenten, a la vez que se optimizan los recursos y mejora la experiencia de los clientes.

Cuando pensamos en tecnología para la banca, rápidamente nos vienen a la mente conceptos como banca online o cajeros de última generación, pero existen multitud de áreas que se han transformado notablemente durante los últimos años. En este sentido, me gustaría destacar los avances conseguidos en los compartimentos de alquiler, un servicio que los bancos ofrecen desde tiempos inmemoriales y del que todos guardamos una idea muy intrigante gracias a la industria cinematográfica y la literatura policiaca. Hoy en día existen compartimentos de alquiler completamente automatizados, con un alto grado de seguridad y que ofrecen a los clientes que buscan productos exclusivos, independencia total a la hora de manejar sus objetos de valor.

Es el caso de SafeStore Auto, desarrollado por nuestra compañía, que representa la última tecnología en compartimentos de alquiler al tratarse de un sistema seguro, fácil de usar y extremadamente rentable en costes. El cliente de este sistema accede al recinto de entrega de cajas con la tarjeta del banco y un código PIN. Introduce esa misma tarjeta en un terminal y vuelve a marcar el código o bien utiliza un lector de huellas digitales. Una vez validada la identidad del cliente, un robot selecciona la caja y se la entrega al usuario a través del terminal. El cliente abre y cierra el compartimento con una llave personal y devuelve el compartimento a la cámara acorazada cuando ha terminado.

Las ventajas para la entidad bancaria son claras, no sólo reduce considerablemente los costes asociados a los compartimentos de alquiler tradicionales, sino que genera una corriente de ingresos superior. Debido a que es un sistema de autoservicio, los clientes pueden acceder a sus compartimentos a cualquier hora del día y cualquier día de la semana. Los clientes ya no tienen que pasar por lentos procedimientos de alquiler y ser acompañados a la cámara acorazada por un empleado del banco, lo que proporciona al personal bancario tiempo extra para concentrarse en actividades más rentables. También se

produce un ahorro de costes derivado de la reducción de los gastos de gestión administrativa que se obtiene gracias a un proceso de registro más simple, la automatización del método de pago y la monitorización y supervisión del sistema. Además, este servicio amplía la cartera de clientes y aumenta los ingresos bancarios gracias a los mayores volúmenes procedentes de su alquiler, ya que la comodidad del servicio permite que los bancos puedan cargar un precio mayor por el alquiler de los compartimentos.

Otra ventaja para el banco reside en la optimización que se consigue del espacio. Con un sistema robotizado se pueden situar los compartimentos de alquiler mucho más cerca unos de otros, acabando con la necesidad de un espacio extra para el acceso de personas. Asimismo, los niveles de seguridad se incrementan, ya que no es lo mismo tener 2.000 compartimentos repartidos en 10 oficinas con sus medidas de seguridad asociadas, que concentrar ese gran volumen en una sola cámara acorazada, lo que permite incrementar los niveles de seguridad del conjunto con un menor coste de equipamientos.

Por otro lado, el sistema es mucho más flexible a la hora de ubicar los compartimentos. En lugar de instalarlos directamente detrás del terminal de autoservicio, pueden situarse en otro lugar, lo que supone ahorros si se encuentran en otras plantas más baratas como, por ejemplo, el sótano.

Comenzábamos el artículo hablando sobre internet y la revolución que ha supuesto, pues bien, los sistemas robotizados como SafeStore Auto se instalan con el software de gestión Safe Control, que suministra a los empleados bancarios acceso a detalles de disponibilidad de compartimentos libres y hace que la gestión de los clientes sea mucho más fácil.

A nivel de oficinas centrales, Safe-Control comunica datos muy valiosos como ratios de uso y el estado de todos los sistemas de la organización en tiempo real. Algo que sería imposible de obtener en organizaciones con varios compartimentos de alquiler no conectados entre sí.

En cuanto a sus prestaciones, SafeStore Auto posee ventajas frente a los sistemas de alquiler de compartimentos tradicionales. Por un lado, su diseño ergonómico con diferentes acabados y colores lo convierte en una solución muy atractiva para el usuario. Además, su pantalla táctil y su software facilitan en gran medida su uso. Y por último, posee una cámara integrada para garantizar la seguridad del usuario sin vulnerar su intimidad.

Para conseguir que todas las ventajas descritas anteriormente redunden positivamente en la entidad bancaria, es necesario contar con un proveedor que esté a la altura de los requerimientos que los bancos necesitan, con experiencia en el sector y que esté a la vanguardia de las novedades tecnológicas

que se lanzan al mercado. Alguien que ofrezca productos y servicios que no solo resulten atractivos para los usuarios de los diferentes bancos, sino que ayuden a optimizar los recursos consiguiendo verdaderos ahorros en costes sin que los niveles de seguridad de las oficinas se vean mermados. ●

Fotos: Gunnebo

Contactos de empresas, p. 8.

ALBERTO ALONSO. BUSINESS DEVELOPMENT MANAGER FOR RETAIL SEGMENT SOUTHERN EUROPE EN AXIS COMMUNICATIONS

Compresión de vídeo: ¿H.264 o H.265?

En la era del vídeo digital hemos visto sucederse diferentes formatos de compresión desde los primeros compases de esta tecnología. Desde los tiempos en los que el formato de fotografía JPEG (M-JPEG para vídeo) convivía con formatos propietarios basados en mayor o menor medida en estándares (MPEG-1, H.263, etc), pasando por las sucesivas mejoras que supusieron el JPEG-2000 (wavelet), MPEG-2, MPEG,4 hasta nuestros días en los que el formato estándar comúnmente usado es el H.264 (MPEG-4 parte 10, AVC), la compresión de vídeo ha intentado facilitar el uso del vídeo digital tanto en la trasmisión como en la grabación.

LAS restricciones de ancho de banda para transmitir vídeo no han dejado de ser una limitación. A pesar de que los avances tecnológicos nos ofrecen capacidades de transmisión mayores cada vez, con aún más rapidez los dispositivos de captura (cámaras) incrementan la resolución, requiriendo siempre mayor ancho de banda. Hoy día, podríamos decir que la resolución más común es de 2 megapixel (full HD, 1080p, unas 4 veces mayor que la de las cámaras analógicas de resolución 4CIF), pero estamos viendo cómo se abren paso resoluciones mayores como 4 megapixel (4xHD), 4K (UHDTV, aprox. 8 megapixel) e incluso otras muy superiores. Esto obviamente afecta no sólo a la transmisión (local y remota), sino también de forma muy directa a la capacidad de grabación y retención de imágenes en dispositivos de almacenamiento.

Está claro que la tendencia es y parece que será la de aumentar la resolución todo lo posible (mayor calidad, detalle, ángulo de visión, etc.), y también el número de flujos de vídeo para transmitir, visualizar y almacenar. Por lo tanto, la necesidad de reducir el ancho de banda (bitrate) para transmitir y el espacio para almacenar va a seguir siendo una constante.

Todos los formatos de compresión utilizados introducen pérdidas de información. No estamos ante sistemas de compresión sin pérdidas como las que usamos para grandes ficheros (.zip). En esos casos, obtenemos relaciones de compresión que se sitúan en torno a 10:1. Para el vídeo eso no es suficiente, necesitamos ratios de compresión de al menos 100:1 o más. Por lo tanto se trata de aplicar algoritmos que desechen información que se interpreta como menos relevante, esto es, que no disminuyan el valor de las imágenes tanto para visualización en tiempo real como en su uso forense como vídeo grabado. Los estándares de compresión actuales (H.264, H.265) están basados en la cuantificación (pixelización) y la composición de las imágenes mediante fotogramas completos (I-Frames, fotograma JPEG), seguidos de fotogramas que contienen sólo alteraciones de la imagen completa (P-frames, B-Frames). Los algoritmos aplicados tratan de analizar esas variaciones y codificarlas como información lo más reducida posible. Cuando aumentamos la tasa de compresión, básicamente forzamos a una mayor pixelización (y consecuente menor nivel de detalle) y a un descarte mayor de alteraciones de la imagen, con el riesgo de perder información relevante. Otro factor que influye en gran medida en el bit rate es el llamado GOV (o GOP), entendido como el conjunto de fotogramas que muestran

sólo variaciones entre dos fotogramas completos. Como esos fotogramas son de tamaño muy reducido respecto a los completos, cuanto mayor sea el GOV menor será la tasa de bits (bit rate).

El formato H.264 se ha manifestado muy eficiente en la compresión de vídeo para seguridad. Aunque no todos los fabricantes utilizan los mismos perfiles, los reproductores son capaces de interpretar cualquiera de ellos (esencia del estándar). Los distintos perfiles y subperfiles del formato se refieren a los algoritmos utilizados para optimizar la compresión. Entre ellos encontramos el Baseline profile, Main profile, High profile, etc. Aún usando el perfil más avanzado, existen algoritmos del formato que no pueden ser usados para videovigilancia. Esencialmente son aquellos que se aplican a información de vídeo ya grabada y que aprovechan la predicción (sabiendo cómo va a continuar el movimiento) para minimizar el tamaño de los ficheros de vídeo. Lamentablemente eso no es aplicable en tiempo real ya que no podemos aventurar los movimientos o cambios de escena a futuro. Llegados a este punto conviene mencionar que los estándares de compresión se desarrollan especialmente para su utilización en la televisión comercial, las grabaciones profesionales de vídeo y el streaming de imágenes. Esto implica que su eficiencia será mayor cuanto más similar sean las condiciones a las que corresponden a esas aplicaciones. Por mencionar alguna de ellas, como la anterior de la predicción de los fotogramas siguientes, tenemos la relación señal / ruido, muy ligada a la iluminación propia de estudios de televisión, algo poco homologable a las condiciones de iluminación en los sistemas de vigilancia que suele ser mucho más desfavorable. Esta consideración nos ayudará a comprender por qué en vídeo vigilancia no es posible aprovechar todas las capacidades

de los formatos de compresión estándar. Así, aunque puedan ser ciertas las anunciadas mejoras que incorpora el formato de compresión H.265 comparativamente con el existente H.264, es muy probable que esas mejoras se encuentren muy atenuadas cuando la utilización es en el ámbito de la vídeo vigilancia. Es decir, que si esperamos un 50% o más de reducción en el bit rate, posiblemente no obtengamos más allá de un 10-15%.

En los últimos meses, se hace más presente la alternativa del nuevo estándar H.265 como reemplazo del H.264 para ser más eficiente frente a las altas resoluciones de vídeo que se van incorporando (HDTV, UHDTV, etc). La cuestión es si la industria de la vídeo vigilancia debe abrazar este nuevo estándar de manera inmediata para ir resolviendo sus problemas de ancho de banda y espacio de grabación o si existen otras alternativas, y en todo caso, las implicaciones que esas alternativas tienen sobre los sistemas y las inversiones a realizar.

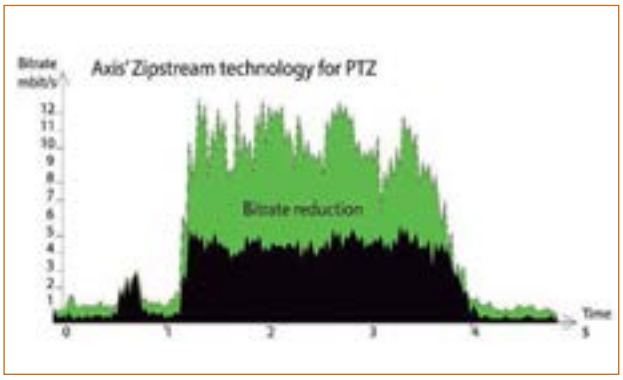
Cuanto más avanzado y eficiente es un formato de compresión, dado que se apoya en complejos algoritmos, precisa de mayor potencia de procesador para su codificación (dentro de una cámara para entendernos) y mucha mayor potencia de proceso aún para su descodificación (para reproducirlo). Esto es aplicable para los distintos perfiles de un mismo formato y por supuesto también al avance desde H.264 hacia H.265. Por ello, podemos entender que una cámara que codifique en H.265 tiene que utilizar más recursos de procesador que una que lo haga en H.264. Esos recursos podrían ser necesarios en la cámara para otras funciones que afecten a los procesos de tratamiento de la imagen (mejoras en la calidad de imagen) o bien deben ser aportados por un procesador más potente que sin duda afectará al coste del dispositivo. Además, si el vídeo se codifica en H.265, los dispositivos de monitorización y reproducción deben ser capaces de descodificarlo, lo que implica también más procesador y posiblemente equipamiento de grabación/reproducción nuevo.

¿Debemos concluir entonces que tendremos un extra coste debido al nuevo equipamiento (cámaras y grabadores) si queremos mejorar nuestra eficiencia en la compresión? No necesariamente en ese sentido.

Durante los últimos dos años, han aparecido en el mercado alternativas intermedias a la migración H.264 -> H.265. Se trata de formatos de com-

presión que manteniendo el estándar H.264 incorporan nuevos algoritmos y técnicas que ayudan a reducir el bit rate de manera muy sustancial. Estas nuevas técnicas de compresión reciben diferentes nombres comerciales pero se engloban en una denominación genérica que se conoce como Smart Codecs.

Estas nuevas técnicas pretenden aprovechar al máximo el estándar H.264 sin salirse de éste, evitando así cualquier cambio obligado de equipamiento en la grabación y reproducción. Se aplican sobre los principios básicos de la compresión tratando de eliminar información irrelevante, mientras se mantiene la calidad aparente del vídeo y su nivel de detalle. Las más avanzadas se orientan a usar algoritmos de análisis de contenidos para establecer las áreas de interés en la escena que deben ser codificadas con menor compresión (más calidad), mientras que mantienen un nivel mayor de compresión en el resto de la imagen. Por lo tanto respecto al estándar normal, diríamos que tienen un grado de compresión variable en función de los contenidos. Otro aspecto en el que incidir es el de la longitud del GOV. Veíamos anteriormente que un GOV mayor reduce considerablemente la tasa de bits, pero puede perjudicar la calidad de imagen cuando existe mucha actividad. Bien, las nuevas técnicas aplican un GOV de longitud variable según la actividad en la escena, reduciendo enormemente el bit rate en los periodos de inactividad (tan abundantes en escenarios de vigilancia). Por último, y no menos relevante, se añaden técnicas de adaptación de la velocidad de refresco o frame rate. Esto es, el número de fotogramas por segundo. Es cierto que cuando tenemos actividad deseamos una mayor velocidad de imágenes por segundo. Típicamente entendemos 25 ips como el máximo, pero hoy podemos obtener 50 ó 100 en algunos modelos de cámara. Sin embargo, solemos adaptar un compromiso de imágenes por segundo que nos ofrezca suficiente información a la vez que no sature nuestra capacidad de transmisión ni agote nuestro disco duro en pocas horas o días. Pues bien, algunos de estos Smart Codecs consiguen adaptar dinámicamente las imágenes por segundo según haya o no actividad en la escena, resultando de nuevo en una enorme reducción de la tasa de bits cuando no existe movimiento. Otros algoritmos, orientados a la identificación del ruido en imágenes con baja iluminación (típicamente nocturnas) proporcionan ahorros en el espacio de grabación que nos resultarán inesperadamente sustanciales. Estos Smart Codecs están disponibles con algunos fabricantes también para su utilización en cámaras motorizadas PTZ.



El uso de estas nuevas técnicas de compresión puede ofrecernos reducciones de la tasa de bits que oscilan entre el 10% y el 80% según la escena y el momento del día. Sin duda pueden ser en muchos casos más eficientes que las mejoras que nos aportaría una eventual migración a formatos de compresión H.265. No obstante, la prudencia y la diversidad de la oferta comercial invita a realizar test y pruebas para poder estimar con solvencia si estos formatos aportarán los resultados esperados. Hay que resaltar que dado que estas técnicas se han desarrollado de modo particular por cada fabricante, no todas ofrecen la misma eficacia, tanto en la pretendida reducción del bit rate como en la necesaria preservación de la calidad del vídeo resultante.

Los Smart Codecs no son una alternativa que pretenda sustituir la adopción del nuevo estándar H.265 a medio o largo plazo. Ni siquiera está descartado que puedan usarse técnicas similares sobre el H.265 que mejoren incluso el nuevo estándar. Lo que pretenden estos formatos es mejorar la eficiencia del H.264 ofreciendo rendimientos similares o superiores al nuevo H.265, mientras la ley de Moore (que vaticina la continua mejora de los procesadores) y la evolución del mercado convierte en menos onerosa e incómoda la adopción del estándar H.265 y cualquier otro que nos depare el futuro.

Fotos: Axis Communications

Contactos de empresas, p. 8.

LA SEGURIDAD QUE DESEA A LA MEDIDA DE SUS NECESIDADES.

Captúrelo en PURPLE

Escálelo en GOLD

Discos duros para vigilancia WD®

wd.com/purpose

2178-800151-B75 Sept 2016

JORDI ALONSO. JEFE DE PRODUCTO DE CCTV. CASMAR

Resolución 4K y **compresión H.265**

Resolución UHD, 4 veces más de información

Muchos de nosotros nos vimos casi obligados a cambiar nuestro viejo televisor de tubo por uno de tecnología LCD con resolución HD Ready. Al poco tiempo el HD Ready (capaz de reproducir resoluciones 720p y 1080i) ya no valía y el LCD tampoco, había que volver a cambiarlo por uno de resolución Full HD (capaz de reproducir resolución 1080p) y tecnología LED. Bien, pues parece que ahora le ha llegado el turno al UHD (también llamado 4K), que con una resolución 4 veces superior al Full HD (3840x2160 pixeles en lugar de los 1920x1080 que ofrece éste) promete imágenes con mayor detalle y mayor sensación de realismo.

NO es que mañana mismo vayamos a estar todos disfrutando de esta resolución en casa, pues la actual TDT tiene considerables problemas para transmitir en 720p, como demuestran algunas publicaciones que se han preocupado de analizarlo. De hecho, el actual estándar europeo de transmisión (DVB) no está preparado aún para soportar varios tipos de transmisión 4K, lo que retrasará su implantación por lo menos hasta 2018, por lo que habrá que esperar bastantes años hasta que los canales convencionales de cada país emitan en esta resolución. Es cierto que ya existen canales vía satélite que ofrecen contenidos en resolución 4K, pero pasará mucho tiempo hasta que podamos disfrutarlo en nuestro día a día.

Aplicaciones actuales del UHD

¿Para qué sirve entonces el UHD? La cadena de televisión norteamericana Fox ya encontró una respuesta y utilizó esta tecnología en la final de la Super Bowl 2014. La propia cadena reconoce que pasarán muchos años antes de que puedan retransmitir en directo en esta resolución, pero han aprovechado la grabación 4k (equivalente a 8 Megapíxeles) para ofrecer a sus espectadores la función Superzoom de las repeticiones, consiguiendo imágenes ampliadas de las jugadas más interesantes en resolución 720p (resolución en la que se retransmite en directo actualmente el partido, equivalente a 1,3 Mpx). Y es aquí donde todos los que nos dedicamos a la seguridad vemos rápidamente la aplicación de esta tecnología. La posibilidad de ampliar detalles de imágenes grabadas para su posterior análisis es algo que nuestros clientes demandan diariamente, y es evidente que disponer de más información facilita esta tarea.

Compresión HEVC, más eficiente

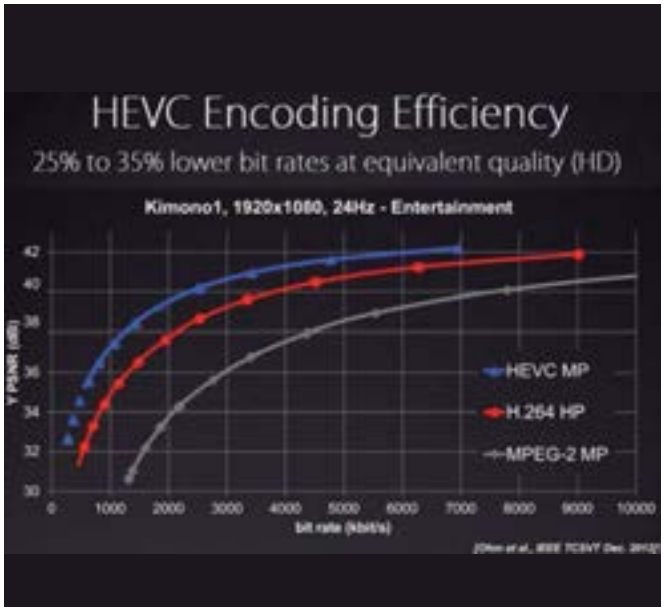
La contrapartida de disponer de tanta información es el flujo de datos que se genera, ya que, del mismo modo que es un problema para las cadenas de televisión, también lo es para nuestras redes y gra-

badores actuales. Conscientes de que parte de la solución pasa por disponer de una compresión más eficiente, las primeras pruebas realizadas utilizan ya la nueva compresión HEVC (High Efficiency Video Coding), también conocida como H.265 y desarrollada conjuntamente por los grupos MPEG y VCE. Ya han transcurrido tres años desde que se publicara su primera versión y se estima que su relación de compresión duplica al ofrecido por el H.264, lo que permite transmitir la misma calidad que en H.264 utilizando la mitad de ancho de banda o transmitir imágenes del doble de calidad utilizando el mismo.

Compresión H.265 aplicada al mercado de seguridad

La compresión H.265 se está utilizando ya en broadcast y algunas cadenas de televisión utilizan este tipo de compresión para emitir en HD 720p, con anchos de banda de entre 1 y 2 Mbps (algo casi conseguible con H.264 y cámaras de vigilancia con escenarios estáticos, pero sorprendente cuando hablamos de una emisión en la que no paran de producirse cambios de plano). También en seguridad hay algunas empresas que ofrecen ya este tipo de compresión, aunque aún habrá que esperar para que este formato se convierta en un nuevo standard, la complejidad de esta codificación y la falta de equilibrio entre precio y prestaciones son aún dos de sus mayores inconvenientes. En cualquier caso, la mayoría de fabricantes de CCTV lo tienen ya en su road map y los más importantes lo están ofreciendo en sus catálogos de 2016 - 2017, por lo que parece claro que este nuevo formato de compresión acabará sustituyendo al actual H.264 como este último lo hiciera con el MPEG-4. Tuvimos nuestras pequeñas decepciones cuando el H.264 empezó a llegar a nuestro mercado y hubo que esperar a que la tecnología madurara para ver una mejora sustancial respecto a MPEG-4, pero parece que esto no ocurrirá con la compresión H.265 y los productos que empiezan a llegar ya ofrecen mejoras sustanciales respecto a sus predecesores. ●

Fotos: Casmar



Contactos de empresas, p. 8.

CARLOS MARTÍNEZ. RESPONSABLE DE CONSULTORÍA DE CUEVAVALIENTE INGENIEROS

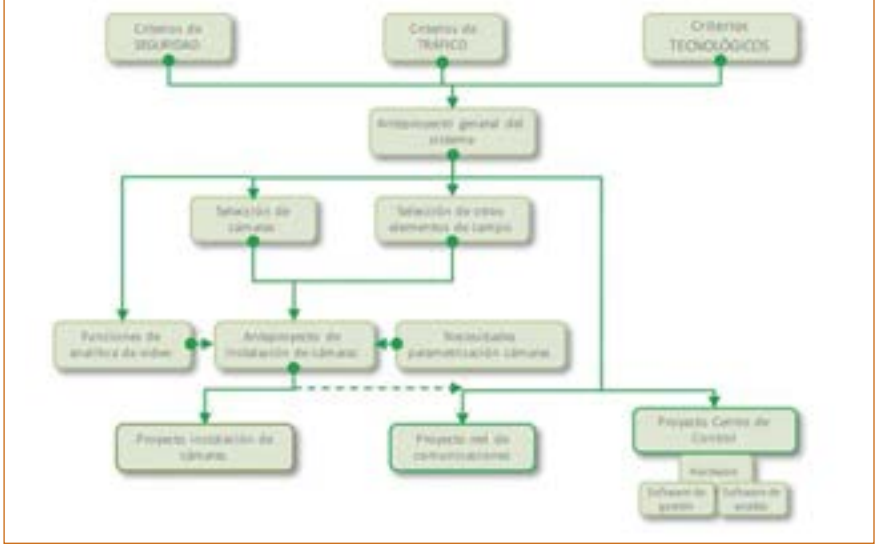
Televigilancia en ciudades

Breve análisis metodológico del proyecto

La televisión, en su perspectiva de circuito cerrado, se comenzó a utilizar en entornos privados con fines de seguridad en la pasada década de los 70, irrumpiendo en al ámbito público en la década de los años 90 como complemento a la vigilancia personal que realizan las policías en las ciudades. Este fenómeno comenzó en Europa, siendo el Reino Unido uno de los máximos exponentes, disponiendo hoy del mayor sistema de videovigilancia del mundo en entornos públicos. En el extremo opuesto, hablando de capitales europeas, se encuentra Dinamarca, país muy restrictivo en los permisos para este tipo de instalaciones.

APESAR de todas las controversias que se suscitan entre seguridad, privacidad, anonimato y otros derechos ciudadanos, se puede afirmar que las grandes ciudades occidentales disponen de sistemas de vídeo para la gestión de la seguridad y también del tráfico. Si bien, respecto a su efectividad en la lucha contra la delincuencia y el terrorismo existen opiniones y estadísticas diversas, incluso contradictorias, sobre su efectividad y rentabilidad, aunque sí parece haber bastante unanimidad respecto a su acción persuasiva y utilidad como elemento de análisis a posteriori.

Proyecto cámara de vigilancia urbana.



En España, la utilización de videocámaras y gestión de imágenes de lugares públicos está regulada por la Ley 4/1997 de 4 de agosto y su Reglamento de desarrollo, Real Decreto 596/1999 de 16 de abril, restringiendo su uso a las Fuerzas y Cuerpos de Seguridad. La propuesta de instalación puede ser solicitada por el delegado o subdelegado del gobierno, los jefes de la comandancia de la guardia civil o de la comisaría provincial (a través de las delegaciones del gobierno), y los alcaldes o concejales con responsabilidades en la seguridad ciudadana. Con el fin de garantizar que no se vulnera ninguno de los principios de utilización establecidos en la Ley, la Comisión de Garantías de la Videovigilancia emite un informe de viabilidad de la instalación.

Entre las restricciones a este tipo de instalaciones cabe destacar la prohibición de registrar audio, la obligación de que las cámaras sean fácilmente visibles, la necesidad de señalizar las zonas videovigiladas y la prohibición de usos

«colaterales» de las imágenes diferentes del fin para el que son captadas.

Por otra parte, el citado reglamento también establece las condiciones para las cámaras destinadas al control de tráfico. Correspondiendo a las Administraciones Públicas con competencia para la regulación del tráfico, autorizar la instalación y el uso videocámaras para este fin.

La evolución tecnológica de la CCTV de la mano del mundo digital, tanto para la captación y creación de imágenes, como para su tratamiento para detectar eventos, generar archivos históricos, etc., pasando por las comunicaciones y la utilización de la fibra óptica, está facilitando la implantación de cámaras de televisión en las ciudades. Esto no significa que el asunto sea sencillo, lejos de ello, se trata de proyectos complejos, que precisan de experiencia y profundos conocimientos, tanto de diversas tecnologías como de los aspectos operativos del sistema. Además, a la complejidad del diseño se une el número de puntos de vigilancia a establecer que suele ser elevado, lo que obliga a un exhaustivo control del desarrollo e implementación posterior del proyecto.

En los párrafos que siguen se desarrollan, en función de nuestra experiencia, algunos criterios metodológicos que deben considerarse para llevar a buen término la elaboración de un proyecto de videovigilancia urbana.

• **Definición de necesidades**.- La tecnología es un medio para lograr un fin, siendo la definición de este fin el primer paso del proyecto. La necesidad que se percibe por parte de los gestores de las ciudades, normalmente cuerpos policiales y los responsables de tráfico, es disponer de imágenes en tiempo real y grabadas para gestionar la seguridad –o quizás la inseguridad– y el tráfico, pudiendo además hacer análisis forenses de acontecimientos pasados. Por tanto, se hace imprescindible la presencia de los citados gestores en la definición del alcance del proyecto: cuáles son los riesgos, criterios para decidir los lugares donde se necesita vigilancia, qué áreas se desean vigilar en cada lugar, con qué nivel de detalle, qué recursos se destinarán a la operación, si tendrán que generarse alarmas automáticas ante determinados eventos, qué legislación y normativa aplica, si son necesarias cámaras de despliegue rápido, envío de imágenes a unidades de respuesta en la calle, etc.

Ejemplo de mapa de resoluciones utilizado en el proyecto para aplicaciones de análisis de imagen

• **Anteproyecto general del sistema**.- Conocidas las necesidades, se estará en condiciones de establecer un primer anteproyecto técnico que aporte las soluciones; un documento que recoja aspectos tales como: funciones de ese punto de supervisión, qué tecnología utilizar, qué tipos de cámaras se van a necesitar, dónde se instalarán, cómo serán las comunicaciones y redes de datos con el centro de control, cuál será su topología, cómo se realizará la integración y centralización del sistema, qué hará el software de gestión y grabación, cómo será el análisis de imágenes y qué eventos debe detectar en cada escenario. En resumen, qué tipos de elementos son necesarios y cómo deben ser las interdependencias entre ellos.

• **Selección de Equipos y software**.- Definido lo anterior, es necesario establecer las prestaciones de las cámaras y resto de elementos del sistema de campo, la red de comunicaciones, la configuración del centro de control y las capacidades de los elementos que lo integran, el software de gestión de cámaras, grabaciones y eventos, el software de análisis de vídeo, etc.

• **Elaboración de anteproyectos de cámaras.**- Una vez acordadas y cerradas las cuestiones precedentes, llega el momento de realizar una de las primeras acciones de campo: determinar las zonas a controlar y establecer las posibles ubicaciones de las cámaras. Para ello, lo más práctico es disponer de cartografía georreferenciada del sitio, obtener imágenes fotográficas de las vías que quieren vigilarse y de los servicios o establecimientos que se desean controlar. Es importante considerar las condiciones de iluminación urbana por si fuera necesario su refuerzo o la instalación de elementos de iluminación adicional (infrarroja, láser, etc.), en la propia cámara.

Con los datos citados se definirán las mejores opciones teóricas de ubicación de cada cámara. Dada la diversidad de arbolados, jardinería, paneles de señalización y publicitarios, mobiliario urbano, toldos y marquesinas de los edificios y otros elementos que pueden obstruir el campo de visión, es conveniente realizar tomas de imagen en altura (la prevista de instalación) desde la ubicación de la cámara para comprobar su viabilidad. Es sorprendente la diferencia de visión entre las imágenes captadas a nivel de suelo y en altura. Nuestra experiencia nos indica que dedicar tiempo a tomar fotografías desde

varios puntos y no sólo desde el elegido a priori es un pequeño esfuerzo que ahorra la repetición de visitas y facilita la toma de decisiones.

Las cámaras son elementos vitales de la solución y, con el estado actual de la tecnología, lo lógico es utilizar cámaras megapíxel, con formato 16:9, fijas o móviles, dotadas de zoom con multiplicador suficiente en función del escenario.

En los casos que sea de aplicación la detección automática de eventos o la realización de identificaciones, es necesario asegurar que la resolución de las imágenes son adecuadas para realizar el análisis de vídeo pertinente, ya sea de registro de matrículas, reconocimiento facial o de acciones relacionadas con el tráfico: vehículos en dirección contraria, aparcados, embotellamientos, etc.

El segundo paso lógico será la realización del proyecto de instalación y parametrización de las cámaras, considerando desde el elemento de soporte de las cámaras, hasta la ubicación de los puntos red de comunicaciones y energía, incluyendo la parte de ingeniería civil necesaria de conducciones.

• **Proyecto de la red de comunicaciones.**- En paralelo deberá realizarse el proyecto de la red de comunicaciones, dimensionando su capacidad para el flujo de datos máximo que vaya a recibir. La utilización de cámaras megapíxel, que puede ser más de una en determinados puntos, junto con una frecuencia de envío de imágenes en tiempo real, la compresión utilizada y la diversidad de stream enviados determinará las capacidades de cada sección de la red que se realice.

La seguridad de la red es también un importante factor a tener en cuenta, tanto la seguridad física como la lógica y, en el caso de utilizarse en alguna fase una empresa proveedora de servicios de telecomunicaciones, hay que considerar los acuerdos de confidencialidad que deban establecerse y las garantías sobre calidad y seguridad del servicio.

• **Proyecto del centro de control.**- Una vez resueltas las comunicaciones y llegados al centro de control, los datos de imágenes deberán encontrar los equipos de grabación dimensionados con capacidad suficientemente en función de los periodos definidos de almacenamiento, con dispositivos de seguridad alternativos en caso de fallo; los servidores con el software de gestión, las bases de datos, los históricos de eventos, la gestión documental, etc.; los elementos de visualización, monitores y videowall.

El proyecto del centro de control debe tener el nivel de detalle suficiente para garantizar la compatibilidad y manejabilidad de todos los elementos. Contendrá también el diseño racional del mismo desde el punto de vista del mobiliario y su disposición que estará realizado con criterios ergonómicos.

La gestión comprende, entre otras funciones, la selección de cámaras desde un sistema cartográfico, la distribución de imágenes en los distintos monitores y videowall, la gestión de alarmas de la detección automática de eventos, la gestión de las unidades de grabación, las herramientas de búsqueda de imágenes y eventos grabados, la gestión de operadores y sus privilegios, la aplicación de las consideraciones relativas a la legislación LOPD, etc.

Respecto al análisis de imágenes deberán establecerse los eventos a detectar y a registrar, y calcular el número de licencias necesario de los distintos tipos en función del número de cámaras en los que habrá que aplicarlas y el conocimiento estadístico de utilización simultánea esperable.

Como se puede deducir de las acciones anteriores, este tipo de proyectos precisa para su desarrollo un equipo multidisciplinar que reúna a expertos de diferentes materias que trabajen en colaboración con los fabricantes, sobre todo de los software de gestión y análisis de imagen, y un equipo de campo para la toma de datos, tanto de ubicación de las cámaras, como para el estudio de alternativas de tomas de energía eléctrica y nodos de datos. En este último equipo es muy conveniente contar con la colaboración de las compañías que suministran energía a la ciudad y las que proporcionen los servicios de telecomunicaciones. ●

La LOPD determina la necesidad de notificar que hay CCTV.

Fotos: Cuevavaliente

Contactos de empresas, p. 8.

UNA CUIDADA SELECCION DE PRODUCTOS Y SISTEMAS DE VIDEO Y TELECOMUNICACIONES DE ALTO VALOR, ACOMPAÑADO DE UNA SINGULAR ELEGANCIA Y GRAN FUNCIONALIDAD, PARA EL USUARIO ACTUAL DENTRO DE UN ENTORNO DE ECONOMIA COMPETITIVA

AVITOM

902 AVITOM | 902 284 866
marcom@avitom.es | @avitom_es

MADRID
C/ León 5/7
Polígono Industrial Cobo Calleja
Fuenlabrada | 28947 – Madrid | España
Tel: 916 420 236 – 916 420 601

VALENCIA
Avda. Mas de L'Oli – 13
Polígono Industrial La Cova
Manises | 46940 – Valencia | España
Tel: 963 218 307 – 961 543 342

BARCELONA
C/ Manuel Fernandez Márquez S/N – Nave 7
Polígono Industrial Badalona Sub
Badalona | 08918 – Barcelona | España
Tel: 933 883 181

CENTRAL LOGISTICA
C/ Lepanto – 70
Numancia de la Sagra | 45230 – Toledo | España
Tel: 925 516 797

WWW.AVITOM.ES

ALFREDO GUTIÉRREZ. BUSINESS DEVELOPMENT MANAGER PARA IBERIA DE MOBOTIX AG

Entornos de **alta seguridad**

¿Qué deben ofrecer las cámaras de seguridad?

Vigilar zonas de seguridad de la forma más exhaustiva posible para garantizar respuestas rápidas supone un gran reto. Actualmente, las tecnologías modernas ayudan a sus responsables a llevar a cabo esta importante tarea. Entre las zonas particularmente delicadas se incluyen instalaciones como tribunales o prisiones. No se trata tan sólo de impedir los intentos de fuga de sospechosos o condenados, sino de garantizar la seguridad de todas las personas que se encuentran en las instalaciones, incluidos los empleados

UN componente esencial de cualquier estrategia de seguridad es el control visual de las áreas y edificios mediante cámaras. Sin embargo, no todas las soluciones de cámaras que se pueden encontrar actualmente en el mercado cumplen los exigentes requisitos necesarios para entornos de alta seguridad.

Multiplicidad de criterios

Debido al carácter delicado de este tipo de instalaciones, los sistemas de seguridad y cámaras que se instalen en ellas deben satisfacer unas condiciones particularmente estrictas. Un factor esencial es la resolución de las cámaras: en las instituciones penitenciarias, los reclusos suelen llevar la misma ropa. Para poder identificar a las personas implicadas en un altercado es por tanto imprescindible que su cara sea claramente reconocible en las grabaciones, de modo que la calidad de la imagen debe ser fiable en cualesquiera que sean las condiciones lumínicas, por ejemplo, a contraluz o al anochecer.

Otro de los puntos importantes es que las cámaras instaladas sean robustas y no requieran mantenimiento. Por un lado, deben estar protegidas de eventuales daños, por ejemplo, en caso de ataques vandálicos. Por otro, deben poder soportar condiciones meteorológicas desfavorables y temperaturas extremas cuando se utilizan en exteriores y, además, estar siempre en funcionamiento con el mínimo mantenimiento.

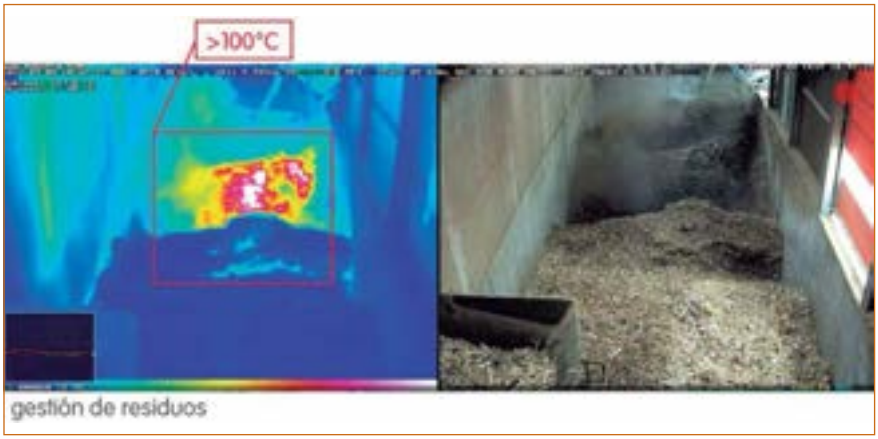
Funciones adicionales

En relación a sus funciones, es importante que los sistemas de cámaras también permitan el control acústico o la intercomunicación mediante altavoces y micrófono. En las puertas o entradas de las zonas de seguridad, la comunicación con la persona que está ante la puerta o la posibilidad de encender la luz a distancia suelen ser decisivas. Así, al elegir una cámara de seguridad, otro de los criterios importantes será que incorpore una función de audio de calidad.

Por último, aunque no por ello menos importante, al elegir el sistema hay que tener en cuenta la alimentación eléctrica y la manera de conectar las cámaras. Así, por ejemplo, una alimentación por Power Over Ethernet permite ahorrarse el doble cableado (red y electricidad) en el momento de realizar la instalación. Mediante una gestión de memoria inteligente y directa en un servidor NAS o de archivos, se hacen innecesarios los grabadores de vídeo digitales. Esto es sinónimo de una seguridad mucho mayor con unos costes mucho menores, puesto que este tipo de solución permite reducir los costes totales de almacenaje hasta diez veces.

El condado de Bergen apuesta por una solución de vídeo moderna

La mejor manera de ilustrar el uso de cámaras en el marco de un concepto de seguridad integral es con un ejemplo práctico. Recientemente, los responsables de los edificios judiciales y penitenciarios de Bergen, Nueva Jersey (EE. UU.) –con capacidad para 1.200 personas– abordaron la modernización de su sistema. El condado de Bergen abarca 70 municipios y es la mayor autoridad de la región en materia penal. La solución existente, que contaba con un sistema informático para vigilar toda la zona de los reclusos, un sistema de seguridad integrado en el muro de la prisión, un sistema de alarma para todas las instalaciones y una sala de control, debía ampliarse con un sistema de cámaras moderno que ofreciera más funciones que el sistema analógico utilizado hasta ese momento.



gestión de residuos

Fotos: Mobotix

Contactos de empresas, p. 8.

EQUIPO TÉCNICO Y DE MARKETING. AVITOM

La convergencia de los **sistemas de vídeo**

Nuevos formatos de compresión

Hoy en día, estamos en la era de la información, y cada vez más son los sistemas que interactúan unos con otros, superando el reto de la conectividad. Usemos los medios de transporte como ejemplo, ya que es quizás el sector donde está cambiando más rápido y de una forma más radical de lo que pensamos.

LOS diferentes sistemas de transporte mueven millones de pasajeros al día; con la amenaza del terrorismo y otras actividades delictivas en aumento, ha habido una mayor conciencia de las amenazas, de todo tipo, contra el transporte público, sea aéreo, marítimo, ferrocarril o terrestre, y en las vulnerabilidades particulares de cada uno de estos medios, convirtiendo la protección de personas y bienes en una prioridad.

Pero al mismo tiempo, no debemos de olvidar que las personas ya no ven el transporte como una interrupción en su rutina del día a día. Los viajes se han convertido en parte de nuestra vida diaria, y los pasajeros deben tener acceso fluido y rápido a las diferentes infraestructuras de transporte, y a la información actualizada al minuto, sobre eventos o emergencias.

Hoy en día, el transporte es uno de los primeros usuarios del IoT (Internet de las Cosas) y por tanto de grandes volúmenes de datos. Dispositivos y sensores a lo largo de las infraestructuras de los diferentes terminales interiores, contribuyen a aumentar la conciencia de la situación a los operadores y a mantener el control y la seguridad de los sistemas de transporte. Es por todo esto que cada vez más los operadores están confiando en los datos para optimizar la gestión, el control, la supervisión y la seguridad. Pero también, hoy en día, existe la necesidad de una explotación adecuada de las terminales del transporte, para que sean capaces de generar más ingresos y beneficios o retornos de inversión. Conociendo y estudiando comportamientos, estableciendo estrategias de marketing enfocadas y dirigidas a optimizar los ingresos y ofrecer al mismo tiempo, a los usuarios de transporte y por tanto de sus infraestructuras, una experiencia más personalizada, ayudando a que su estancia sea agradable y productiva.

Todo esto hace que se esté tomando un giro decisivo hacia el uso, cada vez mayor de la Tecnología y los Datos, o Big Data.

Dentro del Big Data, el vídeo, las imágenes obtenidas por las cámaras instaladas a lo largo de estaciones, terminales, etc., son probablemente una herramienta fundamental para lograr todos estos objetivos: La seguridad, el control y la gestión, y la explotación efectiva de recursos.

Sistemas de vídeo

Los sistemas de vídeo, ayudan a los operadores a la hora de cumplir con sus objetivos en sus diferentes áreas de actuación -Seguridad, Gestión, Explotación-, el uso de grandes volúmenes de datos, generados por un creciente número de cámaras, es cada vez mayor, convirtiéndose la imagen, y por tanto los datos, en «inteligencia procesable», mostrándose como necesarios para mantener un alto nivel de Control y Seguridad en estos entornos. El análisis de todos estos datos permite obtener información fundamental para el control, análisis e identificación de información crítica y ayudar a entender, gestionar, prevenir, responder, mitigar el riesgo y hacer frente a eventos, gestionando situaciones de emergencia y analizando los incidentes, utilizando las imágenes y la información que se les proporciona. Sin embargo toda esta magnitud de datos, de vídeo en concreto, se ha convertido en un desafío ya que trae consigo un inevitable aumento de inversión en la infraestructura de equipos de grabación y almacenamiento.

Formato H-265

Gracias a la evolución constante de la tecnología en los sistemas de captación y almacenamiento de vídeo, es ya una realidad, la adopción del formato estándar de compresión H-265, con una codificación de la señal de Vídeo de Alta Eficiencia.

Una de las principales ventajas de H265-HEVC es la capacidad de codificar de modo muy eficiente los formatos de imagen de muy alta resolución como los nuevos UHDTV, con precisiones por encima de los 10 bit/pixel gracias a su nueva estructura de bloques, y a la capacidad de utilizar transformadas de gran tamaño hasta de 32×32 pixeles. Los nuevos equipos de cámaras 4K se pueden codificar con tasas binarias que varían entre 10Mbps y 15Mbps, que implica rangos de compresión muy cercanos de 500:1.

«Una de las principales ventajas de H265-HEVC es la capacidad de codificar de modo muy eficiente los formatos de imagen de muy alta resolución como los nuevos UHDTV»

El nuevo formato de compresión supone una evolución respecto de los formatos usados hasta el momento, ya que permite una mejora notable en la obtención de imágenes de mayor resolución, mejora del rango dinámico extendido, mejora de la representación colorimétrica de la imagen, mejora de la gestión del tráfico de datos –Anchos de Banda; Tasa de Bits–, y la mejora de eficiencia de la compresión de esta codificación, que puede hacer que sea posible el acceso al vídeo a través de las redes existentes y futuras e incluso sobre conexiones más lentas, como redes móviles con ancho de banda insuficiente para usar el anterior formato H.264, y distribuirlas por los canales de radiodifusión existentes y futuros con una reducción de hasta el 50%, en equipos de almacenamiento de imágenes, ya que la gestión de las imágenes de vídeo se realiza como si fuesen simples datos digitales, pudiendo almacenarlas en diversos tipos de medios de almacenamiento, manteniendo una disponibilidad y volumen de datos adecuados

para una gestión óptima de filtrado, aplicando diferentes sistemas e Inteligencia de análisis de vídeo.

Gracias a estos avances en las tecnologías de compresión y almacenamiento, el vídeo puede ser almacenado por períodos de tiempo más largos, y con mayor nivel de detalle, lo que ayudará a investigadores y operadores a mejorar procedimientos.

Todas estas grabaciones son esenciales para identificar con éxito la actividad criminal y asegurar que los responsables puedan ser procesados por las autoridades, pero también conviene saber que un elevado porcentaje de la actividad capturada por la vídeo vigilancia es irrelevante, y por tanto se necesitan herramientas de filtrado. Sin soluciones de inteligencia de vídeo de alto rendimiento y análisis de vídeo, ya sea integrado en la cámara o de un tercero, el análisis de imágenes de vídeo seguirá siendo una tarea considerable.

El estándar H-265 HEVC permite gestionar el vídeo sobre las actuales analíticas y otras aún por venir, aprovechando las singularidades y ventajas de los diferentes fabricantes, alertando al instante de anomalías o irregularidades, y la interacción de los operadores con los diferentes sistemas de control existentes en las Terminales de Transporte, a través de la integración de todos estos sistemas sobre plataformas VMS, capaces de gestionar todo este flujo de información.

> «El estándar H-265 HEVC permite gestionar el vídeo sobre las actuales analíticas y otras aún por venir»

Analíticas de vídeo

Sobre estas plataformas de gestión VMS no solo es posible visualizar los sistemas de vídeo existentes, sino también gestionar analíticas de vídeo. Con la analítica de vídeo se pueden definir zonas de control, asegurando que los pasajeros no se crucen o accedan de forma inadecuada, generando automáticamente alertas instantáneas cuando alguien cruza las líneas o zonas definidas como prohibidas, permitiendo su control y seguimiento, o ser capaz de consultar e identificar personas por el color de su ropa, o seleccionar a las personas que caminan en una dirección especificada; llamar la atención sobre persona o personas andando en dirección errónea o controlar la gestión de colas, el flujo de tráfico, o si se mueve más rápido que el flujo de tráfico estándar, y comprobar la velocidad de interacción con accesos, torniquetes, escaleras mecánicas, elevadores o cintas transportadoras, pueden ayudar a los operadores a abrir accesos y optimizar la utilización de equipos y personal evitando aglomeraciones, y en evitación de accidentes (nivel de dióxido de carbono), e incluso, tomar decisiones de marketing, reforzando el servicio al cliente y mejorando su satisfaccion.

Pero además de la gestión de eventos en tiempo real, también se necesitan datos de vídeo para las investigaciones y análisis posteriores al evento.

Los datos recogidos de los torniquetes, controles de acceso en entradas, por ejemplo, pueden ayudar al operador o redirigir pasajeros. Sensores que detectan un cambio en la temperatura pueden activar el sistema de climatización. Estas son solo algunas de las formas en que los operadores serán capaces de gestionar toda la información disponible, los datos.

Como vemos el objetivo principal de todo esto es sobre todo la seguridad y la seguridad de los pasajeros. Sin embargo, existen múltiples aplicaciones más, y todo este análisis sólo ocurrirá si abrimos el acceso a integraciones de datos y usos de estándares, de modo que los operadores y proveedores de servicios pueden obtener toda la información necesaria, facilitando a los viajeros la información y los servicios que necesitan, cuando lo necesitan.

Fotos: Avitom/Pixabay

Contactos de empresas, p. 8.

DALLMEIER

Entretenimiento en Full HD, en el Studio City de Macao

Glamour, excitación y diversión: con Studio City, Melco Crown Entertainment ha marcado un nuevo hito en Macao. También hay superlativos en tecnología de vídeo: el fabricante y experto en CCTV/IP con sede en Ratisbona, Alemania, ha instalado aquí el sistema de vídeo Full HD para casinos más grande del mundo con varios miles de cámaras IP.

STUDIO City es un resort de entretenimiento inmenso que no tiene parangón a nivel global. Aquí todo gira en torno al mundo de las películas y el cine. Inspirado por Hollywood, Studio City ofrece emociones de todo tipo, no sólo en el casino glamuroso con sus innumerables mesas de juego y botes increíbles, sino también en las muchas otras atracciones que tematizan el mundo del cine. Quien busca nuevas sensaciones, las encontrará seguramente en «The House of Magic» con magos de fama mundial, o en el «Batman Dark Flight», un vuelo de simulación 4D. Un lujoso hotel con 1.600 habitaciones, una selección internacional de restaurantes exquisitos y una calle comercial inspirada en Nueva York y Hollywood con marcas de diseñadores de fama mundial completan la oferta. El resort incluso alberga la noria con forma de ocho más alta del mundo.

El sistema de vídeo también es único en el mundo: el sistema completo de seguridad por vídeo se basa al cien por cien en tecnología IP y proporciona una calidad de imagen Full HD sobresaliente en todas las áreas. Junto a otros casinos del grupo Melco Crown Entertainment –City of Dreams Macau, City of Dreams Manila y Altira Macau– ahora Studio City también entra en la larga lista de clientes del fabricante bávaro.

Leroy Daniel, Executive Director MCE Surveillance Operations, explica los retos y singularidades del sistema de seguridad de vídeo.

—¿Qué es lo especial del sistema de seguridad de vídeo en Studio City?

—El sistema de seguridad de vídeo de la firma alemana es el primer sistema del mundo cien por cien IP Full HD end-to-end de este tamaño, de estas dimensiones y de esta complejidad dentro del sector de casinos.

—¿Cuáles fueron los motivos principales para elegir esta empresa?

—Fue el socio de nuestra elección por diversas razones: primero, el sector de casinos es el campo de aplicación más exigente para los sistemas de vigilancia en el mundo hoy en día. Aeropuertos, cárceles, centros comerciales, universidades, instalaciones militares, vigilancia de ciudades u otras áreas de aplicación…, sólo en los casinos hay una concentración comparable de cámaras por metro cuadrado, en ningún otro sitio las demandas del tiempo real por parte de usuarios individuales son tan altas como en esta área. Existen muy pocos sistemas que satisfacen perfectamente exigencias de tan alto nivel, sobre todo, cuando se trata de sistemas

Vista externa de Studio City.

Studio City es un resort de entretenimiento.

Full IP. ¡Este fabricante germano es el mejor de ellos!

La excepcional calidad de imagen de las cámaras de esta firma también ha influido en nuestra decisión. Las cámaras móviles y fijas Full HD ofrecen una resolución extraordinaria y una función de zoom excelente. En la vigilancia de casinos, ¡la resolución de detalles juega un papel crucial y puede marcar la diferencia en eventos o incidencias!

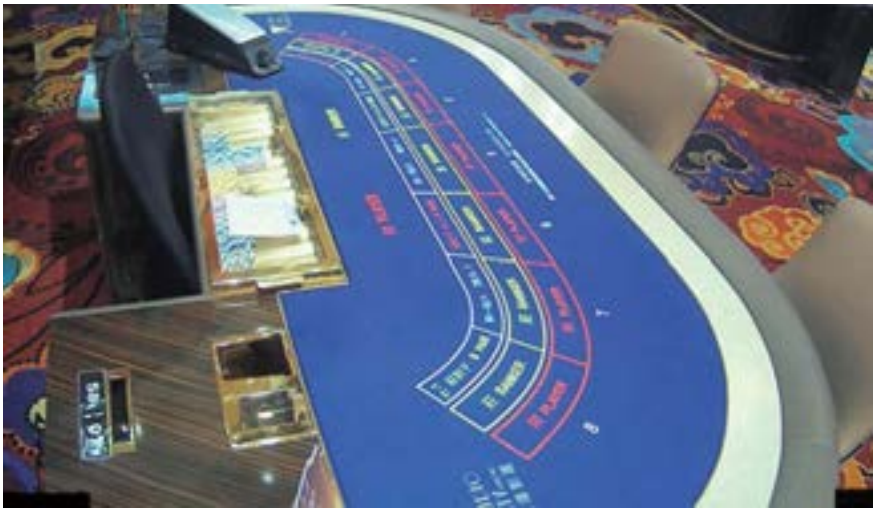
Otro factor decisivo era la posibilidad de ajustar las cámaras mediante una configuración global. Eso significa menos tiempo en escaleras y menos interrupciones en nuestras actividades diarias.

La tecnología de esta empresa bávara es sinónimo de un sistema probado, resistente, con máxima capacidad de rendimiento y disponibilidad. Y sin olvidar la posibilidad de poder adaptar individualmente interfaces de alto y bajo nivel directamente a todos nuestros flujos de ingresos de negocio y sistemas asociados.

Leroy Daniel explica también qué instalaciones se vigilan exactamente con el sistema de vídeo.

«Con el sistema monitorizamos todas las áreas que pertenecen a Studio City: zonas de juego, bulevares comerciales, torres hoteleras, instalaciones de entretenimiento, Back-of-House, áreas de dinero en efectivo y cámaras acorazadas, puntos de venta, aparcamientos, zonas de alta seguridad, perímetro y todos los espacios públicos.

Vista de un tablero de juego desde una cámara HD 1080p.



Más de 6.000 cámaras de red Full HD son grabadas en appliances de vídeo fiables. Adicionalmente, servidores 'standby' y 'failover' proporcionan máxima disponibilidad de todos los datos.

—¿Cuál fue el mayor desafío en este proyecto?

—El mayor reto para nosotros fue la complejidad de la arquitectura del edificio, tanto en cuanto al concepto general como en cuanto al diseño de los techos y las correspondientes instalaciones. Las dificultades surgieron cuando otros elementos de la infraestructura como la iluminación, sistemas contra incendios, ventilación, singularidades de diseño, megafonía y sistemas de sonido estaban montados en el mismo lugar del techo donde había que instalar las cámaras.

Los diseñadores tienden a dar prioridad a la forma sobre la función; en cambio, a los técnicos, más prácticos, les importa más la función que la forma. Y aún así, en una estrecha colaboración con arquitectos y diseñadores es posible encontrar un equilibrio entre función y forma. De esta manera, las cámaras IP (funcionando por cableado CAT-6 y con baja emisión térmica) pudieron ser integradas estéticamente en el diseño del techo o las arañas de cristal. Esto lo hemos logrado muy bien.

—La firma alemana ha desarrollado también una cámara especial para ustedes…

—Sí, es correcto. Pit-View, una cámara HD 1080p pequeña que encargamos específicamente y que está orientada a nuestras necesidades. Ha sido integrada en todos los paneles informativos de las mesas de juego para por fin quitar las cámaras de vigilancia del techo y llevarlas a la altura de los clientes, permitiendo así una mejor visión global de los sucesos en el juego – muy a la satisfacción de los stakeholders internos y sin obviar a las autoridades de regulación del juego

y de procesamiento penal, que en caso de incidentes o actos ilegales exigen pruebas irrefutables.

—¿Cuál es el concepto de su sala de control?

—Nuestro Surveillance Operations Centre pone el foco en su diseño en la funcionalidad y ergonomía, sabiendo que obtenemos resultados mediante los «ojos» de nuestro personal de seguridad. Nuestra atención principal estaba en la creación de un espacio de trabajo que proporcionara un entorno de alto rendimiento orientado a objetivos con el máximo nivel de HCI (Human Computer Interaction – interacción persona-computadora) e intuición. El concepto intuitivo y de fácil manejo del sistema de gestión de vídeo del fabricante germano también está en consonancia con esta filosofía.

En el Surveillance Operations Centre, el equipo de gestión de turno está directamente involucrado en las operaciones, con una línea de visión directa o periférica de todas las estaciones de vigilancia. El personal directivo coadyuvante puede moverse con facilidad detrás de las consolas de control, guiando y dando la formación y la gestión de rendimiento necesarias.

—Usted ha hablado de interfaces. ¿Qué integraciones se han realizado y cuál es su valor añadido?

—Hay algunas integraciones esenciales que hacen la firma alemana única y con las que podemos proteger mejor nuestro negocio. Una de ellas es el desarrollo personalizado de interfaces de alto nivel a sistemas centrales alrededor de nuestras instalaciones. Estas interfaces incluyen, entre otras, máquinas tragaperras, dispensadores de naipes inteligentes, puntos de venta, sistemas de control de acceso y de detección de intrusión, así como fichas RFID.

Esto lleva la convergencia de vídeo y datos o eventos directamente a nuestros operadores –en tiempo real y ya con marcadores para la reproducción y, por supuesto, también disponible para investigaciones, análisis o exportaciones posteriores para buscar tendencias o anomalías.

Sala de equipos y grabadores de videovigilancia. Kevin Iek (Director of Surveillance Technology), Raymond Ho (Sales Engineer, Dallmeier International), Roberto Leong (Manager of Surveillance Systems)

Adicionalmente, las interfaces directas al sistema de seguridad permiten una visualización inmediata en los monitores de las cámaras relacionadas con un aviso de alarma, lo que posibilita una detección, evaluación de la situación y respuesta del equipo de intervención eficientes y rápidas.

Leroy Daniel se muestra satisfecho con la elección tomada. «El permanente trabajo de investigación y desarrollo que la empresa bávara dedica a sus productos es claramente reconocible en esta solución de vídeo integral. Estamos muy satisfechos con el sistema y también con el soporte técnico incondicional por parte del fabricante, tanto a nivel regional como a nivel internacional» ●

Fotos: ***Dallmeier***

Centro de Operaciones de Videovigilancia de Studio City. Leroy Daniel (Executive Director, Melco Crown Surveillance Operations), Damian Phillips (Director of Surveillance, Studio City), Kevin Iek (Director of Surveillance Technology), Roberto Leong (Manager of Surveillance Systems).

Contactos de empresas, p. 8.

MARÍA JOSÉ DE LA CALLE. COFUNDADORA, DIRECTORA DE COMUNICACIÓN & ANALISTA SENIOR DE ITTI. mjdelacalle@ittrendsinstitute.org

El dinero como **datos**

La Comisión Europea, en el documento titulado «Hacia un desarrollo de la economía conducida por los datos»[1] expone los beneficios para Europa del tratamiento de los datos o del Big-Data. Los datos y su tratamiento constituyen una nueva fuente de riqueza. Y al contrario, también es cierto. La realidad física del dinero se está difuminando en una realidad virtual al transformarse en datos residentes en ordenadores y que viajan por las redes de comunicaciones cambiando de propietario, como pago de bienes tangibles o intangibles, realizándose transacciones con intervención humana o sin ella.

EJEMPLO de ello son las contrataciones de valores en las bolsas, que son operaciones informatizadas en base a algoritmos capaces de examinar gran cantidad de parámetros, y que van informando de los cambios o tomando decisiones en tiempo real.

Unas operaciones las realizan los agentes ayudados por las máquinas[2] y otras las realizan las propias máquinas, que lanzan órdenes al mercado financiero en cuestión de milisegundos. Esto último es la «contratación –o negociación– de alta frecuencia» o high frequency trading (HFT), que se utilizan para obtener beneficio a corto plazo, es decir, mantener una posición el menor tiempo posible, que a veces son milisegundos, o segundos, o minutos incluso. Los tiempos en las HFT son tan cortos e importantes que los equipos se suelen colocar lo más cerca posible de la bolsa para reducir el tiempo de comunicación entre la máquina del operador y la de la bolsa en la que opera.

En un ámbito más común, los pagos con tarjeta de crédito ya tienen varias décadas, y con la llegada de internet se adaptó también para pagar en compras por este medio; a día de hoy, ya se pueden realizar pagos con el teléfono –móvil– y almacenar dinero en él como si de una tarjeta de crédito se tratase, a través de una aplicación (App). Es suficiente con acreditar que se dispone de la cantidad a abonar, en el caso de pago, y dónde está direccionado, es decir, la cuenta bancaria. Es el sistema bancario más difundido en África.

¿Seguirán usándose la tarjeta y la cuenta bancaria? Quizás, como afirma Bill Gates en su carta anual de 2015[3] , «hacia el 2030, dos mil millones de personas que no tengan una cuenta bancaria guardarán dinero y realizarán pagos con su teléfono. Y, por entonces, los proveedores de dinero "móvil" ofrecerán un rango completo de servicios financieros, desde cuentas de ahorro con interés para ahorro, a créditos y seguros».

Esta digitalización o virtualización del dinero, junto con la explosión del uso de las comunicaciones móviles, ha tenido como resultado que pequeñas empresas tecnológicas –o grandes, como Apple o Google–, apoyándose en su conocimiento de la tecnología, hayan creado nuevas formas de proveer servicios financieros tradicionalmente ofrecidos por el sector bancario, desde los ya comentados pagos y transacciones, monederos digitales o créditos hasta asesoría financiera e inversiones, lo que ha obligado a la Banca más tradicional a plantearse el cambio hacia esta nueva manera de hacer. Para las tecnológicas «metidas a banqueros» se ha acuñado el término fintech, contracción de los vocablos ingleses «financial»y «technology».

La virtualización del dinero ha tenido su mayor exponente en la moneda nacida ya virtual, sin existencia física previa: el Bitcoin. No depende de ningún gobierno, institución o entidad financiera, como las monedas al uso, el control lo realizan los propios usuarios mediante transacciones directas entre

ellos, anónimas y cifradas. Su uso es a través de aplicaciones y, como tal moneda, se puede utilizar para la compra-venta de productos y servicios allá donde la acepten. Pero el Bitcoin tiene actualmente dos aspectos negativos importantes: por una parte, tiene una alta volatilidad cambiaria; por otra, se ha convertido en la moneda refugio de las mafias, dado su anonimato.

Sin embrago, la verdadera revolución está en el mecanismo en el que se basa el Bitcoin, el «blockchain» o «cadena de bloques», donde se va apuntando cada una de las transacciones realizadas, como si de un libro de contabilidad se tratara, un sistema criptográfico que permite la confianza entre agentes sin necesidad de una autoridad central (el banco emisor), un medio para intercambio y almacenamiento de valor.

Están surgiendo por parte de la Banca tradicional y empresas tecnológicas otras iniciativas de nuevas monedas y servicios basados en el principio funcional del Bitcoin. Veamos algunas aparecidas recientemente:

«Santander se alía con UBS, Deutsche Bank y BNY Mellon para impulsar el uso del dinero digital»[4], noticia del diario Expansión, del 24 de agosto pasado, en la que informa de que dicha alianza desarrollará el sistema 'Utility Settlement Coin' (USC) basado en la tecnología blockchain, el cual «facilitará pagos y liquidaciones de forma eficiente, rápida y segura».

«Microsoft y Bank of America se alían para desarrollar tecnología blockchain»[5], noticia de "elEconomista" del 28 de septiembre pasado, en la que informa que dichas entidades «han acordado colaborar para desarrollar la tecnología 'blockchain' con el objetivo de impulsar la transformación de las transacciones financieras».

La Banca, como otros muchos sectores, está también embarcada en un proceso de digitalización no sólo del dinero sino de sus procesos, a juzgar por las noticias, ya habituales donde aparecen unidas la Banca y la Tecnología. Ejemplo de ello, por citar algunos, es la compra de, o la colaboración con las Fintech, el servicio de asesoramiento personalizado a las empresas a través de vídeo-conferencia lanzado por CaixaBank, o el acuerdo de BBVA y Banco Santander con Red-Hat para desarrollar sus respectivas «nubes».

Seguridad en el sector bancario

Que los bancos utilicen ordenadores para su gestión no es una novedad. Sí lo es que la mayoría de las operaciones se realicen a través de dispositivos y software en cualquier sitio donde haya comunicación por Internet, entre entidades bancarias, entre entidades bancarias y sus clientes, y entre los clientes directamente para sus negocios o sus vidas privadas, fuera de los límites del edificio de una entidad bancaria, por cualquier persona y no por un empleado bancario.

Por ello han aumentado los riesgos de seguridad, del dinero en particular y los activos financieros en general, que se han transformado en información en continuo movimiento por las redes de comunicaciones, con acceso desde cualquier lugar. No hay que olvidar que el sector financiero es el primer objetivo para ladrones en general y cibercriminales en particular, ya que es en estas instituciones donde realmente está el dinero, y la superficie de exposición, como ya se ha visto, ha aumentado considerablemente.

Tanto es así, que la empresa «Raytheon», en el estudio[6] realizado en el año 2015 sobre la seguridad en el sector financiero, encontró lo siguiente:

- Los incidentes de seguridad en entidades financieras son 300% más frecuentes que en otros tipos de industria.
- El 33% de los intentos de ataque tienen como objetivo servicios financieros.

• Las entidades financieras ocupan el tercer lugar en cuanto a objetivos de «typosquatting»[7] .

Es conocido el daño que una crisis financiera causa en la sociedad, y la interconexión y dependencia entre las distintas entidades. Todos recordamos cómo la quiebra de «Lehman Brothers»en el 2008 disparó la crisis. Por este motivo, la importancia de la seguridad en los sistemas financieros es indiscutible ya que, un gran incidente de [ciber]seguridad puede llegar a causar una crisis que afecte no sólo a dicha entidad y sus clientes, sino a otras entidades e incluso al sistema financiero de un país, o de varios países. Tan es así, que España tienen al sistema financiero como perteneciente a uno de los 12 sectores que aseguran la prestación de servicios esenciales, a los que pertenecen las consideradas «Infraestructuras Críticas».

Seguridad del dinero = ciberseguridad

El dinero ha entrado en la corriente de los datos y de la información, y la forma de acceder a él es la misma que a los datos en general; consecuentemente la seguridad del dinero es ciber-seguridad, seguridad informática y seguridad de la información.

La seguridad de los datos o seguridad de la información se apoya en tres principios ampliamente conocidos: confidencialidad, integridad y accesibilidad, o expresado de otra manera, los datos deben ser accesibles por personas o sistemas autorizados cuando éstos así lo requieran, y sólo por éstos, y en la forma en que en ese momento sea pertinente y lo tengan permitido.

Un incidente de seguridad se puede definir como cualquier suceso que no forma parte de la operación normal de un servicio y que causa, o puede causar, una interrupción o una disminución de la calidad de dicho servicio, incluyendo la violación de una norma de seguridad o el fallo de una salvaguarda.

Según esta definición, las causas de los ciberincidentes son múltiples. Un mal funcionamiento o interrupción de un sistema no tienen porqué proceder del ciber-delito. Muchas veces son incidentes producidos por errores o fallos internos: un error de software, eliminación de algún dato por error, actualizaciones no llevadas a cabo adecuadamente, fallos en el mantenimiento del hardware, y errores humanos en general.

Para terminar, los nostálgicos que quieran tener dinero en efectivo, también con el móvil lo pueden tener. El banco «ING Direct» acaba de sacar un servicio que, como si de una compra se tratara, en la caja de algunos supermercados o gasolineras puedes «pagar» con el móvil y se obtiene esa misma cantidad en efectivo.[8]

REFERENCIAS

[1].- «Towards a thriving data-driven economy», (24 de febrero, 2016). European Comission. url [a 9-10-2016] https://ec.europa.eu/digital-single-market/en/towards-thriving-data-driven-economy

[2].- J.A.Pérez (oct, 2011) «Negociación de Alta Frecuencia: Más Ventajas que Inconvenientes» url [a 9-10-2016] http://www.bolsasymercados.es/esp/publicacion/revista/2011/12/46-50_act-rep_alta_frecuencia.pdf

[3].- «By 2030, 2 billion people who don't have a bank account today will be storing money and making payment with their phones. And by then, mobile money providers will be offering the full range of financial services, from interest-bearing savings accounts to credit to insurance.» «2015 Gates Annual Letter». url [a 9-10-2016] https://www.gatesnotes.com/2015-annual-letter?page=0&lang=en

[4].- «Santander se alía con UBS, Deutsche Bank y BNY Mellon para impulsar el uso del dinero digital», (24 de agosto, 2016). Expansión. url [a 9-10-2016] http://www.expansion.com/empresas/banca/2016/08/24/57bd61bce5fdea154d8b467a.html

[5].- Microsoft y Bank of America se alían para desarrollar tecnología blockchain" (28 de septiembre, 2016) url [a 9-10-2016] http://www.eleconomista.es/tecnologia/noticias/7853084/09/16/Microsoft-y-Bank-of-America-desarrollaran-en-conjunto-la-tecnologia-blockchain.html

[6].- «2015 Industry Drill-Down Report Financial Services» (2015). Raytheon/ Websense Lab. url [a 9-10-2016] http://www.websense.com/assets/reports/report-2015-industry-drill-down-finance-en.pdf

[7].- «¿Qué es el "Typosquatting"?». (7 de noviembre, 2004). uni>ersia. url [a 9-10-2016] http://noticias.universia.es/ciencia-nntt/noticia/2004/11/07/610533/que-es-typosquatting.html

[8].- url [a 9-10-2016] https://www.ingdirect.es/twyp/twyp-cash.html

PIMA WIRELESS

PIMAlink

Control total de su panel de alarma desde la palma de la mano

- Servicio en la nube
- Video verificación
- Reciba las notificaciones de su panel de alarma
- Controle su panel de alarma de forma remota
- Conexión vía radio
- Instalación rápida y sencilla

El mejor servicio personalizado de atención al cliente y con técnicos especializados.

35 años de experiencia nos avalan.

HOMMAX

Av. Alquería de Moret, 9
46210 Picanya (Valencia) España
Tel: (+34) 96 159 46 46

hommax@hommax.eu | www.hommaxsistemas.com | Hommax Sistemas | @HommaxSistemas | Hommax

NOEMÍ BRITO. DIRECTORA DE DERECHO DIGITAL LEGISTEL & AP CONSULTORES. MIEMBRO DEL COMITÉ OPERATIVO DEL DATA PRIVACY INSTITUTE DE ISMS FORUM

Los servicios de **Cloud Computing**

En el punto de mira del legislador europeo

La Nube sigue siendo un elemento clave para la plena consecución de los objetivos del Mercado Único Digital[1] y, asociados a éste, los aspectos regulatorios que presenta se erigen en un tema fundamental.

BUENA prueba de ello son los resultados preliminares de la consulta pública sobre el ecosistema normativo relacionado, entre otros ámbitos, con la computación en la nube[2], y que apuntan a que la mayor parte de los participantes opinan/denuncian lo que sigue:

• Que la decisión de localización de los datos e información que manejan no es baladí, muy al contrario, es vital y estratégica para la marcha del negocio, por lo que no debería ser tomada a la ligera.

• Que los proveedores de servicios cloud no son los suficientemente transparentes sobre la seguridad y la protección de los datos personales por relación a los servicios que ofrecen y prestan.

• Que las condiciones y términos a los que se sujetan tales servicios no son, por lo general, negociables.

Principales novedades legislativas en torno a la prestación de servicios en la nube.

A tenor de los citados resultados, en estos momentos, la Comisión Europea evalúa proponer nuevas medidas legislativas para mitigar los indicados problemas. Sin embargo, entre tanto, lo que sí es importante para los prestadores de servicios cloud es conocer las implicaciones jurídicas derivadas de dos recientes normas que, sin duda, impactan y modifican las actuales reglas a las que se sujetan estos servicios a nivel europeo, a saber:

• Del lado de la protección de los datos de carácter personal: El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (en ade-

lante, «el Reglamento General de Protección de Datos» o el «RGPD»)[3].

• Del lado de la seguridad de las redes y los sistemas de información: La Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (en lo que sigue, la Directiva NIS).

Algunas recomendaciones dirigidas a prestadores de servicios cloud para cumplir con el RGPD/GDPR.

En lo que concierne a la protección de los datos de carácter personal, se incluyen en el RGPD sendas obligaciones legales que deben ser consideradas por estos proveedores de servicios. Al respecto, se trasladan algunas recomendaciones específicas de cumplimiento:

• Revisar y reforzar los procesos informativos y de transparencia respecto al usuario (principio de transparencia), quien ostenta un derecho a la información sobre las actuaciones de la empresa en lo que concierne al tratamiento de sus datos personales. Además, si el cliente de estos servicios es una empresa o una persona jurídica, existirá una obligación legal de diligencia por ésta a la hora de comprobar que el respectivo prestador cumple con la normativa aplicable[4].

• Articular una estrategia adecuada y renovada para la correcta atención de los derechos del usuario/interesado sobre todo ante los nuevos derechos que se le reconocen al mismo. Entre éstos se destaca el derecho a la portabilidad de los datos, es decir, el derecho de un usuario a: 1) recibir los datos personales que le incumban, que haya facilitado al prestador de servicios cloud, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro prestador sin que lo impida el primero; 2) que se transmitan directamente sus datos de un prestador a otro, cuando sea técnicamente posible.

«La Nube sigue siendo un elemento clave para la plena consecución de los objetivos del Mercado Único Digital»

• Incorporar desde el diseño de los servicios cloud a prestar los principios de «privacy by design» y «privacy by default» o, dicho de otro modo, que se cumpla con la normativa de protección de datos desde el diseño y por defecto en tales servicios.

• Implementar el principio de «accountability», que alude a la asunción de responsabilidad y de una actitud transparente por el prestador y responsable del tratamiento, sobre todo, en el caso de compañías multinacionales que operan a escala global, respecto a la correcta adopción de medidas y políticas que garanticen el cumplimiento interno (compliance digital).

• Establecer protocolos internos para prevenir y, en su caso, reaccionar en caso de violaciones de la seguridad de los datos o brechas de información personal.

• Prever y contar con políticas claras en orden a la correcta identificación, contratación, control y auditoría de los encargados de tratamiento, en particular, cuando éstos operan fuera del Espacio Económico Europeo (EEA).

• Llevar un Registro de Actividades de Tratamiento que, sin embargo, únicamente será obligatorio en el caso de que el prestador sea una empresa con más de 250 trabajadores o maneje determinadas categorías de datos a los que alude el artículo 30.5 del RGPD.

• Revisar y adoptar medidas de seguridad adecuadas al tratamiento de datos personales actual o proyectado por el prestador de que se trate, incluyendo la posible seudonimización y el cifrado de datos personales, teniendo

«Las redes y sistemas de información desempeñan un papel crucial en la sociedad por lo que garantizar su fiabilidad y seguridad son esenciales»

en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas.

• Realizar, en su caso, una Evaluación de Impacto en Protección de Datos (EIPD) de conformidad con lo previsto en el artículo 35 del RGPD. Destacar que la AEPD cuenta con una Guía, previa a la aprobación de este Reglamento que, sin embargo, nos puede ayudar a orientar cómo enfocar estos procesos[5].

• Si así se considera, nombrar a un Delegado de Protección de Datos o DPO, que actuará como interlocutor de la empresa frente a la autoridad de control y frente a los usuarios, salvo que tal nombramiento tenga carácter obligatorio según dispone el artículo 37 del RGPD.

• Revisar las transferencias internacionales o exportaciones de datos que se estén realizando fuera del EEA, a fin de adecuarlas a la nueva regulación europea. Si tales datos se están transfiriendo a EEUU se tendrá en cuenta el nuevo marco de actuación acordado (Privacy Shield)[6] .

Sin perjuicio de lo anterior, también resulta de interés conocer el nuevo Código de Conducta para Proveedores de Servicios de Infraestructuras Cloud, publicado el pasado 26 de septiembre de 2016[7]. Eso sí, será de cumplimiento obligatorio para todo prestador que voluntariamente de adhiera al mismo.

Consideraciones adicionales de cumplimiento de la Directiva NIS.

El pasado 19 de Julio se publicó de forma oficial la Directiva NIS que parte de dos premisas importantes:

• Las redes y sistemas de información desempeñan un papel crucial en la sociedad por lo que garantizar su fiabilidad y seguridad son esenciales para el desarrollo de las actividades económicas y sociales en la UE.

• Que la magnitud, la frecuencia y los efectos de los incidentes de seguridad se están incrementando de forma exponencial y representan una grave amenaza para el funcionamiento de tales redes y de los sistemas de información pudiendo paralizar o interrumpir la actividad económica y generar considerables pérdidas de todo tipo.

A fin de paliar las consecuencias negativas descritas y mejorar la seguridad de tales redes y sistemas, la Directiva NIS será de aplicación, entre otros operadores, a los proveedores de servicios digitales indicados en el Anexo III de la misma, entre los que se incluyen, proveedores de servicios de computación en la nube.

Conforme al artículo 18 de esta Directiva, un proveedor de servicios de computación en la nube se considerará sometido a la jurisdicción del Estado miembro en el que se encuentre su establecimiento principal (cuando su domicilio social se encuentre en ese Estado miembro). Cuando este proveedor no está establecido en la Unión, pero, sin embargo, ofrece servicios, designará un representante, que se deberá establecer en uno de los Estados miembros en los que se ofrecen tales servicios. En estos casos, el proveedor se considerará sometido a la jurisdicción del Estado miembro en el que se encuentre establecido su representante.

Los Estados miembros velarán por que estos proveedores adopten las medidas técnicas y organizativas adecuadas y proporcionadas para gestionar los riesgos existentes para la seguridad de las redes y sistemas de información que utilizan para la oferta de sus servicios en la UE.

Los Estados también velarán porque, si así ocurriera, notifiquen sin dilación indebida a la autoridad competente o al CSIRT los incidentes que tengan efectos significativos en la continuidad de los servicios que prestan (sistema de notificación obligatoria de incidentes).

Será posible, previa consulta al prestador que corresponda, que la autoridad competente o el CSIRT informe al público sobre ciertos incidentes cuando la concienciación pública sea necesaria para evitar otro incidente en el futuro, o para gestionar aquél que se hubiera producido. También podrá exigir al proveedor que sea él quien lo haga. A fin de determinar la importancia de los efectos de un incidente se atenderá, según los casos, a parámetros como el número de usuarios afectados, la duración del incidente o la extensión geográfica, con respecto a la zona afectada por el incidente, el grado de perturbación de funcionamiento del servicio e, incluso, el alcance del impacto sobre las actividades económicas y sociales.

Por último, es importante indicar que las anteriores obligaciones contenidas en los artículos 16, 17 y 18 no serán de aplicación para aquellas empresas o proveedores que tengan la consideración de microempresas y pequeñas empresas tal como se definen en la Recomendación 2003/361/CE de la Comisión, es decir, para empresas que ocupan a menos de 250 personas y cuyo volumen de negocios anual no excede de 50 millones de euros o cuyo balance general anual no excede de 43 millones de euros (artículo 16.11 de la Directiva NIS). ●

Fotos: ISMS Forum/Freepik

REFERENCIAS

[1].- Para conocer los principales hitos asociados a la «European Cloud Strategy», así como los grupos de partenariado creados en este ámbito («European Cloud Partnership (ECP)» y el «Cloud Select Industry Group (C-SIG)»), puede accederse a la siguiente URL: https://ec.europa.eu/digital-single-market/en/cloud#Article

[2].- Informe accesible desde la siguiente dirección web: https://ec.europa.eu/digital-single-market/en/news/first-brief-results-public-consultation-regulatory-environment-platforms-online-intermediaries y https://ec.europa.eu/digital-single-market/en/news/study-online-platforms-contrasting-perceptions-european-stakeholders-qualitative-analysis

[3].-Puede consultarse el texto del RGPD/GDPR a través del siguiente enlace web: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

[4].- Tal y como se infiere del Documento AEPD de Orientaciones a los prestadores de Servicios de Cloud Computing: «(…) El cliente que contrata a un prestador de servicios de cloud computing tiene una obligación legal de diligencia para 'velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto' en la normativa de protección de datos personales (art. 20.2 del Reglamento de desarrollo de la LOPD –RLOPD–). Este deber de diligencia se traducirá, dadas las características propias de estos servicios, en un abanico de requerimientos de información al proveedor de servicios dirigidos a conocer las garantías que ofrece para la protección de los datos personales de los que sigue siendo responsable. Dicha información le resultará imprescindible para decidir sobre la modalidad de nube y el tipo de servicios que contrata y, específicamente, para discriminar cuál o cuáles le ofrecen garantías adecuadas y elegir entre ellos. El cumplimiento de este deber de diligencia ha de tener como contrapartida por parte del prestador de servicios de cloud computing una correlativa diligencia a la hora de facilitar información, en particular sobre los mecanismos que garantizan el cumplimiento de las obligaciones derivadas de la normativa de protección de datos, para poder considerarlo como un proveedor transparente. La transparencia es, por tanto, un principio esencial que debe presidir las relaciones entre las partes, especialmente en los casos en que el proveedor de servicios ocupa una posición preeminente sobre los clientes. Circunstancia que será habitual cuando estos últimos sean pymes, microempresas, profesionales o Administraciones públicas sin gran estructura orgánica. A tal efecto, la Guía para clientes que contraten servicios de cloud computing incluye un abanico de preguntas sobre las garantías exigibles que han de ser atendidas por el proveedor que los comercializa a cuyo contenido se remite este documento.

Es por ello que la Agencia Española de Protección de datos valorará particularmente la diligencia y transparencia en la contratación de estos servicios.(…)". Pág.6 de esta Guía descargable de forma directa a través del siguiente enlace web: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/ORIENTACIONES_Cloud.pdf

[5].- Puede accederse a esta Guía a través de este enlace: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf

[6].- A fin de ampliar la información necesaria a estos efectos es importante acceder a la información disponible en los siguientes enlaces: http://europa.eu/rapid/press-release_IP-16-2461_es.htm y https://www.privacyshield.gov/welcome.

[7].- El reciente «Code of Conduct for Cloud Infrastructure Service Providers", publicado por CISPE el pasado mes de septiembre incluye la necesidad de realizar este tipo de evaluaciones de forma continuada en el tiempo en su apartado 5.3, relativo a la Seguridad. Puede ser consultado este documento a través de los siguientes enlaces:

https://cispe.net/ ; https://cispe.net/wp-content/uploads/pdf/CISPE-CodeOfConduct-160926.pdf; https://cispe.net/wp-content/uploads/pdf/CISPE-PRESS-RELEASE-27092016.pdf

JUAN ANDRÉS ARIAS MAESTRO. DIRECTOR GENERAL DE DORMAKABA ESPAÑA

«*Dormakaba tiene una clara ambición de convertirse en el líder de confianza de la industria*»

«La protección eficiente de la propiedad siempre ha sido nuestra prioridad estratégica», así lo asegura Juan Andrés Arias Maestro, director general de Dormakaba España, quien además explica que gracias a la fusión de ambas compañías «podremos ofrecer a nuestros clientes un portfolio de soluciones completo, que permitirá diseñar espacios atractivos, eficientes, organizados y seguros en todos los ámbitos de nuestra vida, desde el entorno residencial, el empresarial o el del ocio».

¿Qué razones estratégicas persigue la unión de Dorma y Kaba?

—Mediante la fusión de estos grandes actores en el mercado del control de acceso, perseguimos la ambición de convertirnos en líder de confianza de la industria.

Ambas compañías comparten una historia de éxito que se remonta más de 100 años, ofreciendo soluciones innovadoras y liderando sus respectivos segmentos de mercado.

Gracias a la fusión, podremos ofrecer a nuestros clientes un portfolio de soluciones completo, que permitirá diseñar espacios atractivos, eficientes, organizados y seguros en todos los ámbitos de nuestra vida, desde el entorno residencial, el empresarial o el del ocio.

Dorma+kaba ya se encuentra muy presente en la gran mayoría de edificios que habitamos y utilizamos diariamente.

—¿En qué aspectos complementa Dorma el portfolio de Kaba y viceversa?

—Uno de los puntos más destacables de nuestro proyecto de fusión es precisamente la enorme complementariedad que existe entre nuestros negocios en múltiples ámbitos, desde los productos hasta los canales de venta y los procesos de negocio.

Realmente tenemos un proyecto donde podemos decir que todos somos ganadores, ya que gracias a la unión de nuestras capacidades vamos a ser capaces de servir mejor a nuestros clientes, hacer más competitivos a nuestros distribuidores, y ofrecer uno de los desafíos más interesantes del mercado a nuestros empleados.

—¿Qué ventajas aportará al sector de la seguridad la creación de este nuevo grupo empresarial, concretamente en España?

—La protección eficiente de la propiedad siempre ha sido nuestra prioridad estratégica. Nuestros clientes de seguridad ya confían en nuestras soluciones de cierre y control de acceso desde hace más de 30 años, ahora además complementamos el portfolio con otras soluciones que cada vez están tomando relevancia, como son sistemas de puertas automáticas con certificación de seguridad o sistemas para el control electrónico de puertas de evacuación y emergencia. Todo diseñado e integrado de la mano de un único fabricante, que garantizará que todos los elementos funcionan de forma óptima y tomando la responsabilidad completa de la solución.

Adicionalmente a todo esto, dorma+kaba será el único actor del mercado capaz de armonizar soluciones donde el diseño arquitectónico y la imagen de marca de nuestros clientes podrá convivir con las necesidades de seguridad de nuestros clientes.

—Desde el punto de vista de cultura empresarial, ¿cuáles son los principales valores que comparten Dorma y Kaba y que se aportan a la fusión?

—Tanto Dorma como Kaba ya definían su misión, visión y valores. Ha sido muy sencillo unificar los valores de dorma+kaba que ya hemos activado entre nuestros empleados: el cliente primero, desempeño, coraje, curiosidad y el valor fundamental sobre el que orientamos nuestra forma de trabajar: La confianza.

En la búsqueda de creación de confianza orientamos la forma en la que trabajamos con nuestros clientes, entre nuestros empleados, con nuestros partners y proveedores, así como con nuestros accionistas. Se trata de un elemento realmente potente y que exige no fallar cada día. Todos sabemos que la confianza sólo se puede ganar con esfuerzo y es muy fácil de perder. Desde dorma+kaba estamos comprometidos con nuestros valores y todo nuestro equipo humano trabaja con ellos cada día.

—¿Los actuales clientes de Dorma y de Kaba van a ver afectada en algún aspecto su actual relación con ambas compañías?

—Uno de los objetivos de esta fusión es conseguir que sólo sea visible a nuestros clientes desde la perspectiva de las ventajas y mejoras que van a tener, por lo tanto todas las iniciativas organizativas y de procesos internos que estamos ejecutando en este momento se han diseñado con el objetivo de ofrecer mejor servicio a nuestros clientes sin que se vean afectados por los profundos cambios que conllevan todos los procesos de fusión.

Gracias a la complementariedad que existe entre nuestras compañías, este proceso se va a producir de forma muy natural y satisfactoria para nuestros clientes.

—¿Qué segmento de mercado será el primordial para el nuevo grupo?

—Hemos identificado varios segmentos de mercado estratégicos en los que nos vamos a centrar, y donde colocaremos una oferta completa y adaptada a las necesidades específicas de cada uno.

También tenemos una estrategia de canal con el objetivo de conseguir que todos nuestros partners y distribuidores tengan éxito en un mercado que se ha vuelto muy exigente y competitivo en los últimos años. Para ello les apoyaremos en proyectos y les ofreceremos soluciones diferenciadoras y sostenibles en el tiempo.

—¿Cómo está reaccionando el sector de la seguridad español a la unión de dos empresas de tal envergadura?

—Durante estos meses he tenido la oportunidad de visitar y comentarlo con varios de nuestros clientes, y lo cierto es que todos coinciden en que nuestra fusión tiene mucho sentido. Nos conocen en el mercado desde hace mucho tiempo y valoran lo que cada una de nuestras compañías ha realizado cuando éramos independientes. Poder trabajar con nosotros como una única compañía sólo puede mejorar lo que antes ya era muy bueno.

—¿Cuál será la estrategia comercial, a grandes rasgos, para los próximos años?

—Dorma+kaba tiene una clara ambición de convertirse en el «Líder de Confianza en la Industria». Para ello hemos elaborado una estratégia multicanal que se centra por un lado en el desarrollo de cuentas clave y segmentos de mercado, apoyado por una red de distribución y partners que seguirá creciendo para alcanzar a más clientes.

Apostamos en la innovación tecnológica y la ingeniería del acceso como elemento diferenciador de nuestra propuesta de valor, la cercanía al cliente y en la excelencia operativa de nuestros procesos para sostener nuestra competitividad en el mercado. ●

Fotos: dormakaba

Contactos de empresas, p. 8.

SALVADOR TARAZONA. CORREDOR DE SEGUROS Y ADMINISTRADOR ÚNICO DE SALVADOR TARAZONA CORREDURIA DE SEGUROS

«El *cliente* de *seguridad privada* precisa inmediatez y rapidez; *reclama soluciones* y no problemas»

«Salvador Tarazona Correduria de Seguros tiene como objetivo ofrecer un servicio completo a nuestros clientes en mediación de seguros, buscándole contratación a todos sus riesgos y necesidades en materia de seguros», así lo asegura Salvador Tarazona, responsable de la empresa, quien tras su inclusión hace más de 10 años el mercado de la seguridad privada, apuesta por la constante evolución y mejora de sus productos para adaptarse a las necesidades y demandas de los clientes.

QUÉ características o valores principales definen a Salvador Tarazona como empresa?

—La correduría de seguros que lleva mi nombre tiene como principio el ofrecer un servicio completo a nuestros clientes, en mediación de seguros (brokerage), buscándole contratación a todos sus riesgos y necesidades en materia de seguros, a unos precios muy competitivos y con unas coberturas muy completas y novedosas. En todo momento y lugar defendemos los intereses de los clientes anteponiéndolos a los nuestros. Con todo ello queremos conseguir que el asegurado se sienta en todo momento bien cubierto y protegido.

—¿Cómo surgió la compañía y cómo ha sido su evolución desde entonces?

—La correduría de seguros la fundé en el año 1985 (31 años) y desde entonces no hemos parado de evolucionar para poder dar al cliente un mejor servicio y conseguir su tranquilidad.

En la actualidad contamos con 4 oficinas propias y una red de colaboradores por toda España. Nos hemos especializado en diversos nichos, siendo uno de ellos el sector de la Seguridad Privada, dando un servicio completo desde hace más de 10 años, contando en la actualidad con un importante número de clientes del sector, el cual va creciendo una vez nos conocen, estudian nuestras pólizas de seguros y las coberturas que contienen. Al ser unas pólizas abiertas, en todo momento podemos incluir nuevas garantías o adaptarnos a las características del cliente confeccionando un seguro a «su medida».

En varias ocasiones hemos estado presentes, con un Stand, en la Feria de la Seguridad Privada, siendo desde 2006 socio honorífico de ESA CV (Empresas de Seguridad Asociadas de la Comunidad Valenciana). Participando en varios de sus congresos como ponentes especializados en materia de seguros y normativa de seguridad privada.

—¿Qué servicios presta a empresas de seguridad privada?

—Como he comentado en su pregunta anterior, nuestro interés está en dar un servicio completo a todos nuestros clientes, no siendo menos el sector de la Seguridad Privada, por lo que damos cobertura al seguro de responsabilidad civil, seguro de caución, locales, seguro multirriesgo del comercio, oficinas, instalaciones, almacenes y naves industriales. Seguro de vida o accidentes del

convenio colectivo de los trabajadores o autónomos, seguro de los vehículos incluido los dedicados a transporte de mercancías peligrosas. Seguro de responsabilidad civil de los Administradores, para poder preservar su patrimonio privado en caso de una demanda y ponerle profesionales para su posible defensa penal.

—¿Qué tipo de coberturas ofrece?

—Las coberturas que nuestros contratos de seguro ofrecen están totalmente adaptados a la normativa de seguridad privada en sus últimas actualizaciones, contamos con todas las garantías preceptivas que reglamentariamente se exigen, incluyendo la cláusula de aviso de terminación de contrato, legalmente exigida, y la garantía de objetos confiados en custodia, facilitando la inscripción de las mismas en la DGS, sin ningún tipo de problemática

—¿Qué ventajas aporta a quienes los contratan?

—Además del tratamiento personalizado ya comentado, la resolución y asesoramiento en el posible siniestro por parte de nuestra Correduría, de tal forma que el cliente siempre siente la cercanía de nuestra firma.

—¿Cómo se contrata?

—El mecanismo de contratación es muy sencillo y accesible, a través de nuestra web www.starazona.com, o al teléfono 963734550 o email de nuestro técnico suscriptor Enrique Lozoya: kike@starazona.com, o cualquiera de los teléfonos de nuestras 4 oficinas, y que pueden ver en el detalle de nuestra publicidad, a través de nuestros propios tarificadores, como stbseguros y myseguros, dejándonos sus datos de contacto, les devolveremos la llamada, facilitándoles un cuestionario adjunto para cumplimentar y delimitar el riesgo a sus necesidades.

Instalaciones de Salvador Tarazona Correduria de Seguros.

—¿Qué diferencias distinguen a Tarazona con respecto a la competencia?

—Priorizamos la calidad del servicio frente al crecimiento, nuestra filosofía es un cliente satisfecho es un cliente duradero, defendiendo sus intereses como propios, no hay mejor publicidad que la que emite el propio cliente sobre nuestro servicio.

—¿Cómo está siendo su expansión en el mercado de la seguridad privada?

—Estamos en constante evolución y mejora de nuestros productos, en el sector de la seguridad privada, unas veces por indicación y necesidad del

Equipo de Salvador Tarazona Correduria de Seguros.

Interior de la Correduria de Seguros.

cliente, otras por las exigencias de las normativas, y otras por las nuevas coberturas que nacen por la evolución de las empresas y la tecnología.

Nuestra correduría siempre vende realidades, puesto que tenemos claro que de nada sirve «vender humo» o coberturas inasumibles y luego una vez ocurra el siniestro evidenciar el descubierto de la cobertura. A nuestro modo de ver, el cliente de seguridad privada precisa de inmediatez, rapidez, como en la emisión de certificados, resolución y tramitación de siniestros, en definitiva reclama soluciones y no problemas. Bastante tienen los clientes con su día a día, peleando en un mercado tan competitivo como el actual, para ofrecer sus servicios, como para encontrarse con problemas de tramitación y emisión de certificados, pólizas, etc.

Nos congratulamos de nuestro mantenimiento de cartera de clientes, pese a la acuciante crisis, ya que no solo hemos mantenido nuestra cartera sino que hemos crecido, y eso se logra dando un buen servicio, coberturas y precios acordes con la realidad del sector y trabajar con total honestidad. Quien más recomiendan nuestros servicios son nuestros propios clientes.

—¿En qué consiste el seguro contra ataques cibernéticos y a qué tipo de empresas va dirigido?

—En la actualidad todas las empresas están en peligro de recibir en cualquier momento uno de los temibles ataques cibernéticos, por lo que es importante tener implantado en nuestros servidores lo que se denomina un «corta-fuegos», hacer un cursillo específico, mantener bien informado a los empleados para que eviten que abran archivos maliciosos que vienen por la red o con los correos electrónicos, que lo destruyen todo, encriptan la información o secuestran nuestro ordenador. En el supuesto que nada de esto funcione las empresas deben contar con un seguro que cubra cualquiera de los daños o averías en los programas o secuestro de las bases de datos, ocasionado intencionadamente por terceros o piratas informáticos (hacker). En nuestra web www.starazona.com en el apartado de «Productos» los clientes pueden conseguir una información muy precisa de este producto como de igual manera de todos los ramos de seguros que trabajamos en la actualidad, pudiendo pedir un presupuesto sin compromiso de cualquiera de ellos.

—¿Tienen en mente desarrollar otro tipo de seguros enfocados a las empresas de seguridad privada?

—Como hemos indicado anteriormente estamos constantemente ampliando nuestros servicios a los clientes. Actualmente estamos negociando con diferentes aseguradoras una especie de bonificación para nuestros clientes en seguros adicionales como vehículos, flotas, Locales, D&O, seguros de caución (aval para empresas de seguridad). ●

Fotos: Salvador Tarazona. Correduria de Seguros.

Cepreven: reducir el riesgo inherente a los Trabajos en Caliente

LOS trabajos en caliente son una de las principales causas de incendios en la industria y, sin embargo, siguen llevándose a cabo sin que se apliquen las adecuadas medidas de prevención y protección. Conscientes de este hecho, las Asociaciones Europeas de Protección contra Incendios han establecido un programa basado en el sistema establecido en los países nórdicos, que durante sus 25 años de funcionamiento ha conseguido rebajar un 90% el número de siniestros por esta causa. Cepreven pone en marcha este procedimiento europeo para contribuir a disminuir el riesgo de estos trabajos, contando con la colaboración de Asociaciones del Metal, Asociaciones del sector de la Prevención y la Seguridad contra Incendios y Aseguradoras. Este sistema consiste en el reconocimiento de aquellas personas que en su actividad profesional operan habitualmente con puntos calientes, y que han demostrado poseer los conocimientos necesarios para controlar los riesgos relacionados con el incendio en el desempeño de su labor cotidiana.

La Tarjeta Europea de Operador Seguro de Trabajos en Caliente que otorga Cepreven, con la certificación CFPA Europa, garantiza que el portador conoce los riesgos derivados de su actividad y las medidas de prevención necesarias para su control.

La cámara panorámica PanoVu de Hikvision gana el prestigioso premio GIT SECURITY Award

Para Hikvision, principal proveedor mundial de productos y soluciones de vídeo vigilancia, es un orgullo anunciar que su cámara panorámica de 360 grados PanoVu ha sido nombrada mejor producto de vídeo vigilancia y CCTV en los prestigiosos GIT SECURITY Awards de 2017.

Los premios anuales GIT SECURITY Awards se conocen por ser unos de los más disputados en todo el mundo. De todos los productos, nominados y votados por 75.000 lectores de GIT SECURITY y GIT SICHERHEIT, se escogen tres ganadores para cada categoría. GIT SECURITY y GIT SICHERHEIT son las revistas de seguridad de mayor tirada en la región de EMEA y Alemania.

La cámara ofrece imágenes Ultra HD de 360 grados

La cámara PanoVu DS-2DP1636-D de 16 MP ofrece imágenes Ultra HD de 360 grados y sin distorsión, gracias a su perfecta integración de ocho sensores CMOS de escáner progresivo separados 1/1,9"en cada cámara. Estos ocho sensores se vinculan con la potente unidad óptica PTZ de 36x de PanoVu y las funciones de seguimiento Smart para garantizar que no se pierda ni un solo detalle de la escena panorámica. Capturan imágenes en color de alta resolución y gran nitidez de hasta 0,002 lux para una supervisión constante de 360 grados que resulta ideal para los espacios públicos abiertos de las grandes urbes.

La combinación en una única unidad de visión panorámica y capacidad, gracias a su potente capacidad PTZ de 360 grados, minimiza los costes, reduce la complejidad técnica y simplifica la instalación, permitiendo a los usuarios sustituir varias cámaras por una sola PanoVu. El director de marketing internacional de Hikvision, Keen Yao, declaró que recibir el premio GIT SECURITY Award es un gran honor y reconocimiento al trabajo realizado por los entregados diseñadores de Hikvision. «Estamos encantados de recibir este prestigioso premio que nos han otorgado los entendidos lectores de esta revista tan distinguida.

La serie PanoVu cuenta con un diseño sencillo y discreto, además de una estructura compacta, que ofrece imágenes panorámicas de ultra alta definición, y que integra a la perfección el vídeo de varios sensores en una única imagen. A nuestro parecer, es la solución panorámica de alta gama mejor equipada del mercado».

La serie PanoVu de Hikvision está diseñada para aplicaciones de supervisión de seguridad de gran escala como estadios, centros urbanos, aeropuertos y aparcamientos.

La gama de productos está disponible en los modelos de 8 MP y 180 grados, y en 16 MP y 360 grados, para que los usuarios puedan elegir el modelo que mejor se adapte a su aplicación de vigilancia específica.

En abril de 2016, la serie PanoVu de Hikvision también obtuvo el premio iF Design Award, reconocido como símbolo mundial de la mayor calidad en diseño.

Tecnifuego-Aespi: Beatriz Palmeiro, nueva secretaria general

EN la última reunión extraordinaria celebrada por parte de la Junta Directiva de Tecnifuego-Aespi, el pasado 13 de septiembre, se nombró por unanimidad nueva Secretaria General a Beatriz Palmeiro, estrecha colaboradora del anterior secretario Xavier Grau (DEP).

Beatriz Palmeiro ha ocupado el puesto de apoyo administrativo en Secretaría desde su entrada en la Asociación hace seis años.

Su trayectoria profesional ha estado siempre ligada a cargos como secretaria de dirección y apoyo en la gestión.

En esta nueva etapa de cambios necesarios para superar el vacío administrativo en la Asociación, Beatriz Palmeiro compromete todo su esfuerzo y entusiasmo, en equipo con la Junta Directiva y el resto de profesionales que prestan sus servicios en Tecnifuego-Aespi.

Dallmeier, en la Terminal 3 del aeropuerto de Fráncfort

El Aeropuerto de Fráncfort confía en la tecnología de sensores multifocal Panomera® de Dallmeier para asegurar el terreno de construcción de su nueva Terminal 3.

El Aeropuerto de Fráncfort en Fráncfort del Meno es el mayor aeropuerto civil alemán y uno de los centros de conexión más importantes del mundo. Para poder seguir gestionando el enorme volumen de pasajeros de manera eficaz, otra terminal aeroportuaria, la Terminal 3, se estará construyendo hasta 2022.

Los trabajos de excavación ya se han finalizado; el siguiente paso se dará en otoño con la ingeniería civil especial. Pero antes de que se ponga en funcionamiento el edificio terminado con sus zonas de facturación y muchas posibilidades de compra, es necesario primero asegurar adecuadamente las obras durante los próximos años. La protección perimetral en particular juega aquí un papel importante para proteger el recinto de accesos no autorizados. Los responsables de la compañía operadora Fraport AG se fijaron en la tecnología de sensores multifocal Panomera® de Dallmeier.La tecnología de sensores multifocal trabaja con varios sensores con diferentes distancias focales, de modo que se pueden ver incluso distancias muy grandes con una calidad de resolución definida constante. Por lo tanto, el Aeropuerto de Fráncfort sólo necesitó unos pocos sistemas de sensores multifocales para proteger apropiadamente el terreno completo. Se montaron las cámaras de red en los edificios ya existentes. Un criterio de decisión importante para Fraport fue también la sensibilidad lumínica de las cámaras porque el terreno de construcción sólo está iluminado parcialmente. Para la mayor parte del perímetro sólo hay poca luz residual de una iluminación vial alejada. Por ello, la elección fue la serie Panomera® Nightline que proporciona imágenes detalladas en la oscuridad.

Durante la fase de construcción de varios años, también las exigencias a la tecnología de videoseguridad cambiarán y las cámaras habrán de ser reorientadas a otras áreas según las nuevas circunstancias que determine la actividad de la obra. Para ello, la tecnología de sensores multifocal ofrece la flexibilidad perfecta, como subraya Dirk Lüders: «El Aeropuerto de Fráncfort no tiene que desplazar 20 o 30 cámaras individuales, sino que puede montar fácilmente sistemas Panomera individuales en otro lugar para vigilar una sección de construcción nueva».

Dahua lanza la nueva serie Pro de cámaras PTZ

Dahua Technology, fabricante y proveedor de productos de vídeo vigilancia con sede en Hangzhou, China, presenta su nueva serie Pro de la cámara PTZ. Con un rendimiento de alta luminosidad, zoom óptico de 25x, seguimiento automático y capacidad de detección de rostros, esta cámara PTZ aporta nuevas características en cuanto a rendimiento y eficiencia para conseguir una videovigilancia exigente, por ello se ampliará significativamente el uso de la cámara PTZ de gama media en el mercado. La nueva serie Pro de cámaras PTZ ofrece la apariencia del modelo SD59 / SD50 / SD52C que ha sido la preferida por los usuarios.

Mejor imagen

La función Starlight de Dahua, combinando con el ISP de alto rendimiento, el sensor STARVIS Sony y con el algoritmo avanzado Dahua, permite a la nueva cámara PTZ Pro series proporcionar una alta calidad sin precedentes, bajo ruido e imágenes brillantes en condiciones de luz difíciles. Por otra parte, el Wide Dinamic Range (WDR, 120dB) permite a la nueva Pro series proporcionar más detalles y contenidos en escenas con intensa luz de fondo. La distancia IR de estas nuevas cámaras se extenderá entre 100m y 150m, lo que promueve la cobertura de vigilancia por la noche.

Zoom óptico de mayor potencia

Esta nueva serie Pro, además puede ampliar las imágenes a velocidades de hasta 25x, que es muy superior en comparación con otras cámaras PTZ al mismo nivel de precios en el mercado mundial. La efectividad en los costes es un factor importante para una adopción más amplia en aplicaciones de pequeñas y medianas empresas que necesitan capturar detalles de matrículas de automóviles.

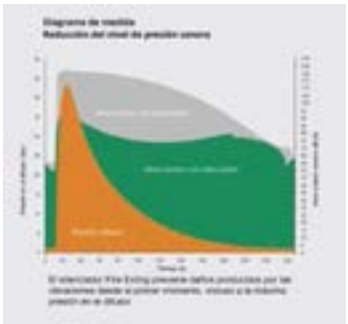
Rendimiento más potente

Auto-tracking, una función inteligente de la serie Ultra, es una característica estándar de la nueva serie Pro de cámaras PTZ, la cual tiene la capacidad de grabar simultáneamente todas las pistas y capturar más detalles al hacer zoom de forma automática, valor que otras cámaras no pueden ofrecer. Además, la tecnología de compresión H.265 compatible con la nueva serie Pro reduce los costes de ancho de banda y almacenamiento hasta en un 50%. Con 60fps@1080P puede capturar movimientos de manera muy nítida, jugando un papel esencial en lugares como casinos o medios de transportes.

La nueva serie Pro de cámaras PTZ de Dahua está diseñada para ampliar las opciones de los usuarios y es ideal tanto para uso al aire libre, como para la vigilancia de las ciudades, centros comerciales, aeropuertos, estaciones de tren y puertos.

Grupo Aguilera: sistema de extinción ArgonAex

El sistema de extinción mediante agente extintor IG55, ArgonAex, incorpora dentro de su gama el silenciador FirExting® Silent. Diseñado para su instalación en salas de servidores y centro de proceso de datos donde existen equipos electrónicos sensibles a las vibraciones producidas por la descarga de gas.



Cuando el sistema de extinción se dispara, el pico de sonido producido puede alcanzar niveles de hasta 120 dB(A) a 1 metro. La vibración puede provocar que los discos duros y otros elementos sensibles se dañen. El silenciador FirExting® SILENT, certificado por VdS, reduce el nivel de presión sonora entre 20 y 38 dB(A), proporcionando una solución eficaz a la pérdida de datos y daños en los discos duros, sin que por ello se vea reducida la eficacia de la extinción.

Certificado por VdS para su uso en instalaciones de gases inertes. Su avanzado diseño permite su instalación incluso en instalaciones ya existentes.

Contactos de empresas, p. 8.

ÍNDICE

MATERIALES, EQUIPOS Y SISTEMAS DE SEGURIDAD

SERVICIOS DE SEGURIDAD

ALARMA Y CONTROL

Techco Security
C/ Barbadillo 7
28042 Madrid
+34 91 312 77 77
www.techcosecurity.com
tcs@techcosecurity.com

GAROTECNIA
Valdelaguna, 4 local 3
28909 Getafe (Madrid)
Tel.: 916 847 767 - Fax: 916 847 769
garotecnia@garotecnia.com
www.garotecnia.com
Autorizada por la D.G.P. con el nº 2.276

Tyco Integrated Fire & Security

Edificio Ecu-I
Ctra. de La Coruña, km 23,500
28290 Las Rozas (Madrid)
Tel.: 902 444 440 - Fax: 91 631 39 78
www.tyco.es

San Fructuoso, 50-56 - 08004 **Barcelona**
Tel.: 934 254 960* - Fax: 934 261 904
Madrid: Matamorosa, 1 - 28017 Madrid
Tel.: 917 544 804* - Fax: 917 544 853
Sevilla: Tel.: 954 689 190* - Fax: 954 692 625
Canarias: Tel.: 928 426 323* - Fax: 928 417 077
Portugal
Rua Ilha da Madeira, 13 A
Olival Basto 2620-045 Odivelas (Lisboa)
Tel.: 219 388 186* - Fax: 219 388 188
www.bydemes.com

FUNDADA EN 1966
INSTALACIONES A SU MEDIDA
ISO 9001

Antoñita Jiménez, 25
28019 Madrid
Tel.: 91 565 54 20 - Fax: 91 565 53 23
seguridad@grupoaguero.com
www.grupoaguero.com

Central Receptora de Alarmas/Videovigilancia
Autorizada por la D.G.P. con el nº. 729
Avda de Olivares 17 – Plg. Industrial PIBO
41110 Bollullos de la Mitación (Sevilla)
Tlfno. 902194814 – 954108887
Fax. 954002319
gerencia@gruporomade.com
SERVICIOS EN TODA ESPAÑA

Accesos | CCTV | Incendio | Intrusión
Oficina Central:
Maresme, 71-79 · 08019 Barcelona
Fax 933 518 554
902 202 206 www.casmar.es

Calle López de Neira, nº3, oficina nº 301
36202 Vigo España
Tel.: +34 986 220 857 / 693 422 688
FAX: +34 986 447 337
www.aforsec.com
aforsec@aforsec.com

CONTROL DE ACCESOS ACTIVO

TALLERES DE ESCORIAZA, S. A. U.
Barrio de Ventas, 35
E-20305 Irún • SPAIN
Tel.: +34 943 669 100
Fax: +34 943 633 221
tesalocks@tesa.es • www.tesa.es

Líderes en Gestión de Horarios y Accesos desde 1978
SKL Smart Key & Lock
Ferrerías 2,
20500 MONDRAGÓN -SPAIN-
+34 943 71 19 52
spec@grupospec.com
www.skl.es

CONTROL DE ACCESO, HORARIO, TIEMPO Y PRESENCIA
C/Samonta 21
08970 Sant Joan Despi
Tel.: +34 934774770
info@primion-digitek.es
www.digitek.es

GRUPO SPEC
Líderes en Gestión de Horarios y Accesos desde 1978
C/ Caballero, 81
08014 Barcelona
Tel. 93 247 88 00 • Fax 93 247 88 11
spec@grupospec.com
www.grupospec.com

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

BIOSYS
(Sistemas de Tecnología Aplicada)

C/ Cinca, 102-104
08030 BARCELONA
Tel. 93 476 45 70
Fax. 93 476 45 71
comercial@biosys.es - www.biosys.es

San Fructuoso, 50-56 - 08004 **Barcelona**
Tel.: 934 254 960* - Fax: 934 261 904
Madrid: Matamorosa, 1 - 28017 Madrid
Tel.: 917 544 804* - Fax: 917 544 853
Sevilla: Tel.: 954 689 190* - Fax: 954 692 625
Canarias: Tel.: 928 426 323* - Fax: 928 417 077
Portugal
Rua Ilha da Madeira, 13 A
Olival Basto 2620-045 Odivelas (Lisboa)
Tel.: 219 388 186* - Fax: 219 388 188
www.bydemes.com

Avda. Roma, 97
08029 BARCELONA
Tel.: 93 439 92 44 • Fax: 93 419 76 73

Delegación Zona Centro:
Sebastián Elcano, 32
28012 Madrid
Tel.: 902 92 93 84

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

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

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

San Fructuoso, 50-56 - 08004 **Barcelona**
Tel.: 934 254 960* - Fax: 934 261 904
Madrid: Matamorosa, 1 - 28017 Madrid
Tel.: 917 544 804* - Fax: 917 544 853
Sevilla: Tel.: 954 689 190* - Fax: 954 692 625
Canarias: Tel.: 928 426 323* - Fax: 928 417 077
Portugal
Rua Ilha da Madeira, 13 A
Olival Basto 2620-045 Odivelas (Lisboa)
Tel.: 219 388 186* - Fax: 219 388 188
www.bydemes.com

GRUPO AGUILERA

FABRICANTES DE SOLUCIONES PCI DETECCIÓN Y EXTINCIÓN DE INCENDIOS

SEDE CENTRAL
C/ Julián Camarillo, 26 28037 MADRID
Tel. 91 754 55 11 • Fax: 91 754 50 98
www.aguilera.es

Delegaciones en:
Galicia: Tel. 98 114 02 42 • Fax: 98 114 24 62
Cataluña: Tel. 93 381 08 04 • Fax: 93 381 07 58
Levante: Tel. 96 119 96 06 • Fax: 96 119 96 01
Andalucía:Tel. 95 465 65 88 • Fax: 95 465 71 71
Canarias: Tel. 928 24 45 80 • Fax: 928 24 65 72
Portugal: Tel. +351 213 563 295 • Fax: +351 213 563 295

Factoría de tratamiento de gases
Av. Alfonso Peña Boeuf, 6. P. I. Fin de Semana
28022 MADRID
Tel. 91 312 16 56 • Fax: 91 329 58 20

Soluciones y sistemas:
** DETECCIÓN **
Algorítmica • Analógica • Aspiración • Convencional • Monóxido • Oxyreduct® • Autónomos • Detección Lineal
** EXTINCIÓN **
Agua nebulizada • Fe-13™ • Hfc-227ea • Co_2

PEFIPRESA, S. A. U

INSTALACIÓN Y MANTENIMIENTO DE SISTEMAS DE SEGURIDAD Y CONTRA INCENDIOS

www.pefipresa.com

Oficinas en: A Coruña, Algeciras, Barcelona, Bilbao, Madrid, Murcia, Santa Cruz de Tenerife, Sevilla, Valencia y Lisboa.

Atención al cliente: 902 362 921
info.madrid@pefipresa.com

¿No cree...
... que debería estar aquí?

El directorio es la zona más consultada de nuestra revista.

Módulo: 660€/año*

Más información:
Tel.: 91 476 80 00
e-mail: publi-seguridad@epeldano.com
* Tarifa vigente 2016

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

PROTECCIÓN CONTRA INCENDIOS. PASIVA

solexin

Calle Alberto Alcocer, 28, 1º A
28036 Madrid
Tel. 913 685 120
info@solexin.es
www.solexin.es

DICTATOR Española

DICTATOR ESPAÑOLA
Mogoda, 20-24 • P. I. Can Salvatella
08210 Barberá del Vallés (Barcelona)
Tel.: 937 191 314 • Fax: 937 182 509
www.dictator.es
dictator@dictator.es

PROTECCIÓN CONTRA INTRUSIÓN. ACTIVA

bydemes

avanzando juntos hacia el futuro

San Fructuoso, 50-56 - 08004 **Barcelona**
Tel.: 934 254 960* - Fax: 934 261 904
Madrid: Matamorosa, 1 - 28017 Madrid
Tel.: 917 544 804* - Fax: 917 544 853
Sevilla: Tel.: 954 689 190* - Fax: 954 692 625
Canarias: Tel.: 928 426 323* - Fax: 928 417 077
Portugal
Rua Ilha da Madeira, 13 A
Olival Basto 2620-045 Odivelas (Lisboa)
Tel.: 219 388 186* - Fax: 219 388 188
www.bydemes.com

DAITEM

ATRAL SISTEMAS
C/ Miguel Yuste, 16 5ª Planta.
28037- Madrid
www.daitem.es

RISCO GROUP

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

Honeywell

Honeywell Security España S. A.
Soluciones integradas de intrusión, vídeo y control de accesos
Avenida de Italia, 7
C. T. Coslada
28821 Coslada
Madrid
Tel.: 902 667 800 - Fax: 902 932 503
seguridad@honeywell.com
www.honeywell.com/security/es

Tecnoalarm

Hi-Tech Security Systems

TECNOALARM ESPAÑA

C/ Vapor, 18 • 08850 Gavà (Barcelona)
Tel.: +34 936 62 24 17
Fax: +34 936 62 24 38
www.tecnoalarm.com
tecnoalarm@tecnoalarm.es

VANDERBILT

VANDERBILT ESPAÑA Y PORTUGAL

Avenida de Monteclaro s/n
Edificio Panatec
CP 28223, Pozuelo de Alarcón, Madrid
Teléfono +34 91 179 97 70
Fax +34 91 179 07 75
info.es@vanderbiltindustries.com
www.vanderbiltindustries.com

PROTECCIÓN CONTRA ROBO Y ATRACO. PASIVA

AGA

HIGH SECURITY LOCK

CERRADURAS ALTA SEGURIDAD
Talleres AGA, S. A.
C/ Notario Etxagibel, 6
20500 Arrasate-Mondragón
GUIPÚZCOA (Spain)
Tel.: (+34) 943 790 922 • Fax: (+34) 943 799 366
talleresaga@aga.es • www.aga.es

diid

Diid Seguridad Gestión y Logística
Pol. Ind. Mies de Molladar D3
39311 CARTES – CANTABRIA
Tlfno.: 902565733 – FAX: 902565884
administracion@diid.es
www.diid.es

TELECOMUNICACIONES

Alai Secure

La solución de seguridad M2M definitiva para las comunicaciones de su CRA

Condesa de Venadito 1, planta 11
28027 Madrid
T. 902.095.196 • F. 902.095.196
comercial@alai.es • www.alaisecure.com

VIGILANCIA POR TELEVISIÓN

HIKVISION

HIKVISION SPAIN
C/ Almazara 9
28760- Tres Cantos (Madrid)
Tel. 917 371 655
info.es@hikvision.com
www.hikvision.com

SAMSUNG Wisenet

Hanwha Techwin Europe Ltd
Avda. De Barajas, 24, Planta Baja, Oficina 1
28108 Alcobendas (Madrid)España(Spain)
Tel.: +34 916 517 507
www.hanwha-security.eu
hte.spain@hanwha.com

GRUPO iPTECNO

Tel. 902 502 035 - Fax 902 502 036
iptecno@iptecno.com - www.iptecno.com
SEDE BARCELONA
IPTECNO Videovigilancia S.L.
C. Pla del Ramassar, 52, Nave 19
08402 Granollers
SEDE MADRID
IPTECNO Seguridad S.L.
Avda. Tenerife, 2 - Blq. 2, Pta. 3
28703 S. S. de los Reyes

alhua TECHNOLOGY

DAHUA IBERIA
C/ Juan Esplandiú 15 1-B. 28007
Madrid
Tel: +34 917649862
sales.iberia@global.dahuatech.com
www.dahuasecurity.com

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

Visiotech
Avenida del Sol, 22
28850, Torrejón de Ardoz (Madrid)
Tel.: 911 836 285 • Fax: 917 273 341
info@visiotech.es
www.visiotech.es

Ballerup, Dinamarca.
Tlf. +34 902 65 67 98
ventas@ernitec.com
www.ernitec.com

AXIS COMMUNICATIONS
C/ Yunque, 9 - 1ºA
28760 Tres Cantos (Madrid)
Tel.: +34 918 034 643
Fax: +34 918 035 452
www.axis.com

EVENTOS DE SEGURIDAD

Expertos en VIDEOVIGILANCIA

LSB, S.L.
C./ Enero, 11 28022 Madrid
Tf: +34 913294835
info@lsb.es

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

GEUTEBRÜCK ESPAÑA
Edificio Ceudas
Camino de las Ceudas, 2 Bis
28230 Las Rozas (Madrid)
Tel.: 902 998 440
Fax: 917 104 920
ffvideo@ffvideosistemas.com
www.geutebruckspain.com

SECURITY FORUM
Tel.: +34 91 476 80 00
Fax: +34 91 476 60 57
www.securityforum.es
info@securityforum.es

C/ Aragoneses, 15
28100 Alcobendas, Madrid
Tlf. 902 902 337
seguridad@eeteuroparts.es
www.eeteuroparts.es

A Western Digital® Company

WD ESPAÑA
4 boulevard des Iles
92130 Issy les Moulineaux · Francia
florence.perrin@wdc.com
Tel.: 615 235 013
www.wdc.com

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

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

Canon España, S.A
Avenida de Europa 6
28108 Alcobendas
Madrid

Tel: +34915384500
www.canon.es
camarasip@canon.es

Josep Estivill, 67-69
08027 Barcelona, Spain.
www.ata98.com
info@ata98.com
Tel. +34 931 721 763

ASOCIACIONES

San Fructuoso, 50-56 - 08004 **Barcelona**
Tel.: 934 254 960* - Fax: 934 261 904
Madrid: Matamorosa, 1 - 28017 Madrid
Tel.: 917 544 804* - Fax: 917 544 853
Sevilla: Tel.: 954 689 190* - Fax: 954 692 625
Canarias: Tel.: 928 426 323* - Fax: 928 417 077
Portugal:
Rua Ilha da Madeira, 13 A
Olival Basto 2620-045 Odivelas (Lisboa)
Tel.: 219 388 186* - Fax: 219 388 188
www.bydemes.com

BOSCH SECURITY SYSTEMS SAU
C/ Hermanos García Noblejas, 19
Edificio Robert Bosch
28037 Madrid • Tel.: 902 121 497
Delegación Este:
Plaça Francesc Macià, 14-19
08902 L'Hospitalet de Llobregat (Barcelona)
Tel.: 93 508 26 52 • Fax: 93 508 26 21
Delegación Norte: Tel.: 676 600 612
es.securitysystems@bosch.com
www.boschsecurity.es

Viladecans Business Park
Edificio Australia. C/ Antonio Machado 78-80, 1ª y 2ª planta
08840 Viladecans (Barcelona)
Web: www.ingrammicro.es
Teléfono: 902 50 62 10
Fax: 93 474 90 00
Marcas destacadas: Axis y D-Link.

C/ Alcalá 99
28009 Madrid
Tel. 915765255
Fax. 915766094
info@uaseguridad.es
www.uaseguridad.es

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

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

C/ Emiliano Barral, 43
28043 Madrid
Tel 91 564 7884 • Fax 91 564 7829
www.aecra.org

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

ACAES
Associació Catalana d'Empreses de Seguretat

C/ Viladomat 174
08015 Barcelona
Tel.: 93 454 48 11
Fax: 93 453 62 10
acaes@acaes.net
www.acaes.net

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

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

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

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

AES

ASOCIACION ESPAÑOLA DE EMPRESAS DE SEGURIDAD
Alcalá, 99
28009 Madrid
Tel.: 915 765 225
Fax: 915 766 094

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

ASELF
Asociación Española de Lucha Contra el Fuego

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

¿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 2016**

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

ASEPAL

ASOCIACIÓN DE EMPRESAS DE EQUIPOS DE PROTECCION PERSONAL
Alcalá, 119 - 4º izda.
28009 Madrid
Tel.: 914 316 298 - Fax: 914 351 640
www.asepal.es

ASIS INTERNATIONAL
Advancing Security Worldwide™
CAPITULO 143 – ESPAÑA
143 CHAPTER - SPAIN

ASIS-ESPAÑA
C/ Velázquez 53, 2º Izquierda
28001 Madrid
Tel.: 911 310 619
Fax: 915 777 190

cepreven

ASOCIACIÓN DE INVESTIGACIÓN PARA LA SEGURIDAD DE VIDAS Y BIENES CENTRO NACIONAL DE PREVENCIÓN DE DAÑOS Y PÉRDIDAS
Av. del General Perón, 27
28020 Madrid
Tel.: 914 457 566 - Fax: 914 457 136

FES

FEDERACIÓN ESPAÑOLA DE SEGURIDAD
Embajadores, 81
28012 Madrid
Tel.: 915 542 115 - Fax: 915 538 929
fes@fes.es
C/C: comunicacion@fes.es

AJSE
Asociación de Jefes de Seguridad de España

ASOCIACIÓN DE JEFES DE SEGURIDAD DE ESPAÑA

Avd. Merididana 358. 4ºA.
08027 Barcelona
Tel. 93-3459682 Fax. 93-3453395
www.ajse.es presidente@ajse.es

sae

ASOCIACIÓN VASCA DE PROFESIONALES DE SEGURIDAD
Parque tecnológico de Bizkaia
Ibaizabal Kalea, 101
sae@sae-avps.com
www.sae-avps.com

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

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

APLICACIONES INFORMÁTICAS

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

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

INTEGRACIÓN DE SISTEMAS

ARQUERO SISTEMA CORPORATIVO

Avda. de la Feria 1
Edificio Incube - sala 8
35012 Las Palmas de Gran Canaria
Tel.: **928 09 21 81**
www.sci-spain.com

CENTRALES DE RECEPCIÓN Y CONTROL

Telecomunicación, Electrónica y Conmutación

Grupo Siemens
Industry Sector
División Building Technologies
Ronda de Europa, 5
28760 Tres Cantos - Madrid
Tel.: +34 91 514 75 00 - Fax: +34 91 514 70 30

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

SOFTWARE DE GESTIÓN DE ALARMAS

Gestión de Incidentes – Plataforma de Vídeo
Mapas Interactivos – Dispositivos Móviles
Innovative Business Software
Tel.: 691 540 499
info@innovative.es
www.innovative.es

INSTALACIÓN Y MANTENIMIENTO

Techco Security
C/ Barbadillo 7
28042 Madrid
+34 91 312 77 77
www.techcosecurity.com
tcs@techcosecurity.com

INSTALACIÓN Y MANTENIMIENTO
INTRUSIÓN – CCTV – INCENDIO – ACCESOS
SUBCONTRATACIÓN
ALICANTE, VALENCIA, MURCIA, ALBACETE
www.seguridadlevante.com
902 400 022
info@seguridadlevante.com

PUBLICACIONES WEB

PUNTOSEGURIDAD.COM
TF: 91 476 80 00

info@puntoseguridad.com
www.puntoseguridad.com

Avda. Manzanares, 196
28026 Madrid
Tel.: 914 768 000 - Fax: 914 766 057
publi-seguridad@epeldano.com
www.instalsec.com

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

MATERIAL POLICIAL

SABORIT INTERNATIONAL

Avda. Somosierra, 22 Nave 4D
28709 S. Sebastián de los Reyes (Madrid)
Tel.: 913 831 920
Fax: 916 638 205

www.saborit.com

VIGILANCIA Y CONTROL

SECURITAS SEGURIDAD ESPAÑA

C/ Entrepeñas, 27
28051 Madrid
Tel.: 912 776 000
email: info@securitas.es

www.securitas.es

Grupo RMD

Autorizada por la D.G.P. con el nº. 729
Avda de Olivares 17 – Plg. Industrial PIBO
41110 Bollullos de la Mitación (Sevilla)
Tlfno. 902194814 – 954108887
Fax. 954002319
gerencia@gruporomade.com
SERVICIOS EN TODA ESPAÑA

TRANSPORTE Y GESTIÓN DE EFECTIVO

LOOMIS SPAIN S. A.

C/ Ahumaos, 35-37
Poligono Industrial La Dehesa de Vicálvaro
28052 Madrid
Tlf: 917438900
Fax: 914 685 241

www.loomis.com

X JORNADAS STIC CCN-CERT

Diez años fortaleciendo la ciberseguridad nacional

Madrid, 13 y 14 de diciembre 2016
Kinépolis (Ciudad de la Imagen)

MÓDULO 1

Ciberespionaje / APTs / Amenazas, Herramientas y Tecnologías

Taller 1:
Herramientas de Detección e Intercambio de Información

MÓDULO 2

Estrategia de Ciberseguridad, ENS Cumplimiento normativo

Taller 2:
Herramientas de Cumplimiento Normativo

GOBIERNO DE ESPAÑA · MINISTERIO DE LA PRESIDENCIA

www.ccn-cert.cni.es/xjornadas
#XJornadasCCNCERT

HIKVISION

UN PARTNER SÓLIDO, COMPROMETIDO, INNOVADOR, FIABLE, PRESENTE.

El valor de un partner tecnológico se mide por su capacidad de generar ventaja competitiva, así como por su actitud y el poder de transmitir determinación, entusiasmo, y motivaciones siempre nuevas. Hikvision garantiza profesionalidad, solidez empresarial, compromiso, fiabilidad tecnológica, innovación continua y un alcance global con presencia local.

Hikvision Spain
C/ Almazara, 9
28760 Tres Cantos (Madrid)
T +34 91 7371655
F +34 91 8058717
info.es@hikvision.com

www.hikvision.com