30 AÑOS
CUADERNOS DE SEGURIDAD

Núm. 339 • DICIEMBRE 2018 • 10,50 euros // cuadernosdeseguridad.com

Seguridad bancaria: una visión integral

Sistemas de Análisis de Vídeo

Seguridad en las ciudades

Edita **Peldaño**

II Jornada Técnica RPAS y Seguridad Privada: crónica del encuentro profesional

Entra en pecket.es
y descubre cómo gestionar
las visitas a tu empresa
de forma inteligente

2019, DESAFÍOS Y OPORTUNIDADES

Un año para el avance y la innovación

Decimos adiós a este 2018 con la satisfacción del trabajo bien hecho. Un año en el que Cuadernos de Seguridad, que ha celebrado su 30 aniversario, ha cumplido de nuevo con su objetivo principal: ser soporte de comunicación y transmisión de información de calidad e interés para el sector de la Seguridad Privada.

Durante estos 12 meses hemos recogido en estas páginas importantes cambios legislativos que afectarán a nuestro sector, así como el imparable avance de la tecnología en un entorno con un enorme potencial, que abrirá las puertas a un año lleno de desafíos pero también de oportunidades.

Además, durante este año que ahora se despide, Peldaño, empresa editora de Cuadernos de Seguridad, ha comenzado una nueva etapa bajo el claim «Comunicamos. Conectamos. Impulsamos». Con una identidad corporativa y una estrategia renovada, que pone en valor el papel de la compañía en el ámbito empresarial, y de manera concreta en el sector de la Seguridad, esta nueva trayectoria tiene como prioridad dar una «mayor y mejor respuesta a la demanda de un mercado cada vez más exigente». Un cambio que muestra nuestra capacidad para adaptarnos a la evolución de nuestro entorno y a la voluntad de acompañar a todos los agentes que forman parte de este sector en este viaje compartido hacia el futuro.

Y en este contexto, y como respuesta a las necesidades del sector, Cuadernos de Seguridad organizó el pasado 30 de octubre la II Jornada RPAS y Seguridad Privada, que contó con la presencia de más de 120 profesionales, en un encuentro en el que se abordaron los retos de futuro y las posibilidades de negocio surgidas tras la reciente aprobación de la nueva normativa. En un foro ameno y distendido en el que se abordaron temas como la normativa actual sobre el uso de RPAS, su aplicación en la seguridad privada; la integración de sistemas y operaciones de seguridad, el control del uso de drones por parte de la Guardia Civil, o la formación profesional en RPAS aplicados a Seguridad Privada, los expertos incidieron en que las empresas del sector incorporen estos dispositivos a su porfolio de servicios con la formación y el cumplimiento de la normativa como ejes fundamentales.

Por otra parte, seguimos con la preparación de Security Forum 2019, que tendrá lugar los días 28 y 29 de mayo en el Centro de Convenciones Internacional de Barcelona, y que tras el éxito del año pasado, volverá a integrar en tiempo y espacio a los sectores de Hotelería y Contact Center, constituyendo una auténtica plataforma de negocio que tendrá como pilares la tecnología y la innovación, donde se expondrán las últimas novedades en materia de Seguridad, y se analizarán las tendencias que marcan el futuro de la industria y del mundo empresarial.

Consolidado como el evento de referencia anual del sector de la Seguridad, Security Forum da un paso más para abrir nuevas oportunidades de negocio proporcionando nuevos modelos y formatos que se adapten a las necesidades de los profesionales y potencien el carácter innovador y emprendedor del sector.

CUADERNOS DE SEGURIDAD

www.cuadernosdeseguridad.com

Nº 339 • DICIEMBRE 2018

Peldaño

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

Presidente: Ignacio Rojas.
Gerente: Daniel R. Villarraso.
Director de Desarrollo de Negocio: Julio Ros.
Directora de Contenidos: Julia Benavides.
Director de Producción: Daniel R. del Castillo.

Director de TI: Raúl Alonso.
Directora de Administración: Anabel Lobato.
Jefe del Dpto. de Producción: Miguel Fariñas.
Jefe del Dpto. de Diseño: Eneko Rojas.

Director Área de Seguridad: Iván Rubio Sánchez.
Redactora jefe de Seguridad: Gemma G. Juanes.
Redacción: Arantza García, Marta Santamarina.
Publicidad: publi-seguridad@epeldano.com
Emilio Sánchez, Beatriz Montero.
Imagen y Diseño: Guillermo Centurión.
Producción y Maquetación: Débora Martín, Verónica Gil, Cristina Corchuelo, Lydia Villalba.

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

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

Printed in Spain

Depósito Legal: M-7303-1988

ISNN: 1698-4269

Precio: 10,50 €. Precio suscripción (un año, 11 núms.) 98 €, (dos años, 22 núms.) 174 € (España).

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

ÍNDICE DE ANUNCIANTES

FEBRERO 2019 - Nº 340

EN PORTADA

SEGURIDAD EN CASINOS

¿Con qué medios y medidas de seguridad cuentan los casinos de nuestro país? ¿Qué papel juega hoy en día la figura del director de Seguridad en este tipo de instalaciones? A día de hoy los directores de Seguridad de los casinos españoles aspiran a que el futuro Reglamento de Seguridad Privada regule aspectos clave de su actividad sin condicionarla en exceso. Para muchos de ellos esta cobertura jurídica dotará a estos profesionales de mayores garantías ante los retos que abordan en su labor. Y es que el avance de la sociedad ha propiciado también que los casinos hayan tenido que ir adaptándose a los continuos cambios de la misma, y en el caso que nos ocupa, en el ámbito de la seguridad. Por eso, son ellos, en esta ocasión, los directores de Seguridad de los casinos, quienes toman la palabra para explicarnos, entre otros aspectos la implantación de nuevos medios y medidas de seguridad, concretamente de prevención y protección. Medidas que también tienen su punto de apoyo en las tecnologías que avanzan rápidamente y las amenazas a las que se enfrentan. Por eso toca ahora preguntarnos: ¿Cómo ha cambiado la seguridad de los casinos en estos últimos años? ¿Cómo gestionan en estos momentos los directores de Seguridad de estas instalaciones la seguridad integral? ¿Cuáles son los riesgos a los que se enfrentan habitualmente? ¿Qué coordinación y colaboración llevan a cabo con las FF. y CC. de Seguridad?

Fer Gregory / Shutterstock

Preechar Bowokitwanchi / Shutterstock

UN NUEVO ESCENARIO PARA LA SEGURIDAD

2019 arranca con perspectivas de mejora, a nivel general y, en particular, en el sector de la Seguridad Privada, que mantiene ese espíritu innovador y emprendedor que le caracteriza ¿Qué deparará 2019 a la industria y al mercado del sector? Una vez más, ¿se hará realidad por fin el desarrollo reglamentario de la Ley de Seguridad Privada? Muchos de los profesionales de la seguridad seguro que se han planteado a lo largo de 2018 éstas y otras muchas preguntas, así como qué pasará, en los primeros meses de 2019. Por ello, en este primer número del año –un clásico ya de nuestra publicación– hemos querido pulsar la opinión de las asociaciones más representativas del sector que muestran su valoración sobre un tema de absoluta actualidad: el futuro del sector y su desarrollo tecnológico. Unas pinceladas donde desvelan algunas de las claves de futuro para el sector.

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

SIMPLE, ELEGANTE, SEGURO

TU SOLUCIÓN DE SEGURIDAD GLOBAL: VÍDEO Y ALARMA

El futuro pasa por la convergencia de todos los elementos de seguridad en lo que llamamos Internet of Security Things, a través de Hik-Connect y de un sistema revolucionario de verificación de vídeo: IVaaS (Intruder Verification as a Service (IVaaS)

EL ENCUENTRO SE CELEBRARÁ EL 28 Y 29 DE MAYO EN EL CCIB DE BARCELONA

Security Forum 2019 conecta con el futuro

La tecnología y la innovación serán los pilares de la próxima edición de Security Forum. Tras el éxito del año pasado, Security Forum compartirá espacio con las áreas de Hotelería y Atención al cliente, constituyendo una plataforma de negocio para las empresas de los tres sectores participantes.

La séptima edición de Security Forum ya está en el horizonte. Tras el éxito de la fórmula rompedora que el evento adquirió en 2018, la apuesta sigue contando con la aportación de los sectores de Hotelería y Contact Center. Estas dos áreas de Peldaño, cuya capacidad de establecer sinergias con Seguridad consiguió el reconocimiento de expositores y visitantes, contarán de nuevo con sus respectivos congresos y áreas de exposición. Todo ello para crear una auténtica plataforma de negocio que tendrá sus pilares en la tecnología y la innovación.

EL punto de encuentro entre el sector de la Seguridad y la industria en 2019 tiene un nombre propio, Security Forum, que se celebrará los días 28 y 29 de mayo en el CCIB de Barcelona. Tras siete años de trayectoria ascendente, el evento se ha convertido en cita ineludible para los profesionales que deseen estar al día tanto de los últimos avances tecnológicos como de las tendencias que marcarán el futuro del sector.

Así lo atestiguan los más de 7.000 visitantes que acudieron a la pasada edición, la primera en la que convergían los sectores de Seguridad, Hotelería y Contact Center. El éxito de esta novedosa fórmula se volverá a repetir este año: los tres sectores, que comparten muchas sinergias en cuanto a estrategia, tecnología y experiencia de cliente, compartirán espacio constituyendo una plataforma de negocio para las empresas y profesionales asistentes. En una edición que tendrá como hilo conductor la «Conexión con el futuro», los visitantes tendrán oportunidad de compartir conocimiento y conocer los últimos lanzamientos de la industria y las tendencias que marcarán el futuro del sector en áreas como la videovigilancia, el control de accesos, la integración de sistemas, la seguridad física y lógica, IP/redes, entre otras. Novedades que se reforzarán con los paneles de expertos que complementan la oferta de soluciones exhibida en los stands.

En paralelo, se celebrará el Congreso, que reunirá a los principales expertos en una primera jornada orientada a la seguridad global, donde se hablará de robótica y tecnología de vanguardia, reservando el segundo día a los especialistas en ciberseguridad, especialmente orientada al ámbito corporativo.

Premios Security Forum

Otro punto ineludible en el evento son los Premios Security Forum, que reconocen y estimulan la innovación y la investigación de proyectos de Seguridad en España. Los Premios cuentan con dos categorías: Mejor Proyecto de Seguridad y Mejor Proyecto de I+D+i. El plazo de inscripción ya está abierto y la fecha límite de recepción de candidaturas expira el 29 de marzo. Los Premios se entregarán en una cena que se celebrará el 28 de mayo en Barcelona.

Las bases de los premios, así como toda la información actualizada sobre el evento se puede consultar en la web **www.securityforum.es**, donde también se encuentra el resumen de la edición 2018. ●

Ficha técnica

Fechas: 28 y 29 de mayo de 2019.

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

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

Periodicidad: Anual.

Carácter: Exclusivamente profesional.

Organiza: Peldaño.

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

INTERNATIONAL SECURITY
CONFERENCE & EXHIBITION

CCIB - BCN
28-29 | 5 | 2019

Security FORUM

Conexión con el futuro

ROBÓTICA | 5G
ÚLTIMAS TENDENCIAS
TECNOLOGÍA | NETWORKING

CUADERNOS DE SEGURIDAD

securityforum.es

Peldaño

EVENTO. EL ENCUENTRO TUVO LUGAR EN EL CÍRCULO DE BELLAS ARTES DE MADRID

Los drones, un aliado para el desarrollo del sector de la seguridad privada

La II Jornada de RPAS y Seguridad Privada concitó a más de 120 profesionales

La II Jornada de RPAS y Seguridad Privada concitó a más de 120 profesionales en el Círculo de Bellas Artes de Madrid para abordar los retos de futuro y las posibilidades de negocio surgidas tras la reciente aprobación de la nueva normativa. Los expertos participantes incidieron en que las empresas del sector incorporen estos dispositivos a su porfolio de servicios con la formación y el cumplimiento de la normativa como ejes fundamentales.

La jornada, organizada por CUADERNOS DE SEGURIDAD, arrancó con las palabras de bienvenida de Iván Rubio, director del Área de Seguridad de Peldaño, quien subrayó que la aplicación de los RPAS al mercado de la Seguridad Privada, «requerirá mayores exigencias, condiciones y garantías que otras aplicaciones. Sin duda alguna será un reto apasionante para ambos sectores».

Según recordó Rubio, la jornada tuvo tres protagonistas. Por un lado, la administración, «estableciendo las garantías legales y normativa necesaria para el desarrollo de la industria», a la que aludió como el segundo actor, y, por último, los usuarios, «los cuales, sin duda, exigirán todas las garantías necesarias para poder afrontar la contratación y utilización de estos nuevos sistemas».

La conferencia de apertura corrió a cargo de Marta Lestau, directora de Seguridad de Aeronaves de AESA (Agencia Española de Seguridad Aérea), quien hizo un análisis del Real Decreto 1036/2017, marco legal que regula el uso de estos aparatos en España.

En su intervención, Lestau aseguró que el actual real decreto «es una evolución normativa» que viene a sustituir a la anterior legislación, «que era muy restrictiva». Esta regulación es, según apuntó, «muy parecida» a la nueva normativa comunitaria, que será más «abierta» y «permitirá las operaciones de drones en todo el entorno europeo».

La directora de Aeronaves de AESA también hizo un balance del estado del sector hasta la fecha en España y que se plasma en 3.509 operadores de drones de menos de 25 kilos, 4.635 aeronaves registradas, 5.354 pilotos y casi 80 expedientes sancionadores incoados a través de las Fuerzas y Cuerpos de Seguridad del Estado. Por su parte, Julio Camino, Jefe del Grupo Operativo de Establecimientos Obligados de la Unidad Central de Seguridad Privada, pronunció la ponencia «Normativa de Seguridad Privada y su aplicación a RPAS». Camino aclaró desde el principio que «los drones no son una medida de seguridad, sino un medio que se puede usar para este fin», por lo que la normativa de seguridad «no regula específicamente su uso».

En todo caso, la legislación sobre los servicios de videovigilancia habla de dispositivos móviles que pueden llevar cámaras, y ahí es donde entrarían los RPAS.

Seguidamente, fue el turno de José Ramón Ferreira, Jefe de grupo de la Oficina de Innovación Tecnológica del CNPIC, quién habló de la relación entre RPAS y Protección de Infraestructuras Críticas desde el punto de vista legal

y operativo, exponiendo los proyectos en los que el Centro trabaja.

Equipo Pegaso

«El control del uso de drones por parte de la Guardia Civil», fue el título de la presentación realizada por el sargento Jorge Pacha, del Equipo Pegaso de la UFAC de la Comandancia de Madrid de la Guardia Civil, en la que dio las claves de la labor que realiza.

Francesc Costa, de Casmar-Aiprox, dedicó su intervención a la integración de sistemas y operaciones de seguridad con RPAS, exponiendo las características del dron que han desarrollado y que permite la aplicación de sistemas de seguridad en entornos que van desde el agrícola a la protección civil, pasando por embajadas o recintos oficiales.

Xavier Peiruza, responsable del Área de Formación de Aircatdrone, se centró en la relevancia de impartir a los futuros pilotos de drones una preparación de calidad e individualizada, mientras que Gonzalo Aréchaga, Responsable de Producto C2IS de THALES, presentó sus soluciones anti drones que permiten inhibir dispositivos maliciosos sin interrumpir el uso de los aparatos que se desean mantener operativos.

La jornada se cerró con la mesa redonda «Retos y oportunidades de los Rpas en la industria de la Seguridad», en la que intercambiaron impresiones el consultor Antonio Sousa, el presidente de AEDRON, Salvador Bellver, y Alfonso Castaño, vicepresidente de ASIS SPAIN. Todos ellos coincidieron en asegurar que gracias a la nueva normativa es un buen momento para que las empresas de seguridad privada apuesten por incorporar a los RPAS a su porfolio de servicios. ●

Texto: *Emilio S. Cófreces*

Fotos: *Xavi Gómez*

MARTA LESTAU. DIRECTORA DE SEGURIDAD DE AERONAVES. AESA

«El Real Decreto es una evolución normativa y se parecerá mucho a la regulación de la UE»

Ponencia: «Normativa actual sobre el uso de RPAS en España»

Marta Lestau, directora de Seguridad de Aeronaves de AESA (Agencia Española de Seguridad Aérea), fue la encargada de ofrecer la ponencia inaugural de la II Jornada de RPAS y Seguridad Privada en la que hizo un análisis del Real Decreto 1036/2017, marco legal que regula el uso de estos aparatos en España.

En su intervención, Lestau aseguró que el actual real decreto «es una evolución normativa» que viene a sustituir a la anterior legislación, «que era muy restrictiva». Esta regulación es, según apuntó, «muy parecida» a la nueva normativa comunitaria, que será más «abierta» y «permitirá las operaciones de drones en todo el entorno europeo».

La directora de Aeronaves de AESA también hizo un balance del estado del sector hasta la fecha en España y que se plasma en 3.509 operadores de drones de menos de 25 kilos, 4.635 aeronaves registradas, 5.354 pilotos y casi 80 expedientes sancionadores incoados a través de las Fuerzas y Cuerpos de Seguridad del Estado.

De igual modo, Lestau destacó los beneficios que permite esta tecnología, entre ellos la generación de negocio en sectores como el de la seguridad privada, a lo que añadió la sustitución del ser humano en tareas peligrosas o la reducción de costes en algunos sectores. En sentido contrario, reconoció que se trata de una normativa sobre drones que no ha sido «fácil, porque desde la Administración se intenta paliar la percepción social negativa derivada de noticias de heridos por drones incontrolados».

Asimismo, explicó que la normativa es aplicable en el territorio y espacio aéreo de soberanía española a aeronaves y elementos que configuran el sistema de aeronave pilotada por control remoto (RPAS); operadores y operaciones que se realicen con ellos, a los requisitos de los pilotos y demás personal involucrado en la operación, a las organizaciones de formación aprobadas y a la aeronavegabilidad y organizaciones involucradas en la misma. Por contra, según apuntó la representante de AESA, no se aplica a los RPAS militares, a los que cuya masa máxima al despegue sea superior a 150 kg, excepto operaciones de aduanas, policía, búsqueda y salvamento, extinción de incendios, etc; y excluidas del Reglamento, a los globos libres no tripulados y los globos cautivos y a los vuelos que se desarrollen en su integridad en espacios interiores completamente cerrados.

Lestau también se refirió a los logros de la División de Drones de AESA, entre los que resaltó la labor de atención a los usuarios e interesados en esta tecnología, plasmada solo en 2018 en 1.080 horas de atención telefónica, 5.535 emails respondidos, 23 ponencias en toda España, y 28 inspecciones para concesión de autorización. De igual modo, hizo referencia a la aportación derivada de los trabajos de la Comisión Asesora de RPAS y al Plan Estratégico 2018-2021 para el desarrollo civil de los drones, elaborado por el Ministerio de Fomento. ●

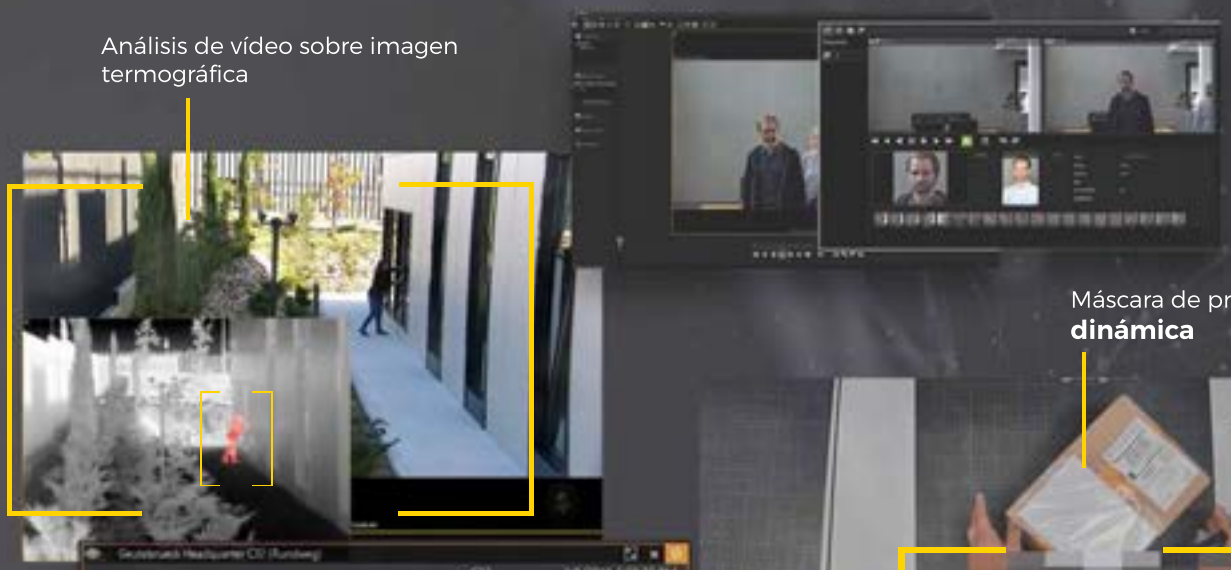
Texto: *Emilio S. Cófreces*
Fotos: *Xavi Gómez.*

GEUTEBRÜCK

Vanguardia en analítica de vídeo

Sistema autómata para la gesión inteligente de toda la información de una instalación de vídeo

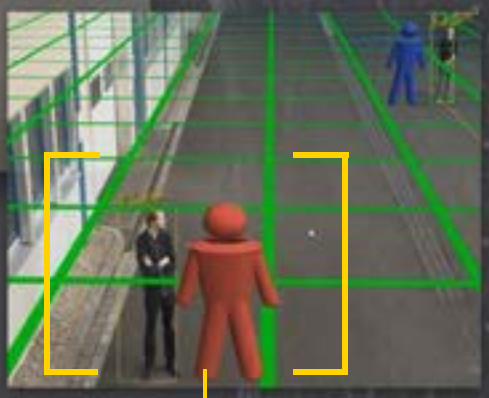
Análisis de vídeo sobre imagen termográfica



Máscara de privacidad **dinámica**

Reconocimiento de matrículas para el control de acceso

Detección de patrones de comportamiento



Detección de movimiento en 3D

Mínima tasa de falsas alarmas

Posibilidad de clasificar los movimientos por tamaño, dirección, distancia y velocidad

Generación de base de datos intuitiva para la localización de los eventos

FF Videosistemas
Distribuidor oficial

Geutebrück España: Calle Vizcaya 2, 28231 Las Rozas (Madrid) | (+34) 91 710 48 04
info@geutebruck.es
Geutebrück México: Anatole France 152PB, 11550 Col. Polanco (CDMX) | (+52) 55 6385 8001
info@geutebruck.mx

JULIO CAMINO. JEFE DEL GRUPO OPERATIVO DE ESTABLECIMIENTOS OBLIGADOS DE LA SECCIÓN OPERATIVA DE INSPECCIÓN. UNIDAD CENTRAL DE SEGURIDAD PRIVADA. CUERPO NACIONAL DE POLICÍA.

«Los drones no son una medida de seguridad privada y por eso la ley no regula su uso»

Ponencia: «Normativa de Seguridad Privada y su aplicación a RPAS»

La aplicación de los drones a la seguridad privada será muy importante en el futuro, pero en el presente es distinto». Con esta contundente puesta en contexto comenzó el inspector Julio Camino, de la Unidad Central de Seguridad Privada de la Policía Nacional, su intervención en la jornada acerca de la «Normativa de Seguridad Privada y su aplicación a RPAS».

Desde el principio, el inspector Camino quiso dejar claro que «la Ley de Seguridad Privada 5/2014 y su desarrollo reglamentario no regulan específicamente el uso de RPAS porque no se trata de una medida de seguridad» En todo caso, explicó, «es un medio material que puede utilizarse con fines de seguridad privada».

A este respecto, ya adelantó que el futuro Reglamento de Seguridad Privada, aún pendiente de aprobación, «tampoco va a regular el uso de RPAS aplicados a este ámbito».

El punto de encuentro entre estos dispositivos y la normativa de seguridad privada estriba en que este texto legal considera a los drones como sistemas que pueden portar cámaras de videovigilancia móviles. Estas cámaras, en el marco de la seguridad privada, solo pueden ser operadas por vigilantes de seguridad o guardias rurales y siempre para prevenir delitos, accesos no autorizados o daños a bienes y servicios. En el ámbito de las empresas de seguridad privada que empleen drones en sus servicios, el inspector Camino recordó que según la normativa deben cumplir una serie de requisitos. Entre otros, habilitarse como operador ante AESA, que la aeronave constituya un medio propio de la compañía o que el piloto sea un vigilante de seguridad o guardia rural y cuente con formación específica.

Medidas de control

Por parte de las Unidades de Seguridad Privada, el inspector Camino señaló que su labor fijada en la normativa pasa por el control del intrusismo, control del ámbito territorial autorizado a la empresa, la verificación de la documentación y el control de las actividades de instalación y mantenimiento. La normativa de seguridad privada incluye la posibilidad de prohibición de usar medios que puedan causar daños o perjuicios a terceros o que pongan en riesgo la seguridad ciudadana, lo que impediría la utilización de drones en caso de darse alguno de estos supuestos.

A modo de conclusión, el representante del Cuerpo Nacional de Policía recordó que AESA establece que «en España no está permitido el uso de drones para aplicaciones civiles sin autorización». En el ámbito de las infraestructuras críticas, apuntó que existe una imposibilidad legal de operar en tareas de vigilancia aérea con drones en el perímetro e interior de instalaciones de una central nuclear, en virtud de una Orden Ministerial de 1993.

Texto: *Emilio S. Cófreces*
Fotos: *Xavi Gómez.*

JOSÉ RAMÓN FERREIRA. JEFE DE GRUPO DE LA OFICINA DE INNOVACIÓN TECNOLÓGICA. CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD. CNPIC

«La suma de esfuerzos multiplica los resultados»

Ponencia: «RPAS y protección de Infraestructuras Críticas»

EL Centro Nacional de Protección de Infraestructuras y Ciberseguridad participó en la «II Jornada RPAS y Seguridad Privada» celebrada en Madrid a través de la intervención de José Ramón Ferreira, responsable de la Oficina de Innovación Tecnológica del centro, con una ponencia sobre «La protección de la Infraestructuras ante la amenaza de un dron».

A modo de introducción, el ponente comenzó exponiendo el funcionamiento y actividades que lleva a cabo el CNPIC, haciendo especial hincapié en la normativa aplicable a estas infraestructuras -Ley 8/2011, de 28 de abril, por las que se establece medidas para la protección de las IC. Ley PIC; Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las IC, etc., así como en los sectores estratégicos existentes en España -Administración, Químico, Energía, Financiero, Alimentación, TIC, Salud, Espacio, Investigación, Transporte, Agua y Nuclear-, de los que en su gran mayoría ya han sido aprobados sus planes estratégicos sectoriales. «No todas las infraestructuras estratégicas son críticas, si bien todas las críticas son estratégicas», matizó Ferreira.

Tras explicar la estructura y funciones de los departamentos que componen el CNPIC, el ponente centró su discurso en las actividades y líneas de actuación que desarrolla el Grupo de Trabajo de RPAS, entre las que destacó: desarrollo normativo; desarrollo tecnológico; antidrones; y proyecto.

En cuanto a normativa, Ferreira puso su atención sobre el artículo 32 del RD 1036/2017 de 15 de diciembre, por el que se regula la utilización civil de las aeronaves por control remoto, y en el que se especifica que «El sobrevuelo por aeronaves pilotadas de las instalaciones e IC de los sectores estratégicos previstos en la Ley 8/2011 de 28 de abril..., estará sujeto a las prohibiciones o limitaciones que establezca el Secretario de Estado de Seguridad del Ministerio del Interior...», además, «El sobrevuelo por aeronaves pilotadas por control remoto de instalaciones afectas a defensa nacional o a la seguridad del Estado, así como las actividades dentro de su zona de seguridad, y de centrales nucleares, sólo podrá realizarse con el permiso previo y expreso del responsable de la infraestructura».

Algunos de los proyectos en los que está inmerso este Grupo de Trabajo RPAS, y a los que hizo referencia el ponente, son el Surveiron, dentro del Proyecto Horizon 2020, un proyecto de investigación europeo que integra innovadoras tecnologías en el ámbito de la inteligencia artificial y la robótica aplicada a flotas de drones, para el desarrollo de centros de control y vigilancia de alto valor añadido. El proyecto DroneCaptor es el desarrollo de un sistema para la detección y neutralización de amenazas con drones. El sistema estará constituido por un potente núcleo basado en la inteligencia artificial y cuyas funciones son: detectar las amenazas, discriminar la peligrosidad, plantear un plan de actuación y tomar medidas de neutralización no destructivas.

Para finalizar José Ramón Ferreira destacó la importancia del trabajo conjunto entre operadores públicos y privados, y FF. y CC. de Seguridad, ya que «La suma de esfuerzos multiplica los resultados». ●

JORGE PACHA. SARGENTO DEL EQUIPO PEGASO DE LA UFAC DE LA COMANDANCIA DE LA GUARDIA CIVIL DE MADRID

«La concienciación y formación es la única forma de reducir incidentes»

Ponencia: «El control del uso de los drones por parte de la Guardia Civil».

EL control del uso de los drones por la Guardia Civil», fue el título de la ponencia impartida por Jorge Pacha, sargento del «Equipo Pegaso» de la Guardia Civil, unidad encargada del control de aeronaves pilotadas por control remoto (drones) en la Comunidad de Madrid. ¿Qué no es Pegaso? fue la pregunta que inició la intervención del ponente y que despejó dudas a los asistentes. «Nos somos la autoridad aeronáutica; ni proveedores de servicios aeronáuticos; ni una unidad de reciente creación», apuntó, al tiempo que matizó «Nuestra misión es controlar el uso de los drones».

En el año 2015, y en previsión a posibles incidentes, la Guardia Civil, a través de la Unidad Fiscal y Aeroportuaria de la Comandancia de Madrid, destinó una serie de recursos humanos y materiales al estudio del uso y control de este tipo aernaves que por entonces empezaban a proliferar. De esta manera, la Guardia Civil creó el «Equipo Pegaso», una inciativa pionera en España que controla las aeronaves pilotadas por control remoto en la Comunidad de Madrid, además de asesorar a unidades policiales a nivel nacional en esta materia.

Conocimiento y preparación

Durante su intervención, Jorge Pacha, hizo hincapié en que el principal peligro del uso de los drones es la falta de preparación y el desconocimiento de la normativa por parte de los que lo usan de forma recreativa. Así, la función principal del equipo es concienciar a los ciudadanos que «el uso de estos drones requiere un mínimo de conocimiento para evitar accidentes aéreos con otras aeronaves que van tripuladas y que llevan pasajeros».

Pacha también hizo referencia al marco legal que regula el uso de drones en España, así como a otras normativas relativas al uso de aeronaves relacionadas con el medio ambiente, protección de datos, protección civil, etc.

El ponente recalcó que las claves para una adecuada utilización de las aeronaves es la concienciación y formación, y «la única manera de reducir incidentes», añadió. Y es que la proliferación de este tipo de aeronaves ha ocasionado diversos incidentes generando un riesgo potencial y causando sensación de inseguridad en los diferentes usuarios del espacio aéreo, originado en su mayoría por la falta de concienciación y desconocimiento de las reglas de circulación aéreas vigente para los usuarios de estas aeronaves. El «Equipo Pegaso», tal y como apuntó, se trata de una unidad policial, proactiva, que cuenta con un equipo consolidado, y que apuesta por la formación y concienciación, como elementos clave a la hora de utilizar los RPAS. «El objetivo es que el sector crezca, pero de forma segura». ●

Texto: Gemma G. Juanes
Fotos: Xavi Gómez

GESTIÓN DE TRÁFICO EFICIENTE PARA NUEVOS RETOS DE MOVILIDAD
MEJORAMOS LA MOVILIDAD EN LAS CIUDADES
MEJOR CONTROL EN LAS INSTALACIONES

Inteligencia Artificial
Identificación inmediata de vehículos sospechosos
Reconocimiento de matrículas
Reconocimiento de placas de mercancías peligrosas
Soluciones para trazabilidad de vehículos y mercancía
Análisis forense de bases de datos
Sistemas embarcados
Control de accesos y aparcamientos

Analíticas de vehículos
- Categoría
- Marca
- Matrícula
- Velocidad
- Color

Generación de alertas instantáneas
- Semáforo en rojo
- Radar de tramo
- Giro indebido
- Zonas peatonales

www.casmarglobal.com
info@casmarglobal.com
933 406 408 • 902 202 206

FRANCESC COSTA. DIRECTOR DE PROYECTOS RPAS. CASMAR- AIPROX.

«La integración de RPAS con sistemas de seguridad es posible legal y técnicamente»

Ponencia: «Integración de sistemas y operaciones de seguridad con RPAS»

LA integración de sistemas de Seguridad y RPAS no solo es posible, sino que es el elemento clave y definitivo para poder pensar en operativas con estos aparatos de forma eficiente, controlada y continuada.Esta es la premisa que inspiró la ponencia de Francesc Costa, director de Proyectos de RPAS en Casmar-Aiprox, en la II Jornada de RPAS y Seguridad Privada.

En su intervención, Costa repasó los elementos necesarios para esa integración, las posibilidades tecnológicas actuales para ello, la filosofía de trabajo necesaria para la integración en el ecosistema de negocio de las compañías, así como los beneficios de la digitalización.

Para empezar, Costa definió a un dron destinado a labores de seguridad como «un multicóptero con cámaras», que para operar precisa de «piloto, copiloto y sistemas de transmisión». Además recordó que para llevar a cabo misiones 24/7 también requiere de «todo el personal necesario en la zona». Esta realidad supone que todo ello sea «tan eficiente e integrado como un operador por cada cámara IP», afirmó Costa, quien a renglón seguido se preguntó «por qué» tiene que ser así.

«¿Es un problema legislativo o técnico?», planteó el ponente, quien señaló que la integración de los RPAS en sistemas de seguridad «no es un problema ni legal ni técnicamente». En relación a la normativa, aludió a la evolución del marco legal en el ámbito europeo impulsada por el proyecto SESAR hasta el año 2030 y su tendencia hacia esa integración, mientras que en el plano técnico recalcó los avances en materia de comunicaciones, carga de batería, tiempo de vuelo e integración de sistemas a través del software Gyroos, un sistema operativo de nivel empresarial dentro del drone creado para Airprox para controlar todas las operaciones en tiempo real.

Un sistema integrado

«Ya que no había problemas para crear un dron así, ya lo hemos fabricado», aseveró Costa. El sistema integrado de Aiprox permite drones autónomos, con pistas de aterrizaje y cargas automáticas, comunicaciones bidireccionales, pulseras y localizadores interactivos, integración de sistemas de seguridad como cámaras de videovigilancia o Centrales Receptoras de Alarmas, todo ello gestionado desde Gyroos.

Este sistema está ideado para constituir «una nueva perspectiva de seguridad» que tiene como objetivo «alinearse con el negocio», subrayó el representante de Casmar-Aiprox.

Los sectores y ámbitos de aplicación de este sistema son amplios y variados, desde instalaciones eléctricas, líneas ferroviarias, pasando por piscifactorías, minas a cielo abierto hasta campos de cultivo, recintos oficiales o tareas relacionadas con la protección civil.

Texto: *Emilio S. Cófreces*
Foto: *Xavi Gómez.*

XAVIER PEIRUZA. RESPONSABLE DEL ÁREA DE FORMACIÓN. AIRCATDRONE; **CHRISTIAN SÁNCHEZ.** COO. AIRCATDRONE; **ÓSCAR MATEOS.** DIRECTOR DE MARKETING. AIRCATGLOBAL

«La calidad en la formación es garantía de la prevención de accidentes»

Ponencia: «Formación profesional en RPAS aplicados a Seguridad Privada»

LA calidad en la formación es garantía de la prevención de accidentes». Así lo aseguraron los representantes del Grupo Aeronáutico Aircatglobal -compañía que engloba 3 divisiones: Aircatsim, Aircatfly y Aircatdrone-, durante su intervención en la II Jornada de RPAS y Seguridad Privada, en la que abordaron «Formación profesional en RPAS aplicados a Seguridad Privada».

Óscar Mateos, director de Marketing de la compañía, explicó las actividades del Grupo Aircatglobal, del que aseguró ofrece «formación en aeronáutica de máximo nivel», haciendo hincapié en que la experiencia y la formación son elementos fundamentales para la seguridad en el uso de RPAS.

A continuación, y siguiendo con el tema de la formación como eje central de las intervenciones, Christian Sánchez, COO de Aircatdrone, apostó por la formación integral, conjugando la parte teórica con la práctica. Bajo su punto de vista, tres son los pilares para conseguir profesionales adecuadamente preparados: por un lado, calidad en la formación, «ofreciendo un seguimiento formativo del alumno y una calidad máxima en vuelo real sin simuladores»; por otro, contar con el «mejor material posible para los alumnos sobre la base de I+D»; y, finalmente, disponer de un servicio de gestoría y asesoría.

Xavier Peiruza, responsable del Área de Formación de Aircatdrone.

Por su parte, Xavier Peiruza, responsable de Área de Formación de Aircadrone, explicó que el primer sector donde creció el uso de los drones y se profesionalizó fue en el ámbito audiovisual, ahora es el sector de la Seguridad Privada y Seguridad Pública donde ya se utilizan como «una herramienta de trabajo». Y así es, tal y como explicó, algunas de las aplicaciones profesionales de RPAS en el sector de la seguridad serían la vigilancia, protección de personas y bienes, acciones proactivas,... «La seguridad es un sector emergente en el uso de drones», apuntó Peiruza, quien además destacó la necesidad de contar con profesionales perfectamente formados. ●

Texto: *Gemma G. Juanes*
Fotos: *Xavi Gómez.*

Óscar Mateos, director de Marketing de Aircatglobal.

Christian Sánchez, COO Aircatdrone.

GONZALO ARÉCHAGA. RESPONSABLE DE PRODUCTO C2IS. THALES

«El mayor problema que existe es el mal uso que se hace de los drones»

Ponencia: «El desafío de la Seguridad ante los drones».

CON el ejemplo de varios incidentes protagonizados por drones publicados en medios de comunicación — «Un drone fuerza el cierre de la pista de aterrizaje del aeropuerto londinense de Gatwick», «Un Airbus A320 evita "in extremis" el choque con un dron durante su aterrizaje en Francia», o «Un avión tuvo que esquivar tres drones para aterrizar en Bilbao», comenzó la intervención de Gonzalo Aréchaga, responsable de Producto C2IS de Thales, bajo el título «El desafío de la seguridad ante los drones».

«El mayor problema es el mal uso que se hace de los drones», aseguró el ponente, para quien hoy en día existe una proliferación de drones en el mercado de consumo electrónico debido a su facilidad de operar sin necesidad de licencia y su venta a precios muy asequibles. «La principal amenaza son los micro y mini drones, muy difíciles de detectar y que pueden volar a velocidades de hasta 80 Km/h», apuntó.

Bajo estas premisas, Aréchaga explicó la funcionalidad del sistema antidrones de última generación C-UAS, de Thales, entre cuyas funciones destaca: detección, clasificación, identificación y seguimiento, y neutralización.

La solución se compone de un radar Squire para la detección activa de micro drones a cuatro kilómetros de distancia, fácil de transportar y óptimo para un sector de 90. Además y, de manera opcional, se puede disponer de un Radiogoniómetro RF One, con hasta 5 kilómetros de alcance.

En la fase de Identificación y Seguimiento, la solución cuenta con Gecko Optronics: un sistema optrónico de largo alcance compuesto por una cámara térmica y una cámara visible HD, así como tracking de vídeo. Ya, en la fase de neutralización, cuenta con un Inhibidor Drone Gun, que interfiere las bandas seleccionadas: radiocontrol, vídeo, GPS, con un alcance de hasta 2 kilómetros.

Además, la solución cuenta para el Control y Visualización con el software de control HORUS, para controlar estos sistemas sobre el terreno o de manera remota desde un Centro de Control. El software fusiona información de los sensores y ayuda a analizar la amenaza. Permite la fusión de información, análisis de amenazas, seguimiento automático de trazas, fusión de información, etc.

Texto: Gemma G. Juanes

Fotos: *Xavi Gómez*

HDCVI 5.0.
Perspectiva de vigilancia

- Ventajas para usuarios de HDCVI con tecnología y productos innovadores basados en el chipset AI (Inteligencia Artificial) y el algoritmo de aprendizaje profundo.
- Alarmas precisas en la protección del perímetro a través de la identificación humana y del vehículo.
- Alarmas de sospechosos en lista negra o habilitación de acceso autorizado en lista blanca con aplicación de reconocimiento facial.
- Búsqueda inteligente de rostros humanos obteniendo atributos de características y modelado, mejorando la eficiencia de rescate.
- Alerta activamente a los intrusos con una sirena y linterna detectadas con movimiento dual PIR y movimiento.
- Seguimiento fiable 24 horas con tecnología a todo color, aumento de visibilidad en evidencias y eventos.

Modelos recomendados

DH-XVR8000-4K/4KL-I
HDCVI 4K & H.265 AI XVR

HAC-ME2241C(-W)
Camara HDCVI de disuasión activa

HAC-2802/2501/2241 Series
Cámara HDCVI Starlight 4K/5MP/1080P

HAC-2249-LED Series
Cámara HDCVI 1080P a todo color

ISO 9001:2000

DAHUA IBERIA, S.L.
Juan Esplandiú 15-1B-28007 Madrid, SPAIN
+34 917649862
http://www.dahuasecurity.com/es/
sales.iberia@dahuatech.com

ANTONIO SOUSA. DIRECTOR GENERAL DE SOUSA CONSULTOR. **SALVADOR BELLVER.** PRESIDENTE DE AEDRON. **ALFONSO CASTAÑO.** VICEPRESIDENTE DE ASIS SPAIN.

«Es un momento dulce para usar drones en seguridad privada»

Mesa de debate: «Retos y oportunidades de los RPAS en la industria de la Seguridad»

Los drones constituyen ya una tecnología madura para ayudar a las empresas de seguridad privada a generar negocio. Es la principal conclusión que transmitieron los expertos participantes en la mesa de debate «Retos y oportunidades de los RPAS en la industria de la Seguridad» con la que se clausuró la II Jornada Técnica de RPAS y Seguridad Privada.

«Es un momento dulce para que el sector de la Seguridad Privada apueste por los drones», en palabras de Salvador Bellver, presidente de la asociación de usuarios de drones AEDRON y uno de los participantes en el coloquio. Bellver sostuvo su opinión al afirmar que «el sector de los drones ha comenzado a moverse y se está focalizando hacia la Seguridad» y recordó que «para las empresas de Seguridad el hecho de que incorporen drones a su oferta de servicios supone una promoción espectacular».

La misma visión positiva transmitió el consultor Antonio Sousa, quien, no obstante, recordó a los asistentes que la incorporación de este tipo de tecnología debe realizarse siempre que el servicio que se vaya a prestar así lo requiera. «No hay que meter los drones allí donde no haga falta», aconsejó Sousa.

El contrapunto a este optimismo lo puso Alfonso Castaño, vicepresidente de la asociación ASIS España, para quien la normativa «aún no deja hacer muchas cosas y para generar negocio la Administración debe abrir la mano».

Esa visión fue rebatida por Sousa, para quien la legislación vigente no es una cortapisa a la hora de que las empresas de seguridad privada añadan drones a su porfolio de negocios. «Todo se puede hacer pero hay que cumplir

Antonio Sousa, director general de Sousa Consultor.

la normativa», puntualizó. En esta línea, el consultor animó a los asistentes a la mesa redonda a familiarizarse con la legislación relativa a drones. «Si conocéis la normativa, vais a hacer las cosas bien», apuntó Sousa, para quien las claves de una buena utilización de los RPAS en seguridad privada son la «concienciación y la formación».

Por su parte, Bellver asumió que la legislación «impone limitaciones al uso de los RPAS, pero es algo temporal y en breve esperamos que haya cambios, además, la normativa siempre va por detrás y tenemos que ser proactivos». En ese punto, el presidente de AEDRON también reclamó a la Administración que apueste por un texto legal «más comprensible y ágil».

A este respecto, Sousa, que ha participado en la elaboración del Real Decreto, remarcó que «Europa está bebiendo de nuestra normativa, y será más fácil que se adapte la regulación española a la europea que otras como la portuguesa, donde se pueden hacer cosas que la UE no va a permitir».

Desafíos tecnológicos

Al margen de cuestiones legales, las cuestiones puramente tecnológicas también centraron parte del intercambio de opiniones.

En ese punto, Alfonso Castaño se refirió a las que son, a su juicio, cuestiones clave a las que un futuro desarrollo técnico de los RPAS debe dar solución: La duración de las baterías y la capacidad de recarga de los aparatos, que se va reduciendo en cada uso. Castaño también apuntó a la Ley Orgánica de Protección de Datos como otro escollo en la utilización de drones con cámaras de vigilancia para fines de Seguridad Privada, unas cámaras que reclamó sean «certificadas por la Unidad Central de Seguridad Privada de la Policía, porque no vale cualquiera».

Alfonso Castaño, vicepresidente de ASIS España.

«Los expertos reclaman a la Administración una norma más ágil para generar negocio en el sector»

«Los aspectos tecnológicos se irán solventando en poco tiempo», vaticinó Salvador Bellver. Para Antonio Sousa, la clave tecnológica pasa por mejorar los sistemas de comunicaciones.

Respecto a la labor de los directores de Seguridad en relación al uso de los RPAS, Alfonso Castaño recordó que «hay que justificar que es un dron lo que se necesita», y subrayó que para los vigilantes de seguridad supone «una multitarea guiar a los drones hasta un punto de peligro».

Texto: *Emilio S. Cófreces*
Fotos: *Xavi Gómez*

Salvador Bellver, presidente de AEDRON.

Marta Lestau. Directora de Seguridad de Aeronaves. AESA.

Iván Rubio. Director del Área de Seguridad de PELDAÑO.

Alex Martínez, director de Seguridad del Centro Comercial La Vaguada; Gemma G. Juanes, redactora jefe de la revista CUADERNOS DE SEGURIDAD; Javier Calderón, director de Seguridad de Centro Comercial Plaza Río 2; junto a José Antonio Organista Ortega, jefe de Proyectos y Desarrollo de negocio. Securitas (de dcha. a izq.)

Xavier Peiruza, Christian Sánchez y Óscar Mateos, de Aircatglobal.

Julio Camino. Jefe del Grupo Operativo de Establecimientos Obligados de la Sección Operativa de Inspección. Unidad Central de Seguridad Privada del CNP.

Jorge Pacha. Sargento. Equipo Pegaso de la UFAC de la Comandancia de la Guardia Civil de Madrid.

Beatriz Montero, consultora de Comunicación de PELDAÑO, con representantes de Aircatglobal.

José Ramón Ferreira. Jefe de Grupo de la Oficina de Innovación Tecnológica del CNPIC.

Iván Rubio, director del Área de Seguridad de PELDAÑO, moderador de la Mesa de Debate en la que participaron, Salvador Bellver, presidente de AEDRON; Alfonso Castaño, vicepresidente de ASIS Spain, y Antonio Sousa, director general de Sousa Consultor.

Anna Aisa, gerente de ACAES; Carmen Moraleda, de la Guardia Civil; y Gemma G. Juanes, redactora jefe de la revista CUADERNOS DE SEGURIDAD.

Francesc Costa. Director de Proyectos RPAS en Casmar-Aiprox.

Gonzalo Aréchaga. Responsable de Producto C2IS de Thales.

Anna Aisa, gerente de ACAES; Carmen Moraleda, de la Guardia Civil; Juan Carlos Ferrera, director de Seguridad del Canal de Isabel II; Javier Dario. Gerente Delegación Centro. Ilunion; Beatriz Montero, consultora de PELDAÑO; Miguel Ángel Gallego, director de Seguridad de la Estación Sur de Autobuses de Madrid; y Gemma G. Juanes, redactora jefe la revista CUADERNOS DE SEGURIDAD.

Manuel Yanguas. Comisario Jefe de la Unidad Central de Seguridad Privada del CNP, acompañado de Beatriz Montero, consultora de Comunicación de Peldaño, y Gemma G. Juanes, redactora jefe de la revisa CUADERNOS DE SEGURIDAD.

Fotos: *Xavi Gómez*

KEDACOM

Especialistas en analítica de video

COREA - SINGAPUR - CHINA

Video Sinopsis - Video Recognitivo - Deep Learning
Reconocimiento Facial - Smart City - Análisis de Video
Cámaras IP Inteligentes - NVRS profesionales - Software de análisis

EUROMA

www.euroma.es

MADRID
C/ Emilia 55 local 4 28029 Madrid
Tel: +34 91 571 13 04 / 15 19
Fax; +34 91 570 68 09
Email: euroma@euroma.es

BARCELONA
C/ Bogatell 43-49 1º 2ª 08930 Sant Adriá de Besos
Tel: +34 93 381 24 58 / 22 12
Fax: +34 93 381 57 34
Email: barcelona@euroma.es

ÁLVARO ECHEVARRÍA ARÉVALO. DIRECTOR DE SEGURIDAD Y SERVICIOS CORPORATIVOS. BANC SABADELL

«La dirección de Seguridad ha de basarse en la transversalidad y visión de conjunto»

ATRÁS quedaron los tiempos en los que la dirección de Seguridad de un banco solo se preocupaba de reaccionar ante posibles amenazas contra sus instalaciones. La evolución a un modelo predictivo y alineado con la operativa de negocio es una realidad en el Banc Sabadell, cuyo director de Seguridad repasa las claves de esa evolución.

—¿Qué objetivos y estrategia se ha marcado tras su nombramiento como director de Seguridad y Servicios Corporativos de Banc Sabadell?

—Los objetivos se dividen en cuatro ejes fundamentales:

Consolidar la evolución de la Dirección de Seguridad Corporativa desde un modelo tradicional más reactivo a uno con un componente anticipativo y predictivo 24x7, basado en el tratamiento analítico de datos y con vocación de servicio de valor añadido al resto de direcciones corporativas de Banc Sabadell.

Un buen ejemplo es lo que pretendemos hacer con la clásica gestión de Hechos Delictivos, ofreciendo a la estructura de Banc Sabadell en su conjunto, gestionar informaciones que permitan una mayor facilidad para la toma de decisiones con el objetivo que éstas tiendan a ser acertadas en sus diversas funciones dentro de la Entidad, manteniendo el riesgo delincuencial y reputacional en niveles de control bajos.

En segundo lugar, la adaptación de los sistemas de seguridad, no sólo a los requerimientos legales establecidos, sino a los niveles que forman parte del criterio de seguridad de Banc Sabadell. Estos sistemas de seguridad se adaptan a las funcionalidades y necesidades de los usuarios con una serie de facilidades propias, que están siendo posibles gracias a la implementación a gran escala de la tecnología.

Por otro lado, la transformación del Security Operations Center (SOC). El SOC ha evolucionado históricamente desde las iniciales responsabilidades como Central Receptora en que únicamente recepcionaba y verificaba señales de alarmas, su posterior aumento de perímetro como Centro de Gestión de Alarmas, ya que a su anterior función se añadió el proceso de gestión integral de los avisos ante otros incidentes que pudieran afectar el normal funcionamiento de las oficinas y cajeros automáticos, hasta las actuales funciones ya implementadas y que pueda desarrollar en el futuro.

Así, el SOC se ha configurado como punto de centralización 24x7 de la seguridad de empleados en viajes profesionales, gestión de alarmas, tele-mantenimiento de sistemas de seguridad, tele-vigilancia en situaciones de riesgo por inoperatividad o afectación de los sistemas de seguridad, manifestaciones y otros conflictos sociales, seguimiento y resolución de averías de sistemas de seguridad de primer nivel, incidentes de seguridad en el perímetro personas y coordinación de acciones y punto de referencia sobre la Continuidad Operativa, ante procesos disruptivos varios

que pudieran incidir sobre los centros de trabajo de Banc Sabadell. Así mismo, facilita servicio de manera transversal a otras direcciones (Obras y Mantenimiento, IT Tecnología, Continuidad y Organización, entre otras).

Finalmente, como complemento a las anteriores, afianzar, como venimos haciendo hasta ahora, la necesaria e ineludible coordinación de la Seguridad Corporativa con la Seguridad de la Información mediante mecanismos de colaboración y control que configuren un Government of Integral Security efectivo, atendiendo a un perímetro Global incluidas las singularidades y requerimientos regulatorios de nuestras estructuras en el extranjero.

—¿Podría describirnos las particularidades sobre la gestión de seguridad en Banc Sabadell?

—La respuesta a ésta pregunta podríamos alinearla a la propia evolución de Banc Sabadell y su transformación dentro del sector financiero desde su entorno geográfico inicial muy localizado, la expansión registrada y su evolución, hasta convertirse en un banco global caracterizado por su agilidad de adaptación al cambio.

La gestión de la seguridad de Banc Sabadell se ha desarrollado, en su última etapa, centrándose en el objetivo de convergencia de trece culturas diferentes en materia de seguridad, fruto de las fusiones y adquisiciones realizadas tanto a nivel nacional como internacional por la Entidad.

Con el máximo respeto a las estructuras de seguridad de las entidades fusionadas, sus realidades, condicionamientos, singularidades y el aprovechamiento de las mejores prácticas de todas ellas se determinó, para cada una de las operaciones de fusión realizadas, la convergencia hacia un Banc Sabadell Security Steering Model que nos permitiera continuar dentro de los niveles

«Banc Sabadell y su dirección de Seguridad se han visto envueltos en un meteórico proceso de transformación»

delincuenciales bajos en los que históricamente se ha situado Banc Sabadell. Lógicamente, lo que dentro de nuestra Organización denominamos Modelo Preventivo de la Seguridad, no sólo se limita a una declaración de intenciones o de la aplicación de los principios que configuran la Política de Seguridad. El proceso de convergencia ha necesitado de cambios sustanciales de adaptación en sistemas de seguridad, formación, protocolos, normativas y la evolución de nuestra estructura a estas necesidades.

Resumiendo, Banc Sabadell, al mismo tiempo que su Dirección de Seguridad, se han visto envueltos en un meteórico proceso paralelo de transformación y adaptación a las circunstancias sobrevenidas y a la ejecución de los diversos Planes Estratégicos de la Entidad muy dinámicos.

—Pregunta obligada hoy en día es si ¿cree que ha llegado el momento de adaptar las estructuras de los departamentos de Seguridad a las nuevas necesidades empresariales?

—Indiscutiblemente. La alta velocidad de transformación social, cultural, la aplicación en el tradicional negocio bancario de nuevos canales, formas y dispersión de centros de trabajo, los impactos reputacionales, el cumplimiento normativo y, sobre todo, los modelos delincuenciales globales e industrializados hacen necesaria una ágil adaptación de las estructuras de seguridad no sólo para paliar o minimizar de forma reactiva los riesgos, materializados o no, sino para que el modelo de seguridad tienda a ser más predictivo que el histórico modelo reactivo que hasta ahora se aplicaba en las Direcciones de Seguridad tanto en el sector financiero como en el resto.

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

—Ha de tener una visión amplia del concepto de la Seguridad, ya no sólo de la seguridad física o de la información, sino también de todo lo que supone mantener operativa la entidad. Ayudar

«La colaboración entre el departamento de Seguridad y el departamento de Seguridad de la Información es total y bidireccional»

desde el punto de vista de la Seguridad a mantener operativos los centros de producción en relación a la accesibilidad a los centros de trabajo, los procesos críticos que pudieran desarrollarse en su interior, suministros, etc., y en general a procurar que en el entorno de trabajo no se produzcan incidentes disruptivos.

Por otro lado debemos asegurar la cobertura de las necesidades en seguridad de algunos reguladores no necesariamente relacionados con Seguridad Privada, vinculados a los procesos que se desarrollan o a proveer los controles en seguridad establecidos por reguladores nacionales o internacionales.

Gestionar y vigilar anticipativamente las repercusiones mediáticas y el riesgo reputacional sobre las entidades financieras que, no olvidemos, durante los últimos diez años han estado permanentemente examinadas por la sociedad en general y especialmente por algunos colectivos organizados.

—¿Qué protocolos de colaboración y coordinación existen entre el departamento de Seguridad y el departamento de Seguridad de la Información de Banc Sabadell?

—La colaboración es total y bidireccional. No sólo a efectos de la valoración de riesgos y gestión de incidentes. Es imposible separar causas y efectos en ambas disciplinas. Las tipologías delictivas clásicas han mutado mediante la utilización del factor tecnológico pero mantienen el mismo fin, beneficio económico, extracción de información, bloqueo operativo, difamación, extorsión...

Así pues las dos direcciones convergen en el desarrollo de los protocolos de activación, gestión y reporting de incidentes tecnológicos y en todos aquellos relacionados con la seguridad corporativa en los que intervenga la tecnología que, como es evidente, difícil es encontrar alguno en que no se produzca.

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

—Transversalidad. La dirección de Seguridad ha de tener visión y capacidad de gestión sobre un conjunto de direcciones corporativas que, al margen de la entidad, suelen ser coincidentes en todos los casos (Seguridad de la Información, Operaciones, Continuidad, RRHH, Gabinete de Comunicación, Cumplimiento Normativo, Asesoría Jurídica, Obras/Mantenimiento, Prevención de Riesgos Laborales, etc.).

Servicios de valor añadido para el resto de la organización. Como consecuencia de la transversalidad detallada en el punto anterior, las direcciones de Seguridad han de poder identificar oportunidades en otras direcciones corporativas para implementar, participando ya desde la fase de diseño, las medidas, criterios y protocolos alineados a la Política de Seguridad de cada entidad, aportando servicios que sean de interés para cada dirección y que al final del proceso se demostraran útiles para la Seguridad Integral de la estructura organizativa.

Explotación, análisis, conclusiones y aplicación en el entorno del Data Analitycs (DA). Más allá de los datos que de forma autónoma hasta ahora las direcciones de seguridad han explotado y que configuran sus respectivos Cuadros de Mando, estadísticas y Memorias de Actividad, etc., nos encontramos con

la necesidad de explotación de los datos que gestionamos y que con las herramientas informáticas adecuadas nos pueden ofrecer conclusiones que ayuden a adoptar medidas, criterios, normativas internas, sistemas más adecuados a las necesidades reales.

—Con una visión de futuro, ¿cómo imagina el futuro de la seguridad en las entidades bancarias donde los grandes avances tecnológicos serán los protagonistas?

—El futuro de la seguridad en las entidades financieras deberá ir, ineludiblemente, de la mano de los Planes Estratégicos de la misma aprovechando lo que denominamos paraguas tecnológico. La fortaleza de los sistemas informáticos de las entidades financieras y su continua evolución configuran, sin duda, el Core de su propia actividad y ofrece total garantía también sobre los sistemas que gestiona la Dirección de Seguridad.

La ayuda a la toma de decisiones, el control sobre el fraude en las operaciones bancarias presenciales y con mayor tendencia a que no lo sean por la potenciación de los canales remotos, el seguimiento sobre la globalidad e internacionalidad de las mismas, etc., será un gran soporte para que la estrategia empresarial se convierta en realidad.

Por otro lado los proveedores de seguridad, atendiendo a las necesidades del sector, se convertirán en colaboradores muy especializados, por ejemplo, en explotación de datos aportando experiencia sobre herramientas de gestión, integración y mejora de la eficiencia en el sector de la seguridad.

Las empresas proveedoras de servicios se configuran como un eslabón más en la cadena de la Seguridad y deben mantener niveles de calidad, eficiencia y especialización, como mínimo, equiparables al emanado por la entidad que les contrate.

«La toma de decisiones es objetiva, tangible y demostrable, ayudando a la entidad más allá del espacio acotado»

—¿Cómo ha variado la seguridad, en cuanto a logística y estrategia en las grandes entidades bancarias como Banc Sabadell?

—Notablemente. Debemos olvidarnos de aquellos argumentos, ya desfasados, que todos hemos escuchado sobre que las direcciones de seguridad son un centro de coste que sólo provoca gastos y que trabajan sobre intangibles que pueden o no materializarse.

Ahora las direcciones de seguridad trabajan con matrices de riesgo, evalúan probabilidades y niveles de criticidad, participan en la homologación de productos o servicios comerciales desde el punto de vista de posibilidad de materialización de fraude, son habitualmente consultadas y aportan información sobre tendencias delictivas y zonas delincuenciales, evalúan riesgos personales o que puedan provocar personas propias o de empresas subcontratadas atendiendo a las funciones que ha de desarrollar, lideran y forman parte de comités de primer nivel y de notoria relevancia.

En definitiva, la toma de decisiones es objetiva, tangible y demostrable, ayudando al conjunto de la entidad más allá del espacio acotado que históricamente ocupaba.

Por todo ello me congratulo de poder vivir este momento de transformación, colaborar con grandes profesionales y amigos del sector, aportando mi experiencia personal y la de mi equipo. ●

Texto: Gemma G. Juanes.
Fotos: Banc Sabadell

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

En la senda de la digitalización... con reparos

La realidad de la operativa bancaria, la realidad de la banca, es la de la diversidad, la de la multicanalidad

NO me toca hoy hablarles de blockchain o cadena de bloques, que para unos (incluida la ONU) añade transparencia, eficiencia, seguridad, resolución de problemas globales y un menor tiempo en el movimiento del dinero, y muchas dudas para otros hasta hace poco; tampoco del bitcoin y las criptomonedas (hay más de 1.600), puestas en cuestión por todo tipo de gobiernos y Organismos, entre ellos el FMI, aunque algunos bancos ya tengan start-ups utilizadas como billeteras digitales para su compra y venta; ni tampoco hablaremos de los bots que protagonizan nada menos que el 52% del tráfico de Internet, ni de los métodos empleados en la ingeniera social, que no pierde su capacidad de engañar a ciudadanos y empresas.

Me propongo contarles qué están haciendo algunos bancos españoles en su andadura digital, en un entorno que está cambiando a gran velocidad y que pretende llevarse a cabo respetando valores y principios, de manera que ningún resultado pueda cambiar esos objetivos. No olvidemos que en la última década se ha registrado en España una pérdida del 28% de las Entidades Financieras y del 39% de las sucursales. Y, probablemente, la reducción no habrá llegado a su final. Los recortes tampoco han respetado a los cajeros automáticos.

Dentro del modelo de Gestión Responsable, tres son las palancas que facilitan el proceso: Posicionamiento, Tecnología y Gestión del Riesgo. La que nos ocupa hoy, la tecnología, que tiene una gran repercusión en la operativa bancaria actual, tiene como meta la consecución de un alto nivel de eficiencia, en el marco de una visión global. Un ejemplo de esta eficiencia en la reducción de los procesos en alguna entidad ha sido reducir en un 55% el tiempo necesario para abrir una cuenta y otras operaciones con porcentajes similares.

Sin embargo, nuevas herramientas, como es el caso especial de la inteligencia artificial o el Big Data, no les han distanciado del concepto de Servicio, con mayúsculas. Por un lado, no cabe la menor duda de que las nuevas tecnologías están teniendo un gran impacto en los clientes pues es una realidad que la sociedad es cada vez más digital, como lo demuestran los datos de alguna entidad: el número de clientes

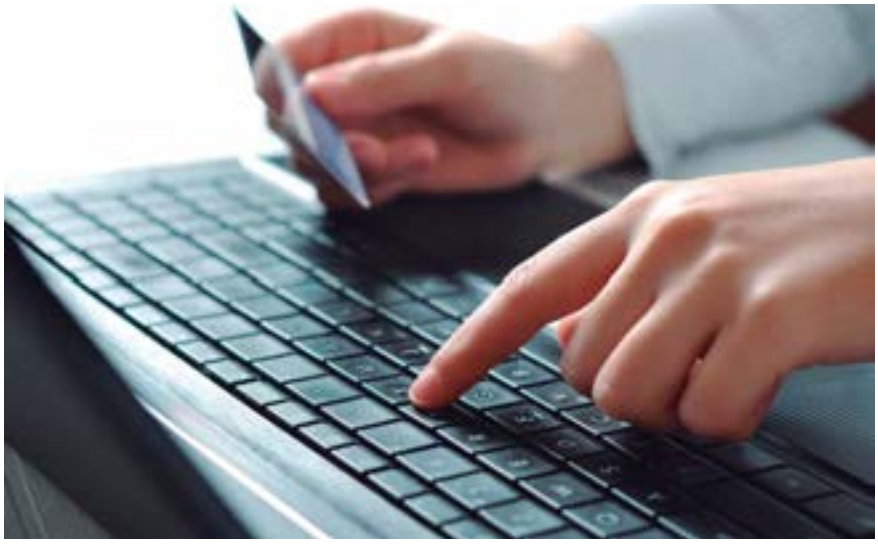
que usan canales digitales se ha multiplicado por 1,5 desde 2014, el 21% de los clientes que han contratado algún producto en diciembre de 2017 lo han hecho a través de compras online, la utilización del móvil representa las 2/3 partes del uso de los canales digitales.

Pero, por otro lado, como es el caso en algunas entidades, la realidad de la operativa bancaria, la realidad de la banca, es la de la diversidad, es, en definitiva, la de la multicanalidad.

Un ejemplo significativo de esta realidad es que un 43% de los clientes de alguna de las entidades tomadas como muestra, prefieren operar en sucursales físicas y cajeros automáticos (según el Banco de España, en los últimos nueve años hasta 2017, el valor medio de las retiradas de efectivo ha pasado de 114 a 131 €). Otros datos ofrecidos recientemente por el Banco Central Europeo estiman que en 2016 el efectivo fue el medio de pago dominante y, más concretamente, el 79% de todas las transacciones de la zona euro se llevaron a cabo con efectivo.

Esta realidad es mucho más complicada que situar las operaciones bancarias solo en los canales digitales. Se parte de un contexto basado en la visión global de la tecnología, que nos informa de que la satisfacción de los clientes es mucho mayor cuando tienen alguien (no algo) que los atienda, o que en algún caso el 80% de los clientes hayan utilizado las oficinas además de otros canales en los últimos 12 meses. El mercado en general no difiere en este sentido y en este porcentaje (84%). En algún caso, además, la mitad del porcentaje de los clientes señalados como contratantes de algún producto a través de compras online lo han hecho también en oficinas.

Por ello, en el caso de la entidad a la que represento en estas líneas, se ha segmentado a los clientes en: los que reciben servicio digital (banca online), tradicional (oficinas), remoto (con un experto) y transaccional. El resultado es que en 2020 las dos terceras partes de nuestros clientes utilizarán los canales digitales y en ese mismo año el 35% de nuestras ventas serán digitales.



«El 43% de los clientes prefiere operar en sucursales físicas y cajeros automáticos»

En los planes estratégicos de algunas Entidades, la tecnología estará acompañada de fuertes inversiones, en gran parte dirigidas a la digitalización del Banco, con un objetivo: la eficiencia, fundamental si se pretende conseguir una rentabilidad sostenible.

Nuevas amenazas y avances en la seguridad física

La protección de las nuevas amenazas en la era digital tiene como principal eje la potenciación de la seguridad de la información de las empresas. Ese eje incluye la actualización de las tecnologías que gestionan la seguridad física para reducir su vulnerabilidad ante posibles ataques contra sus equipos, cuyas consecuencias podrían acarrear graves daños a las organizaciones. Como bien conocen los responsables de seguridad de las Entidades Financieras, por citar un sector cuyos integrantes son sujetos obligados, los sistemas de seguridad de las sucursales y edificios bancarios están compuestos, si nos referimos a las primeras, por detectores volumétricos, sísmicos, y equipos que gestionan en local el sistema de seguridad de la instalación, el equipo de cámaras y los retardos y bloqueos de los contenedores de efectivo. De los edificios destacaría además los sistemas de control de accesos y los movimientos de personas (lectores y tarjetas). Todos estos medios electrónicos están conectados a direcciones IP, por lo que su vulnerabilidad ante ataques lógicos dependerá de la robustez de los sistemas operativos y la de los equipos que los gestionan.

Estos equipos se clasifican en soportados o no soportados, según su nivel de riesgo. Los primeros son revisados por los equipos de ciberseguridad en distintos periodos, mientras que los segundos hay que sustituirlos. Pues bien, la sustitución de estos últimos (para cada 1.000 sucursales) está exigiendo in-

versiones de más de 20 millones de euros. Por su parte, la actualización de los equipos de control en los edificios exige unas inversiones que en muchos casos son millonarias, difíciles incluso de imaginar en aquellas entidades bancarias con amplia presencia internacional.

En el lado opuesto, la tecnología también ha puesto en manos de los equipos humanos de la seguridad física herramientas como nuevas aplicaciones que tratadas en iSOC experimentados, permite no solo reducir los tiempos de detección de amenazas, sino conocer en poco espacio de tiempo otras nuevas, identificadas anteriormente tras exhaustivos procesos, o mejoras en las acciones de colaboración con las Fuerzas y Cuerpos policiales.

Viejos delitos con nuevas tecnologías

Muchos de los nuevos delitos que sufrimos hoy las entidades financieras, no son más que consecuencia de las viejas tipologías delictivas ayudadas por herramientas digitales, la facilidad para que el cliente pueda realizar operaciones bancarias y en no pocos casos la falta de precaución de la víctima.

Los cheques enviados por correo ordinario a miles eran y siguen siendo especial atención de grupos especializados de delincuentes, que encuentran el tiempo y los medios para su manipulación y cobro.

Hoy, el apoderamiento de la dirección del correo electrónico de los propietarios o directivos de empresas facilitan que el delincuente usurpe su identidad y ordene transferencias por el mismo medio a las sucursales titulares de la cuenta, a pesar de que las entidades establecen para estas operaciones el uso de una Oficina de Internet de Empresas, pues cuenta este medio con unos altos niveles de seguridad y autenticación.

La clásica llamada telefónica, con el objetivo de conocer el PIN tras haberse apoderado en el buzón de correos domiciliario de la tarjeta renovada, era un método eficaz para los delincuentes. Hoy, la llegada de un correo electrónico con forma de Web del banco o de oferta con enlace (phishing, pharming), que le aporta al criminal los datos de la cuenta bancaria de la víctima, es la nueva versión digital de la llamada telefónica.

Hoy, los cajeros automáticos permiten todo tipo de operaciones, desde consultas del estado de nuestras inversiones a ordenar transferencias o solicitar e ingresar en la cuenta préstamos de importe significativo. Facilita operar en sus cuentas a muchas personas que no tienen tiempo para ir a su sucursal. Pero esa facilidad requiere que los clientes custodien la tarjeta y presten especial atención a la hora de marcar el PIN, y que las entidades financieras desarrollen herramientas que detecten movimientos inhabituales en las cuentas de sus clientes.

Más peligrosos por su impacto económico son los ataques contra cajeros originados por grupos criminales. Históricamente estos dispositivos bancarios han sufrido toda suerte de ataques, desde los físicos como el Lazo libanés, arrancamiento, forzamiento con cuñas y mazos, soplete, radial, lanza térmica, cepos, gas propano, gas acetileno, explosivo sólido.., hasta los lógicos, que no se han quedado atrás: Skimming, Black Boss, Spear Phishing, Carnabak...

Paralelamente a lo que se ha dado en llamar «ingeniería social» o lo que es igual, «los mismos perros con distintos collares», los sistemas informáticos de las empresas son objetivo de «hackers» con toda una batería de malware desde la Denial of service attack o Ataque de negación de servicio al Ransomware, con distintos y muy variados objetivos: económicos, reputacionales, espionaje empresarial, o simplemente la consecución de méritos.

Sea como fuere, toda esta larga relación de riesgos, amenazas, vulnerabilidades exigen de grandes inversiones en tecnología que se suman al costoso proceso de digitalización, al que lamentablemente poco van a poder ayudar los tipos de interés, actualmente en negativo, origen de la fuente más importante de ingresos de las entidades financieras.

Fotos: Shutterstock

PARTNER LÍDER

EN LA BANCA ESPAÑOLA

Más de 20 años garantizando la seguridad de las principales entidades financieras del país

Techco security

Soluciones multicanal de seguridad que se adaptan a cada proyecto y entidad bancaria para garantizar la integridad de las personas e instalaciones.

TU SEGURIDAD, LO PRIMERO.

@Techco_Security | linkedin-techco-security-españa | www.techcosecurity.com | 900 77 77 80

SEBASTIÁN GARCÍA SERRANO. DIRECTOR DE SEGURIDAD. UNICAJA BANCO

Evolución de las **CRA** hacia las **nuevas tecnologías**

DESDE la entrada en vigor de la anterior Ley 23/1992 de 30 de julio, de Seguridad Privada, cuando se produjo a su amparo la desconexión de las alarmas que hasta entonces tenían conectadas directamente la Policía, y su posterior conexión a una Central Receptora de Alarmas (CRA) privada, ha habido una clara evolución. En el caso de Unicaja Banco se optó en su momento por disponer de una CRA de uso propio, lo que desde entonces ha proporcionado una mayor autonomía en la gestión, integridad y seguridad de los sistemas de alarmas.

A lo largo de los años, las CRA han venido experimentado una serie de cambios debido a las evoluciones tecnológicas. Así, se ha pasado de las líneas analógicas de comunicaciones, a través de un par de hilos de cobre, a las digitales, utilizando los mismos medios físicos. Más tarde llegó la fibra óptica.

Los transmisores de alarmas se comunicaban con las CRA mediante llamadas telefónicas, con su correspondiente lentitud en la comunicación, independientemente del protocolo que se utilizara. Eran transmisiones de unos 35 segundos como mínimo utilizando el protocolo más rápido. Por aquel entonces, también existían las comunicaciones de vídeo de forma analógica, con una calidad de imagen deficiente ante el escaso ancho de banda existente. Utilizábamos receptoras físicas, de gran volumen donde había que dimensionar el uso con tarjetas de líneas telefónicas (ej. Las Telettras – 4+1).

Al final la tecnología avanza de una manera vertiginosa y en un breve espacio de tiempo hemos pasado a tener comunicaciones digitales a través de fibra óptica, lo que ha provocado un gran avance en las telecomunicaciones. Por otro lado, la electrónica de seguridad también ha experimentado unos importantes avances con nuevas funcionalidades y con elementos electrónicos más potentes debido a la gran capacidad de procesamiento de las nuevas generaciones de procesadores, de memorias, de discos duros y demás componentes.

Soluciones virtualizadas

Actualmente se están utilizando soluciones virtualizadas permitiendo tener distintos servidores con sistemas operativos de distinta índole de una forma virtual, corriendo en una potente máquina de forma local o en cloud (en la nube). Esto permite realizar un gran ahorro de costes, y gran seguridad frente a una avería de máquina, aunque en el caso de la nube todavía, para ciertas entidades como las financieras, se cuestiona la seguridad, aunque se recomienda que si se utiliza esta tecnología la información vaya encriptada y que los servidores físicamente se hallen en Europa. Esto es debido a los grandes problemas de ciberseguridad que a día de hoy se está sufriendo mundialmente y a la necesidad de cumplimiento del Reglamento General de Protección de Datos (RGPD).

Por tanto, la protección ante ciberataques empieza a tomar un papel muy importante en una CRA y es necesario que toda la infraestructura esté protegida adecuadamente y, además, se cuente con personal cada día más especializado, ya que dentro de las mismas se maneja información sensible, que tendría unas consecuencias graves en el caso de que tuviera lugar una filtración o una pérdida de esa información. Esto nos hace reflexionar y plantearnos que no sólo las infraestructuras tienen que estar protegidas, sino que a nivel operativo tenemos que tener implementados unos planes de seguridad preventivos, correctivos y/o evolutivos de sistemas y redes, lo que se conoce hoy en día como un plan 360, donde se realizan planes de adecuación, implantación y auditorías periódicas. Con esto se consigue analizar continuamente las posibles vulnerabilidades que se puedan tener y así poder operar para corregirlas.

Además, hay que tener un plan ante catástrofes y contingencias muy bien definido, un denominado Plan de Continuidad de Negocio (BCP, por sus siglas en inglés). En Unicaja Banco, y

dentro del Acuerdo de Basilea, disponemos, además, de una duplicidad de sistemas y servicios, también de la CRA.

Actualmente, en las CRA ya no sólo se gestionan señales de alarma. Ahora se tiene una gran cantidad de información para poder discernir entre si dicha señal es una falsa alarma o no. Se cuenta con sistemas de comunicaciones TCP/IP y GPRS y 3G, donde la rapidez adquiere un papel esencial. Además, sobre las primeras normalmente se conectan transmisiones de vídeo procedentes de sistemas de CCTV (Circuito Cerrado de TV).

Estos sistemas de CCTV pueden ser básicos e inertes o contener analíticas de vídeo que hoy en día son capaces de realizar numerosas funciones en milésimas de segundo y determinar si tenemos que gestionar una alarma dándole paso al operador a su actuación y llamando la atención del mismo, justo en el momento que se precisa. En este campo se está investigando muchísimo y, actualmente, hay sistemas que pueden crear perímetros virtuales, reconocer el merodeo de personas cerca de áreas sensibles y reconocer rostros independientemente de la raza, color, sexo y otras características. Se pueden diferenciar intrusiones por animales y/o personas y también se están utilizando cámaras térmicas para realizar coberturas de grandes extensiones, para detectar posibles conatos de incendio, tanto en exterior como en interior, o restringir el acceso de una persona a un área sensible si tiene fiebre o no.

En suma, se trata de algoritmos muy complejos, donde la capacidad de computación de los sistemas juega un papel esencial, aunque también se está trabajando mucho en la calidad de las imágenes con un reducido ancho de banda H264, H265 y estandarización de las mismas, para no caer en detrimento de la velocidad de transmisión de las comunicaciones y uso en multitud de plataformas.

Los sistemas de control de accesos también han experimentado una gran evolución y han pasado a utilizar rasgos biométricos de distintos tipos (huella, iris, rostro, venas en dedo o palma de mano) para garantizar la seguridad de los sistemas. Están preparados para trabajar con un gran número de patrones y de registros debido a las continuas mejoras en las bases de datos y en la electrónica de los sistemas. Actualmente, desde la CRA se puede realizar una telegestión como puede ser abrir una puerta de una oficina a distancia, el desbloqueo de un submostrador de efectivo para su uso en caso de avería del dispensador o reciclador, etcétera.

Dispositivos móviles

Otro tema que cabe destacar, aunque de menos aplicación en el sector bancario, es el uso de dispositivos móviles por parte de los usuarios de las Centrales Receptoras de Alarmas. Se han creado aplicaciones para que el usuario final pueda controlar sus sistemas de seguridad casi al cien por cien, y esto va a hacer que se tengan que reorientar los servicios ofrecidos por las CRA y también diversificarlos, ya que los paquetes de servicios completos que se ofrecían hasta ahora dejan de ser los más atractivos por los clientes actuales, como por ejemplo pulsadores de emergencia con escucha de lo que ocurre alrededor y transmisión de coordenadas GPS al centro receptor.

Los softwares de gestión más novedosos de las CRA no paran de actualizarse y de adaptarse para ofrecer más tipos de servicios como pueden ser algunos muy demandados hoy en día para control de personas o de vehículos (GPS), controles técnicos de sistemas (calderas, cámaras frigoríficas, aperturas de puertas a distancia, etcétera) o de posible implantación y gran utilidad como alarmas si en un conteo de personas mediante análisis de vídeo en un recinto se supera un aforo (por ejemplo, en un concierto, evento o calle y zona como puede ser el caso de Semana Santa, Sanfermines...).

Con respecto a la nueva Ley 5/2014 de Seguridad Privada, cabe destacar que en materia de CRA ha sido constructiva, ya que en el Capítulo 1, que trata de las Disposiciones Comunes, en su artículo 6 de Actividades Compatibles, establece, en su apartado 1.c: «la conexión a centrales receptoras de alarmas de sistemas de prevención o protección contra incendios o de alarmas de tipo técnico o asistencial, o de sistemas o servicios de control o mantenimiento». Este hecho ofrece las nuevas oportunidades de mejoras y valor añadido en seguridad analizadas para nuestras CRA. ●

Fotos: *Unicaja Banco*

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

Formación en seguridad en entidades financieras: materias y destinatarios

Claves para definir en qué debe consistir la capacitación en este ámbito y a qué personal tiene que dirigirse

PARTIENDO desde la convicción de la importancia que tiene la seguridad como materia y como elemento estratégico diferencial para las compañías en un mundo tan competitivo como el actual escenario económico y empresarial, no podemos obviar que uno de sus pilares fundamentales es siempre la formación.

Hablamos de una capacitación no sólo inicial para conseguir las aptitudes necesarias para el desarrollo de una función, sino también de una formación permanente que permita la actualización de conocimientos.

Debe ser, además, una formación específica, particularizada en supuestos y servicios concretos cuando no personalizada en personas y colectivos.

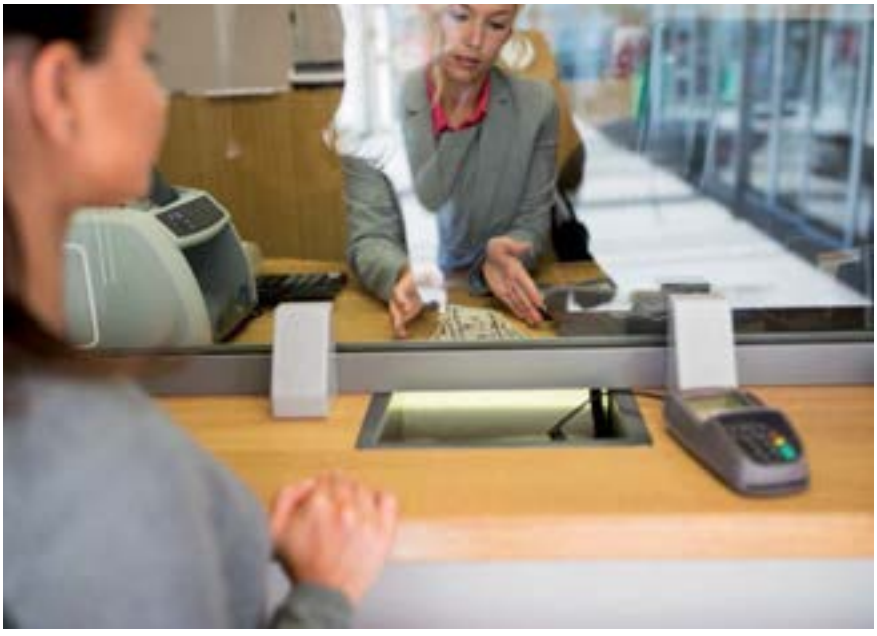
Pero, tras mencionar estas generalidades más o menos conocidas por todos, ahondemos un poco en la cuestión, en la medida que nos permite la brevedad de un artículo periodístico. ¿Qué materias serían las adecuadas referidas al sector de la seguridad bancaria? ¿Qué sujetos serían destinatarios de esa formación?

La primera puntualización es que los dos factores mencionados deben abordarse conjuntamente, pues van de la mano indisolublemente unidos. Y, entrando en el asunto, respecto a la primera cuestión, hay que entender cuál es el ámbito extensivo que tendrá en la organización la seguridad como materia transversal.

Además de la seguridad física y electrónica y cuestiones esenciales como análisis de riesgos, otras materias relacionadas con el cumplimiento normativo cobran cada vez más importancia (prevención de blanqueo de capitales) y actualidad (protección de datos de carácter personal); el poner énfasis en estas disciplinas no es baladí y es un buen argumento para potenciar los departamentos de Seguridad Corporativa, tanto por las cuantiosas sanciones que pueden llegar a imponerse como por el daño reputacional que pueden sufrir las entidades.

Y sí las entidades financieras fueron siempre el paradigma de establecimiento obligado en materia de seguridad física, lo han de seguir siendo en la actualidad en el ámbito de la ciberseguridad, pues uno de los mayores enemigos del negocio es el cibercrimen.

Otras materias como la inteligencia cobran cada vez mayor importancia,



Shutterstock / Syda Productions.

precisamente por las ventajas competitivas que pueden aportar en el negocio. La propia continuidad del negocio como disciplina es esencial como soporte básico de la actividad, y su implantación debería venir de la mano de la certificación en normas como la ISO.

La prevención de riesgos laborales y las emergencias de todo tipo también son esenciales y, como no puede ser de otra manera porque es la tendencia actual imperante, también deberían las organizaciones estar certificadas. Existe igualmente certificación normativa en un aspecto recurrente por obligación normativa: las centrales receptoras de alarmas.

Recursos humanos

Respecto a los recursos humanos que deben recibir formación en las diferentes materias, haremos una triple clasificación, al menos de modo inicial: personal del departamento de Seguridad, personal de seguridad subcontratado a empresas de seguridad y empleados propios de la entidad del resto de departamentos.

En nuestro último artículo ya abordamos en profundidad la formación del personal directivo que, dentro del departamento de Seguridad, debe realizar tareas de gestión y organización en sus distintos niveles, por lo que nos remitimos a él.

El resto de empleados de la entidad, deben recibir de forma periódica formación en las materias que puedan estar presentes en el ámbito de su puesto de trabajo, que en gran parte de los casos, serán muchas de las que hemos apuntado; el empleado puede ser un activo valioso para los objetivos del departamento de Seguridad, porque presencialmente está en todas partes con una inmediatez que no siempre puede alcanzar el departamento de Seguridad; un empleado puede ser para muchos riesgos, tanto en fase preventiva como en caso de su manifestación, los ojos, el olfato y, no pocas veces, las propias manos del departamento en la prevención o la minimización de daños.

> «La formación debe ser permanente, para permitir la actualización de conocimientos, y específica»

Esta circunstancia, a veces, viene ya impuesta como obligación esencial en la normativa, como es el caso de la prevención del blanqueo de capitales y financiación del terrorismo.

Personal de seguridad

El caso del personal de seguridad perteneciente a empresas de seguridad (fundamentalmente la figura de los vigilantes de seguridad y en menor medida de los escoltas privados) que desempeña su labor en puestos operativos, aunque normativamente no recaiga de forma directa en la responsabilidad del director de Seguridad de la entidad, es un factor importantísimo y en el que sí debe tener voz el departamento de la entidad. Esto debería reflejarse tanto en la elección de las materias en las que deberían formarse anualmente con lo dispuesto en el artículo 57 del Reglamento de Seguridad Privada, como en propuestas específicas a establecer en pliegos de contratación de los servicios.

Esta decisión, aunque parezca evidente, en base a mi cercana experiencia en este campo, puedo decir que ni es tan habitual, ni se controla, supervisa o planifica como sería deseable.

Buenas intenciones en un papel, si no se llevan a término, quedan en un mero elemento decorativo para el despacho si se encuadernan adecuadamente. ●

Shutterstock / SFIO CRACHO

JAVIER AGUILERA. DIRECTOR GENERAL. STRONGPOINT IBERIA

Automatización de procesos e innovación tecnológica

Entidades Bancarias

LA tecnología es la ciencia que lidera en estos momentos cualquier mercado del mundo. Todas las empresas de los diferentes sectores buscan soluciones tecnológicas para mejorar sus negocios en cualquiera de sus aspectos.

Desde el área de contabilidad hasta el área de atención al cliente se encuentra en proceso de digitalización y automatización gracias a las diferentes medidas tecnológicas que las compañías expertas ofrecen a los diferentes tipos de negocio.

Es la tecnología la que avanza sin descanso para maximizar rentabilidad y optimizar los procesos del negocio.

De modo que, siendo la tecnología la que está en cabeza de todos los mercados para su mejora, no es desconcertante el gran cambio de los métodos de pago desde hace unos años, que tienden a ser electrónicos.

Estos métodos buscan la automatización del proceso de cobro, haciendo más sencillo la gestión de los ingresos en efectivo, pero, indiscutiblemente, buscan abaratar los costes que el negocio asume con la gestión manual.

La gestión manual del efectivo es verdaderamente costosa y la automatización de ésta también supone una importante inversión de tiempo, tanto para los propietarios como para los empleados.

Además, no debemos olvidar que otro de los motivos para la automatización de la gestión del efectivo es que el poder ejecutivo y legislativo presionan para esta automatización mediante la regulación normativa, pretendiendo alcanzar el complejo objetivo de control total de todas las transacciones del mercado. Para alcanzar este objetivo,

es absolutamente necesario automatizar las operaciones de efectivo, de modo que todas las transacciones estén registradas y bajo un exhaustivo control.

Paralelamente al desarrollo tecnológico en los mercados, observamos un cambio en el modelo de inversión. Cada vez es más común la inversión en servicios y no en equipamiento, como la subcontratación de servicios bancarios, dentro de las propias entidades, a empresas ajenas al propio banco.

La banca está arrendando cajeros automáticos (ATM) y otros medios de pago, destinando por lo tanto su inversión a servicios externos.

Del mismo modo, el mantenimiento de los contenedores de seguridad pro-

pios de la entidad bancaria, como reciclladores de efectivo y cajas fuertes, pueden ser incluidos en este nuevo modelo de inversión en servicios.

Con la existencia del nuevo Reglamento de Seguridad Privada se destapa el nuevo e interesante escenario del transporte de efectivo en contenedores con maculación de billetes, haciendo más seguro el transporte de efectivo, además de agilizarlo y optimizarlo.

Actualmente, uno de los principales riesgos que afectan a las entidades bancarias, provienen de los medios en que transportamos los fondos en efectivo.

Estos medios implican procesos muy vulnerables, ya que es el momento en que nuestro capital en efectivo abandona la seguridad de nuestro dominio para llegar al Banco Central u otra entidad.

En este instante, la seguridad de nuestros fondos pasa a un tercero cuyas técnicas suponen invertir una suma elevada para la seguridad en el transporte y, es en este escenario, donde las tecnologías de sistemas inteligentes de neutralización de billetes (IBNS) aparecen para proteger el efectivo sin necesidad de utilizar armas o costosos vehículos blindados, a la vez que mejoran la seguridad y la protección personal.

Existen también soluciones combinadas de contenedores de efectivo y transporte para entidades bancarias con un fondo de efectivo reducido.

Este sistema fusiona los procesos de almacenamiento y transporte del efectivo de la entidad bancaria, protegiendo los fondos con su tecnología de neutralización de billetes, impregnando el efectivo de su interior con tinta irreversible en el momento en que uno de sus múltiples sensores detecta intentos de intrusión.

Fotos: *StrongPoint Iberia*

JORDI GALLEGO. DIRECTOR COMERCIAL. LANACCESS

Ciberseguridad en sistemas de **CCTV**

EL Spectre, el Metdown, los Ransomware han vuelto a poner encima de la mesa la importancia de la ciberseguridad. Vivimos en un mundo donde todo está interconectado, y los sistemas están expuestos a ataques de todo tipo. Los correos electrónicos y los dispositivos USB han dejado de ser la única puerta de entrada de virus y malware a las organizaciones. Ahora cualquier dispositivo conectado a la red puede ser el receptor–difusor de un ataque.

Cómo protegerse es uno de los mayores retos de prácticamente cualquier organización.

Si trabajamos aportando seguridad a nuestra empresa, no podemos pasar por alto las implicación de los dispositivos que seleccionamos ni de la arquitectura de interconexión de todos ellos. Es muy importante seleccionar sistemas ciberseguros.

Las auditorías de los departamentos de IT y de Seguridad Informática son cada vez más frecuentes: quieren tener analizado y controlados todos los equipos IP que se conectan a las redes del banco. Es por ello, que cada vez es más habitual que la homologación de equipos de seguridad (videograbadores, cámaras…) también requiera de su aprobación. Es muy importante ser conocedores de aquellos requisitos que obligatoriamente deben cumplir los equipos seleccionados, para evitar de este modo demoras en las homologaciones, que puedan retrasar campañas de instalación, sustitución de equipos … Podría darse también el caso que no superen dichas pruebas, y que haya que volver a lanzar un proceso de búsqueda de nuevos proveedores.

A continuación repasaremos las principales características a tener en cuenta relacionadas con la ciberseguridad.

Sistema Operativo

El software malware se desarrolla para atacar sistemas operativos concretos. Tradicionalmente han sido Windows y Linux la diana de los creadores del malware, aunque recientemente también IOS y Android han sido objeto de ofensivas. Es por ello muy importante tener protegidos los equipos, tanto los grabadores como las cámaras IP, contra carga de software y aplicaciones externas.

Todos aquellos equipos que utilicen estos sistemas operativos, deberán presentar sus planes de actualización de versiones, tanto de sistema operativo como de los antivirus y firewalls. Además debe tenerse en cuenta la discontinuidad de estos sistemas operativos, por ejemplo en el caso particular del Windows, vivimos recientemente la finalización del soporte de Win-XP y ya se ha anunciado la de Windows-7.

Sin embargo a aquellos equipos con un diseño hardware y sistema operativo propietario, es casi imposible cargarles versiones firmware o aplicaciones maliciosas. Solo sería posible teniendo el código fuente, y ser conocedor exacto del hardware utilizado.

Stack TCP-IP (comunicaciones)

La utilización de protocolos de comunicaciones seguros y encriptados es también esencial para proteger la integridad de los videograbadores. Es importante que los sistemas puedan trabajar con los https, ftps y ssh. Además todos aquellos protocolos de comunicaciones propietarios deben ser también autenticados.

StrongPoint

Expertos en la seguridad del efectivo

CashGuard

Sistema de gestión de efectivo

- Solución de front-office, fiable, rápida y robusta

- El sistema más implantado del mercado. 35.000 sistemas funcionando cada día

- Gestión centralizada de su efectivo que incluye ciclo cerrado de efectivo

Vesta

Sistema de ingreso de monedas y billetes

- Solución de back-office para recaudaciones por usuario

- Cuenta y custodia el total de la recaudación diaria

- Control completo de todos los ingresos del negocio

Empleados
600

Visión
Convertirnos en un proveedor global de soluciones tecnológicas para el Retail

StrongPoint

www.strongpoint.es

Países
30

Ambición
Trabajar conjuntamente con los retailers para la implantación de soluciones a medida

El DDoS (denegación de servicio distribuida) ha sido otro de los ciberataques que han conseguido afectar a grandes corporaciones. Para protegerse de este tipo de actuaciones, es importante que los equipos supervisen y detecte ataques a puertos UDP y TCP y lo bloqueen a bajo nivel. El bloqueo de acceso tras repetidos intentos de autenticación erróneos, también aporta seguridad contra ataques obtención de credenciales por fuerza bruta.

El poder modificar los puertos de comunicaciones habituales es también una herramienta útil para evitar ataques.

Control de acceso a la Red Corporativa

Para ofrecer mayor seguridad a la red corporativa, los departamentos de IT demandan que los sistemas soporten el standard 802.1x. Este protocolo obliga a todos los equipos que se conectan a la red a identificarse con un servidor central. Si consigue acreditarse correctamente el equipo tendrá acceso a la red corporativa, y si por el contario falla, quedará aislado. De este modo se consigue fácilmente impedir que equipos no autorizados puedan conectarse a las redes bancarias.

Cámaras IP. Switch PoE integrado

Las cámaras IP de vídeo ya se cuentan por centenares y millares en las redes bancarias. Sin duda alguna han aportado un salto de calidad en la imagen muy importante, pero desgraciadamente han sido los elementos de sistema de vídeo a los que más agujeros de seguridad se han detectado. Es por ello que para dotar de mayor seguridad e integridad al sistema de CCTV, es altamente recomendable utilizar videograbadores con Switch PoE integrado, para que aislen las cámaras IP de la red corporativa.

El switch también servirá para conectar otros dispositivos como videporteros, panels,… que utilizan la misma tecnología que las cámaras y por tanto son igualmente vulnerables. El videograbador deberá aislar las cámaras: no serán directamente accesibles y todas las comunicaciones serán a través del grabador. Es decir, para la red del banco no existirían cámaras IP, y por tanto no serán atacables.

El grabador como gestor del switch deberá gestionar correctamente los puertos del Switch. Deberá supervisar la no suplantación de elementos de seguridad, y que todos aquellos puertos vacantes queden cerrados e inoperativos.

Actualización de usuarios y versiones de firmware

La utilización de passwords seguros, y la posibilidad de cambios masivos periódicos, son también buenas herramientas para prevenir ataques indeseados. También es importante disponer de una plataforma que permita cambios de firmware de manera ágil, que permita tener siempre la planta actualizada tanto a nivel de seguridad como de nuevas prestaciones. De manera masiva debe poderse actualizar de manera segura millares de equipos automáticamente.

Monitorización del sistema

Para poder detectar vulnerabilidades y corregirlas es muy importante tener herramientas de monitorización de los equipos, para tener la planta bien controlada y detectar cualquier incidencia y fallo en los sistemas. Igualmente tanto los grabadores, cámaras y aplicaciones de gestión deben de tener un completo sistema de logs, que permitan extraer la máxima información de intentos de acceso, usuarios, IP destino y origen, y así poder detectar las máquinas o usuarios que están generando ataques.

La ciberseguridad es uno de los aspectos más importantes a considerar parar garantizar la integridad del sistema de CCTV y los datos que se almacenan, pero no es el único. A modo de resumen se listan:

- Ciberseguridad: Sistema operativo (versiones, antiviurs, firewalls), protocolos seguros, 802.1x, DDos, switch PoE integrado, usuarios, versiones, logs, …
- Acceso físicos: chasis antisabotaje o arcones de seguridad.
- Discos duros: sistemas de ficheros especiales para vídeo y configuraciones en Raid.
- Alimentación: Fuentes UPS o SAIs externos.
- Supervisión equipos: temperatura, fallos de vídeo, control de días grabados, sincronización horaria.
- Exportación de vídeo: encriptación y firmas.

Fotos: Lanaccess

Proselec compañía líder en seguridad empresarial ofrece soluciones de ciberseguridad 360º, al tiempo que ayuda con el nuevo Reglamento General de Protección de Datos (RGPD).

Monitorizamos y auditamos (24x7) cualquier tipo de sistema conectado a su red (Pcs, servidores, cámaras, control de acceso, firewall, switchs, etc.) sin instalar ningún tipo de software en sus equipos. Nuestra solución detecta y resuelve vulnerabilidades y mejora el rendimiento y productividad de sus sistemas.

Protegemos sus datos, Las mejores y más modernas soluciones de DLP y NAC para conocer en todo momento que ocurre con sus datos y quién accede a su red.

Blindamos su correo contra cualquier tipo de ataque tanto de entrada como de salida.

*Soluciones implantadas en empresas del IBEX35

“Proselec, ciberseguridad 360º para su empresa”

Estas herramientas, combinadas con nuestros servicios de revisión de líneas y ambientes (despachos, salas de reuniones, vehículos, etc.) que permiten detectar cualquier intrusión en sus comunicaciones (analógicas y digitales), proporcionan un nivel de seguridad superior, lo que se traduce, en la mayoría de los casos, en que los esfuerzos de los posibles ciberdelincuentes se deriven a otros objetivos más fácil de lograr.

C/ Ochandiano, 14, Parque Empresarial El Platío
28023 Madrid (Madrid) España
(+34) 91 121 71 50 - www.proselec.com
pro@proselec.com

JAVIER FLOR PINCHETE. BANK & POST BUSINESS UNIT DIRECTOR. TECHCO SECURITY

Banca 4.0: Un escenario digital y disruptivo, pero seguro

ACERCARSE al cajero y que éste, mediante el reconocimiento facial, sepa quién eres y te muestre los movimientos más recientes de la cuenta corriente o sugiera, en un menú táctil, las operaciones más habituales que realizas, parece que es el comienzo de una novela futurista, pero lo cierto es que la tecnología digital y disruptiva ha venido para quedarse, y mucho más en el sector bancario y en las entidades financieras.

Con frecuencia escuchamos que nos encontramos en la era de la transformación digital; pero lo cierto es que, sin darnos cuenta, lo que estamos atravesando es un camino sumergido en AI (Inteligencia Artificial), minerías de datos (también llamado big data), machine learning y otros cuantos conceptos más.

Algunos países de nuestro entorno ya han eliminado las monedas y billetes físicos; y otros muchos le han puesto fecha de caducidad. Esto hace prever que todas las transacciones pasarán a ser digitales, una medida que conllevará un mayor control de las operaciones y, por lo tanto, una mayor eficacia en la lucha contra el fraude y la economía sumergida.

Cuando este nuevo escenario llegue a nuestro país, la banca se habrá transformado con respecto a cómo la conocemos hoy. El acceso a la tecnología y la conectividad determina un nuevo modelo de comunicación entre la entidad y el cliente, que influye directamente en cómo se consume la información y se realizan transacciones financieras, entre otras cosas.

Soluciones de seguridad

Al igual que otros muchos sectores, la banca 4.0 ya es una realidad y la mayoría de las entidades ya están desarrollando proyectos de transformación digital, mejorando la experiencia del cliente e interactuando con él, tanto físicamente en las oficinas como online a través de aplicaciones y banca online.

En los próximos años es probable que los cajeros pasen a ser oficinas virtuales atendidas remotamente e integren alguna de las tecnologías que se han adentrado en nuestra vida cotidiana. Entre ellas se encuentran la analítica avanzada, la inteligencia artificial, los servicios cognitivos, el IoT (Internet de las Cosas), el blockchain o las API (open banking), que permitirán a empresas, startups y desarrolladores lanzar nuevos productos y servicios, incorporando en las aplicaciones, con el permiso de los clientes, los datos bancarios.

Todo ello siendo capaces de operar en esta transición tecnológica de manera dual, integrando las necesidades de los nativos digitales (también llamados millennials) y de las personas de generaciones posteriores y seniors, que se están incorporando a la revolución tecnológica y superando su resistencia al cambio.

Sin embargo, lo que el sector no aborda con la misma fuerza es la seguridad y la ciberseguridad, un importante reto en el que Techco Security colabora y es empresa de referencia desde hace 20 años, ofreciendo soluciones innovadoras y tecnológicas para garantizar la seguridad de las instalaciones y la integridad de los movimientos bancarios y transacciones de dinero.

Un futuro cada vez más digital y tecnológico, pero seguro

Quizá las sucursales bancarias pasen a ser puntos de encuentro y reunión para la gestión y asesoramiento de activos financieros, donde la seguridad vaya bajo el brazo de la estética y la tecnología. Serán espacios donde las cámaras, además de su función de seguridad, incorporen nuevas utilidades, como averiguar el número de personas que entran en una sucursal, controlar el aforo, detectar qué clientes entran a informarse o a comprar productos financieros, a qué hora se comercializan los no financieros, etc. Estamos hablando de dispositivos tecnológicos de última generación que las entidades pueden utilizar en exclusiva para su venta en su red de oficinas.

En este nuevo contexto, la banca y el retail se entrecruzarán en la venta de algunos productos y también en materia de seguridad tecnológica. La banca seguirá requiriendo profesionales especializados en su negocio que posean CRA y centros de operación remota que gestionen servicios únicamente para el sector. En estas plataformas no sólo se centraliza la seguridad, sino también se monitoriza y analiza toda la información de los sistemas para detectar cualquier desviación de seguridad y dar la voz de alarma cuanto antes.

> «El acceso a la tecnología y la conectividad determina un nuevo modelo de comunicación entre la entidad y el cliente»

En cuanto a los empleados, los accesos y las salidas de las oficinas serán muy similares a los actuales, si bien se incorporarán soluciones de seguridad biométrica en la gestión de los controles de acceso o con servicios embebidos en los propios dispositivos móviles.

Toda esta oferta integral de seguridad y tecnología deberá estar avalada por sistemas que transmitan la información mediante redes de comunicaciones securizadas al máximo. El sector tiene el gran reto de protegerse, prevenir y monitorizar sus redes y sistemas para evitar ataques cibernéticos que vulneren su integridad y la de sus clientes.

En este sentido, sólo las grandes compañías, como nuestra empresa, con el potencial y la experiencia de ofrecer continuamente soluciones innovadoras de seguridad y tecnología, son capaces de garantizar la integridad a las entidades bancarias y dar una respuesta eficaz y rápida a sus necesidades. En nuestra compañía proporcionamos un servicio integral y «llave en mano», que contempla la convergencia entre los riesgos habituales de seguridad y los nuevos que proceden del entorno digital y han venido para quedarse.

Nos sentimos muy orgullosos de acompañar a las entidades financieras en este nuevo y apasionante reto, que ya es una realidad en esta primera mitad del siglo XXI, a través de innovadoras soluciones multicanal que se adaptan a cada proyecto y entidad bancaria, garantizando la integridad de las personas e instalaciones. ●

Fotos: *Techco Security*

STEFAN ALFREDSSON. GERENTE DE MARKETING DE SOLUCIONES GLOBALES. RESPONSABLE DE SAFE CITIES. AXIS COMMUNICATIONS

Eliminando barreras para crear ciudades inteligentes y eficientes

Estrategias para mejorar la gestión de los núcleos urbanos

Se espera que el número de personas que viven en las ciudades se duplique en 2050 hasta 6.400 millones de habitantes. Para hacer frente a este aumento de la población y para ajustarnos a las nuevas necesidades de unos mayores entornos urbanos, las ciudades van a precisar unos métodos nuevos para gestionar sus bienes y recursos.

POR ese motivo cada vez más existen distintas iniciativas para el desarrollo de ciudades inteligentes, donde los mecanismos para conectar tecnologías, datos y partes interesadas generan como resultado unos instrumentos totalmente nuevos para gestionar, por ejemplo, el tráfico, la iluminación urbana, el aparcamiento, la recogida de residuos o la seguridad pública.

Pero, para que una ciudad sea verdaderamente inteligente, también necesita eliminar las barreras que a menudo existen entre los diferentes departamentos, además de las que existen entre las organizaciones públicas y privadas.

Compartiendo cámaras para el beneficio de todos

En la actualidad, los sistemas de vigilancia funcionan en muchas ciudades como compartimentos cerrados, en donde los diferentes componentes no están directamente interconectados. Puede que tengamos cientos de cámaras de tráfico, y otros cientos en vigilancia urbana, establecimientos comerciales y transporte público, pero todas ellas tienen un ámbito limitado de cooperación en estos departamentos o proyectos.

La vigilancia representa un terreno típico, en donde una ciudad puede hacerse más inteligente cuando se comparten datos determinados entre múltiples partes interesadas. Con la eliminación de las barreras entre los com-

partimentos cerrados, podemos obtener múltiples beneficios, tanto para las ciudades como para los organismos privados y para los ciudadanos.

Cooperación público privada para mejorar la vigilancia

El Proyecto Green Light Detroit es un ejemplo de una iniciativa que actúa como puente entre las instituciones públicas y las privadas. Hace unos años, cuando los funcionarios de la ciudad de Detroit examinaron de cerca las estadísticas sobre los delitos que tenían lugar en dicha ciudad, observaron que cerca de un cuarto de los más violentos tuvieron lugar cerca de una gasolinera.

Teniendo como objetivo evitar y resolver los delitos, mejorar la seguridad de los barrios y promover el crecimiento de las empresas locales, la ciudad y el departamento de policía se asociaron con los negocios locales para poner en marcha el Proyecto Green Light Detroit.

Para sustentar y desarrollar el Proyecto, y para compartir al mismo tiempo los costes, se solicitó a cada una de las partes interesadas:

• La instalación y el mantenimiento por parte de las empresas privadas individuales de cámaras de alta definición, además de una conexión de red de alta velocidad e iluminación adecuada, tanto externa como interna.

• El establecimiento de un centro de delitos en tiempo real para la ciudad de Detroit y para la policía, con personal especializado para recibir, monitorizar y analizar de manera efectiva imágenes de vídeo suministradas por las empresas participantes en la iniciativa.

En la actualidad, más de 200 empresas forman parte del proyecto, y los delitos violentos han disminuido hasta un 50% en algunas de las zonas monitorizadas.

Otro proyecto interesante en esta misma línea es la Operación Shield en Atlanta, en donde más de 10.000 cámaras públicas y privadas se conectan a una red de vigilancia.

De esta forma, se proporciona al Departamento de Policía de Atlanta una visión más completa y en tiempo real de lo que sucede en toda la ciudad, incluyendo los colegios públicos, el sistema de transporte, las empresas locales y las propiedades residenciales donde viven varias familias.

Esta cooperación permite compartir los costes de unas instalaciones de seguridad rentables y de alta calidad, ahorrando costes individuales y sin pérdida de cobertura. La eliminación de compartimentos cerrados entre las instituciones públicas y privadas permite ampliar los sistemas de vigilancia de red en las ciudades.

Asimismo, se proporciona a los cuerpos locales de policía el acceso a todas las cámaras, mejorando así la monitorización de la ciudad y actuando más rápidamente y con mayor precisión cuando sea necesario.

Conectando departamentos para múltiples objetivos

Además de la seguridad de los ciudadanos, una red de cámaras interconectadas también puede servir de ayuda para ocuparnos de otros retos urbanos. Por ejemplo, la ciudad de Brno, en República Checa, ha puesto en marcha una solución de vídeo conectada para ocuparse de los problemas de tráfico en el centro de la ciudad y para reducir los pequeños delitos.

La Administración de Carreteras de Brno ha instalado cámaras en algunos cruces, en terminales de tranvía y en el pasadizo subterráneo de la estación central de ferrocarril. Como resultado de ello, la Administración de Carreteras y la Policía Municipal ya pueden monitorizar el tráfico en lugares centrales clave desde el centro de control recientemente construido.

Las nuevas cámaras proporcionan imágenes actualizadas en tiempo real mucho más nítidas y de mayor calidad sobre los incidentes de tráfico, y los cuerpos de policía pueden aprovechar las prestaciones de las cámaras – como un potente zoom -para seguir a los delincuentes, a los conductores indisciplinados y a los pequeños ladrones.

Con la eliminación de los departamentos cerrados, varias entidades — como las comisarías de policía y los centros de gestión de tráfico— pueden tener acceso a un mayor número de cámaras, mejorando así su capacidad de monitorización. Asimismo, una

mayor cobertura genera una gestión más eficaz de los incidentes, ya que los operadores pueden valorar la situación e informar a las autoridades pertinentes, dependiendo del asunto que se trate.

Beneficios de las cámaras de red conectadas a servicios públicos y emergencia

Las soluciones de vídeo conectadas también pueden mejorar en gran medida la ayuda que proporcionan los servicios de emergencia. La ciudad de Copenhague deseaba simplificar su capacidad de respuesta y reducir el tiempo necesario para hacer frente a los incidentes, incluyendo los incendios, especialmente aquellos con vidas humanas en riesgo.

En el pasado, los servicios de emergencia han confiado en las radiocomunicaciones para transmitir información sobre el estado de un incendio, pero estas situaciones de alta presión pueden hacer que se omitan de forma no intencionada algunos detalles importantes.

Debido a esto, los parques de bomberos decidieron poner en marcha un nuevo mecanismo para proporcionar informes y conocer mejor la gravedad de la situación.

Teniendo esto en cuenta, adoptaron una solución para transmisión de vídeo en red. Los vehículos que utilizan los bomberos se encuentran equipados con cámaras, una en la parte delantera y otra en la parte trasera, para enviar información al centro de operaciones. Las personas al cargo de la observación de las cámaras pueden posteriormente decidir si necesitan enviar refuerzos para ayudar a apagar el incendio.

Asimismo, también pueden compartir las imágenes con expertos para determinar si el edificio corre algún tipo de riesgo para derrumbarse. De esta manera se mejoraron los tiempos de servicio y se obtuvo una respuesta general más eficiente, gracias a la capacidad para valorar los incidentes en tiempo real.

Además de esto, la visualización en directo de las escenas donde se registran los incidentes ha ayudado a mejorar la información de los servicios públicos en situaciones críticas.

La gestión interna de las operaciones puede facilitar una toma de decisiones más rápidas e informadas sobre la posibilidad, el alcance y el momento preciso para comunicar al público un evento determinado, sin que la información tenga que pasar por varias personas, algo que produce un retraso en dicho proceso de comunicación.

Con la creación de unas redes de cámaras conectadas, los servicios de emergencia pueden acceder a las imágenes en tiempo real y enviarlas a otras personas interesadas, incluyendo los expertos en construcción, para facilitar una mejor respuesta ante una situación determinada.

Gracias a esta alianza, la ciudad se puede hacer «más inteligente» y estas acciones pueden tener un impacto positivo en las vidas de los ciudadanos que allí residen.

Unas ciudades más inteligentes con soluciones para múltiples compartimentos

La capacidad para compartir vídeo entre varias organizaciones ofrece unas magníficas posibilidades para mejorar la eficiencia operativa y la colaboración entre múltiples partes interesadas, además de servir de buen ejemplo para explicar la eliminación de compartimentos cerrados y ayudar a una amplia variedad de organizaciones a mejorar la eficiencia en toda la ciudad. Asimismo, puede mejorar la gestión del tráfico, facilitar una mejor y una más rápida respuesta a cualquier incidente por parte de los diferentes servicios y proporcionar a los ciudadanos una sensación de seguridad en todo momento.

En el caso de las alianzas públicas/privadas, la distribución de los costes y de las cargas asociadas con algunos de los sistemas de gama más alta puede proporcionar beneficios a todas las personas.

Estas colaboraciones permiten a los cuerpos de seguridad la monitorización de amplias áreas y responder más eficientemente a los incidentes que tengan lugar en toda la ciudad. Algunas ciudades inteligentes ya han implementado en sus compartimentos cerrados soluciones de vídeo conectadas para mejorar la gestión de sus recursos y la vida de sus ciudadanos. ¿Puede ser tu ciudad la próxima que se beneficie de ello? ●

Fotos: Axis

Un gran cambio

es sólo un pequeño paso.

Con las soluciones de videovigilancia de Axis para ciudades seguras usted se sentirá más seguro gracias a la visión clara mediante vídeo HDTV a tiempo real allá donde esté. Es fácil coordinar todo el sistema de vigilancia de forma centralizada e incluso compartir el vídeo en vivo.

Además, puede estar seguro de que Axis tiene una solución a prueba de futuro que está lista a día de hoy con la tecnología más avanzada para el día de mañana.

www.axis.com/safecities

AXIS COMMUNICATIONS

ELÍAS VALCARCEL TORRES. CEO & CO-FOUNDER. NEURAL LABS

Soluciones eficientes para ciudades más seguras

Uno de los aspectos más importantes en el entorno urbano es la seguridad de los ciudadanos. La seguridad puede ser vista desde 2 perspectivas, la primera tiene que ver con la delincuencia (robos, atracos y delincuencia en general) y la segunda tiene que ver con la seguridad en el tráfico.

MUCHOS municipios y ciudades de la mano de empresas y organismos, están realizando proyectos de alto impacto para fortalecer la seguridad de sus ciudades y entornos, promovidos en gran medida, por la necesidad de convertir las ciudades en lugares más humanos y en definitiva con mejor calidad de vida.

Movilidad y tránsito

Retos que nos llevan a anticiparnos y a estar preparados, con herramientas eficientes que permitan a las ciudades avanzar, no solo en temas de seguridad sino también paralelamente en movilidad y tránsito.

Ante el gran desafío que supone estar preparados para manejar con eficiencia la movilidad en las ciudades y entendiendo que según sus particularidades es necesario adoptar diferentes estrategias, surge la necesidad de apropiar los avances tecnológicos que ayuden a simplificar procesos y brinden tiempo de respuesta más cortos.

Dentro del ámbito de los últimos avances y tendencias tecnológicas aplicadas a las problemáticas de seguridad y movilidad, encontramos las redes neuronales y el Deep Learning (inteligencia artificial). Dichas tecnologías sirven para identificar personas, vehículos, patrones u objetos, con la finalidad de generar una acción, por ejemplo activando una alarma o lanzando una sanción. Un claro ejemplo de su utilidad se evidencia cuando hablamos de detección temprana de vehículos involucrados en delitos o potencialmente sospechosos de cometerlos, con lo cual se pretende evitar así daños a personas, bienes, e inclusive, evitar muertes.

Esta información se obtiene a través de las analíticas de vídeo aplicadas al tráfico, una tendencia mun-

dial en auge, que está siendo usada cada vez más por los departamentos de policía y gobiernos, debido a que ayuda a identificar además de la matrícula, todas las características del vehículo como son, color, marca, clasificación, velocidad y permite a través de éstas, realizar cálculos de exceso de velocidad, identificar comportamientos incívicos como detectar si un vehículo ha realizado un cruce indebido o se ha pasado una luz roja, lo cual podría llegar a ser potencialmente peligroso si pensamos en zonas escolares, pacificadas, y en general cualquier lugar donde se pueda poner en peligro la vida de los peatones o ciudadanos.

Gracias al desarrollo de este tipo de tecnologías y a las herramientas efectivas que brindan las analíticas de vídeo para diferentes entornos urbanos, las ciudades se convierten en lugares más seguros, más eficientes y más humanos.

RAFAEL SERRANO. DIRECTOR COMERCIAL DE SIEMENS TECOSA.

Seguridad inteligente, clave para las ciudades del futuro

La creciente expansión de los núcleos urbanos da lugar a una agudización de los riesgos en términos de seguridad

Las ciudades son el entorno cotidiano de la población mundial. La ONU estima que, en el año 2050, cerca de 2.500 millones de personas vivirán en áreas urbanas. Esto supone que el proceso de urbanización sea un fenómeno global que está alcanzando sorprendentes magnitudes y que tiene como consecuencia, la mayor construcción de edificios. Esta creciente edificación da lugar a una agudización de los riesgos en términos de seguridad.

ASÍ, bandas de delincuentes que toman edificios enteros, explosiones o incendios son amenazas que acechan a los ciudadanos en su día a día. Y es que a todas las personas les gustaría vivir en la ciudad más segura del planeta. De acuerdo con el índice de las Ciudades Seguras 2017, realizado por la Unidad de Inteligencia de The Economist (EIU), Singapur se ha impuesto en el número uno en términos de seguridad de la Infraestructura, seguida de Madrid y Barcelona. Pero ¿y si todas las metrópolis pudieran alcanzar el primer puesto? En las últimas décadas las nuevas tecnologías han favorecido la eliminación de las vulnerabilidades con respecto al control de accesos, vigilancia, o protección de personas y edificios característicos de la ciudad del siglo XXI.

Shutterstock / 24Novembers

No obstante, para llegar a esta posición, hoy en día los propietarios de los edificios y sus responsables de seguridad se enfrentan continuamente al reto de cuidar de las instalaciones de forma eficiente. En este sentido, las nuevas tecnologías nos han blindado con sistemas de seguridad antes inimaginables para conformar el tándem perfecto.

Tal es así que, actualmente existen sistemas de reconocimiento facial que permiten detectar múltiples rostros en tiempo real, sistemas de detección perimetral multi-sensorial, basados en analítica con cámaras térmicas, radares y detectores de movimiento. No en vano, estos dispositivos tecnológicos no reemplazan la vigilancia física, pero sí se han convertido en aliados indispensables a la hora de evitar la incursión de delincuentes en las instalaciones, sea de día o de noche.

Unido al desafío del intrusismo, otro de los riesgos a los que se enfrenta la población mundial en los últimos años es la amenaza terrorista. A pesar de que, como índica el reciente informe anual sobre el terrorismo en el mundo del Departamento de los Estados Unidos, los atentados se redujeron un 23% a nivel global en 2017, los niveles de alertas siguen patentes en todos los rincones del planeta. Frente a esto, el desarrollo de equipos de inspección y detección, como escáneres o rayos x, detectores de explosivos o de armas de alto calibre y otros elementos metálicos que pueden suponer una amenaza, continúa en auge. Así, estos sistemas de seguridad de prevención han disminuido la sensación de desprotección que estas acciones han generado en la vida cotidiana en general. Ahora bien, ¿y si el peligro al que se enfrenta la población no está estrechamente ligado a un tercero? Más allá del control de intrusismo y de las amenazas terroristas, existen una serie de incidentes que pueden generar múltiples problemas con graves consecuencias.

Incendio en la Torre Grenfell

Es el caso de los incendios. A raíz del dramático incendio de la Torre Grenfell de Londres el año pasado, las preguntas sobre la seguridad de los edificios han vuelto a emerger. Y es que a pesar de que las medidas de prevención que se han desarrollado para este siniestro han mejorado, ninguna infraestructura está exenta de sufrir posibles incendios por causas naturales, ya sea aplastamiento y roturas de cables, conexiones sueltas o mordeduras de ratones.

La tecnología ha facilitado el desarrollo de sistemas de prevención que se convierten en la herramienta base para evitar incidentes en cualquier tipo de infraestructura, desde pequeños inmuebles como hogares o tiendas de barrio, hasta grandes superficies como aeropuertos o estadios deportivos. Conscientes de todos estos imprevistos, y considerando que el 90% de las personas pasan sus vidas en estas infraestructuras, resulta indispensable implementar una seguridad inteligente para las ciudades del futuro. Sólo así, los edificios serán espacios perfectos para desarrollar las funciones del día a día.


Shutterstock / Vasin Lee

«Más allá del intrusismo y las amenazas terroristas, hay incidentes que pueden generar graves consecuencias»


Shutterstock / Gui jun peng

ALEJANDRO GARCÍA MARTÍN. INGENIERO INDUSTRIAL. SALES DISTRICT MANAGER. BOSCH SECURITY & SAFETY SYSTEMS

Cámaras inteligentes para ciudades más seguras

De los sistemas de videovigilancia pasivos a los activos

Las cámaras de videovigilancia tradicionalmente se han utilizado en las ciudades como elementos pasivos captadores de imágenes, que han requerido de una elevada componente humana en cuanto al visionado de imágenes en directo para detectar posibles situaciones de riesgo o hacer búsquedas en grabaciones de hechos delictivos. El Instituto Nacional de Seguridad e Higiene en el Trabajo, en su publicación «Instrucción básica para el trabajador usuario de pantallas de visualización de datos», identifica que los principales problemas asociados al uso habitual de estos equipos son la fatiga visual, los trastornos musculoesqueléticos y la fatiga mental.

ESPECIALMENTE esta última, hace que el operador de un sistema de videovigilancia pierda la capacidad de detectar situaciones de riesgo transcurrido escasamente veinte minutos, quedando limitado a funcionar como registrador de imágenes, sin apenas posibilidad de anticiparse a los hechos.

En la última década, las cámaras de videovigilancia han evolucionado exponencialmente en cuanto a su capacidad de procesado de imágenes, posibilitando la utilización de algoritmos informáticos capaces de detectar de forma automática situaciones de riesgo y comunicarlas en tiempo real, lo que convierte a las cámaras de videovigilancia en dispositivos inteligentes capaces de anticiparse al delito. Los operadores de la nueva generación de sistemas de videovigilancia ya no observan pantallas, sino que atienden aquellos eventos o alarmas generados por las cámaras inteligentes, dedicando el máximo de atención a las situaciones reales de riesgo, y desarrollando otras tareas más productivas durante el tiempo que no ocurre nada. Si, además, se suma la posibilidad de que estos avisos se den a dispositivos móviles, como tabletas o teléfonos inteligentes, el operativo de seguridad será mucho más eficiente.

La última evolución de las cámaras inteligentes es el conocido como «machine learning», tecnología que permite a la cámara aprender en base a la experiencia, de forma que las reglas de detección se irán ajustando y mejorando

en el tiempo, al principio con la ayuda del operador, y de forma continua por la propia cámara. La posibilidad de buscar en las grabaciones por tipo de objetos o situaciones concretas que se pudieran haber producido, es lo que se denomina búsqueda forense o científica, y es una herramienta clave para la optimización de los recursos a la hora de hacer búsquedas entre cientos de cámaras y ciento de miles de horas de grabación.

Cámaras inteligentes que actúan como sensores

El desarrollo de procesadores cada vez más potentes, el ajuste de precio de la electrónica, y el desarrollo de algoritmos de visión artificial, han favorecido la aparición de una nueva generación de cámaras de vídeo que generan datos y los envían en tiempo real a los gestores municipales. La clave está en la inteligencia distribuida, tecnología que posibilita el uso de redes de ancho de banda limitado como 3G/4G, WiFi, WiMax, Satélite o sistemas B-PLC sobre la red de alumbrado público. Esta tecnología permite, incluso, usar la cámara exclusivamente como sensor (desactivando la capa de vídeo), lo que facilita su despliegue en una ciudad al estar fuera del ámbito de la normativa de protección de datos.

Algunas de las funciones que ya permiten hacer de forma autónoma las cámaras inteligentes son:

- Detectar cualquier objeto en la escena.
- Detectar objeto en un campo virtual.
- Cruce de línea, ya sea una, dos, o tres líneas virtuales.
- Objeto entrando en campo virtual.
- Objeto saliendo del campo virtual.
- Merodeo.
- Seguimiento de ruta.
- Conteo y ocupación.
- Cambio de la relación de aspecto horizontal/vertical.

- Búsqueda de similitud.
- Flujo/contraflujo.
- Detección de rostros.
- Sabotaje.
- Objeto inactivo o abandonado.
- Objeto eliminado o sustraído.
- Estimación de grado de ocupación.

Todas estas funciones de detección pueden aplicarse a diferentes tipos de objetos, pudiendo distinguir entre personas, motocicletas, turismos o camiones, o estableciendo filtros por tamaño, relación de aspecto, color, o velocidad. Dependiendo del tipo de aplicación, podrán ser útiles a diferentes verticales relacionados con la gestión municipal como pueden ser el tráfico, el transporte, y la movilidad, el ahorro energético, el turismo, la limpieza y, por supuesto, la seguridad.

Automatización de los procesos en la seguridad de las ciudades

Una ciudad es un ecosistema en el que conviven cientos o incluso miles de recursos relacionados con la seguridad, desde los Cuerpos y Fuerzas de Seguridad del Estado, Policía Autonómica, Policía Local, Protección Civil, Bomberos, Sanitarios, o centros de coordinación, hasta los servicios públicos de transporte o limpieza, que también se ven afectados en caso de emergencia. Cualquier evento en la ciudad afecta de forma más o menos importante a cada uno de estos servicios, ya sea una prueba deportiva, una manifestación, un concierto, las fiestas locales, o una concentración religiosa, por lo que todos los recursos deben estar perfectamente alineados para ofrecer una respuesta rápida y eficiente.

La automatización de los procesos y la integración de todos los recursos técnicos y humanos en una sola plataforma de gestión es una de las claves para que los dispositivos de seguridad sean exitosos. En este escenario, las cámaras inteligentes funcionan como sensores capaces de detectar situaciones de riesgo, informar al centro de coordinación, y servir como elemento de verificación por vídeo de la incidencia. Debe existir una plataforma de ciudad o plataforma horizontal en la que se conecten, además de las cámaras inteligentes, otros servicios relacionados con la seguridad para compartir datos, encadenar procesos, y servir de ayuda para la toma de decisiones, todo ello dirigido a reducir los tiempos de reacción e intervención.

En relación a la biodinámica de las personas, en una ciudad es muy importante conocer cuáles son los flujos principales de movimiento, la distribución temporal de los mismos, la posible existencia de aglomeraciones, ocupación de vías de evacuación, superación de los aforos máximos, o la detección de situaciones que pueden ser de riesgo como la existencia de personas corriendo, un nivel de ruido excesivo, o la presencia de vehículos pesados en zonas peatonales. Determinados avisos requieren de una intervención rápida, por lo que cada vez es más frecuente conectar los sistemas de radiocomunicaciones de emergencia de los agentes, con la plataforma horizontal, permitiendo que, frente a una detección de una cámara inteligente ubicada en una determinada vía de la ciudad, se generen avisos de forma automática a los agentes más cercanos, incluyendo la posibilidad de ver vídeo en directo y grabaciones desde su dispositivo móvil mientras se aproxima.

Otra aplicación muy interesante para la gestión integral de la seguridad de una ciudad es la conexión a la plataforma horizontal de la red de alumbrado público, de forma que, frente a una detección de situación de riesgo, el alumbrado pueda reaccionar, normalmente incrementando su nivel lumínico. En las ciudades, una de las principales medidas de ahorro energético, es la reducción de los niveles de iluminación a ciertas horas de la noche, lo que puede incrementar la sensación de riesgo en determinadas zonas que queden excesivamente oscuras, como puede ser el caso de parques, jardines, o vías con mucha arboleda. Las cámaras inteligentes pueden detectar la presencia de personas, enviar un aviso a la plataforma horizontal, y ésta ordenar al alumbrado público el incremento de los niveles de iluminación en esa zona, lo que genera mayor sensación de seguridad al ciudadano, además de un efecto disuasorio. En eventos multitudinarios, como concentraciones religiosas, donde en muchas ocasiones se requiere bajar, o incluso eliminar la iluminación, este tipo de soluciones ya han sido probadas con éxito, estableciendo diferentes niveles de iluminación en relación a la situación de seguridad, incluso modificando la colorimetría o la temperatura de color de las lámparas, ofreciendo una luz cálida al paso de las imágenes, que puede tornar de forma automática a luz blanca a máxima potencia en caso de emergencia.

Para todos estos escenarios, es importante, además de una detección de incidencias fiable, disponer de imágenes de calidad suficiente como para poder identificar, ya sea de forma manual o automática, a los infractores. En este apartado entran en juego características y funcionalidades de las cámaras como la resolución o la cantidad de píxeles del sensor para que sea posible identificar personas. Otra característica importante es la sensibilidad, que es la iluminación mínima necesaria para que la cámara pueda ver, tanto en color como en blanco y negro. Poder ver en color escenas en las que apenas hay luz, es muy importante en la seguridad de las ciudades, así como el rango dinámico, concepto que mide la capacidad de gestionar de forma rápida y solvente contraluces y cambios rápidos de la iluminación de la escena. Por último, y no menos importante para el despliegue de cámaras inteligentes en una ciudad, es el concepto de ancho de banda o necesidades de red que las cámaras tienen, tanto para transmitir vídeo, como las alarmas. Una de las ventajas de disponer el análisis de vídeo inteligente embebido en las cámaras, es que se reduce notablemente las necesidades de conectividad, ya que todo el procesado de vídeo se hace en el dispositivo, pudiendo enviar vídeo a alta calidad solo en la situación de riesgo. La posibilidad de grabar imágenes de forma redundante en la cámara y en los servidores centrales, es una prestación que simplifica de forma notable las redes de telecomunicaciones y por tanto las inversiones necesarias para acometer estos proyectos.

*Fotos: **Bosch***

ComNet es la solución completa en comunicaciones a todos sus desafíos

RENDIMIENTO GARANTIZADO
HOY Y MAÑANA

Cuando ***la fiabilidad de la red es crítica,*** ***los productos de transmisión que elija hoy*** afectarán al ***rendimiento de su red en el futuro.***

Comnet – Soluciones de comunicación con garantía de futuro.

- Sólo ComNet ofrece una solución completa de comunicaciones en Fibra Óptica, UTP, Coaxial e inalámbricas.
- Los productos ComNet son "MADE IN USA"
- Garantía exclusiva Vitalicia
- Especializados en atención y soporte técnico al cliente en múltiples diseños y aplicaciones.
- Consulte su a nuestro representante local.

"Un solo fabricante para todos sus retos de transmisión"
Donde la Garantía y Calidad del producto y de su proyecto son una exigencia…
Y donde… la mejor solución y el mejor precio son necesarios.

comnet
Communication Networks

www.comnet.net • ccortes@comnet.net • +34 673 48 89 22

MADE IN THE USA

JORGE ESPERÓN. SECURITY ARCHITECT. CONTINUUM SECURITY

Cuida la seguridad desde el diseño con el Modelado de Amenazas

«El diseño no es solo lo que ves, sino cómo funciona», Steve Jobs

A menudo asociamos el diseño como una propiedad visible, algo que entra por los ojos. Sin embargo, el diseño de cualquier sistema está estrechamente relacionado con su funcionamiento. Y un buen diseño debe incluir la seguridad, porque muy a menudo un sistema tendrá que operar bajo condiciones adversas, sobre todo en nuestro mundo hiperconectado.

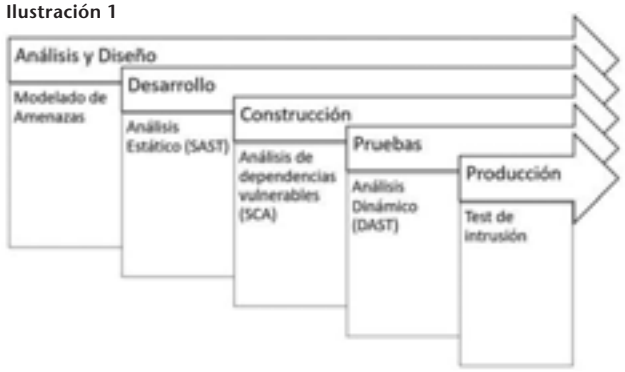
FALLOS de seguridad en el diseño. Existen fundamentalmente dos tipos de fallos de seguridad en las aplicaciones:

- Fallos de seguridad en la implementación. Por ejemplo, construyendo una consulta de base de datos que concatena texto SQL con variables que pueden ser modificadas por el usuario.
- Fallos de seguridad en el diseño. Por ejemplo, confiar controles de seguridad únicamente en el lado cliente de una aplicación web.

Las herramientas de análisis estático (SAST) y dinámico (DAST) de seguridad no son suficientes a la hora de detectar fallos de seguridad en el diseño de las aplicaciones. Estos fallos, en promedio, son los causantes de algo más de la mitad de las vulnerabilidades detectadas cuando una aplicación llega a producción, y suelen ser los más caros de corregir en términos de recursos y tiempo invertidos. Con el objetivo de concienciar acerca de esta problemática, en los últimos años se han lanzado varias iniciativas de ámbito internacional:

- El Instituto de Ingeniería Eléctrica y Electrónica creó su propio centro para el diseño seguro (IEEE Center for Secure Design). Como parte de sus iniciativas de comunicación, en 2015 publicó una lista[1] con los diez fallos de seguridad en el diseño más comunes.
- La Organización Internacional de Normalización (ISO) publicó en 2017 un catálogo[2] de principios de diseño y arquitectura orientados a mejorar la seguridad de productos, sistemas y aplicaciones.

Ilustración 1



El modelado de amenazas comienza con la arquitectura

A nivel de diseño tendremos que plantearnos algunas preguntas para definir el nivel de servicio de nuestra aplicación (con los usuarios legítimos), mientras actores externos pueden estar intentando abusar de cada una de sus funcionalidades. En estas preguntas y en las soluciones de compromiso alcanzadas para responderlas se encuentra el núcleo del modelado de amenazas como proceso. Se trata de un análisis sistemático de la arquitectura de un sistema para detectar y corregir fallos de seguridad en el diseño. El objetivo es obtener una serie de requisitos de seguridad que permitan contener el nivel de riesgo por debajo de un valor previamente acordado.

Una de las principales ventajas del modelado de amenazas es que nos permite empujar la seguridad hacia la izquierda dentro del ciclo de desarrollo (tal como se puede observar en la **Ilustración 1**). De este modo, podremos incluir importantes principios de seguridad en el diseño, como la defensa en profundidad, antes de que se haya escrito la primera línea de código de la aplicación.

La arquitectura de un sistema debe de reflejar el entendimiento compartido del mismo entre los diferentes equipos involucrados en su desarrollo (desarrolladores, arquitectos, analistas de seguridad, ingenieros de sistemas y de comuni-

caciones, etc.). Esto no solo se aplica a los componentes que están siendo desarrollados, sino también a los sistemas externos que interaccionarán con la aplicación una vez que se encuentre en producción (servicios de analítica, pasarelas de pago, sistemas de notificaciones, etc.).

Caminos para definir una arquitectura

IriusRisk[3] es una herramienta de modelado de amenazas que usa patrones de riesgo basados en la arquitectura para facilitar la identificación consistente de amenazas y contramedidas.

Existen cuatro modos de definir una arquitectura para un sistema o aplicación en IriusRisk. Cada uno de ellos está enfocado a un caso de uso particular, pero todos ellos son complementarios y comparten una visión común de la arquitectura a la hora de identificar las amenazas relevantes para una aplicación.

Ilustración 2

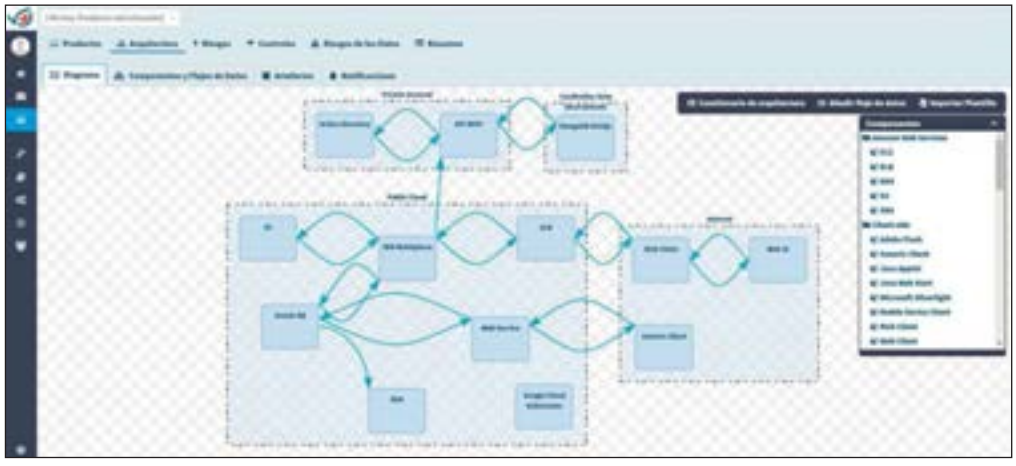
> «La arquitectura de un sistema debe reflejar el entendimiento compartido del mismo entre desarrolladores, arquitectos, analistas de seguridad,...»

1. Con un formulario

La aproximación basada en formulario (**Ilustración 2**) permite una definición ágil de la arquitectura de la aplicación y de los activos involucrados en base a la contestación de una serie de preguntas. Dicho cuestionario puede ser completado por el jefe de proyecto cuando la aplicación se da de alta en el sistema de seguimiento de la Oficina de Gestión de Proyectos (PMO). De este modo, el equipo de desarrollo puede obtener un conjunto adecuado de requisitos de seguridad sin involucrar directamente al equipo de seguridad.

Ilustración 4

Ilustración 3



2. Con un diagrama

La definición de la arquitectura usando diagramas DFD (de flujo de datos) suele ser la opción preferida por los equipos de DevOps y Seguridad. Un ejemplo de esta aproximación puede apreciarse en la **Ilustración 3.** De un solo vistazo, es posible determinar dónde se producen los intercambios de información que cruzan las diferentes zonas de confianza de los componentes de la aplicación.

Ilustración 5

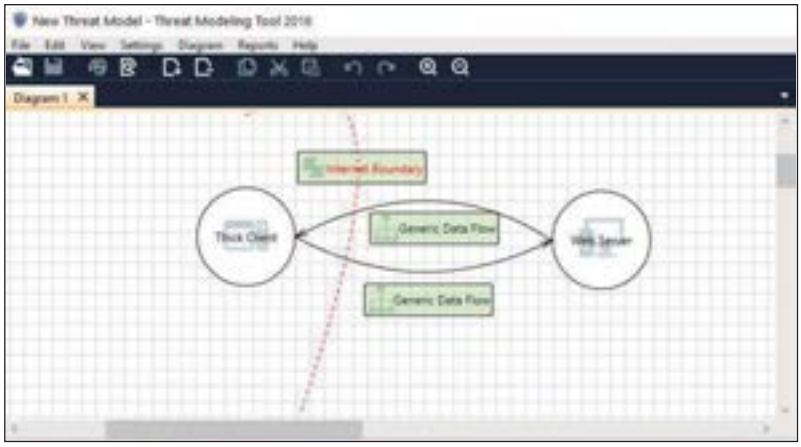


Ilustración 6

3. Por medio de un API de servicios.

Esta suele ser la opción preferente a la hora de integrar IriusRisk dentro de una estrategia de integración continua. Con esta opción ni siquiera es necesario usar la interfaz de usuario de IriusRisk. Es posible definir la arquitectura en base a un fichero XML, tal como se aprecia en la **Ilustración 4.** Esta aproximación permite definir con facilidad umbrales cuantitativos de riesgo que podrán detener el proceso de compilación bajo ciertas circunstancias.

> «La definición de la arquitectura usando diagramas DFD (de flujo de datos) suele ser la opción preferida por los equipos de DevOps y Seguridad»

En la **Ilustración 5** se puede apreciar un ejemplo de un cliente escrito en Ruby que consume el API REST de IriusRisk para implementar una lógica de aceptación del riesgo en base a una serie de criterios predefinidos.

4. Importando arquitecturas modeladas previamente.

Esta opción es especialmente relevante para equipos con una madurez media o alta en procesos de modelado de amenazas. Es habitual que estos equipos dispongan de modelos de amenazas previos, creados con otras herramientas, como Microsoft Threat Modeling Tool[4] (**Ilustración 6**), que desean reutilizar.

Este modelo de amenazas puede ser importado en IriusRisk ampliando el catálogo de amenazas para la arquitectura modelada, tal como se muestra en la **Ilustración 7**.

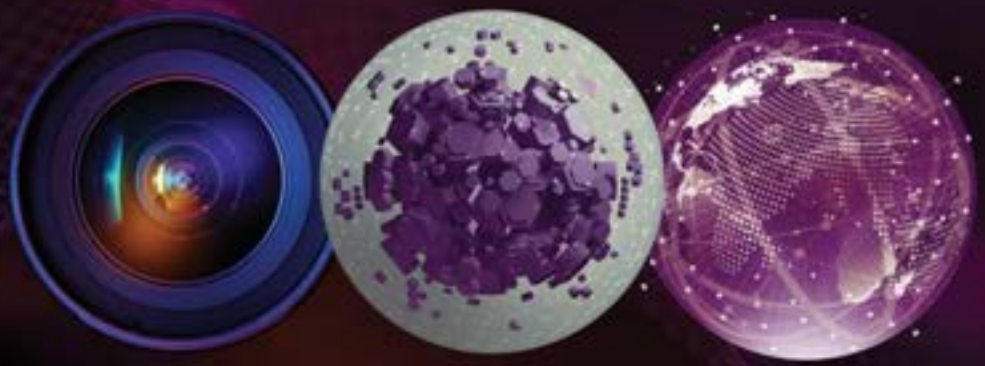
Ilustración 7

1. «Avoiding the Top 10 Software Security Design Flaws», https://cybersecurity.ieee.org/blog/2015/11/13/avoiding-the-top-10-security-flaws/.
2. «Catalogue of architectural and design principles for secure products, systems and applications (ISO/IEC TS 19249:2017)», https://www.iso.org/standard/64140.html
3. «IriusRisk - Threat Modeling Tool», https://www.continuumsecurity.net/threat-modeling-tool/.
4. «Microsoft Threat Modeling Tool», https://docs.microsoft.com/en-us/azure/security/azure-security-threat-modeling-tool

Fotos: Continuum

Western Digital.

MUCHO MÁS QUE VIDEOVIGILANCIA



CAPTURE **ALMACENE** **ANALICE**

UNA GAMA INCOMPARABLE DE PRODUCTOS OPTIMIZADOS PARA LA VIDEOVIGILANCIA

Western Digital cuenta con soluciones integrales ajustadas a los requisitos específicos de la videovigilancia, para que pueda capturar, almacenar y analizar los datos con una tecnología que se adapta a las últimas novedades.

wd.com/edge-to-core

JOSEP ALBORS. RESPONSABLE DE INVESTIGACIÓN Y CONCIENCIACIÓN. ESET ESPAÑA

Inteligencia artificial y seguridad, ejes de la innovación IT en la empresa

Mientras los ciberataques evolucionan, también lo hacen las medidas contra ellos

Hablar de seguridad informática de las redes corporativas actualmente abarca tantos campos que muchos profanos en la materia pierden el interés incluso antes de empezar a abordar el tema, a pesar, incluso, de que resulta vital para proteger los activos de la empresa y evitar nefastas consecuencias.

YES que los retos a los que las empresas y usuarios se enfrentan en esta materia pueden parecer inabarcables o aparentar que nos superan. Sin embargo, de la misma forma que los ciberataques han ido evolucionando, también lo han hecho las medidas de seguridad que nos protegen de ellos. Y están ahí para ayudarnos.

Probablemente, la tecnología de la que más se ha hablado durante los últimos años es la aplicación de la inteligencia artificial, redes neuronales, machine learning o deep learning. Todas son palabras que suenan muy bien en el portfolio de cualquier empresa pero pocos llegan a comprender su verdadero alcance.

Un uso que no es nuevo

Para empezar, la utilización del aprendizaje automático en soluciones de seguridad informática no es nueva. A mediados de los 90, muchos de los fabricantes veteranos de antivirus como ESET empezaron a aplicar machine learning a sus soluciones para hacer frente a una necesidad que ya empezaba a causar problemas: poder analizar la cantidad creciente de muestras de malware. Esta cantidad no ha hecho más que aumentar hasta nuestros días, siendo más que necesaria la aplicación de estas tecnologías. Desde entonces hasta ahora esta tecnología ha jugado un papel importante en las capacidades de detección, principalmente por su capacidad para descubrir el grueso de las muestras menos interesantes y que repetían patrones conocidos.

Esto ha evitado que los verdaderos protagonistas en la industria de la seguridad, los analistas de malware, malgastaran su tiempo analizando

muestras de poco interés y centraran su atención en aquellas que presentan alguna innovación y, por ende, una mayor amenaza para los usuarios. Así pues, la aplicación de IA y ML en los modelos de seguridad actuales supone una capa más que nos ayuda a detectar posibles amenazas, una capa que se debe complementar con otras igualmente eficaces como las sandbox, la detección de malware en memoria e incluso las tan denostadas bases de firmas.

No obstante, tanto la IA como el ML son herramientas que, por si solas son incapaces actualmente de sustituir el modelo de seguridad tradicional, pero junto a otras tecnologías representan unas poderosas aliadas para la detección de amenazas, especialmente si hay detrás personal experto que es capaz de sacar el máximo rendimiento de ellas.

En este sentido, desde ESET, viajamos por todo el mundo para hablar con los especialistas en seguridad IT empresarial y saber cuáles son sus necesidades. Lo que demandan es una única empresa que cubra todas las etapas para interceptar las amenazas: predicción, prevención, detección y reparación.

Últimos descubrimientos

ESET, dispone de laboratorios en distintas partes del mundo que constantemente analizan las amenazas y ciberataques que se producen.

Uno de los últimos descubrimientos ha sido Lojax, un potente rootkit UEFI que ha sido utilizado activamente contra organizaciones gubernamentales en los Balcanes, Europa Central y del Este: nunca antes había sido detectado un malware de este tipo en un ataque real, algo que puede suponer un peligroso avance en las herramientas utilizadas por los delincuentes o grupos especializados en realizar ataques dirigidos.

> «Es importante que los usuarios sepan que ellos suelen ser uno de los motivos de que los ciberataques tengan éxito»

Sin embargo, tampoco podemos olvidar la formación y concienciación de los usuarios/trabajadores ya que, si bien se pueden limitar los efectos de una imprudencia al ejecutar un archivo malicioso o pulsar sobre un enlace preparado por un atacante, siempre es importante que ellos sepan que son uno de los motivos principales por los cuales los ciberataques suelen tener éxito y así puedan tomar decisiones que los eviten. A pesar de que muchas empresas y particulares ven la ciberseguridad como un gasto, la realidad es que se trata de una inversión a tener muy en cuenta.

Fotos: Eset

PABLO LAS HERAS. ANALISTA DE INTELIGENCIA. EULEN SEGURIDAD

El sesgo tecnológico en el **análisis de inteligencia**

En el ámbito de la inteligencia, tanto productores como consumidores somos conscientes de que la condición humana dirige, cuando no limita, nuestra capacidad de análisis. El análisis de inteligencia requiere, por definición, que el analista, dentro de su condición humana, realice una serie de procesos sobre la información con el objetivo de convertirla en conocimiento.

ESTOS procesos, sólo posibles desde la «humanidad» del analista, están ligados intrínsecamente a una falla, a un error, a un riesgo: el sesgo cognitivo, que el Diccionario LID de Inteligencia y Seguridad define como: «Inclinación o predisposición a favor o en contra de algo, que genera una desviación en el procesamiento de la información y puede dar pie a una interpretación equivocada o a un juicio inexacto».

Este sesgo supone un problema, pero se resuelve, al menos en parte, con su simple conocimiento. Por ejemplo, si una empresa tiene una oportunidad de negocio con una empresa estatal del país X para el cual necesita un análisis de inteligencia (sobre la compañía, sobre el contexto de seguridad del país, sobre la fiabilidad de la empresa), teniendo en cuenta que el país X carga con una profunda y polarizada crisis política, el cliente sabe que un analista de ese país tiene altas posibilidades de tener un nivel de sesgo cognitivo mayor que un analista de cualquier otro país. Las soluciones a esta problemática son diversas, pero lo relevante es que conocemos que los sesgos cognitivos existen, pudiendo cuestionar sobre ellos a un interlocutor, a un tercero o a nosotros mismos. Esto ha supuesto que, a lo largo del tiempo, se hayan establecido numerosos protocolos destinados a corregir –o reducir– el impacto de los sesgos del analista sobre el producto final.

Contextualizada la importancia de los sesgos cognitivos en el ámbito de inteligencia, cabe dirigir la atención hacia la automatización; un proceso que, de forma inapelable, se está integrando en el análisis de inteligencia, especialmente en la etapa de recolección de información y de forma muy pronunciada en la inteligencia basada en información en fuentes abiertas OSINT. Cada vez es más común ver servicios de inteligencia donde la etapa de recolección de información está automatizada en una herramienta informática, que incluso llega a los primeros estadios de la siguiente fase, el análisis; sin que en estos procesos participe, salvo de forma residual, un analista de inteligencia.

La intervención de la máquina, de la herramienta, previene a priori del riesgo que supone un sesgo cognitivo. Al no haber intervención de personas, no hay riesgos asociados a la condición humana. La herramienta no tiene ideas preconcebidas, la herramienta no asume una causa común para hechos sincrónicos; la herramienta, en definitiva, goza de una presunción de «objetividad».

Si una herramienta tiene un fallo, este será técnico o de parametrización, pero no un sesgo. ¿Esto es así?

Los sesgos tecnológicos

Las herramientas, el software, también presentan sesgos. También tienen «ideas» preconcebidas, también tienen «predisposiciones», las cuales dirigen e influyen en su labor a pesar de que a nivel técnico puedan funcionar a la perfección. El efecto de estos sesgos en el análisis de inteligencia debe conocerse y ser tenido en cuenta para una correcta integración de las herramientas dentro del proceso de inteligencia.

María Díaz Monzón, Carlos Blanco Torres y el autor de este artículo en un trabajo presentado en el XIII Congreso bianual de Ciencia Política y de la Administración organizado por la Asociación Española de Ciencia Política y de la Administración (AECPA), definimos el sesgo tecnológico como:

«debilidad tecnológica [...] originada durante el diseño de la misma, con capacidad para distorsionar los resultados del trabajo en mayor o menor medida, y que obedece a las limitaciones presentadas por las personas y la propia naturaleza no neutral del avance científico».

Es decir, las herramientas tienen, debido a ciertos factores como el ámbito geográfico/cultural/lingüístico donde se desarrollan o los propios sesgos humanos de sus desarrolladores, características que pueden, acabar influyendo en el análisis de inteligencia de una manera similar al que lo harían los sesgo cognitivos del analista.

Por poner un ejemplo ilustrativo de lo que es un sesgo tecnológico; si usamos un conocido tracker de la red social Twitter para realizar un análisis cuantitativo de menciones sobre el Parque Nacional de Doñana, marcando como término a monitorizar la palabra «Doñana» durante varias semanas, es probable que nos encontremos, entre los meses de septiembre a junio con un pico de menciones los sábados o los domingos.

Si concedemos a la herramienta, en este caso al tracker de la red social Twitter, la presunción de objetividad, cogeremos esos datos cuantitativos y realizaremos la fase de análisis. Hemos elegido un término único «Doñana», que no es ambiguo o polisémico, buscado exclusivamente en una fuente, por lo que asumimos que el tracker, si funciona correctamente, nos dará los datos que hemos pedido sin fallo.

Efectuando un análisis sobre la base cuantitativa sacaremos unas conclusiones. Simplificando mucho esta fase, podríamos concluir, por ejemplo, que ese pico de menciones se debe a un aumento del nivel de visitas al Parque Nacional, que probablemente suba durante el fin de semana. El análisis es recibido por la dirección del Parque Nacional y esta, en base a la información que se le ha proporcionado, toma la decisión de reforzar sus servicios e incrementar el número de agentes medioambientales durante el fin de semana. Al final el objetivo de la inteligencia es proporcionar información que apoye el proceso de toma de decisiones.

Sin embargo, existe un error destacable en la fase de recolección de la información. Al comprobar manualmente, es decir, con la intervención de un analista, los tuit contabilizados por el tracker de manera automática, nos damos cuenta de que hay un número destacable de contenidos en turco durante el fin de semana, el sábado o el domingo. ¿Por qué? Es imposible que la palabra «Doñana» exista en turco, donde de hecho no existe siquiera la letra Ñ, que es una letra exclusiva del alfabeto castellano.

Twobee/shutterstock

Viendo más en detalle esos tuits en turco, descubrimos que se repite la frase «cehennem DONANA kadar», que en turco se traduce como «hasta que el infierno se congele» y que sirve como uno de los lemas del equipo de futbol Fenerbahçe de Estambul. Lema que los seguidores del equipo cuelgan de manera destacable los días de partido, normalmente sábado o domingo.

¿Ha fallado el funcionamiento de la herramienta? No, ha monitorizado todos los contenidos sin excepción. ¿Ha cometido el analista un fallo de parametrización del tracker? No, se ha elegido un término donde las posibilidades de falsos positivos es mínima. ¿Cuál ha sido, entonces, el error?

El «error» está en que el tracker que hemos usado es una herramienta de origen anglosajón, en cuyo alfabeto no existe la letra Ñ la cual reconoce como N. Es decir, para la herramienta la suma de letras «doÑana» es igual que la suma de letras «doNana», reportando ambos resultados sin distinción. La herramienta está influida por su contexto, en este caso por su contexto lingüístico, por lo que tiene un sesgo que afecta a su función, en este caso de recolección y presentación de información; funciona bien, pero no nos sirve.

> «Hoy por hoy, renunciar a herramientas de inteligencia sería un paso atrás para cualquier Unidad que esté prestando servicios de inteligencia»

Este sencillo ejemplo ilustra a la perfección la presencia de un sesgo en la herramienta que va más allá de un fallo de funcionamiento. Si no nos percatamos de su presencia y delegamos en la herramienta la totalidad de la función de recolección de información, su sesgo influirá el análisis, una fase donde, además, se sumará el sesgo cognitivo del analista, produciéndose una convergencia de sesgos.

En conclusión

Las herramientas facilitan el trabajo del analista de inteligencia, son útiles e incluso necesarias dentro de ciertas fases del proceso de inteligencia. Su desarrollo es rápido, habiendo cada año un mayor número de opciones disponibles en distintos formatos, y su alcance cada vez mayor.

Hoy por hoy, renunciar a herramientas de inteligencia sería un paso atrás para cualquier Unidad que esté prestando servicios de inteligencia.

Sin embargo, debemos analizar las herramientas como lo que son, programas creados por una determinada persona (o grupo de personas), en un determinado contexto social, político, lingüístico y cultural. El hecho de que no tengan sentimientos y/o emociones no supone que la información que presenten sea una imagen objetiva, real y fidedigna de toda la información disponible dentro de los parámetros marcados. La herramienta tiene sesgos que debemos analizar y entender de cara a corregir su impacto en las fases en las que participe.

En el ámbito de la inteligencia la suspicacia e incluso la desconfianza deben marcar nuestros primeros contactos con fuentes e información. Un proceso similar al que seguimos a la hora de dar validez a la información que presenta una fuente humana –o la que, valga el caso para un consumidor de inteligencia, presenta un analista– debe ser usado a la hora de tratar con una herramienta dedicada a la recolección, cribado y/o análisis de información. ●


FERRIMAX
ADVANCEDSECURITYSYSTEMS
Your potential is our future
Cajas Fuertes Certificadas
Fabricadas según la Norma Europea de Seguridad EN-1143/1.
Puertas y Cámaras Acorazadas
Certificadas según la Norma EN-1143/1.
Compartimentos de Seguridad
Certificados según la Norma 108115.
Compartimentos Robotizados
Acceso a sus valores con máxima flexibilidad.
www.ferrimax.com
madrid@ferrimax.com
917 960 896

ÁLVARO MOCHOLI. CEO. GREKKOM TECHNOLOGIES

«Innovación, calidad de producto y servicio son nuestros principales valores»

Innovación, calidad de producto y calidad de servicio y adaptabilidad, son, en palabras de Álvaro Mocholi, CEO de Grekkom Technologies, los principales valores que definen a la compañía, que nació en 2014 con el objetivo de convertirse en el principal proveedor y comercializador de analíticas de imagen gestionadas bajo una misma plataforma. Con un producto diferenciador, eficiente y efectivo, y un servicio profesional, ágil e incondicional a sus clientes, Grekkom Technologies apuesta para los próximos años por consolidar su expansión internacional con la apertura de nuevos canales de distribución y delegaciones en EEUU, Oriente Medio, Francia, China, entre otros países.

CUÁL es el origen y evolución de la compañía Grekkom en España?

—Grekkom nace en 2014 con el objetivo de convertirse en el principal proveedor y comercializador de analíticas de imagen, todas ellas gestionadas bajo una misma plataforma. Actualmente contamos con 28 analíticas en nuestra cartera que abarcan áreas como vigilancia perimetral, vigilancia marítima, prevención y detección de incendios, control de procesos de producción, prevención de riesgos, salud y tráfico. Gracias a este amplio abanico de analíticas, nos hemos convertido en un referente tanto a nivel nacional como internacional en analíticas para cámaras térmicas.

—¿Cuáles son las características y valores principales que definen a Grekkom como empresa?

—Los principales valores que nos caracterizan son innovación, calidad de producto, calidad de servicio y adaptabilidad. El sector de las analíticas, como cualquier sector directamente vinculado a la tecnología, está en constante renovación y adaptación a las demandas del mercado, es por ello por lo que nuestro departamento técnico está inmerso en un proceso de constante mejora y desarrollo. Las claves de nuestra empresa radican en ofrecer un producto diferenciador, eficiente y efectivo, en dar a nuestros clientes un servicio profesional, ágil e incondicional y tener la capacidad de adaptarnos e integrarnos con plataformas y sistemas de seguridad ya existentes.

—¿Podría explicarnos la estrategia de la compañía para los próximos años?

—Actualmente exportamos nuestras analíticas a 34 países. Nuestra estrategia a corto-medio plazo, desde el punto de vista comercial, pasa por consolidar nuestra expansión internacional mediante la apertura de nuevos canales de distribución y delegaciones en los principales mercados como EEUU, Oriente Medio, Francia, Italia, Inglaterra, Alemania y China. Desde el punto de vista de producto, seguiremos con nuestro compromiso de constante mejora de nuestras analíticas, potenciaremos nuestras líneas de analíticas de prevención de riesgos y detección de incendios y ampliaremos nuestra cartera de analíticas en las áreas de tráfico, retail y control de procesos de producción.

—¿Qué aspectos diferenciales distinguen a Grekkom en relación a su competidores?

—Grekkom está muy especializada en analíticas de imagen para cámaras térmicas, de hecho, gran parte de nuestras analíticas han sido desarrolladas específicamente para este tipo de cámaras. El estar tan especializados, nos ha permitido conocer a la perfección este tipo de cámaras, sacarles el máximo rendimiento y prestaciones y en consecuencia diferenciarnos de

nuestros competidores. Las principales ventajas competitivas que aportamos respecto a nuestra competencia son distancia de detección; gracias a nuestros alcances conseguimos ahorrar en torno al 30%-40% el número de cámaras y en consecuencia reducir el coste de obra civil, estructura informática y cableado. Además, nuestra filosofía de análisis nos permite discriminar objetos por tamaño, comportamiento y sensibilidad, consiguiendo los ratios de falsas alarmas más bajos del mercado 2-5%. Por último, y no menos importante, somos capaces de obtener las coordenadas UTM de todos los objetos que detectamos, la distancia a la que se encuentran respecto a la cámara y orientar las cámaras domo a dichas coordenadas y garantizar una correcta verificación de nuestras detecciones.

«Grekkom se ha convertido en un referente a nivel nacional e internacional en analíticas para cámaras térmicas»

—¿Qué analíticas ofrecen y para qué tipo de cámaras térmicas?

—Grekkom está muy especializada en analíticas para cámaras térmicas aunque el mercado cada vez nos solicita más analíticas para diferentes tipos de cámaras. Una de las claves de nuestro éxito es estar integrados con prácticamente todos los fabricantes de cámaras del mercado. Nosotros tenemos dos niveles de integración con las cámaras, el básico que es con el que funcionan la gran mayoría de nuestros competidores, que consiste en obtener el flujo RSTP de la cámara o en analizar las imágenes extraídas del grabador, y el nivel de integración avanzado, que es el que habitualmente tenemos, que consiste en controlar los parámetros de las cámaras y en consecuencia controlar la cámara para que la calidad y contraste de imagen sea lo más estable y óptima posible para garantizar así la eficacia de nuestras analíticas.

—¿A qué sectores van destinadas sus soluciones? ¿Tienen en mente ampliar con nuevos mercados?

—Gracias a nuestro extenso número de analíticas, estamos presentes en prácticamente todos los sectores, aunque los que más demandan nuestras analíticas son el petroquímico, energías renovables, defensa, eléctrico, aeroportuario, piscícola, administración pública, residencial y portuario.

En Grekkom, más que tener en mente abrir nuevos sectores, pensamos en nuevas fórmulas de comercialización. En fórmulas que se adapten a la operatividad y necesidades de nuestros clientes objetivo, en fórmulas más flexibles y eficientes y en ofrecer un servicio profesional, que garantice un perfecto funcionamiento de nuestras analíticas y libere a nuestros clientes de las constantes revisiones y ajustes. ●

Fotos: Grekkom Technologies

JOAN BALAGUER. DIRECTOR COMERCIAL. GRUPO IPTECNO

La combinación perfecta para seguridad perimetral: Radar + Deep Learning

Existe una máxima en seguridad que nos impide confiar en una sola tecnología para garantizar la protección de un perímetro o área bajo vigilancia. El sistema que más se acerca a la perfección, con un mínimo de falsas alarmas suele ser la combinación de varias tecnologías. No en vano los perímetros de infraestructuras críticas ya están siempre dotados de varios sistemas en paralelo que nos permiten garantizar la detección.

VISTO lo cual parece lógico pensar que cualquier dispositivo destinado a la detección de amenazas de seguridad será mejor cuantas más tecnologías en paralelo o interrelacionadas aglutine. Así un detector volumétrico de doble tecnología IR más microondas siempre será más fiable que uno simplemente basado en IR.

Vídeo Análisis

Pero centrémonos en el control perimetral o de vastas extensiones de terreno como zonas portuarias, campas de contenedores, perímetros de seguridad de infraestructuras críticas donde solemos instalar sistemas de análisis de vídeo. El mundo del vídeo análisis basado en Inteligencia Artificial, y más concretamente en algoritmos «Deep Learning» que autoaprenden del entorno en que se instalan, han llegado a un estado de gran precisión. No obstante uno de los impedimentos más frecuentes para que el Deep Learning pueda clasificar objetos una vez detectados y determinar si se trata o no de una amenaza real, sigue siendo la perspectiva de los objetos detectados. Me explico, la cámara fija con lente ajustada a un determinado plano focal que usamos en análisis de vídeo adolece del problema de no saber si el objeto que capta está cerca o lejos, de manera que un objeto grande a gran distancia aparece como un objeto pequeño, que ocupa pocos píxeles de imagen y que probablemente no será clasificado como lo que realmente es, y por el contrario un objeto pequeño cercano a la cámara puede aparecer como un intruso cuando a lo mejor se trata de una pequeña araña. A tal efecto los programas de vídeo análisis ya disponen de ajustes que intentan minimizar este efecto, pero igualmente debemos instalar muchas cámaras cada pocos metros paras que estos ajustes sirvan para algo.

Radar

Por el contrario disponemos de una tecnología de detección muy diferente a la óptica o térmica que se usa en vídeo análisis; efectivamente un emisor lanza

un haz de microondas que se refleja en los objetos que se encuentran a un kilómetro en visión directa y esa señal reflejada es «escuchada» y procesada en el dispositivo que llamamos «RADAR», las diferencias de frecuencia y fase entre la señal emitida y recibida que se generan por efecto doppler debido al movimiento de algunos objetos en la escena supervisada, nos indica dónde exactamente se encuentra el objeto en movimiento, qué tamaño tiene y en qué dirección y a qué velocidad se mueve. Todo esto sin que le influya negativamente ni las condiciones de luz, temperatura o climatológicas. Además el radar también dispone de su Inteligencia Artificial y algoritmos Deep Learning que le permiten discriminar objetos en movimiento que no deben ser detectados como amenazas, tales como vegetación y similares. El software de control del radar nos permite programar las zonas de inclusión o exclusión de alarma, dispone de perfiles que se pueden activar por horario y toda suerte de facilidades para que la detección de objetos en movimiento, presuntamente intrusos, sea lo más fiable posible. Además el radar puede dirigir una cámara con sistema de posicionamiento, tal como un speed dome o una combinada de espectro visible y térmico, a fin de hacer un seguimiento perfecto del intruso dándonos un primer plano del mismo.

«El mundo del vídeo análisis basado en Inteligencia Artificial, y más concretamente en algoritmos Deep Learning, ha llegado a un estado de gran precisión»

Lo mejor de ambos mundos

De lo explicado anteriormente se deduce que es precisamente la falta de un plano «perfecto», de no saber si el objeto captado está cerca o lejos, del conocimiento de su tamaño real, o de un seguimiento adecuado en vídeo del intruso lo que nos impide que los algoritmos de Deep Learning del vídeo análisis puedan funcionar al máximo de sus posibilidades.

Pues bien imaginemos que mediante la combinación de radar, cámara con posicionamiento y sistema de vídeo análisis, podemos proporcionarle a este último una imagen perfecta y cercana del objeto a clasificar, así como su tamaño, ¿se lo estamos poniendo fácil verdad?, pues de eso se trata. La combinación de sistemas radar + vídeo análisis, ambos dotados de algoritmos de detección que aprovechan la inteligencia artificial, cada uno en su terreno, en el del análisis de señales de radio y en el del análisis de las imágenes de vídeo. La mezcla de ambos nos ofrece una potente herramienta de detección perimetral, con un ahorro en infraestructura importante, por cuanto ya no se necesitaría «coser» el perímetro con cámaras fijas y una costosa red, sino que basta con ubicar estratégicamente sendos radares con sistemas de posicionamiento de vídeo y conectarlos a un VMS dotado de vídeo análisis inteligente que recibirá gracias al radar «la mejor imagen posible» del intruso, la procesará en menos de un segundo y generará la alarma solo cuando realmente se clasifique el objeto como intruso potencial. ●

Fotos: ***Grupo Iptecno***

MIGUEL ÁNGEL LOBO. DIRECTOR DE EUROMA TELECOM

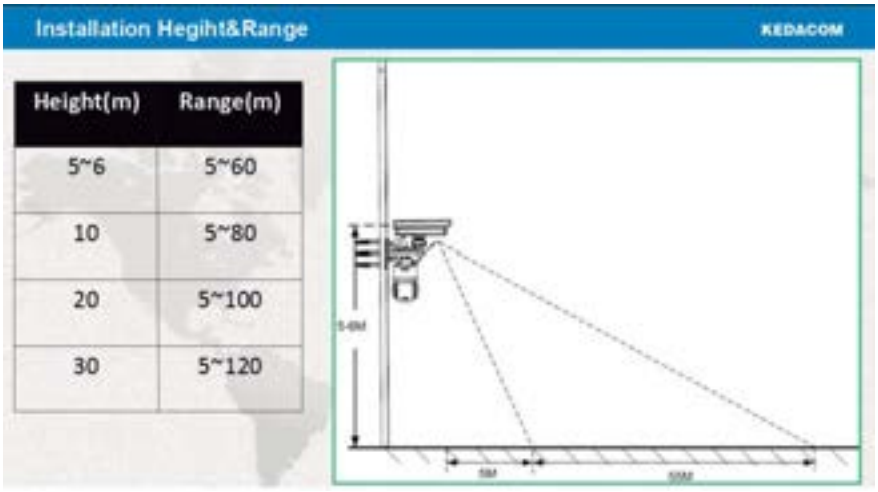
Tracking recognitivo

Los sistemas de tracking inundaron el mercado hace unos pocos años, algunos se integran dentro del propio domo motorizado y los menos usan dos cámaras: una de visualización general y otra para hacer el zoom. Todos estos sistemas causaron más de una frustración debido a que se esperaba bastante más de ellos. Muchos esperaban poder visualizar cualquier objeto (persona o coche) que estuviera en una zona delimitada de una forma totalmente automática, evitando que el personal de seguridad tuviera que estar manejando el «joystick» para seguir la trayectoria. Estos sistemas solo son útiles en lugares en donde no hay casi ninguna invasión y donde el sistema no tiene que gestionar más de un objetivo a la vez, se cruzan dos objetivos, etc.

La solución real para cubrir grandes áreas de una forma automática y totalmente desatendida es el uso de sistemas de tracking recognitivo.

El sistema se compone de dos elementos: Por una lado una cámara box del tipo «recognitivo». Estas cámaras incorporan un pequeño ordenador con «analítica de vídeo integrada», que es el elemento que toma la decisión de a qué objeto o persona seguir según unos parámetros definidos por el usuario previamente. El segundo elemento es una domo motorizada (se pueden colocar hasta 3 domos motorizados en el mismo lugar), que recibe la orden de en qué posición debe estar y la trayectoria. Estos elementos pueden funcionar de una forma totalmente independiente, es decir, no necesitan el uso de ningún otro dispositivo (lease grabador, ordenador, etc); por supuesto las imágenes de las dos cámaras pueden ser grabadas, visualizadas en remoto y lo que necesitemos, pero no son necesarios para el correcto funcionamiento. La cámara incorpora un slot para tarjeta SD (de hasta 128 Gb) en donde se grabarán las imágenes.

Imagen 1.



Discriminar entre personas y coches

El sistema de «tracking recognitivo» puede discriminar entre personas y coches, activándose solo por el objetivo definido, además podemos definir el color, el tamaño y la trayectoria, es decir, podemos indicar al sistema que solo nos haga el seguimiento de «coches rojos que salgan de un parking»; esta discriminación nos permite no perder el tiempo con «objetivos» que no nos son interesantes. Ademas gracias a la potencia del procesador integrado en la cámara recognitiva se pueden distinguir hasta 60 objetivos simultáneos en una escena. La cámara motorizada irá «saltando» de un objetivo a otro para no «perdernos nada»; si el volumen de tráfico es elevado se pueden colocar hasta 3 camaras domo motorizadas conectadas a la misma cámara recognitiva para repartirse el trabajo, y

poder permanecer más tiempo en cada objetivo.

El área que queramos cubrir puede ser definido en 3 diferentes niveles de prioridad de alarma, dando a cada uno un tiempo de estancia si un objetivo se situa en dicho área; también podemos discriminar áreas que no nos interesan para no perder tiempo.

La cámara se instala según el cuadro de imagen que deseamos cubrir **(Imagen 1)**.

El primer paso a realizar después de instalar físicamente la cámara es activar la misma y calibrar la detección de la misma, para ello indicamos cuáles son las áreas que vamos a analizar y pulsamos sobre la calibración automática; por último seleccionamos la agenda de armado (podemos activar una detección 24H o por calendario a ciertas horas). Tras esto el sistema queda completamente funcional realizando las capturas correspondientes. Es muy sencillo de instalar, no requiere grandes calibraciones y puede ponerse en marcha en solo 5 minutos.

La cámara realiza una captura optimizada almacenando solo la imagen de mayor interés y definición.

Es un sistema utilizado para controlar zonas (se pueden cubrir hasta 10.000 m^2) donde es de crucial importancia no perder detalle relacionado con los objetos en movimiento al entrar en un área determinada como por ejemplo una cárcel, huerto solar, plazas, casinos, parkings, etc. Está demostrado que después de una hora de vigilancia por un vigilante se seguridad, comienza el periodo de «fatiga», en donde se empieza a perder concentración y capacidad de observación. El sistema de tracking recognitivo es totalmente «desatendido» y funciona 24 horas al día (Iluminacion IR) y nos proporciona un ahorro considerable en instalaciones, ya que podemos cubrir un amplio área con tan solo dos cámaras y sin personal de seguridad que se encargue de su gestión. ●

«La solución real para cubrir grandes áreas de una forma automática y totalmente desatendida es el uso de sistemas de tracking recognitivo»

Fotos: ***Euroma***

JOSÉ MARÍA GARCÍA DE PRADO. DETECTIVE PRIVADO Y PERITO JUDICIAL EN SEGURIDAD PRIVADA

Luces y sombras sobre la legislación en investigación privada

Antes de empezar a desarrollar este artículo sobre la importancia de una correcta legislación en el sector de la investigación privada, es imperante destacar que nuestra Constitución establece, a lo largo de gran parte de su articulado, los mecanismos para que los ciudadanos puedan disfrutar del pleno ejercicio de los derechos fundamentales y de las libertades públicas. En este sentido, en la Ley Orgánica 1/1992, sobre Protección de la Seguridad Ciudadana, se establece que la competencia de la Fuerzas y Cuerpos de Seguridad del Estado para proteger y garantizar la seguridad ciudadana corresponde al propio Estado.

SIN perjuicio de ello, la realización de actividades de seguridad e incluso de investigación, suponen un reforzamiento de las encomendadas al Estado teniendo en cuenta que, según se establece en la Ley 5/2014, estarán sujetas a los controles e intervenciones administrativas necesarias para el ejercicio de las actividades por los particulares.

Entre los objetivos que se plantean en la Ley de Seguridad Privada, que deroga la anterior Ley 23/1992, cabe destacar la mejora de la eficacia en la prestación de los servicios de Seguridad Privada, la eliminación del intrusismo en el sector, la dotación de un respaldo jurídico necesario para el ejercicio de sus inherentes funciones legales y establecer unas pautas e instrumentos de colaboración entre estos servicios privados y la seguridad pública, contemplado en el Título I. La regulación jurídica de las empresas de Seguridad Privada y los despachos de Detectives Privados viene detallado en el Título II. Las funciones específicas de los profesionales, requisitos de acceso, formación y principios de actuación vienen reglados en el Título III. Es en el Título IV, donde se establece como objeto de tratamiento específico los servicios de Investigación Privada conjuntamente con los de videovigilancia, por la incidencia que pueden tener en la vulneración del derecho a la intimidad protegido en nuestra Carta Magna (artículo 18). Quedando desarrollado el régimen sancionador en el Título VI.

Pero la crítica principal de este artículo recae en una evolución de una normativa reguladora, que ha sido desaprovechada al encajar y cuartelar de forma forzada el ámbito de la Investigación Privada dentro de la Ley 5/2014 de Seguridad Privada, para regular las específicas actividades de los Detectives Privados, perdiendo la oportunidad de desarrollo en un marco jurídico más apropiado y específico a las actividades que se desarrollan. Y es en el nuevo Reglamento de Seguridad Privada, en donde es posible inferir con una nueva oportunidad que posibilite el desarrollo de los cometidos, generando cambios sustanciales con respecto al vigente Real Decreto 2364/1994, que regula los distintos ámbitos de actuación y los diferentes empleos profesionales que integran el sector de la Seguridad Privada. Pero como viene siendo habitual en las últimas legislaciones, parece que no será así con respecto a los profesionales que integran el colectivo de los Detectives Privados.

En el borrador publicado por el Ministerio del Interior, se continúa sin crear un articulado propio, continúan sin especificar sus atribuciones y sus actividades, así como la participación e inclusión de los colegios profesionales en la Ley o la figura del detective de oficio (tal y como sería preceptivo en vista a los motivos expositivos de la nueva Ley).

Más aún, continúa sin regularse la imposibilidad de establecer protocolos de colaboración con las Fuerzas y Cuerpos de Seguridad en puntos en los que el Detective Privado puede llegar a ser una figura indispensable en temas concretos como el tráfico de capitales, las investigaciones sobre corrupción, la localización de delincuentes en nuestro territorio, y un largo etcétera que es cohibido por ámbitos que son prohibitivos, al considerar muchos de estos como jurisdicción exclusiva de la Seguridad Pública, y obviando el Preámbulo de la propia Ley 5/2014 que recoge en el apartado III: «La ley pasa de poner el acento en el principio de la subordinación a desarrollar más eficazmente el principio de complementariedad a través de otros que lo desarrollan, como los de cooperación o de corresponsabilidad…». No se trata de crear una policía paralela investigando, sino de aprovechar más y mejor la figura del Detective Privado, de igual forma que se aprovecha por medio de los Vigilantes de Seguridad debidamente habilitados complementando la seguridad ciudadana. En definitiva, no se genera el espíritu especificado en el resumen del Preámbulo, en su apartado III «…complementaria, subordinada, colaboradora y controlada por la seguridad pública…».

Visión normativa

Por otro lado, tanto en la Ley como en el futuro Reglamento de Seguridad Privada, se limitan aún más si cabe, con respecto a la «vigilancia» que podía realizar de determinados espacios públicos como ferias, hoteles, exposiciones o ámbitos análogos, incluyendo grandes superficies comerciales, que con esta nueva Ley y el futuro Reglamento dará la posibilidad de realización por parte de Vigilantes de Seguridad que no se encuentren uniformados, limitando a los Detectives Privados a la mera «obtención de información». Otra de las cuestiones planteadas son las medidas de seguridad física con las que han de contar los despachos, que, a todas luces, pueden ser consideradas excesivas para proteger la documentación de la investigación en curso si son comparadas con las exigidas al cliente y a dichos documentos tras finalizar las investigaciones.

Por último, pero no menos importante, la obligatoriedad de poseer un aval o seguro de caución que abocaría al Detective Privado a desempeñar sus funciones amparado por una gran corporación en Investigación Privada que haga frente a ello, despojando al empresario autónomo (la gran mayoría de los Detectives Privados en España) de poder acceder a la profesión de forma independiente. Y sumemos a esta lista que el régimen de sanciones impuestas a los Detectives Privados es asimilado al de empresas.

Por otro lado, no podemos obviar que, en esta reglamentación adaptada al espacio europeo, se establece en el Artículo 28 de la Ley, que cualquier miembro de la Unión Europea con «habilitación o cualificación profesional» expedida en su país de origen podrá desempeñar actividades de Seguridad Privada. Como es el caso de Portugal, donde la profesión no está regulada y sólo exige haber dado de alta la actividad en Hacienda con el código 80300 y pertenecer a una asociación de Detectives Privados. En el caso de Francia, su Ley 239/2003 establece como únicos requisitos: ser francés o miembro de la Unión Europea; tener la calificación definida por decreto en el Consejo de Estado; estar matriculado ante el organismo autorizado; y por último, carecer de antecedentes penales. Sin llegar a exigirse una formación mínima, llegando a crear un agravio comparativo en la propia UE.

Pero estos errores –en opinión personal- continúan dentro de la Ley 5/2014, cuando establece en su propio Preámbulo: «…reconocer la especificidad de los servicios de investigación privada, el papel que han alcanzado en nuestra sociedad en los últimos años. Siendo diferentes de los demás servicios de seguridad privada... que contribuye a garantizar la seguridad de los ciudadanos, entendida en un sentido amplio». Por ende, las actividades de los Detectives Privados que están legalmente facultados para la obtención y aportación de informaciones y pruebas sobre hechos y conductas de índole privado y orienta-

das en los ámbitos económicos, laborales, mercantiles, financieros y en la vida familiar y personal, siempre manteniendo y sin que medie la intromisión y vulneración de la esfera privada del investigado, no deberían de estar incluidas y englobadas en la actual Ley de Seguridad Privada. Asimismo, considero que no se ha abordado el tema formativo acorde a lo exigido en España, también echo en falta que la profesión pueda convertirse en figura de auxilio judicial en listados de Detectives Privados de oficio, al igual que lo son los Peritos en sus distintas especialidades establecidos en el artículo 335.1 de la LEC (Ley 1/2000). Además, considero un error introducir un régimen sancionador asimilado a empresas, ya que sería inasumible por parte de trabajadores independientes en la modalidad de autónomos y en el epígrafe 773 del IAE.

Por todo lo anteriormente expresado, las diferentes Asociaciones y Colegios Profesionales del sector (APDPE, ADAE, Colegio Profesional de la Comunidad Valenciana y de Cataluña) se unieron para hacer un frente común y tratar de encauzar las reformas necesarias que la Ley 5/2014 y el futuro Reglamento de Seguridad Privada desarrollará, contemplando las demandas nacidas desde el sector de la Investigación Privada. El Ministerio del Interior desveló y sacó a la luz pública, el pasado mes de mayo, el borrador oficial del nuevo Reglamento de Seguridad Privada dando de plazo hasta el 22 de junio de 2018 para poder realizar las aportaciones que se crean convenientes, atendiendo a las demandas del sector.

Demandas solicitadas

Entre otras demandas solicitadas para el desarrollo de la profesión de Detective Privado incluidas en la Ley, se encuentran las siguientes:

a) La derogación de 7 artículos de la Ley 5/2014 de Seguridad Privada.

- Art. 2 Despachos de detectives privados: las oficinas constituidas por uno o más detectives privados que prestan servicios de investigación privada.
- Art. 9 Contratación y comunicación de servicios.
- Art. 24, 2, aptdo. c), f) y h). Apertura de despachos de detectives privados.
- Art. 25, 1, aptdo. j) Depositar, en caso de cierre del despacho por cualquier causa, la documentación profesional sobre contratos, informes de investigación y libros-registros en las dependencias del Cuerpo Nacional de Policía o, en su caso, del Cuerpo de Policía Autonómico competente.
- Art. 39.2. Prestación de servicio uniformado.
- Art. 61. Régimen sancionador para empresas, despachos de detectives y centrales de alarma.
- Art. 62 Sanciones a personal de seguridad privada.

b) Petición de promulgación del «Estatuto Profesional del Detective Privado», con rango de Ley.

Para concluir, comentar que se preveía que a principios de 2018 viera la luz el nuevo reglamento de Seguridad Privada, cuya estructura se dio a conocer, tal y como especificó. Esteban Gándara en su última conferencia en Córdoba, con motivo de la celebración del Día de la Seguridad Privada, antes de su despedida como Comisario Jefe de la USCP (Unidad Central de Seguridad Privada). De igual modo, el anterior Ministro del Interior. Juan Ignacio Zoido, aseguró el pasado 19 de mayo de 2017, que el primer borrador se encontraba en muy «avanzado estado de elaboración» y que «en un corto plazo de tiempo» se iniciaría su tramitación, durante la que se comprometió a consultar y «considerar» las opiniones del sector. Pero a día de hoy, finalizado el plazo dado para la realización de aportaciones, con las convulsas en el Gobierno y sus cambios de políticas, retrasará algún tiempo la reglamentación de una Ley promulgada hace más de cuatro años, dilatando lo ya realizado hasta que las prioridades lo permitan. Y, presumiblemente, las propuestas aportadas serán valoradas aunque no contempladas en el nuevo reglamento. Por tanto, ¿deberemos esperar a una nueva Ley que acometa la realidad de un sector que ha ido evolucionando y dignificándose con el buen hacer de sus profesionales, que son los más y mejores formados de Europa? ●

Fotos: Shuterstock

Juntos con un único objetivo: construir un futuro sin incendios

LOS INCENDIOS MATAN

LA PROTECCIÓN ES POSIBLE

tecnifuego

www.tecnifuego-aespi.org

EMPRESAS ASOCIADAS


Advantronic
aguilera
RICONSISTEMAS
Fire Protection Systems
AM.CON
amPimex
andreu
The Steel Door Company
AUXQUIMIA
THE FOAM SOLUTION
AXTER
BACH
Berbel Porcel
BOSCH
Innovación para tu vida
Budenheim
cofem s.a.
1973
COLT
CPI
CISA
CONTROL HOMOLOGADO
cottes
LIFE SAVING SOLUTIONS
DAS EXTINTORES, S.L.
Instalaciones y mantenimiento contra incendios
ENERGIMAC
enesa
continental
eNGie
Engineered FIRE PIPING
EUROFIRE
Falck SCI
FIRELANZ
FIREX
FISEG
ZENITH
Gext
Grupo
IGNIWOOL
IMPLASER
AUCA
Insacuatro
GRUPO
IMABER
MÜPRO
PROTECHL
nsc
OBEYSA
odice
Ondoan
PLASFOC
Prefire
PREVINSA
procaval
productos mesa
PROSEGUR
ROCKWOOL
ROPER
PUERTAS METÁLICAS
RUCA
SFE Systems
S21
SEÑALIZACIÓN
SABO
española
SIEX
Sinalux
MERA
sistemas de seguridad
ntcl
SODECA
SOLER
Techco
tipsa
Kerlyoma Group
TEPROSOL
Tecnitex
Tecnofire
DETECTION
HI-TECHNOLOGY & DESIGN
WORLDWIDE FROM ITALY
Termodinair
Victaulic
VIKING
OPENERS & CLOSERS
Secure locking solutions
inn.
SOLUTIONS
KRIPFIRE
SABICO
contra incendios

COMISIÓN NACIONAL PARA LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

Aprobado el Plan Estratégico del sector de la Salud

El Sistema de Protección de Infraestructuras Críticas cuenta ya con 171 operadores

La Comisión Nacional para la Protección de las Infraestructuras Críticas, presidida por la secretaria de Estado de Seguridad, Ana Botella, aprobó el pasado 30 de octubre el Plan Sectorial Estratégico del sector de la Salud. De esta forma, se han aprobado ya 16 de los 18 planes estratégicos previstos. El plan relativo al sector de la Salud se suma a los ya vigentes relativos a los ámbitos de electricidad, gas, petróleo, nuclear, sistema financiero y tributario, agua, transporte urbano y metropolitano, marítimo, aéreo, ferroviario y por carretera, industria química, alimentación, TIC y espacio.

ESTÁ previsto que los dos planes pendientes (Administración e Instalaciones de Investigación) se aprueben a lo largo del próximo año.

Esta ha sido la séptima reunión de la Comisión desde su constitución en junio de 2014, y la primera que preside Botella desde su nombramiento como secretaria de Estado de Seguridad.

El encuentro también sirvió para revisar los planes estratégicos ya en vigor de los sectores del transporte aéreo, carretera, ferroviario y marítimo, así como el del sector del agua.

También se llevó a cabo la designación oficial de los operadores críticos (aquellos con especial responsabilidad sobre sus infraestructuras) en el ámbito de la Salud, con lo cual, a partir de este momento, el Sistema de Protección de Infraestructuras Críticas involucra también a estos nuevos actores.

En total, son 24 los nuevos operadores críticos que se incorporan al sistema, 11 del sector de la Salud, cinco del Agua, cuatro en el Aéreo, y otros cuatro en el de la Carretera. Con estas incorporaciones, el Sistema de Protección de Infraestructuras Críticas cuanta ya 171 operadores.

Durante su intervención en la reunión, Botella aseguró que la protección de las infraestructuras críticas es «uno de los elementos de mayor interés y con mayor proyección de futuro que existen en la agenda del Gobierno de España». «Las infraestructuras críticas son trascendentales para el normal funcionamiento de los servicios esenciales al constituir éstos la columna vertebral de toda la actividad humana (individual, social, industrial, comercial y de gobierno) de cualquier país moderno», señaló.

La secretaria de Estado destacó en este sentido «la trascendencia de la reciente aprobación del Real Decreto-ley 12/2018, de seguridad de las redes y sistemas de información» y subrayó la necesidad de «cooperación y enfoque integral» en esta materia ya que «la mayoría de nuestras infraestructuras está en manos del sector privado». ●

Fotos: MIR

SIMPOSIUM 2018. REUNIÓ A 2.500 VISITANTES Y 100 EMPRESAS

Ingram Micro reforzará su porfolio con soluciones anti intrusión

El mayorista informático incorporará a su división de Physical Security los sistemas de protección perimetral de Axis, su partner de referencia

Ingram Micro se propone reforzar la división de Physical Security que creó en 2015 con la incorporación a medio plazo de sistemas anti intrusión que complementen su actual porfolio, basado fundamentalmente en videovigilancia y control de accesos. La idea que baraja el mayorista informático no pasa por llegar a acuerdos con fabricantes nuevos, sino por seguir explotando el amplio abanico de soluciones que ya ofrece su partner de referencia, el fabricante sueco Axis, en este caso en el campo de la protección perimetral.

Así lo explicó el director ejecutivo de Ingram Micro Madrid y responsable del Área de Valor, Alberto Pascual, quien resaltó que las prestaciones que ofrece Axis «cubren todo el abanico de la seguridad física», destacando la relevancia que sus cámaras de videovigilancia IP orientadas al business intelligence tiene para el sector retail y sus posibilidades en el campo de la Inteligencia Artificial y el Internet de las Cosas.

En el ámbito de la videovigilancia, además de Axis, el mayorista ya cuenta con los productos de Trendnet, que se suman al porfolio de software de grabación, almacenamiento NAS, control de accesos o infraestructuras de red y cableado, de la mano de fabricantes de primer nivel como WD, Seagate, Synology, ZKTeco, D-Link o MCL, entre otros. De forma complementaria, Pascual anunció la reciente incorporación del fabricante Devo, antes conocido como Logtrust, focalizado en el software de analítica de vídeo.

Con la entrada de sistemas anti intrusión solo quedaría por incorporar al porfolio de Ingram Micro soluciones de protección contra incendios, un objetivo que también persigue la compañía para reforzar una división que alcanzará este año un crecimiento superior al 20%, por encima del incremento global de la compañía.

Pascual hizo este análisis tras la celebración del Simposium 2018, que reunió en la Cúpula de las Arenas de Barcelona a más de 2.500 asistentes y más de un centenar de fabricantes, según los datos ofrecidos por la compañía.

En la misma rueda de prensa, Jaime Soler, VP & Country Chief Executive Iberia de Ingram Micro, avanzó que la compañía va a estabilizar este año su ritmo de crecimiento hasta situarse entre un 6-7%, en sintonía con la media de crecimiento del mercado, que será del 8%, según los datos de la consultora Context. Soler explicó que se ha decidido «revisar el modelo de negocio para poner recursos en otras necesidades de la compañía», trabajando en cuatro palancas fundamentales: Valor, Mobile, Mercado tradicional del canal y Logística y Servicios. ●

Texto y foto: Emilio S. Córreces

ENCUENTRO ORGANIZADO POR TECNIFUEGO EN MADRID

I Jornada Técnica «Lucha contra Incendios Forestales»

Ponentes expertos, audiencia especializada e interés en la actualización de conocimientos han marcado la 1ª Jornada Técnica Lucha contra Incendios Forestales (IIFF), organizada por Tecnifuego, Asociación Española de Sociedades de Protección contra Incendios, con la colaboración del Ministerio de Agricultura, Pesca y Alimentación, MAPAMA; y APTB, Asociación Profesional de Técnicos de Bomberos. La Jornada, celebrada en la sede del MAPAMA, incidió en el análisis de las causas, los factores, las estadísticas comparadas, la comunicación interna y externa, y las estrategias en la lucha contra los incendios forestales en el área de interfaz urbano forestal.

DURANTE la presentación, Vicente Mans, director del Área de Protección Pasiva de Tecnifuego, agradeció la alta asistencia y el interés de los participantes, y comentó la necesidad entre los profesionales de la lucha contra IIFF de jornadas de este tipo para la ampliación y actualización de conocimientos, pero también de debate e intercambio de experiencias y sinergias. «Esto es lo que nos ha animado a organizar esta 1ª Jornada que nace con afán de continuidad. La protección contra incendios ha cobrado un especial significado en los últimos años por su proximidad a las poblaciones. Ante nosotros tenemos el reto de ofrecer soluciones a los ciudadanos. Esperamos que esta jornada contribuya a ello».

A continuación José Manuel Jaquotot, subdirector general de Política Forestal, Dirección General de Desarrollo Rural, Innovación y Política Forestal (MAPAMA), felicitó a los organizadores por la celebración de esta jornada que ahonda en temas «que a todos nos preocupan, porque la gestión de los incendios forestales no debe entenderse solo desde la extinción, intervienen múltiples factores como meteorología, orografía, cambios socioeconómicos, abandono rural, etc.».

Concienciar a los municipios

Por su parte, Carlos Novillo, director de la Agencia de Seguridad y Emergencias Madrid 112, de la Comunidad de Madrid, destacó el reto que tiene ante sí la CAM para que los Ayuntamientos sean autosuficientes: «En áreas interfaz urbano-forestal, y la complejidad de protegerlas frente a IIFF, un reto: concienciar a los municipios de la importancia de tener un Plan de Autoprotección». Novillo incidió en la importancia de la comunicación tanto interna como externa. En este sentido, defendió que la comunicación externa es esencial. «Saber cómo y qué comunicar es saber cómo proteger a la población».

La jornada continuó con las intervenciones sobre las «Necesidades y áreas de mejora en la defensa contra los incendios forestales: visión estatal», impartida por Elsa Enríquez, jefe del Área de Defensa IIFF, MAPAMA, que adelantó los últimos datos sobre la temporada de incendios 2018 comparándolos con los del último decenio. «No se puede analizar un año aisladamente. Las cifras significativas se encuentran en la comparativa del histórico». La ponente abordó las causas de

los IIFF, los factores que incluyen, etc. «Los datos señalan que cada vez hay menos grandes incendios (mayor 500 hs.), y que la mano del hombre intencionada o fortuita es la causa del 85% de los mismos». El siguiente tema fue «Un caso real: Evaluación del Incendio de Galicia», donde Eduardo García, de APTB, señaló la problemática existente en Galicia con el territorio distribuido en minifundios y donde la limpieza del monte está en manos de los propietarios. El ponente describió la problemática de los Bomberos en los IIFF que se enfrentan a situaciones muy complicadas, simultaneidad de los IIFF y «donde la realidad supera a la ficción, y a veces hasta 24 horas sometidos a temperaturas muy altas, con estrés térmico, sin máscaras, con el humo que va y viene» relató García.

La comunicación eficaz

«La comunicación eficaz en las emergencias 1ª Parte: coordinación entre efectivos», fue la ponencia abordada por Alfonso Muñoz, de APTB, que expuso las normas de comunicación entre intervinientes e las diferentes tecnologías que ayudan: «el futuro está en las redes inteligentes conectadas a nivel europeo para geoposicionamiento de equipos, etc. O a través del móvil, montados ya en el camión, el mando sabe dónde estás, la conexión por satélite.» Igualmente, mencionó la importancia de tener un canal de comunicación directo e independiente del puesto de mando hacia los efectivos de bomberos.

La jornada continuó en formato de mesa redonda, titulada la «Comunicación exterior de las emergencias», moderada por Rosa Pérez, directora de Comunicación de Tecnifuego, y contó con la intervención de los periodistas Francisco Javier Barroso, sección Sucesos de El País, que abordó cómo se gestiona una emergencia desde un medio de comunicación, y la necesidad de que el periodista en las emergencias disponga

de una comunicación fluida por parte de los portavoces o mandos del efectivo para transmitir así información rápida y fiable a la población. Gema Ibáñez, directora de Comunicación de Cruz Roja Castilla -La Mancha, que defendió la función del periodista como un «interviniente» más en las emergencias: «la información salva vidas», y la difícil tarea de «extinguir fuegos en las redes sociales», poniendo como ejemplo el incendio de Yeste de 2017 (Albacete), donde a través de un tuit se solicitaban ayudas y herramientas que pudieron haber colapsado las operaciones de los equipos de extinción. Y Diego Herrera, miembro de VOST Spain, Asociación Nacional de Voluntarios Digitales de emergencias, que informó de cómo surge en España esta asociación, en el año 2012, como consecuencia de los grandes incendios forestales de Carlet (Valencia) y Canarias. Los equipos voluntarios VOST trabajan desde entonces para combatir los bulos en los IIFF, remitiendo siempre a contrastar la información con fuentes oficiales.

Interfaz urbano-forestal

La segunda mesa redonda trató de la «Interfaz urbano forestal: descripción de la situación y estrategias de protección», moderada por Ramón María Bosch, coordinador Comité Defensa contra IIFF de Tecnifuego, contó con la presencia de la investigadora Elsa Pastor, de Universidad Politécnica de Cataluña; el sociólogo Javier Jiménez, de Fundación Pau Costa; y el mando bombero, Eduardo García. En la misma se analizaron desde diversas perspectivas una problemática en alza, desde el conocimiento y la experiencia los IIFF en IUF: las necesidades y oportunidades de investigación; las deficiencias en la legislación, la escasez de recursos, la falta de interés, la problemática y dificultad de la intervención de los bomberos, etc. Elsa Pastor postuló por la investigación en las zonas de interfaz y puso como ejemplos las fajas perimetrales, las casas como refugios o los depósitos GLP; además informó sobre el nuevo proyecto europeo WUI-VIEW en el que Tecnifuego participará como usuario final. Javier Jiménez puso el énfasis en los comportamientos y cambios sociales y cómo influyen en la vulnerabilidad de estas zonas de IUF. Eduardo García insistió en las dificultades con que se encuentran los operativos en estas zonas por el hecho de no seguir una reglamentación.

La jornada finalizó con un animado e interesante debate entre los asistentes y los ponentes. Durante la clausura, Vicente Mans anunció que la 2ª. Jornada en 2019 será ampliada dado el éxito, el interés y la extensa temática que aborda las complejidades y soluciones de los incendios forestales. ●

Texto y Fotos: Tecnifuego

ENCUENTRO. EL HOSPITAL PRÍNCIPE DE ASTURIAS DE ALCALÁ DE HENARES ACOGIÓ LA CITA

Las jornadas de seguridad sanitaria abordan los retos del sector

La XV edición de estas jornadas, organizadas por el OSICH, abordó desde las agresiones a personal sanitario a la protección de los hospitales como infraestructuras críticas pasando por la seguridad desde la gerencia hospitalaria

El Hospital Universitario Príncipe de Asturias de Alcalá de Henares acogió las XV Jornadas Técnicas de Seguridad en Centros Sanitarios. El director general de Sistemas de Información Sanitaria de la Consejería de Sanidad, José Antonio Alonso, inauguró esta cita de referencia para los directores de seguridad, donde a lo largo de dos jornadas se abordaron en mesas y actividades paralelas los retos de este colectivo.

LAS mejoras en la gestión de la Seguridad fue el tema sobre el que giró la primera de las mesas de estas jornadas, organizadas por el Observatorio de Seguridad Integral en Centros Hospitalarios (OSICH). En ella participaron como ponentes Fernando Bocanegra, director de Seguridad Corporativa del Servicio Madrileño de Salud; Alejandro Fondón, director de Seguridad del Grupo Ribera Salud, y José Miguel Delgado, representante del departamento de Seguridad del Hospital Universitari Son Espases de Mallorca, que se centró en «Gestión de la Seguridad: la perspectiva del vigilante de Seguridad». La segunda de las mesas versó sobre los hospitales y su protección como infraestructuras críticas. Como expertos participantes contó con Carlos García, del Centro Tecnológico de Seguridad del Ministerio del Interior; David Lleras, subdirector general de Innovación y Arquitectura Tecnológica del Servicio Madrileño de Salud; Martín González y Santiago, director corporativo de Seguridad, Protección de Datos y Calidad de los Hospitales San Roque de Las Palmas de Gran Canaria; José Javier Larrañeta, secretario general de PESI, y Enrique Polanco, experto en Planes de Protección de Infraestructuras Críticas.

Los grados universitarios en Seguridad centraron la tercera mesa, que tuvo como integrante a Lucas Andrés, profesor de la Universida de Las Palmas de Gran Canaria; José Julián Isturitz, director general corporativo de Hospitales San Roque y representante del Grado de Seguridad de la Universidad Autónoma de Barcelona, y Víctor Rodríguez, decano de la Facultad de Criminología y director del Grado en Ciencias de la Seguridad de la Universidad Isabel I de Castilla.

La primera jornada se cerró con la mesa «Prevención de agresiones a

personal sanitario», en la que intervinieron Manuel Alcaide, vocal de la Secretaría de Estado del Ministerio del Interior; Javier Galván, Interlocutor Nacional Agresiones a Sanitarios del CNP; Basilio Luis Sánchez, Interlocutor Nacional Agresiones a Sanitarios de Guardia Civil; José Alberto Becerra, coordinador del Observatorio Nacional de Agresiones a Sanitarios de la Organización Médica Colegial; Rafael Lletget, Director del Gabinete del presidente de la Organización Colegial de Enfermería; y Miguel Ángel Peñalba, responsable de Comunicación e Imagen Corporativa del OSICH y director de Seguridad del Área de Salud Oeste de Valladolid. La segunda y última jornada se abrió con la mesa «Fuentes radiactivas. Radiaciones Ionizantes y Fuentes Biológicas como factores de Riesgo en Instituciones Sanitarias»

Como ponentes estuvieron Javier Negredo, director de Seguridad del Hospital Universitario La Paz; Kefrén Sánchez, responsable del Servicio de Radio Física del Hospital Universitario Príncipe de Asturias, y José Antonio Torres, brigada de la Unidad Técnica de NRBQ de la Guardia Civil.

La segunda mesa del día abordó las «Emergencias en instituciones sanitarias». Para analizar esta temática se contó con las aportaciones de Pedro Omar Sevilla; Manuel Martínez, director del Área de Protección Activa de Tecnifuego; Antonio Pérez, responsable de IMV y de planes de emergencia de Summa 112, y Carlos Novillo, director de la Agencia de Seguridad y Emergencias Madrid 112.

La mesa que cerró las jornadas tuvo como tema central «La seguridad desde la perspectiva de la Gerencia Sanitaria» En ella intervinieron Carmen Martínez de Pancorbo, directora gerente del Hospital Universitario Doce de Octubre de Madrid; Ricardo Herranz, director gerente del Hospital Universitario Puerta de Hierro de Majadahonda; Juan José Equiza, director gerente del Hospital Universitario Ramón y Cajal de Madrid, y Carlos Mur de Viu, director gerente del Hospital Universitario de Fuenlabrada.

Las jornadas concluyeron con el acto de clausura en el que estuvieron Félix Bravo, director gerente del Hospital Universitario Príncipe de Asturias de Alcalá de Henares; Carlos Novillo, director de la Agencia Madrileña de Emergencias, y Antonio Ponce, director de Seguridad del Hospital Universitario Son Espases y miembro de la Junta Directiva de OSICH. ●

FOTOS: OSICH

EL EVENTO CONTÓ CON LA PARTICIPACIÓN DE 47 EMPRESAS EXPOSITORAS

ENISE se afianza como la cita de referencia en ciberseguridad

La duodécima edición superó los datos de 2017 al concitar a más de 2.000 personas en el evento anual organizado en León por el INCIBE

Además, más de 3.000 personas siguieron vía streaming las conferencias del centenar de expertos que participaron como ponentes; 10 inversores internacionales procedentes de Chile, México, Colombia y Alemania mantuvieron 170 encuentros bilaterales con emprendedores y empresas españolas, y 47 empresas participaron como expositores y realizaron presentaciones y demostraciones de producto

En la parte de conferencias, prestigiosos expertos nacionales e internacionales abordaron riesgos, retos y nuevas soluciones del sector de la ciberseguridad además de temas de actualidad y de emprendimiento. Entre ellos, destacaron cuestiones relacionadas con el Internet de las Cosas o el primer Foro sobre Coches Conectados que incidió en la importancia de que este tipo de vehículos incorpore la ciberseguridad desde el diseño. En la clausura del acto, el director general de INCIBE, Alberto Hernández, aseguró que más allá de los datos, 12ENISE, que se celebró bajo el claim «Ciberseguridad: un pilar de la transformación digital», sirvió para generar oportunidades de negocio e internacionalización para la industria española, impulsar el networking entre profesionales y reunir a los agentes del ecosistema emprendedor. «12ENISE ha servido también para demostrar el enorme potencial de la industria de ciberseguridad en España y para poner en evidencia las oportunidades que se abren en este ámbito», afirmaba Hernández, quien añadió que «12ENISE se ha afianzado como el gran evento de referencia para los profesionales de la ciberseguridad y se ha consolidado como la gran plataforma para fomentar el emprendimiento, la competitividad empresarial y la innovación en ciberseguridad».

Ciberseguridad & Centros Educativos

En el acto de clausura también se hizo entrega del «Premio ENISE a la mejor iniciativa en materia de ciberseguridad» implantada en centros educativos durante el curso escolar 2017-2018. El IES Rafael Alberti de Cádiz se alzó con este galardón gracias a su proyecto «El ciberespacio: Amenazas y oportunidades», «un proyecto ambicioso y muy completo con complejidad técnica, organizativa y de alto impacto», como se refleja en la valoración del jurado.

El secretario de Estado para el Avance Digital, Francisco Polo, inauguró 12ENISE e indicó que España debe ser una nación ciberemprendedora y señaló que por primera vez el Gobierno cuenta con una estrategia para impulsar el emprendimiento tecnológico.

Texto y Foto: ***INCIBE***

Hikvision amplía sus horizontes con una nueva generación de paneles de alarma

Hikvision, proveedor mundial destacado de soluciones globales de seguridad, ha lanzado una nueva gama de paneles de alarma. En este lanzamiento se combina la potencia del proveedor de referencia del mercado CCTV, con la experiencia de una compañía como Pyronix, especializada desde hace más de 30 años en intrusión. Así, la nueva gama de paneles de alarma proporciona a los instaladores profesionales sistemas de seguridad innovadores y fiables para cada función.

Con diseños elegantes la amplia gama ofrece soluciones avanzadas que dan respuesta a las diferentes necesidades de todos los segmentos del mercado: aplicaciones residenciales, comerciales e industriales.

Compatible con los productos CCTV Hikvision

Compatible con todos los productos de CCTV de Hikvision, la gama se integra a través del iVMS y la aplicación para dispositivos inteligentes, Hik-Connect. Esta nueva e innovadora combinación ofrece capacidades de alarma y vídeo muy fiables, junto al control remoto completo y monitorización con IVaaS (Intruder Verification as a Service) para la videoverificación de eventos.

Una sinergia de las tecnologías de intrusión y vigilancia permite a los usuarios finales armar, desarmar, ver, grabar e interactuar con su sistema de seguridad como nunca antes a través de una única plataforma. De esta forma, ayuda a los profesionales a centrarse en nuevas aplicaciones para crecer y maximizar todo su potencial comercial.

«Nos complace enormemente ofrecer la próxima generación de soluciones de intrusión en una plataforma totalmente integrada, que fusiona la innovación de un líder mundial como Hikvision con la contrastada experiencia de un especialista en intrusión», señala Jiang Feng Zhi, director de la División de Alarmas de Hikvision.

«Una gran ventaja de la nueva generación de paneles de alarma de Hikvision es que proporciona tecnologías de intrusión y vídeo que se han desarrollado y diseñado para funcionar en perfecta armonía, para ofrecer ventajas únicas en el mercado y un rendimiento óptimo.

Al ofrecer una plataforma a través de nuestro software y aplicaciones iVMS y Hik-Connect, estamos maximizando el valor y la efectividad de los sistemas de seguridad tanto para los instaladores como para los usuarios finales, con productos innovadores que integran multitud de funciones», añade Jiang Feng Zhi.

Presentación en España

Hikvision presentó esta nueva generación de paneles de intrusión en un encuentro en el que reunió a todos sus distribuidores tanto de España como de Portugal. El evento, al que acudieron más de 50 representantes de la industria de la seguridad, tuvo lugar en las renovadas instalaciones de Hikvision en Tres Cantos (Madrid) y sirvió además para dar a conocer a los asistentes el nuevo -showroom de la compañía.

Showroom

El showroom de Hikvision está distribuido en cuatro áreas diferenciadas: Dos centradas principalmente en producto (una exclusivamente para CCTV y otra para intrusión, control de accesos y videoporteros) y otras dos dedicadas a la aplicación de los productos (la primera, destinada a los sectores verticales: infraestructuras críticas, banca, retail y movilidad/tráfico y la segunda, a nuevas tecnologías como la robótica, los drones o los escáneres de chasis).

Las cuatro áreas convergen en el videowall que muestra el funcionamiento de HikCentral, el revolucionario sistema de gestión de vídeo de Hikvision.

Iseo Ibérica exhibe sus nuevas instalaciones para mejorar el servicio al cliente

ISEO Ibérica, empresa de referencia en el sector de la cerrajería y la seguridad, ha concitado a sus principales distribuidores en sus Jornadas de Puertas Abiertas para mostrarles sus nuevas dependencias en su sede de Ajalvir (Madrid), pensadas para dar un mejor servicio al cliente, y para presentarles las últimas novedades en su catálogo de productos, incluidas dentro de sus ecosistemas Argo y Vega.

Las nuevas instalaciones de Iseo Ibérica se dividen en tres zonas diferenciadas:

–Sala de formación: donde se realizarán presentaciones y cursos a los distibuidores y colaboradores de las familias de control de accesos y de producto mecánico especializado, como los cilindros de perfiles especiales.

-Showroom: el corazón del nuevo espacio. Una sala donde se exponen los productos, desde el más innovador, como los productos electrónicos, hasta los artículos más tradicionales, como las cerraduras mecánicas o los antipánicos.

–Nueva área departamento Zero1: donde se ubicará el departamento de atención al cliente y postventa de ISEO Zero1, y una sala de reuniones.

Además, durante las Jornadas de Puertas Abiertas se presentaron las últimas prestaciones que Iseo ha lanzado en sus ecosistemas Argo y Vega, y se organizaron talleres de configuración de dispositivos de control de accesos y visitas guiadas a la producción de ensamblaje de cilindros y cerraduras.

Esta iniciativa se enmarca dentro de la línea de desarrollo de la compañía, basada en producir los mejores productos en materia de seguridad, ser pioneros desarrollando nuevas soluciones y todo con una atención cercana y personalizada.

Synology introduce el deep learning en sus paquetes de Surveillance Station

Synology refuerza su apuesta por el mercado de la videovigilancia. El próximo año, la compañía agregará por primera vez en 2019 técnicas de deep learning a sus populares paquetes de Surveillance Station, lanzando la función avanzada de análisis de vídeo Deep Video Analysis (DVA). DS1419dva, el primer producto de hardware equipado con DVA, también hará su debut.

La tecnología VADVA se incorpora para mejorar la precisión del reconocimiento de objetos y centralizar los recursos informáticos y los costes de inversión. Las seis reglas de reconocimiento de imagen en DVA incluyen detección de objetos, detección de movimiento, zona de inactividad, conteo de personas, objetos extraños y objetos perdidos, lo hacen ideal para aplicaciones en la industria minorista, y proporciona una amplia gama de seguridad para los hogares.

Así lo expuso la compañía durante su evento anual Synology 2019 celebrado en Madrid y en el que intervinieron Marcos de Santiago, Head of Product Management France & SE, y Álvaro González, product manager de Synology en España.

Durante el acto, se presentaron productos y aplicaciones completamente nuevos, como la nueva versión DiskStation Manager 7.0 (DSM 7.0), que es más estable e intuitiva; una nueva línea de productos; el controlador unificado Dual- active UC300, que proporciona un servicio ininterrumpido a las empresas; Active Backup Suite con licencia gratuita dirigido al mercado de backup empresarial, y el Mesh Router MR2200ac equipado con Synology Router Manager 1.2 (SRM 1.2), entre otros.

Grupo EULEN: Ignacio Sánchez, nuevo subdirector general de Seguridad

El Grupo EULEN, empresa de referencia en la prestación de servicios generales a empresas y administraciones públicas, ha nombrado recientemente a Ignacio Sánchez Caballero, nuevo subdirector general de Seguridad en España.

Sánchez Caballero es Ingeniero Superior Agrónomo por la Universidad Politécnica de Madrid y PDD por ESADE, y ha ocupado a lo largo de su dilatada carrera profesional diferentes posiciones directivas, como director del Departamento de Supply Chain en TelePizza de 2004 a 2007, director general de COFAS desde 2007 hasta 2012 y director general de Relaciones con la Industria en COFARES, último cargo desempeñado hasta su incorporación al Grupo EULEN.

Desde su nuevo puesto, y reportando directamente al director general de España, Portugal, Qatar y Emiratos Árabes del Grupo EULEN, Sánchez Caballero dirigirá la actividad de EULEN Seguridad de la que será el máximo responsable.

Actualmente, EULEN Seguridad genera un volumen de ventas de alrededor de 240 millones de euros, lo que supone el 20% de la actividad de la Compañía en nuestro país, dando empleo a más de 7.000 profesionales en el sector.

Hikvision obtiene el certificado Common Criteria

Hikvision, el proveedor mundial de referencia de soluciones globales de seguridad, ha anunciado que su serie 5 (DS-2CD5XXX) ha obtenido el Certificado Common Criteria (CC) –un estándar con reconocimiento internacional que evalúa las funciones de seguridad y el nivel de confianza de un producto IT (ISO 15408)– con una garantía de tipo EAL2 ampliada con ALC_FLR.2 (EAL2+). Esta certificación es una muestra más del compromiso de Hikvision con sus clientes de todo el mundo en términos de fiabilidad y ciberseguridad.

Como uno de los estándares internacionales más ampliamente reconocidos en el ámbito de la seguridad de las tecnologías de información (ISO/IEC 15408), el Certificado CC se aplica principalmente a la evaluación de la seguridad y la fiabilidad de productos y soluciones en el ámbito de la tecnología de la información y se centra en la protección de la información privada. Organizaciones y agencias gubernamentales de 28 países –entre otras la National Information Assurance Partnership (NIAP) estadounidense y el Departamento de Defensa de los EE. UU.– han suscrito el Acuerdo de Reconocimiento de Common Criteria (CCRA). Numerosas entidades empresariales utilizan también los CC como requisito a la hora de procurar soluciones y productos tecnológicos de este tipo.

«Con la transformación digital y la llegada de una era conectada e inteligente, el sector de la seguridad afronta oportunidades de desarrollo sin precedentes y, al mismo tiempo, se enfrenta a nuevos desafíos. Hikvision está siempre comprometida con el desarrollo de productos de seguridad de máxima calidad, seguros e innovadores», dijo el Dr. Wang Bin, director del Laboratorio de Redes y Seguridad de la Información y del departamento de Seguridad de Red.

Para obtener el Certificado Common Criteria, Hikvision superó con éxito una rigurosa evaluación realizada por el laboratorio de pruebas de CC de Brightsight, una institución de evaluación de estándares de seguridad de fama internacional.

Más de 200 profesionales asisten a las I Jornadas EPSEB sobre Seguridad en Eventos Musicales y Deportivos en Barcelona

La EPSEB (Universidad Politécnica de Cataluña) fue escenario el pasado 26 de octubre de la 1ª Jornada sobre Seguridad en Eventos Musicales y Deportivos, que reunió en Barcelona a más de 200 asistentes y 25 ponentes de toda España. El acto se organizó en colaboración con el Congreso de Comunicación y Seguridad en Eventos que cada año se celebra en la Universidad Complutense de Madrid y el Observatorio Científico de Eventos.

A lo largo de la jornada, profesionales de la seguridad privada y pública, criminólogos, técnicos y expertos trataron diferentes aspectos relacionados con la seguridad en los eventos. En las diferentes ponencias se insistió continuamente en la necesidad de ser rigurosos con la normativa para garantizar la seguridad de los asistentes y trabajadores, y también de diseñar procedimientos de buenas prácticas en eventos multitudinarios para aplicar allí donde la ley no llega. No faltaron temas tan actuales como los protocolos para la prevención de la violencia sexual en espacios de ocio, el uso de drones, los eventos bajo la sombra del terrorismo o cómo identificar a grupos urbanos violentos. Por varios ponentes también se señaló la urgencia de una regulación específica para los grandes festivales, así como se destacó la necesidad de poder compatibilizar esa imprescindible seguridad con el respeto a la experiencia de ocio que busca el asistente de un evento de estas características, sin el cual, el espectáculo no se llevaría a cabo.

La coordinadora del acto, Anna Almécija, manifestó que «la gran acogida que ha tenido la Jornada, tanto por la seguridad pública como privada, como por los diferentes agentes que trabajan e intervienen en un gran evento musical o deportivo, demuestra la necesidad de poner en común y compartir experiencias y buenas prácticas con el objetivo de conseguir unos eventos cada vez más seguros». La EPSEB ha manifestado su voluntad de dar continuidad a esta Jornada.

Nueva incorporación en Grupo IPTECNO

En la estrategia de crecimiento de Grupo IPTECNO en el área de proyectos con alto valor añadido se ha incorporado a nuestra sede de Madrid, Alejandro Castedo Vaquero, profesional de reconocida reputación y muy amplia experiencia de más de 10 años en el sector de sistemas de seguridad en España y Portugal. Además de su formación superior en sistemas electrónicos, Alejandro aporta amplia experiencia en redes y sistemas informáticos con una sólida metodología que se remonta a sus orígenes en IBM.

Alejandro da soporte técnico-comercial a los proyectos de nuestros clientes garantizando así un buen cumplimiento de las expectativas de funcionamiento del sistema ofertado y un soporte a la puesta en marcha que nos permite acompañar al integrador desde la prescripción a la entrega de la obra y puesta en producción de los sistemas.

«Estamos convencidos que la incorporación de Alejandro Castedo al equipo generará más oportunidades de negocio pero lo más importante es que optimizaremos el nivel de soporte que ofrecemos a nuestros clientes», aseguran desde la compañía.

Iván Rubio, director del Área de Seguridad de Peldaño, recibe la Medalla al Mérito Policial

Iván Rubio, director del Área de Seguridad de Peldaño –grupo de comunicación que edita CUADERNOS DE SEGURIDAD–, recibió el pasado 23 de octubre la Medalla al Mérito Policial con Distintivo Blanco. Con motivo de la festividad de los Ángeles Custodios, patronos del Cuerpo Nacional de Policía (CNP), Rubio fue condecorado en un acto en el que también se impusieron diferentes distinciones al Mérito Policial, entre otros a funcionarios del Cuerpo Nacional de Policía (CNP), Guardia Civil, Fuerzas Armadas y personal ajeno al CNP.

Diplomado en Magisterio por la Universidad Complutense y titulado en Dirección y Gestión de la Seguridad por la UNED, Iván Rubio cuenta con más de 15 años de experiencia en el sector de la seguridad. Actualmente es director del Área de Seguridad de Peldaño, cargo que ocupa desde 2012.

Inició su trayectoria profesional en 2002 como ejecutivo de cuentas de la revista CUADERNOS DE SEGURIDAD hasta su incorporación como publicación de cabecera del sector de Seguridad en Peldaño, en el año 2007. Desde entonces ha promovido la creación de la publicación Instalsec en 2008 (dirigida a instaladores de sistemas de seguridad) y la organización de diferentes eventos sectoriales, entre los que destacan Security Forum (congreso y exposición internacional con sede en Barcelona) desde 2012, y del Congreso de Seguridad Privada en Euskadi desde 2014, posicionando el área de Seguridad de Peldaño como un referente de la Industria de Seguridad.

«Para mí es un orgullo formar parte de este sector que ha enriquecido mi trayectoria profesional y del que sigo aprendiendo. Quiero compartir este reconocimiento con todo el equipo y con los profesionales que me acompañan cada día y me brindan la oportunidad de promover iniciativas que aporten al sector valor, conocimiento y negocio.

Manuel Yanguas, comisario jefe de la Unidad Central de Seguridad Privada del CNP, e Iván Rubio, director del Área de Seguridad de Peldaño.

También expresar mi agradecimiento al Cuerpo Nacional de Policía por la concesión de esta distinción, la cual ratifica mi compromiso con el sector de la Seguridad», señaló Iván Rubio.

Peldaño recibe el Premio Especial ADSI 2018

Asimismo, el pasado 22 de noviembre Peldaño recibió el Premio Especial ADSI 2018 «Por su contribución a la difusión de la cultura de la seguridad», a través de sus publicaciones Cuadernos de Seguridad, Instalsec, y eventos como Security Forum, entre otros.

Durante la celebración de la Cena Anual que cada año ofrece la Asociación de de Directivos de Seguridad Integral (ADSI), Francisco Poley, presidente de la asociación, entregó el premio a Iván Rubio, director del Área de Seguridad de Peldaño.

Detnov amplía sus instalaciones con una nueva fábrica

DETNOV cuenta con una nueva planta ubicada en Viladecans que ha supuesto una inversión superior a los 3 millones de euros, incluida la compra del terreno, construcción de la nave, modernización de la capacidad de producción e implementación de nuevos procesos de calidad. Es «una de las más modernas del sector de la seguridad electrónica nacional», según destacó Raúl García, gerente de Detnov, ya que cuenta con los máximos estándares de calidad y seguridad gracias al conocimiento y experiencia de 10 años de historia en el sector y a los modernos equipos que se utilizan en la cadena de producción.

Las instalaciones, con una superficie de más de 3.000 metros cuadrados, tienen varias líneas de producción de las diferentes gamas de productos de detección de incendios, un centro de I+D con los laboratorios necesarios para pasar todas las certificaciones necesarias del sector, un almacén logístico y las oficinas centrales de los servicios de administración, finanzas y comercial.

Además, cuenta con un showroom para las presentaciones comerciales y una sala de formación técnica para que los clientes puedan recibir la certificación de uso de nuestros productos.

Los factores decisorios para la selección de Viladecans como ubicación han sido la disponibilidad de materias primas, mano de obra, las buenas infraestructuras y comunicaciones de la zona, y la cercanía con la antigua fábrica.

Con estas nuevas instalaciones, Detnov sienta las bases para seguir sus planes de crecimiento. En los últimos cinco años Detnov ha cogido una importante cuota de mercado en el ámbito nacional y ha expandido sus exportaciones a más de 40 países en 4 continentes.

Nuevo acuerdo de distribución entre Casmar y Aiprox

Casmar y Aiprox han firmado un acuerdo de distribución por el que Casmar comienza a comercializar y promocionar los sistemas de drones autónomos para operaciones de seguridad integrada e inteligente Aiprox.

Drones Autónomos

Estos equipos están especialmente concebidos para misiones de seguridad autónomas y la toma de decisiones inteligente en base a los protocolos de seguridad establecidos. Son aparatos blindados contra interferencias y cuentan con hasta diez cámaras convencionales, térmicas y especializadas, además de sensores de gases y con hasta cuatro potentes ordenadores de abordo. Son equipos operativamente autónomos, es decir, aterrizan, se cargan y despegan de forma completamente automática en las pistas diseñadas especialmente para ellos.

Integración de sistemas

Es el elemento más importante en seguridad, y los drones Aiprox son un paso más, aportan niveles de operación nuevos y más eficientes en cada escenario, coordinando cámaras de tierra, radares, alarmas e interactuando con el personal y vehículos a través de localizadores.

Todo ello integrado con la central de operaciones gracias a un sistema de comunicaciones multicliente que envía y recibe información de la central de alarmas, centros de control de flota drone, personal de tierra o fuerzas de seguridad y emergencias, creando operaciones realmente sincronizadas de todos los actores, que reciben en todo momento la información precisa para su actuación.

Software Gyroos

Esta integración con la central de alarma y operaciones se realiza a través del software de flota Gyroos para la gestión de drones de Aiprox. Con él se pueden controlar las misiones, ubicar los elementos de seguridad, realizar control manual del drone y crear el calendario de misiones automatizadas y protocolos cerrando de esa forma todo el círculo del sistema de seguridad

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

ALARMA Y CONTROL

PYRONIX

C/Almazara, 9
28760 Tres Cantos Madrid
Tel. 91 737 16 55
marketing@pyronix.com
www.pyronix.com

Techco Security
C/ Barbadillo 7
28042 Madrid
+34 91 312 77 77
www.techcosecurity.com
tcs@techcosecurity.com

GAROTECNIA
Valdelaguna, 4 local 3
28909 Getafe (Madrid)
Tel.: 916 847 767 - Fax: 916 847 769
garotecnia@garotecnia.com
www.garotecnia.com
Autorizada por la D.G.P. con el nº 2.276

San Fructuoso 50-56 - 08004 **Barcelona**
Tel.: 934 254 960 / Fax: 934 261 904

MADRID: Avda. Somosierra 22, Nave F, Planta 1 Inferior - 28703 S.S de los Reyes • Tel.: 917 544 804
CANARIAS: Ctra. del Norte 113 - 35013 Las Palmas de Gran Canaria • Tel.: 928 426 323
Fax: 928 417 077
PORTUGAL: Rua Fernando Namora 33, 2º-I
4425-651 Maia (Porto) • Tel.: (+351) 932 220 421
bydemes@bydemes.com
www.bydemes.com

FUNDADA EN 1966

INSTALACIONES A SU MEDIDA

Antoñita Jiménez, 25
28019 Madrid
ISO 9001
Tel.: 91 565 54 20 - Fax: 91 565 53 23
seguridad@grupoaguero.com
www.grupoaguero.com

Accesos | CCTV | Incendio | Intrusión

Oficina Central:
Maresme, 71-79 · 08019 Barcelona
Fax 933 518 554
902 202 206 *www.casmar.es*

CONTROL DE ACCESOS ACTIVO

TALLERES DE ESCORIAZA, S. A. U.
Barrio de Ventas, 35
E-20305 Irún • SPAIN
Tel.: +34 943 669 100
Fax: +34 943 633 221
tesalocks@tesa.es • www.tesa.es

GRUPO SPEC
Líderes en Gestión de Horarios y Accesos desde 1978
C/ Caballero, 81
08014 Barcelona
Tel. 93 247 88 00 • Fax 93 247 88 11
spec@grupospec.com
www.grupospec.com

BIOSYS
(Sistemas de Tecnología Aplicada)

C/ Cinca, 102-104
08030 BARCELONA
Tel. 93 476 45 70
Fax. 93 476 45 71
comercial@biosys.es - www.biosys.es

San Fructuoso 50-56 - 08004 **Barcelona**
Tel.: 934 254 960 / Fax: 934 261 904

MADRID: Avda. Somosierra 22, Nave F, Planta 1 Inferior - 28703 S.S de los Reyes • Tel.: 917 544 804
CANARIAS: Ctra. del Norte 113 - 35013 Las Palmas de Gran Canaria • Tel.: 928 426 323
Fax: 928 417 077
PORTUGAL: Rua Fernando Namora 33, 2º-I
4425-651 Maia (Porto) • Tel.: (+351) 932 220 421
bydemes@bydemes.com
www.bydemes.com

Avda. Roma, 97
08029 BARCELONA
Tel.: 93 439 92 44 • Fax: 93 419 76 73

Delegación Zona Centro:
Sebastián Elcano, 32
28012 Madrid
Tel.: 902 92 93 84

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

SUPPORT SECURITY
Polígono Industrial de Guarnizo - Parcela 48-C Naves "La Canaluca" 2 y 4
39611 GUARNIZO-CANTABRIA. ESPAÑA
Tel.: 942 54 43 54
support@setelsa.net
www.support-seguridad.es

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

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

C/ Ochandiano, 14
(Centro Empresarial El Plantío)
28023 Madrid
Tel.: 91 121 71 50
Fax: 91 171 71 70
Email: pro@proselec.com

www.proselec.com

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/ de la Ciència nº30-32
08840 Viladecans (Barcelona)

Delegación Centro:
C/ La Granja nº30 Bajo
28108 Alcobendas (Madrid)

Tel: +34 93 371 60 25
www.detnov.com
info@detnov.com

San Fructuoso 50-56 - 08004 **Barcelona**
Tel.: 934 254 960 / Fax: 934 261 904

MADRID: Avda. Somosierra 22, Nave F, Planta 1 Inferior - 28703 S.S de los Reyes • Tel.: 917 544 804
CANARIAS: Ctra. del Norte 113 - 35013 Las Palmas de Gran Canaria • Tel.: 928 426 323
Fax: 928 417 077
PORTUGAL: Rua Fernando Namora 33, 2º-I 4425-651 Maia (Porto) • Tel.: (+351) 932 220 421
bydemes@bydemes.com
www.bydemes.com

GRUPO AGUILERA

FABRICANTES DE SOLUCIONES PCI DETECCIÓN Y EXTINCIÓN DE INCENDIOS

SEDE CENTRAL
C/ Julián Camarillo, 26 28037 MADRID
Tel. 91 754 55 11 • Fax: 91 754 50 98
www.aguilera.es

Delegaciones en:
Galicia: Tel. 98 114 02 42 • Fax: 98 114 24 62
Cataluña: Tel. 93 381 08 04 • Fax: 93 381 07 58
Levante: Tel. 96 119 96 06 • Fax: 96 119 96 01
Andalucía:Tel. 95 465 65 88 • Fax: 95 465 71 71
Canarias: Tel. 928 24 45 80 • Fax: 928 24 65 72

Factoría de tratamiento de gases
Av. Alfonso Peña Boeuf, 6. P. I. Fin de Semana
28022 MADRID
Tel. 91 312 16 56 • Fax: 91 329 58 20

Soluciones y sistemas:
** DETECCIÓN **
Algorítmica • Analógica • Aspiración • Convencional • Monóxido • Oxyreduct® • Autónomos • Detección Lineal
** EXTINCIÓN **
Agua nebulizada • IG-55 • NOVECTM • SAFEGUARD • Hfc-227ea • Co_2

PEFIPRESA, S. A. U

INSTALACIÓN Y MANTENIMIENTO DE SISTEMAS DE SEGURIDAD Y CONTRA INCENDIOS

www.pefipresa.com

Oficinas en: A Coruña, Algeciras, Barcelona, Bilbao, Madrid, Murcia, Santa Cruz de Tenerife, Sevilla, Valencia y Lisboa.

Atención al cliente: 902 362 921
info.madrid@pefipresa.com

PROTECCIÓN CONTRA INCENDIOS. PASIVA

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

San Fructuoso 50-56 - 08004 **Barcelona**
Tel.: 934 254 960 / Fax: 934 261 904

MADRID: Avda. Somosierra 22, Nave F, Planta 1 Inferior - 28703 S.S de los Reyes • Tel.: 917 544 804
CANARIAS: Ctra. del Norte 113 - 35013 Las Palmas de Gran Canaria • Tel.: 928 426 323
Fax: 928 417 077
PORTUGAL: Rua Fernando Namora 33, 2º-I 4425-651 Maia (Porto) • Tel.: (+351) 932 220 421
bydemes@bydemes.com
www.bydemes.com

RISCO Group Iberia
San Rafael, 1
28108 Alcobendas (Madrid)
Tel.: +34 914 902 133
Fax: +34 914 902 134
sales-es@riscogroup.com
www.riscogroup.es

PROTECCIÓN CONTRA ROBO Y ATRACO. PASIVA

TELECOMUNICACIONES

La solución de seguridad M2M definitiva para las comunicaciones de su CRA

Condesa de Venadito 1, planta 11
28027 Madrid
T. 902.095.196 • F. 902.095.196

comercial@alai.es • www.alaisecure.com

SOLUCIONES INTEGRALES DE TELECOMUNICACIONES Y SEGURIDAD

C/ Diputación 118, Bjos.
08015 Barcelona
expocom@expocomsa.es
www.expocomsa.es
Tel. : **93 451 23 77**

VIGILANCIA POR TELEVISIÓN

HIKVISION SPAIN

C/ Almazara 9
28760- Tres Cantos (Madrid)
Tel. 917 371 655
info.es@hikvision.com
www.hikvision.com

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

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

Avda. Roma, 97
08029 BARCELONA
Tel.: 93 439 92 44 • Fax: 93 419 76 73

Delegación Zona Centro:
Sebastián Elcano, 32
28012 Madrid
Tel.: 902 92 93 84

AXIS COMMUNICATIONS
Vía de los Poblados 3, Edificio 3,
Planta 1 – 28033 Madrid
Tel.: +34 918 034 643
Fax: +34 918 035 452
www.axis.com

C/ Viladomat 174
08015 Barcelona
Tel.: 93 454 48 11
Fax: 93 453 62 10
acaes@acaes.net
www.acaes.net

GRUPO IPTECNO
Tel. 902 502 035 - Fax 902 502 036
iptecno@iptecno.com - www.iptecno.com
SEDE BARCELONA
IPTECNO Videovigilancia S.L.
C/ del Besos, 12 - P.I. Can Buscarons de Balx
08170 Montornès del Vallès
SEDE MADRID
IPTECNO Seguridad S.L.
Avda. Tenerife, 2 - Blq. 2, Pta. 3
28703 S. S. de los Reyes

San Fructuoso 50-56 - 08004 **Barcelona**
Tel.: 934 254 960 / Fax: 934 261 904

MADRID: Avda. Somosierra 22, Nave F, Planta 1 Inferior - 28703 S.S de los Reyes • Tel.: 917 544 804
CANARIAS: Ctra. del Norte 113 - 35013 Las Palmas de Gran Canaria • Tel.: 928 426 323
Fax: 928 417 077
PORTUGAL: Rua Fernando Namora 33, 2º-I
4425-651 Maia (Porto) • Tel.: (+351) 932 220 421
bydemes@bydemes.com
www.bydemes.com

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

DAHUA IBERIA, S.L.

C/ Juan Esplandiú 15 1-B. 28007
Madrid

Tel: +34 917649862
sales.iberia@global.dahuatech.com
www.dahuasecurity.com

DALLMEIER ELECTRONIC ESPAÑA
C/ Princesa 25 – 6.1 (Edificio Hexágono)
Tel.: 91 590 22 87
Fax: 91 590 23 25
28008 • Madrid

dallmeierspain@dallmeier.com
www.dallmeier.com

F.F. VIDEOSISTEMAS & GEUTEBRÜCK
Calle Vizcaya, 2
28231 Las Rozas (Madrid)
Tel.: 91 710 48 04
ffvideo@ffvideosistemas.com
www.ffvideosistemas.com

ASOCIACION ESPAÑOLA
DE DIRECTORES DE SEGURIDAD (AEDS)
Rey Francisco, 4 - 28008 Madrid
Tel.: 916 611 477 - Fax: 916 624 285
aeds@directorseguridad.org
www.directorseguridad.org

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

ASOCIACIONES

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

Expertos en VIDEOVIGILANCIA

LSB, S.L.
C./ Enero, 11 28022 Madrid
Tf: +34 913294835
info@lsb.es

BOSCH SECURITY SYSTEMS SAU
C/ Hermanos García Noblejas, 19
Edificio Robert Bosch
28037 Madrid • Tel.: 902 121 497
Delegación Este:
Plaça Francesc Macià, 14-19
08902 L'Hospitalet de Llobregat (Barcelona)
Tel.: 93 508 26 52 • Fax: 93 508 26 21
Delegación Norte: Tel.: 676 600 612
es.securitysystems@bosch.com
www.boschsecurity.es

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

C/ Albarracín, 58, Local 10, Planta 1ª
28037 Madrid
Tel 91 055 97 50

www.aecra.org

ASOCIACION ESPAÑOLA
DE EMPRESAS DE SEGURIDAD
Alcalá, 99
28009 Madrid
Tel.: 915 765 225
Fax: 915 766 094

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

ASOCIACIÓN PROFESIONAL DE COMPAÑÍAS PRIVADAS DE SERVICIOS DE SEGURIDAD
C/Princesa, 43 - 2ºIzq
28008 Madrid
Tel.: 914 540 000 - Fax: 915 411 090
www.aproser.org

ADISPO
Asociación de Directores de Seguridad ADISPO
Av. de la Peseta, 91 -3ºB- 28054 Madrid
Tf: 657 612 694
adispo@adispo.es
www.adispo.es

ASIS-ESPAÑA
C/ Velázquez 53, 2º Izquierda
28001 Madrid
Tel.: 911 310 619
Fax: 915 777 190

ASOCIACIÓN DE INVESTIGACIÓN PARA LA SEGURIDAD DE VIDAS Y BIENES CENTRO NACIONAL DE PREVENCIÓN DE DAÑOS Y PÉRDIDAS
Av. del General Perón, 27
28020 Madrid
Tel.: 914 457 566 - Fax: 914 457 136

FEDERACIÓN ESPAÑOLA DE SEGURIDAD
Embajadores, 81
28012 Madrid
Tel.: 915 542 115 - Fax: 915 538 929
fes@fes.es
C/C: comunicacion@fes.es

ASOCIACIÓN DE JEFES DE SEGURIDAD DE ESPAÑA

Avd. Merididana 358. 4ºA.
08027 Barcelona
Tel. 93-3459682 Fax. 93-3453395
www.ajse.es presidente@ajse.es

ASOCIACIÓN VASCA DE PROFESIONALES DE SEGURIDAD
Parque tecnológico de Bizkaia
Ibaizabal Kalea, 101
sae@sae-avps.com
www.sae-avps.com

CENTRALES DE RECEPCIÓN Y CONTROL

ALARMAS SPITZ S. A.
Gran Vía, 493 - 08015 Barcelona
Tel.: 934 517 500 - Fax: 934 511 443
Central Receptora de alarmas
Tel.: 902 117 100 - Fax: 934 536 946
www.alarmasspitz.com

INSTALACIÓN Y MANTENIMIENTO

Techco Security
C/ Barbadillo 7
28042 Madrid
+34 91 312 77 77
www.techcosecurity.com
tcs@techcosecurity.com

FUNDADA EN 1966
INSTALACIONES A SU MEDIDA
ISO 9001
Antoñita Jiménez, 25
28019 Madrid
Tel.: 91 565 54 20 - Fax: 91 565 53 23
seguridad@grupoaguero.com
www.grupoaguero.com

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

¿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 2018

TRANSPORTE Y GESTIÓN DE EFECTIVO

LOOMIS SPAIN S. A.
C/ Ahumaos, 35-37
Polígono Industrial La Dehesa de Vicálvaro
28052 Madrid
Tlf: 917438900
Fax: 914 685 241
www.loomis.com

Peldaño te desea feliz Navidad
y un próspero 2019

DEEP LEARNING

En una era de continua expansión tecnológica, el crecimiento de la industria de vigilancia solo puede basarse en el Deep Learning: un concepto que engloba el propio aprendizaje de los sistemas, de forma muy similar al que emplea la mente humana para procesar la información.

Los equipos desarrollados en base al Deep Learning, como las cámaras DeepinView y los NVRs DeepinMind de Hikvision lideran el futuro de la tecnología de videovigilancia en todos los sectores: retail, tráfico, edificios y ciudades inteligentes, aeropuertos y estaciones, vigilancia urbana, infraestructuras críticas, etc.

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