SEGURITECNIA

REVISTA DECANA INDEPENDIENTE DE SEGURIDAD

Nº 483 - FEBRERO 2021

ENCUENTRO: LA NUBE COMO NUEVO MODELO DE NEGOCIO EN VIDEOVIGILANCIA

SEGURIDAD PORTUARIA

Las fuerzas que se asocian para el bien no se suman, se multiplican (Concepción Arenal)

www.fundacionborreda.org

Patrocinadores: Editorial BORRMART, S.A. · BOSCH SEGURIDAD Y CONTROL · GLOBAL TECHNOLOGY · SAIMA SEGURIDAD, S.A. · SEGURLEX

Colaboradores: ASIS · continuam · PROTECTURI

SEGURITECNIA

Fundada en 1980 por D. RAMÓN BORREDÁ GARCÍA

SUSCRIPCIÓN ANUAL (suscripciones@borrmart.es)
España . . . . . 70 €
Europa . . . . . 130 €
Resto del mundo . . . . . 160 €
I.V.A. no incluido

REDACCIÓN, ADMINISTRACIÓN Y PUBLICIDAD
C\ Don Ramón de la Cruz, 68.
28001 MADRID. ESPAÑA
Tel.: + 34 91 402 96 07
Dirección en Internet: www.seguritecnia.com
E-mail: seguritecnia@borrmart.es
Depósito legal: M - 4204-2012
ISSN: 0210-8747
ISSN versión electrónica: 2530-8459
Impresión: COMECO INTEGRA, S.L.U.

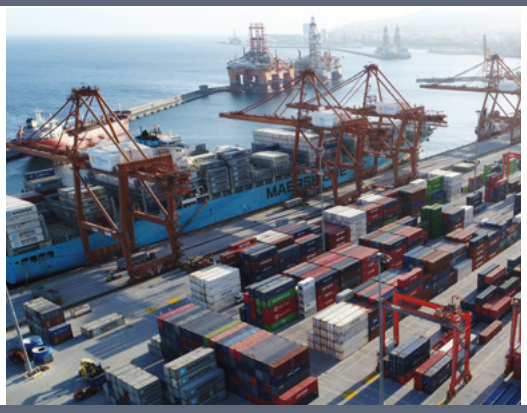
Edita: BORRMART, S.A.
C\ Don Ramón de la Cruz, 68.
28001 MADRID. ESPAÑA
Tel.: + 34 91 402 96 07. (Centralita)
Dirección en Internet: www.borrmart.es
E-mail: seguritecnia@borrmart.es

sumario

12

18

26



78

7
EDITORIAL
Esenciales de veras

12
DESAYUNO DE TRABAJO
El futuro de la videovigilancia 'cloud' pasa por despejar algunos nubarrones

18
EMPRESAS Y EMPRESARIOS
Montse Castro
CEO de Casmar

26
ESPECIAL SEGURIDAD PORTUARIA
Entrevista a Víctor A. Gil
Jefe de Seguridad Corporativa de la Autoridad Portuaria de Santa Cruz de Tenerife

30
ESPECIAL SEGURIDAD PORTUARIA
Sostenibilidad, digitalización y transparencia, ejes de innovación en seguridad del Port de Tarragona
Por José Luis Díez y Jesús A. Teva

40
ESPECIAL SEGURIDAD PORTUARIA
Entrevista a Víctor C. Rubio
Jefe de la División de Protección Portuaria del Puerto de Huelva

54
ESPECIAL SEGURIDAD PORTUARIA
Entrevista a Joan Bergadá
Director de Seguridad Corporativa de Global Technology

78
FUNDACIÓN BORREDÁ
"El *Zoom* de la Fund. Borredá"
El transporte de seguridad en España: parte cosustancial de la seguridad privadaidad privada

80
ACTUALIDAD
La Seguridad Privada clama por incluir a sus profesionales en la segunda fase de vacunación

MAGNUM®

Suceder a la excepcional Elite 900 no ha sido fácil. La nueva colección **ELITE WATERPROOF** lo ha conseguido con su diseño elegante, pero eficiente, añadiendo estilo a la deportividad y por sus excelentes prestaciones.

EN ISO 20347 : 2012 O3 FO HRO SRC

EU
FABRICADO EN EUROPA

DRI-TEC WATERPROOF
POWERED BY MICHELIN TECHNICAL SOLE
MICHELIN

Hi-Tec Sports España, S.A. · T. 965 681 423 · E. magnum@hi-tec.es · www.magnumboots.com

Hanwha Techwin

WISENET

Capte la perspectiva completa

Descubra hasta el mínimo detalle

La TNB-9000 cubre grandes áreas con suficiente densidad de píxeles, para permitir a los operadores ampliar digitalmente la imagen e investigar todos los detalles. Todo ello sin dejar de grabar la imagen completa.

www.hanwha-security.eu

8K
INDUSTRY FIRST

"Ser lo que soy, no es nada sin la Seguridad" (Shakespeare)

Esenciales de veras

Los servicios de seguridad privada han sido considerados esenciales para luchar contra la pandemia, y como tal debería tratárseles para la vacunación

El Ministerio de Sanidad ha anunciado en febrero el inicio de la segunda fase de vacunación contra el Covid-19, en el que están incluidos los miembros de las Fuerzas y Cuerpos de Seguridad, equipos de emergencia y Fuerzas Armadas. Sin embargo, la relación de órganos cuyos profesionales recibirán el compuesto en las próximas fechas excluye al personal de seguridad privada. Una circunstancia que ha importunado al sector, como demuestran los comunicados emitidos por varias asociaciones y agrupaciones sindicales solicitando que se incorpore también a los trabajadores de la seguridad privada en esta fase de vacunación.

La reivindicación viene motivada por un argumento que la autoridad sanitaria debería tener en cuenta. Muchos profesionales de la seguridad prestan servicio actualmente en instalaciones de elevado riesgo de contagio, como podrían ser hospitales o redes de transporte. Es decir, son personal muy expuesto a infectarse por motivo de su función, al igual que lo pueden ser los profesionales incluidos en la segunda fase de la estrategia de vacunación. Por tanto, no se trata de reclamar la vacunación de todo el sector, pero sí al menos del personal que trabaja en entornos con alta probabilidad de contagiarse como pueden ser los vigilantes de seguridad. No olvidemos que los servicios de seguridad privada han sido considerados esenciales para luchar contra la pandemia y, como tal, debería tratárseles en este caso. La cualidad de esencial para la sociedad no puede ser un calificativo de ida y vuelta vacío de contenido, ha de considerarse una función a valorar y para la que hace falta especial protección.

No cabe duda de que la pandemia del Covid-19 ha demostrado la importancia de la seguridad privada no solo como una actividad económica, sino también como un servicio a la sociedad. De ahí la conveniencia de aprovechar todo su potencial en cualquier ámbito en el que pueda aportar sus recursos. En ese sentido, desde diferentes organizaciones también se está planteando la posibilidad de que los transportes de seguridad se hagan cargo del traslado de las vacunas, siempre bajo el seguimiento estricto de las medidas de conservación que exijan las autoridades sanitarias. Ejemplo de ello es la Fundación Borredá, que ha transmitido a la Administración dicha posibilidad. De esa manera, los transportes de fondos contribuirían a agilizar la distribución del compuesto y favorecer toda la cadena de suministro.

En definitiva, la seguridad privada merece que el reconocimiento como servicio esencial durante las primeras fases de la pandemia tenga eco a la hora de establecer los grupos de vacunación. Porque muchos de sus profesionales se enfrentan a una exposición similar a otros miembros del sistema de seguridad y emergencias en España. Porque este personal todavía contribuye con su labor a superar uno de los peores episodios de nuestra sociedad que se recuerdan.

ACAES ELIGE A MONTSE CASTRO COMO NUEVA PRESIDENTA

La Asociación Catalana de Empresas de Seguridad (ACAES) ha nombrado a Montse Castro Roca como nueva presidenta. Tras el inesperado fallecimiento de su padre y anterior presidente, Gonzalo Castro Mata, su hija toma el relevo al frente de la asociación por decisión de los asociados.

Montse Castro es la CEO de Casmar. Antes de asumir la máxima responsabilidad de la empresa, ejerció durante seis años como jefa del Área Internacional y de Recursos Humanos. En esa etapa lideró la apertura de filiales de la compañía en Chile y Colombia.

HIKVISION E HIPER SUMINISTROS ACUERDAN COMERCIALIZAR LOS PRODUCTOS HIWATCH SERIES

Hikvision ha alcanzado un acuerdo de distribución con Hiper Suministros, empresa que se ha fusionado con la marca comercial ECV video seguridad, para comercializar los productos HiWatch Series.

Gracias a esta alianza, Hikvision sigue reforzando su propuesta como *total solution provider*, ofreciendo un amplio abanico de soluciones convergentes de seguridad en CCTV, Intercom, control de accesos e intrusión.

LA FUNDACIÓN BORREDÁ CELEBRARÁ LA V CONFERENCIA SECTORIAL DE SEGURIDAD EN PUERTOS EL 2 DE MARZO

La Fundación Borredá llevará a cabo, el 2 de marzo con la colaboración de la revista Seguritecnia y de Puertos del Estado, la V Conferencia Sectorial de Seguridad en Puertos. Este evento bianual abordará numerosas cuestiones de interés encaminadas a mejorar la protección en el ámbito portuario de la mano de varios expertos en la materia.

Algunos de los temas que tratará la jornada serán la situación actual de la seguridad en el ámbito portuario, el sistema nacional de inspecciones de protección o la nueva regulación en seguridad de las redes y sistemas de información, entre otros elementos. Además, se darán a conocer diversas soluciones tecnológicas implantadas en puertos, así como experiencias compartidas en el ámbito de la seguridad.

LA SEGURIDAD PRIVADA, EN CONTRA DE LIMITAR A 1.000 EUROS LOS PAGOS EN EFECTIVO

Varias agrupaciones de seguridad privada han mostrado su rechazo a las medidas del proyecto de Ley de Medidas Contra el Fraude encaminadas a limitar las cantidades de los pagos en efectivo. FES-UGT, FTSP-USO, Aproser y Asecops han emitido un comunicado en el que consideran "un ataque" la propuesta de no poder pagar en metálico bienes o servicios por encima de 1.000 euros.

Si bien estas organizaciones muestran su respaldo al espíritu de la ley para contribuir a la erradicación de la economía sumergida, consideran que "no hay ningún fundamento" para querer reducir los límites del pago del efectivo. "La experiencia de los países de nuestro entorno no demuestra que exista una vinculación directa entre los porcentajes de utilización del efectivo y los niveles de economía sumergida", sostienen.

En todo caso, las cuatro entidades solicitan que la reducción de los límites para los pagos en efectivo sea más gradual en el tiempo y se haga de manera coordinada con la Unión Europea.

EL SECTOR DE LA PCI NO ESPERA UNA RECUPERACIÓN TOTAL DE SU ACTIVIDAD EN 2021

El sector de la protección contra incendios (PCI) vive momentos complicados. La actividad de este mercado se redujo a la mitad durante el estado de alarma, llegando incluso a descender un 90 por ciento durante el periodo de parón de la economía. Es decir, los proyectos, instalación, mantenimiento, comercialización de soluciones, etcétera, quedaron en límites nunca antes vistos. Son datos ofrecidos por la asociación Tecnifuego, que acaba de hacer balance del impacto económico del COVID-19 en este sector.

La asociación espera un efecto rebote para este año, si bien no cree que la recuperación llegue al cien por cien respecto a etapas anteriores. Tecnifuego prevé que, "como máximo", la actividad aumente un 80 por ciento. "Actualmente hay una gran incertidumbre sobre el futuro próximo, el 56 por ciento de las empresas de la industria en general tienen previsto prescindir de personal en el otoño", afirma la entidad.

GRUPO AEROPORTUARIO DEL PACÍFICO Y 'SEGURILATAM' ORGANIZAN EL X SIMPOSIUM DE SEGURIDAD GAP

Del 22 al 24 de marzo, el Grupo Aeroportuario del Pacífico (GAP) y nuestra revista hermana *Segurilatam* organizarán el X Simposium de Seguridad GAP. Durante tres días, el evento virtual se convertirá en punto de encuentro para los profesionales de la seguridad de la aviación civil y del sector del transporte, quienes podrán seguir las intervenciones de destacados expertos.

A falta de concretar y hacer pública la agenda del simposio, se prevé la presencia de cualificados ponentes de los ámbitos público y privado. Conferencistas que abordarán temas de sumo interés: desde los sistemas de gestión de seguridad hasta los procesos de medición de calidad, pasando por la afectación de la COVID-19 a la aviación civil y el transporte o las medidas de seguridad asociadas a la protección de las infraestructuras críticas.

JAIME DURBÁN LIDERARÁ LA ESTRATEGIA PARA INFRAESTRUCTURAS CRÍTICAS EN EMEA DE MILESTONE

Milestone Systems ha nombrado a Jaime Durbán nuevo *Vertical Specialist* para la región de EMEA. Concretamente, la compañía ha elegido a este profesional para hacerse cargo de la estrategia dirigida a las infraestructuras críticas, un sector clave para la empresa.Entre otras tareas, Durbán se centrará en definir el potencial de las soluciones de vídeo en éste ámbito, analizar las necesidades de los usuarios finales y abordar las soluciones para dichos requerimientos.

MÁLAGA, SEDE DEL CENTRO DE EXCELENCIA PARA LA CIBERSEGURIDAD DE GOOGLE

Google ha anunciado la inversión de más de 650 millones de dólares durante cinco años para acelerar la transición digital de España. Y la seguridad lógica será uno de los pilares de este proyecto. En concreto, el gigante tecnológico ha elegido Málaga para albergar su nuevo Centro de Excelencia para la Ciberseguridad. Estas instalaciones, ubicadas en el Paseo de la Farola, tendrán un espacio de 2.500 metros cuadrados. En ellas se impartirán formación, charlas, talleres y mentorías sobre ciberseguridad. Y también se llevarán a cabo investigaciones y desarrollos de producto.

SÚMATE A NUESTRO
NUEVO ECOSISTEMA DIGITAL

SEGURITECNIA

El futuro de la videovigilancia 'cloud' **pasa por despejar algunos nubarrones**

Con el nombre "La nube como nuevo modelo de negocio para la videovigilancia", la revista Seguritecnia, en colaboración con Panoptico, celebró un desayuno de trabajo virtual donde varios profesionales analizaron las oportunidades y retos de la tecnología cloud. Aspectos como la ausencia de una normativa específica, la protección de los datos o las opciones de revertir el modelo preocupan; pero la nube es un entorno al que se encamina irreversiblemente la videovigilancia.

Por David Marchal

La consultora MarketsandMarkets publicó el año pasado un informe según el cual la facturación de la videovigilancia crecerá a un ritmo anual del 10,4 por ciento, hasta situarse en los 74.600 millones de dólares en 2025 en todo el mundo. Esta cifra viene motivada por la una mayor preocupación ciudadana en la seguridad, así como por una mayor adopción de cámaras IP e inalámbricas, con avances en tecnologías de inteligencia artificial y de aprendizaje automático. Además, el estudio revelaba la importancia creciente que va a tener el *cloud* en este mercado.

Por ese auge de la nube como entorno de alojamiento de las soluciones de videovigilancia, la revista *Seguritecnia* organizó, con la colaboración de la compañía **Panoptico**, un desayuno de trabajo virtual en el que poder analizar las posibilidades de generar nuevos modelos de negocio basados en dicha tecnología. Participaron en el encuentro: **Miguel Ángel Gallego**, gerente del Área Operativa de Seguridad en Renfe; **Juan Carlos Robledo**, director del Área Organización Operativa de Caja Rural Salamanca; **Carlos Vázquez**, director de Seguridad de Unicredit; **José María Saiz**, director de Operaciones Grupo On Seguridad; **Jordi Alonso**, director de la División de Vídeo y Accesos de Casmar; **Julio Pérez**, director de Operaciones en Eulen Seguridad; **Jesús Docasal**, director nacional de las CRA de INV Protección; y **Pedro Navajas**, CEO de Panoptico y fundador de NoSoloSoftware.

Antes de entrar en materia, los invitados pusieron contexto y establecieron las diferencias entre el concepto de virtualización y *cloud*. Al respecto, Gallego, de Renfe, afirmó: "la virtualización es un entorno simulado de la versión física que se puede replicar en hardware y otros sistemas operativos con el objetivo de ahorrar costes y mantenimiento. En cambio, el *cloud* es un servicio a través del cual podemos almacenar, gestionar, automatizar, organizar *software*…". Una definición que Navajas, de NoSoloSoftware-Panóptico, matizó al sostener que "ambos conceptos suelen ir de la mano, aunque sean cosas distintas".

Se trata, en cualquier caso, de tecnologías que van a experimentar una gran evolución en los próximos años en el ámbito de la videovigilancia. No en vano, tal como consideraron los asistentes al desayuno virtual, la nube ofrece un buen número de oportunidades. Para Robledo,

Miguel Ángel Gallego
Gerente del Área Operativa de Seguridad en Renfe

"La tecnología avanza cada día y cuando salga una normativa sobre seguridad, CRA y centros de control en la nube va a estar desfasada de salida"

Pedro Navajas
CEO de NoSoloSoftware-Panoptico

"El modelo 'cloud' ya viene con seguridad intrínseca, si bien el hecho de que haya más o menos seguridad dependerá de cómo se haga el despliegue"

Juan Carlos Robledo
Director del Área Organización Operativa de Caja Rural Salamanca

"La 'cloud' va a ser una de las opciones con mayor prospección de futuro para la videovigilancia, porque mejora el modelo de gestión y contratación"

de Caja Rural Salamanca, "va a ser una de las opciones con mayor prospección de futuro para la videovigilancia, porque mejora el modelo de gestión y contratación". A lo cual añadió: "con ella eliminamos la administración propia en las organizaciones y la cambiamos por servicios externalizados de gestión de seguridad y videovigilancia". Este profesional hizo también hincapié en la importancia que ha supuesto en este sentido la publicación de la normativa de la EBA (European Banking Autority) de la Unión Europea, "que pone las reglas del juego para que estos servicios estén regulados". "Ahora tenemos derecho a conocer dónde están almacenados los datos", agregó.

A esto, Navajas, de Panoptico, le sumó también otros beneficios como "la flexibilidad, la escalabilidad y la rapidez de los servicios". Y Alonso, de Casmar, recalcó como otra de las ventajas de los sistemas de videovigilancia en la nube la facilidad para "generar y visualizar analíticas".

Falta de normativa

A pesar de los beneficios mencionados, la sensación general de los participantes es que el sector aún no está seguro de dar el paso a la nube. "Pensábamos que estábamos preparados para la nube, pero con la pandemia nos hemos dado cuenta de que no. Además, nos da miedo la regulación. Es muy bonito dar este servicio, pero la seguridad privada está regulada y hay que tener claro qué se puede hacer y qué no", opinó Saiz, de Grupo On Seguridad.

La normativa es uno de los temas que más discrepancias suscita. Para Pérez, de Eulen Seguridad, "la regulación de los centros de videovigilancia se encuentra actualmente muy limitada a los condicionamientos de la seguridad física. Esto choca con la virtualización y la nube, que van en la línea contraria, pues fomentan la deslocalización física de la prestación de los servicios desde centros que no están limitados físicamente", comentó. Tal como observó este profesional, tecnológicamente "ha pasado un siglo" desde que se aprobó la legislación, a pesar de que se hayan ido implementando otras normas relacionadas con la seguridad de la información y de las comunicaciones. "En tanto en cuanto no se acoten los posibles condicionamientos de los servicios que se pueden prestar desde un centro de videovigilancia que se apoya en la nube, hay cuestiones que se quedan en el alero", concluyó.

En esa línea, Alonso, de Casmar, sentenció: "vengo del mundo del vídeo desde hace muchos años, y veo que, aunque la normativa ha de existir, frena el desarrollo de la tecnología. En el caso de la videovigilancia, esto es lo que está pasando". A lo cual añadió: "hay sistemas de videovigilancia que se están moviendo al *cloud*, aunque puede que no al nivel que nos gustaría, sobre todo los que no están conectados a las centrales receptoras de alarmas (CRA)". En este punto, Alonso remarcó la necesidad de adaptar la legislación a esta nueva realidad.

A juicio de Gallego, de Renfe, el problema se produce por una descompensación importante entre la normativa y la realidad que se vive en este momento. "La tecnología avanza cada día y cuando salga una normativa o reglamento relacionado con seguridad, CRA o centros de control de videovigilancia, va a estar desfasada de salida", observó.

Jordi Alonso
Director de la División de Vídeo y Accesos de Casmar

"Hay que estudiar cada caso y cliente para decidir la mejor solución. Lo bueno es tener la posibilidad de contar con distintas opciones a nuestro alcance"

José María Saiz
Director de Operaciones Grupo On Seguridad

"La nube será en una opción más en el sector de la videovigilancia que se comerá una parte importante del mercado"

Julio Pérez
Director de Operaciones en Eulen Seguridad

"Toda la flexibilidad económica y técnica que te proporciona la nube a la ida se vuelve en contra cuando intentas regresar"

En este punto del encuentro, Pérez añadió otras cuestiones relativas a la videovigilancia en la nube que preocupan a las empresas, como por ejemplo la regulación y normativa referente a la protección de datos de carácter personal. "Desde el punto de vista de la seguridad, la videovigilancia tiene un interés público que legitima la utilización de los datos de carácter personal que proporcionan las imágenes; es importante tenerlo en cuenta porque es un condicionante más que tenemos", apuntó el representante de Eulen Seguridad.

¿Quién lidera?

Vázquez, de Unicredit, remarcó la necesidad de que el debate sobre la legislación esté participado y liderado por la Administración con una premisa clara, que "no se puede legislar con ojos de hoy, sino previendo todo lo que se nos puede venir encima". "La Administración tiene que ser más flexible y no perder el control de este proyecto, que deberíamos liderar los profesionales de la seguridad, tanto empresas como usuarios", sostuvo. "La nube tiene que ser tan universal que podamos encajar todos, pequeños, grandes y consumidores de paso. Hay gente que no está sujeta a regulación, pero tiene conexión a sistemas de videovigilancia, que es algo a tener en cuenta", añadió el responsable de seguridad de Unicredit.

Docasal, de INV Protección, coincidió con esta observación. "Las empresas de seguridad tienen mucho que decir a la hora de preparar la legislación y no dejar solo al Estado que lo regule", sostuvo. Para este profesional, al fin de al cabo son las empresas de seguridad las que han de aplicar la normativa.

Pérez, de Eulen Seguridad, añadió al respecto que la norma además ha de ofrecer garantías de seguridad. "Seguimos teniendo problemas de vulnerabilidades en los centros de control de videovigilancia. Y si hablamos de infraestructuras críticas, también se debe considerar el hecho de que la información en la nube pueda ser accesible por terceros. Hay que regular, pero alineando tecnología con ciberseguridad", apuntó.

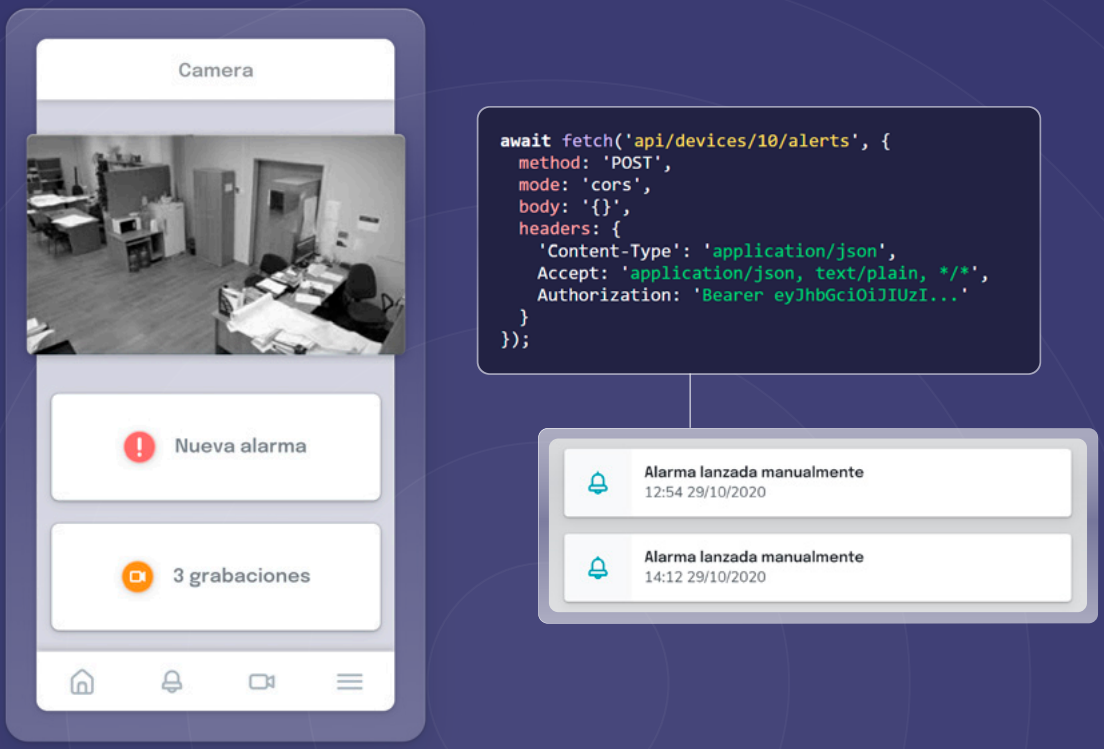
Sobre esto último, Navajas, de Panoptico, aseguró que "el modelo *cloud* ya viene con seguridad intrínseca, si bien el hecho de que haya más o menos seguridad dependerá de cómo se lleve a cabo el despliegue". Docasal, de INV Protección, puso como ejemplo las medidas que adopta su compañía para proteger estos servicios: "tenemos copia de seguridad de la nube del proveedor en nuestro data center y contamos con tres centros de datos enlazados entre sí con fibra óptica que no pasa por Internet. Además, disponemos de un departamento de ciberseguridad propio".

Transmisión de datos

Además de la normativa o la seguridad, los asistentes al desayuno de trabajo pusieron sobre la mesa otra serie de inquietudes respecto a la videovigilancia en la nube. Robledo, de Caja Rural Salamanca, mostró su preocupación por la capacidad de transmisión de datos por los canales existentes. "Las imágenes ocupan ancho de banda, y realizar una copia seguridad implica muchos costes

panoptico

Una infraestructura de software multicloud que conecta con todos los sistemas de intrusión



Sin **necesidad** de dispositivo presencial

Integración y personalización para fabricantes de cámaras CRAs e integradores.

panoptico
NOSOLO SOFTWARE

info@panoptico.video **+34 957 326 715** https://panoptico.video/

Carlos Vázquez Souto
Director de Seguridad de Unicredit

"La Administración tiene que ser más flexible y no perder el control de este proyecto, que deberíamos liderar los profesionales de la seguridad"

y la necesidad de tener capacidad para hacerlo", expresó.

Una preocupación que también trasladó Pérez, de Eulen Seguridad. "El ancho de banda disponible es una cuestión importante. Gran parte de las cámaras que están conectadas a la nube son de uso doméstico y se trata de sistemas inseguros, fácilmente accesibles, a los que cualquiera puede conectarse y visualizar las imágenes", comentó. No resulta extraño, por tanto, como apuntó Alonso, de Casmar, que muchos de estos dispositivos "estén grabando por debajo de sus prestaciones reales" para disminuir el ancho de banda que utilizan para la transmisión de imágenes y su almacenamiento.

Docasal, de INV Protección, llamó la atención sobre la imposibilidad de grabar 24 horas y luego subir las imágenes a la nube, por la gran cantidad de recursos que esto consume. "La manera en la que trabajamos normalmente es con grabadores en local y dejamos las incidencias o las alarmas para las grabaciones en remoto en la nube", explicó.

En este punto, Pérez, de Eulen Seguridad, apuntó que el desarrollo de tecnologías disruptivas contribuirá a solucionar estas cuestiones. "La tecnología 5G va a ser vital en la próxima década para la gestión remota de servicios. El mayor ancho de banda y la menor latencia del 5G revolucionará el actual mercado de seguridad. En las redes 5G proliferarán las cámaras inalámbricas y se conectarán más dispositivos en ubicaciones remotas. De igual manera, la incorporación del audio IP al vídeo IP de manera integrable, sin latencia en comunicaciones de ambos, aportará nuevas posibilidades. Esto facilitará la rápida implementación de aplicaciones de Inteligencia Artificial abiertas para integrar distintos algoritmos que posibiliten la toma de decisiones tanto desde el punto de vista de seguridad como de otras actividades del negocio.

Asimismo, Vázquez, de Unicredit, señaló que "la tecnología viene para ayudar y resolvernos los problemas, por lo que hay que aprovechar lo que ofrece y no intentar aplicarlo a lo que se estaba usando". Gallego, de Renfe, abogó también por utilizar la tecnología existente para otros usos adicionales a los actuales. "Unas cámaras en una estación, aparte de contar las personas que pasan, pueden verificar si ha pasado el billete o no", puso como ejemplo. En definitiva, "hay que unificar la tecnología y hacerla más útil", opinó.

Los proveedores

Otra de las cuestiones en torno a la capacidad tecnológica de procesar las imágenes y resto de información fue la necesidad de almacenamiento. Al respecto, Alonso, de Casmar, recomendó "hacer un *backup* local para tener la seguridad absoluta de que se almacena la información y luego tener una copia en la nube". "Creo que no hay ningún sistema cien por cien perfecto, ni en local ni en *cloud*, por lo que hay que estu-

Jesús Docasal
Director Nacional de las CRA de INV Protección

"La forma en la que trabajamos normalmente es con grabadores en local y dejamos las incidencias o las alarmas para las grabaciones en remoto en la nube"

diar cada caso y cliente para decidir la mejor solución. Lo bueno, de cualquier forma, es tener la posibilidad de contar con distintas opciones a nuestro alcance", observó.

La idea de recurrir a sistemas mixtos también tuvo el respaldo del resto de los presentes. "Lo ideal es gestionar, dimensionar y controlar mi CPD físico o en *cloud* de manera que haya posibilidades en los dos terrenos", consideró Pérez, de Eulen Seguridad, quien también reconoció que en este caso "las inversiones se multiplican".

Por esto último, algunas empresas prefieren recurrir a los grandes proveedores *cloud* como Amazon, Microsoft o Google. A juicio de Navajas, de Panoptico, "si se quiere lanzar un modelo de negocio sin hacer inversión, lo más fácil es recurrir a servicios como Amazon o Google, porque con los ingresos que se tenga se paga la infraestructura. Ahora bien, si quieres migrar el servicio a otro proveedor, ya tienes que hacer una inversión mayor". En otras palabras, resumió, "si no haces inversión, tienes

un modelo de negocio rápido, pero con menos control".

En cualquier caso, el directivo recomendó no apostar al cien por cien por un modelo de este tipo. "Yo no contemplaría el lanzamiento de un servicio únicamente en Amazon o Azure. Es cierto que estos modelos permiten una puesta en marcha rápida, pero el siguiente paso debe ser hacer una nube propia; no solo por cuestión de costes, sino también por la propiedad de los datos", afirmó.

No obstante, los invitados comentaron los inconvenientes y posibilidades de depender tecnológicamente de estos gigantes tecnológicos que pueden imponer sus propias condiciones sin que el usuario tenga muchas opciones.

Externalización

Por motivos como este, Grupo On Seguridad, tiene implantado su sistema de central de alarmas "en local con respaldo en la nube por temas de seguridad".

Vázquez, de Unicredit, abogó por romper con el pasado a la hora de contratar servicios a proveedores. "Hace años estábamos acostumbrados a que teníamos que trabajar con sistemas propietarios, con los cuales había que ir de la mano para ser punteros. Te casabas con una marca y hasta que no se cambiaba la instalación completa te morías con ella; pero eso ahora no pasa. De hecho, si algo hemos aprendido es que hay que ir de la mano del instalador, y que este sea un partner de verdad. Hay que ser serios y trabajar conjuntamente con ellos y con los departamentos de TI, porque corremos el riesgo de quedarnos fuera del juego si no contamos con estos departamentos", manifestó.

"En nuestro caso", comentó Docasal, de INV Protección, "somos una CRA con nube propia. De momento, no nos hemos decidido a irnos a Amazon o Microsoft porque manejamos datos muy delicados, sobre todo de videograbación".

A todo lo anterior se unen las dificultades de revertir el servicio de cloud contratado. Así lo puso de manifiesto Pérez, de Eulen Seguridad: "Toda la flexibilidad económica y técnica que te proporciona la nube cuando migras hacia ella se vuelve en contra cuando intentas regresar. Es decir, lo que te ahorras en el camino de ida lo duplicas a la vuelta", añadió. Una idea que apoyaron otros ponentes, quienes ven dificultades para cambiar de modelo una vez realizada la inversión. Sin embargo, frente a esta solución, Navajas, de Panoptico, planteó como alternativa servicios de pago recurrente que eviten un gasto inicial elevado. De este modo, las compañías que adquirieran este servicio únicamente tendrían que abonar una cuota y beneficiarse de toda la infraestructura del proveedor.

> Los invitados pusieron el foco en la normativa, la protección de datos y la capacidad para revertir el modelo, pero coincidieron en las posibilidades de la videovigilancia en la nube

Opción de futuro

A pesar de todos los escollos que pueda presentar la videovigilancia en la nube, los especialistas coincidieron en señalar que esta tecnología será una alternativa a tener muy en cuenta en los próximos años. "No tengo duda de que va a ser el futuro. A lo mejor tarda más de lo que pensamos en desarrollarse, tanto en una nube privada como virtual; pero lo que está claro es que todos los proveedores van encaminados a la nube", opinó Docasal, de INV Protección.

De igual manera se pronunció Vázquez, de Unicredit, lanzando una serie de recomendaciones: "Debemos tener claro qué proyecto queremos realizar, qué seguridad necesitamos, qué nos aporta el *cloud* sobre la solución tradicional, cómo se compagina y cómo nos afecta la normativa y la calidad del partner elegido para acometer la instalación". Luego se le irán sumando otras tecnologías que complementarán el proceso como la inteligencia artificial, el Internet de las Cosas, el Blockchain…

No obstante, Gallego, de Renfe, puntualizó que "aunque la nube será una solución de futuro", no en todos los casos será la opción necesaria. "Habrá usuarios que decidan optar por la nube para ciertas cosas, pero para otras no, y esto incluye la videovigilancia", comentó. Motivo por el que, desde su punto de vista, el hecho de que existan novedades tecnológicas no significa que haya que abandonar otras soluciones que ahora funcionan. "Hay mercado para todos", sentenció.

En cualquier caso, la nube debe verse, como apuntó Navajas, de Panoptico, "no como un sustitutivo, sino como un añadido a los servicios y al modelo de negocio". Algo similar opinó también Saiz, de Grupo On Seguridad, para quien la nube se va a convertir en una opción más "que se va a comer una parte importante del mercado, pero no todo". Y es que, como concluyó Pérez, de Eulen Seguridad, "la nube abre un abanico de grandes posibilidades, pero también de grandes interrogantes; por eso, lo mejor es ir con prudencia y responsabilidad".

Montse Castro

CEO de Casmar

"Casmar siempre ha tenido un objetivo claro: aportar valor al sector de la Seguridad y al cliente"

Por Juanjo S. Arenas. Fotos: Casmar

Montse Castro asumió la posición de CEO de Casmar tras el triste fallecimiento de su padre, Gonzalo Castro, fundador de la compañía y referente del sector de la Seguridad Privada. No obstante, la empresa ya se encontraba inmersa en un proceso de relevo generacional cuyo objetivo era continuar con la línea de crecimiento experimentada estos años y alinear su misión con la estrategia de futuro. Una transformación que no ha desviado el rumbo del principal objetivo de Casmar: aportar valor al sector de la Seguridad y a sus clientes.

Casmar ha iniciado recientemente una nueva etapa con la renovación de su cúpula directiva tras el triste fallecimiento hace unos meses de Gonzalo Castro, fundador de la compañía. De hecho, usted ha asumido la posición de CEO del grupo. ¿Qué cambios implementará Casmar en este nuevo ciclo y hacia dónde se dirigirá la organización?

Desde hace ya más de un año, en Casmar iniciamos un proceso de cambio que nos permitiera seguir creciendo y alinear la misión de la compañía con la estrategia de futuro. Ahora, debido al fallecimiento de mi padre y tras asumir la posición de CEO, hemos reorganizado la cúpula directiva en cuatro áreas de gestión: producto, comercial, operativa y finanzas. Además, un comité ejecutivo nos permitirá ser más flexibles y evolucionar conforme con nuestra estrategia.

Casmar siempre ha tenido un objetivo claro: aportar valor al sector de la Seguridad y al cliente. Obviamente, lo que se define como valor, en los más de 40 años de trayectoria de la compañía, ha ido cambiando, pero nuestro objetivo no. Trabajamos en base a nuestros valores para ser innovadores, proponer soluciones de calidad, identificar tendencias del mercado y ofrecer el mejor servicio a nuestros colaboradores y, sobre todo, a nuestros clientes.

¿Qué objetivos a corto, medio y largo plazo establece Casmar con esta reorganización que comenta?

Los objetivos a corto, medio y largo plazo del Grupo siguen siendo los mismos que hace un año: crecer en el mercado nacional y consolidarnos a nivel internacional, así como mantener nuestro posicionamiento, establecernos como referentes y ser un promotor de evolución en el sector de la Seguridad.

No obstante, el relevo generacional sí que comporta un cambio organizativo y en la manera de trabajar de la compañía y del equipo para alcanzar nuestros objetivos en el mínimo tiempo posible, con éxito y que, además, nos permita identificar y aprovechar las oportunidades que se nos presenten por el camino.

Su padre, Gonzalo Castro, fundó Casmar hace más de 40 años. ¿Cómo ha evolucionado desde entonces tanto la compañía como el sector de la Seguridad Privada? ¿Qué futuro les augura a ambos?

Obviamente, en 40 años, tanto la compañía como el sector han evolucionado, y mucho. Casmar ha pasado de ser una pequeña empresa de seguridad, que incluso llegó a fabricar algunos de sus productos, a ser uno de los distribuidores más importantes del sector en España.

Imagen de la nueva cúpula directiva de Casmar.

Asimismo, ha evolucionado de un despacho en la calle Padilla de Barcelona a ser una compañía formada por cuatro empresas ubicadas en España, Portugal, Chile y Colombia, y con más de 100 trabajadores.

Paralelamente, el sector de la Seguridad es cada vez más tecnológico y ofrece un mayor número de soluciones innovadoras que permiten optimizar los recursos, ser más ágiles y garantizar el bienestar de la sociedad. Ahora, con la pandemia que estamos sufriendo, esto se ha puesto en evidencia y se ha reconocido lo necesario y lo importante que es nuestro sector.

Tenemos que aprovechar este impulso e invertir recursos para ser capaces de adelantarnos a las necesidades de la sociedad. De este modo, seguro que podremos seguir creciendo y cumpliendo nuestro objetivo, como compañía y como sector.

> "En Casmar trabajamos con diferentes fabricantes para ofrecer una solución ajustada a las necesidades y posibilidades de cada cliente"

Casmar cuenta con productos para todos los ámbitos de la seguridad electrónica. ¿Cuáles son las principales soluciones que ofrece en este campo?

En Casmar trabajamos con diferentes fabricantes de todos los ámbitos para poder ofrecer siempre una solución que se ajuste a las necesidades y posibilidades de cada cliente, velando siempre por un producto de calidad.

Por ello, tenemos un catálogo extenso que cubre desde soluciones para un entorno residencial o edificios corporativos hasta *smart cities*, *retail*, industria, infraestructuras críticas, centros de control y mucho más.

Además, es cada vez más evidente el rol que tiene la tecnología en el desarrollo de soluciones de seguridad, y el cliente también lo solicita. Pensamos, por ejemplo, en la integración de la tecnología IoT [Internet de las Cosas, por sus siglas en inglés], las aplicaciones de analítica de vídeo en los sistemas de videovigilancia, los drones de vuelo autónomo y autorrecargables, los sistemas de control de accesos de identificación biométrica o la gestión de la seguridad desde la nube, entre otros.

Una de las características de la seguridad electrónica es la competencia. ¿Cómo se diferencia Casmar del resto de empresas presentes en este sector? ¿Qué valor añadido ofrece?

En Casmar estamos constantemente buscando maneras de aportar valor a nuestros clientes. Ello implica no solo aportar soluciones y productos innovadores o colaborar con reconocidos fa-

bricantes de vídeo, intrusión, incendio y acceso, sino acompañar al consumidor desde la detección de la necesidad hasta la puesta en marcha de la instalación.

Para ello es muy importante, por ejemplo, el desarrollo y la formación interna de los comerciales para poder asesorar con conocimiento al cliente en la toma de decisión. Y también del equipo técnico para poder resolver con rapidez las dudas que puedan surgir en el momento de la instalación o *a posteriori*.

Además, para el año 2021 estamos trabajando en diversos proyectos, especialmente en el lanzamiento de la nueva página web, que permitirá al cliente adquirir mucha más autonomía y flexibilidad en todas sus gestiones con nosotros.

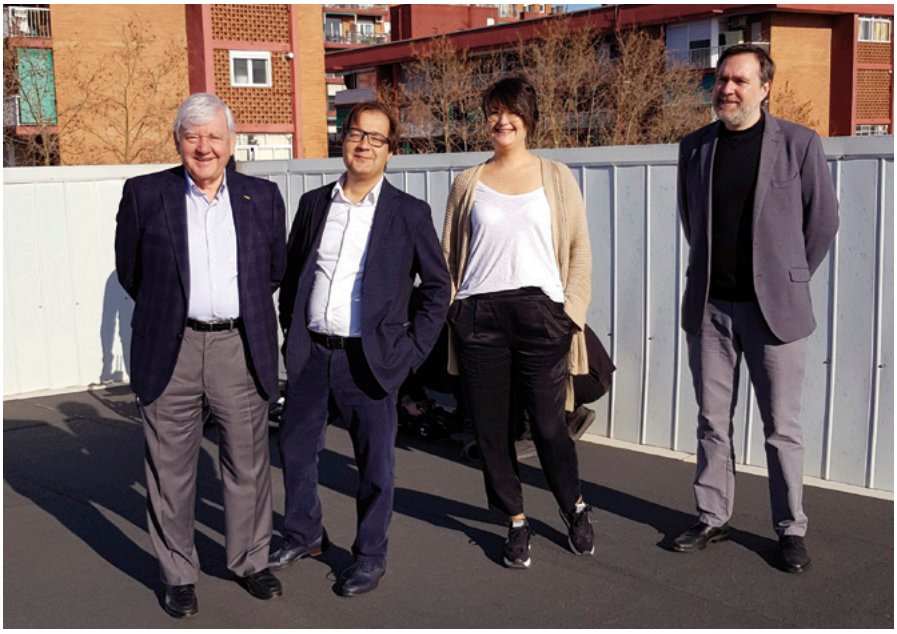


Imagen de Gonzalo Castro (a la izquierda) con la segunda generación de Casmar.

¿Qué tendencias en seguridad electrónica se están produciendo en la actualidad? ¿Cómo será el futuro de este sector?

La tecnología aplicable a la seguridad electrónica evoluciona, y seguirá evolucionando, cada vez más rápido. Y con ello surgen nuevas tendencias y posibilidades para un sector que es cada vez más imprescindible.

Ya existen varias soluciones de seguridad que integran sistemas de Inteligencia Artificial, *Machine Learning* y *Deep Learning*. Nosotros lo denominamos *Smart Security*. La incorporación de estas tecnologías permite transformar una solución de seguridad de pasiva a activa, minimizar el error humano y conseguir una seguridad más integral y fiable.

El uso de soluciones de Smart Security permite una reducción significativa de falsas alarmas, un análisis de vídeo mucho más preciso y eficaz o un reconocimiento detallado y rápido de vehículos o personas, entre otras cosas.

Por ejemplo, la analítica de vídeo es, sin duda, una de estas soluciones-tendencia que, gracias al desarrollo y a la aplicación de la Inteligencia Artificial, permite extraer una serie de datos de imágenes que facilita la discriminación de objetos, la identificación de comportamientos y la realización de búsquedas utilizando criterios como color, tamaño o dirección, entre otras funciones.

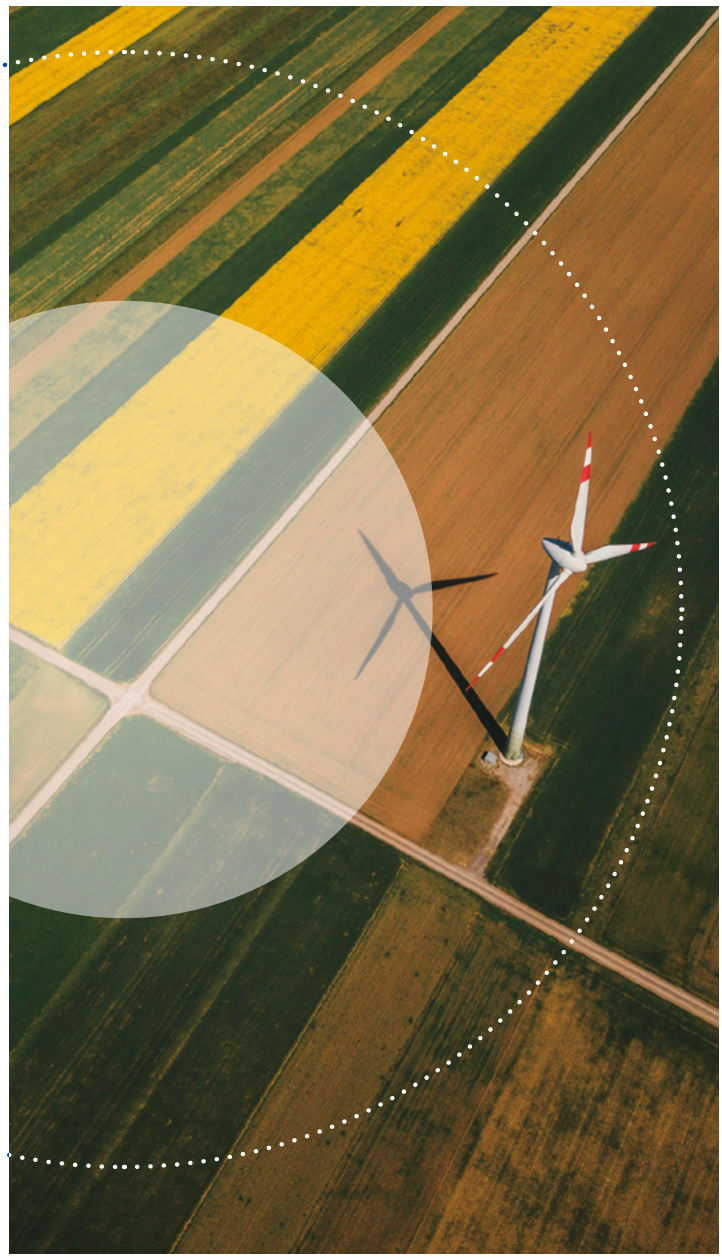
> "En épocas de crisis, la PCI suele sufrir más desinversiones al no existir una mentalidad arraigada en nuestro país sobre su importancia"

El Ministerio del Interior amplió el pasado año el plazo de adaptación de las medidas de seguridad electrónica y los sistemas de alarmas en la seguridad privada hasta el 31 de diciembre de 2023. ¿Qué opinión tiene al respecto?

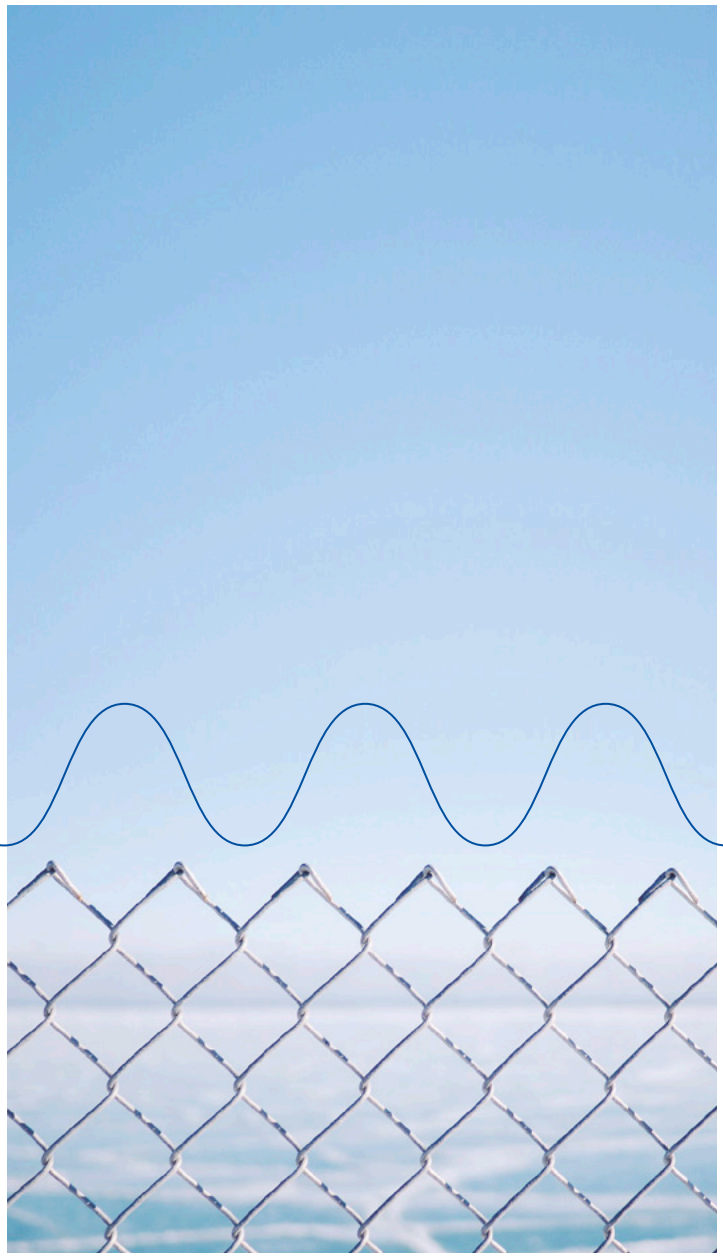
El año pasado, realmente, constituyó unos meses muy imprevisibles y excepcionales para todos. Dadas las circunstancias es perfectamente comprensible la decisión tomada por parte del Ministerio de ampliar los plazos de adaptación de las medidas de seguridad.

Desde nuestro punto de vista, las mejoras siempre son positivas, dada la voluntad de que conllevan de mejora. Tratándose, en este caso concreto, de los sistemas de seguridad, es necesario que se adapten cada cierto tiempo; pero entendemos perfectamente el aplazamiento a consecuencia de la pandemia que estamos viviendo.

Casmar está presente también en el campo de los drones. Ejemplo de ello



La protección perimetral más fiable mediante tecnología radar y sensores inteligentes



DEA SECURITY | SpotterRF

casmar®

ESPAÑA - PORTUGAL - CHILE - COLOMBIA

casmarglobal.com

es que su compañía ha incluido en su catálogo un sistema de seguridad perimetral desarrollado por Nightingale Security, compañía especializada en seguridad aérea robótica. ¿Qué importancia tendrá el uso de los drones en la seguridad privada?

El uso de drones se ha ido popularizando en aplicaciones tan distintas como la agricultura, el control de incendios forestales o la topografía, y poco a poco irá tomando más importancia también en nuestro sector. Es una herramienta eficaz, tanto para el control fronterizo como para la vigilancia perimetral, aportando funcionalidades adicionales muy útiles para este tipo de instalaciones. La nueva normativa europea, sin duda, también colaborará a usarse cada vez más esta tecnología.

La posibilidad de trabajar con drones autónomos permite al usuario realizar rondas, detectar intrusos o verificar eventos producidos por otros sistemas sin necesidad de contar con personal *in situ*, lo que puede conllevar un importante ahorro que sabrán poner en valor las empresas.

Otro de los campos en los que está presente Casmar es el de la protección contra incendios (PCI). En su opinión, ¿en qué momento se encuentra este sector en nuestro país? ¿Qué elementos se deben mejorar en él?

Actualmente, el sector de la PCI se encuentra en un momento de cambios. Después de varios años de necesidad de introducir mejoras en los ámbitos normativo, tecnológico y económico, la aprobación del nuevo Reglamento de Instalaciones de Protección Contra Incendios en 2017 supuso un impulso al sector en cuanto a profesionalización y actualización normativa.

Sin embargo, la pandemia ha supuesto un freno importante. En épocas de crisis es uno de los sectores que suele sufrir más desinversiones al no existir una mentalidad arraigada en nuestro país sobre su importancia. No obstante, existe una voluntad de mejora por parte de todas las partes implicadas, como fabricantes, instaladores, etc., con el fin de apostar por una mejora tecnológica en los equipos y en los procesos, como se ha aplicado en otros ámbitos de la seguridad. De hecho, se está trabajando intensamente para introducir, en un futuro cercano, una serie de cambios importantes al respecto.

Sin duda, esta es la mejora que necesita la PCI: una actualización tecnológica en muchos aspectos, tales como las comunicaciones, monitorización de los sistemas e implantación de IoT, que actualmente se utilizan ampliamente pero que no han recalado aún en la gestión de la detección contra incendios.

Su compañía dispone de una gran variedad de soluciones basadas en el IoT. ¿Cuáles son sus principales características? ¿En qué entornos y aplicaciones de seguridad se pueden emplear esta clase de soluciones?

El objetivo del IoT es acercar la interconexión digital a los objetos y dispositivos cotidianos para optimizar los recursos, reducir los costes y proporcionar un funcionamiento óptimo y seguro de los elementos que participan en la instalación, con un eficaz y seguro sistema comunicación entre ellos. De este modo, se consigue una reducción de los costes de instalación gracias al uso de dispositivos vía radio de muy bajo consumo, con autonomías de varios años y que permiten un rápido despliegue de los mismos en la instalación.

Las soluciones ofrecidas por IoT pueden aplicarse en multitud de entornos y aplicaciones. Los dispositivos ofrecen control de temperatura, de humedad, de iluminación, de aperturas en arquetas y canalizaciones, así como medición del nivel de líquidos, sensores de movimiento y consumo energético, entre otros. Sus aplicaciones son ilimitadas y es, además, una tecnología que está en pleno auge. Podemos destacar, por ejemplo, la aplicación de soluciones IoT en el sector sanitario con el control de temperatura de las neveras que contienen medicación; en *Smart Cities* al controlar el alumbrado de las ciudades o la ocupación de plazas de aparcamiento; en *Smart Buildings* gestionando la ocupación de salas, puertas y ventanas abiertas, así como control energético, temperatura y humedad; y otros como museos, ayuntamiento, trenes, flotas de caminos o industria.

LA CONVERGENCIA DE DOS MUNDOS

ESS+
FERIA INTERNACIONAL DE SEGURIDAD

25 AL 27 AGOSTO 2021

BOGOTÁ / CORFERIAS

SEGURIDAD 4.0 / CIBERSEGURIDAD / BIOSEGURIDAD

- EXHIBICIÓN TECNOLÓGICA
- RUEDA DE NEGOCIOS
- EVENTOS ACADÉMICOS POR VERTICALES
- FOROS ACADÉMICOS
- CENTRO DE EXPERIENCIA

CONTACTO Adriana Márquez | amarquez@securityfaircolombia.com | Tels. (571) 510 3494 - 510 3330

ALIADOS

ORGANIZADORES

WWW.SECURITYFAIRCOLOMBIA.COM

FUNDACIÓN BORREDÁ
al servicio de la seguridad

V CONFERENCIA SECTORIAL

Seguridad en Puertos

2 de marzo

evento virtual

Colabora

Puertos del Estado

es.movilidad
evento colaborador

SEGURITECNIA
REVISTA DECANA INDEPENDIENTE DE SEGURIDAD

Inscripción gratuita

Más información: publicidad@borrmart.es

BORRMART EVENTOS

Patrocina

AXIS COMMUNICATIONS

EXCEM TECHNOLOGIES

SAES

TECOSA

2 de marzo

PROGRAMA

evento virtual

09:30-09:45	**Bienvenida y presentación de la jornada.** **María José Rallo del Olmo.** *Secretaria General de Transportes y Movilidad.* **MITMA**
09:45-10:10	**Situación actual de la Seguridad en el ámbito Portuario.** María del Mar Chao López, *Directora de Explotación* y Javier Gesé Aperte, *Subdirector de Seguridad y Protección de* **Puertos del Estado**
10:10-10:30	**Sistema de Inspecciones de la EC.** Mario Carvajal de la Torre, *Maritime Security Inspector, European Commission*
10:30-10:50	**Sistema Nacional de Inspecciones de Protección.** Celia Tamarit de Castro, *Jefa de Área de Protección de* **Puertos del Estado**
10:50-11:00	Preguntas público
11:00-11:20	**Nueva Regulación en seguridad de las redes y sistemas de información**. Juan Carlos Galán Méndez, *Responsable de Sistemas de Información y Comunicaciones.* **Puerto de Castellón**
11:00-11:20	Preguntas público

PANEL: SOLUCIONES TECNOLÓGICAS IMPLANTADAS EN PUERTOS

11:30-12:30	- **La mejor vigilancia en puertos. Caso de estudio del Puerto de Las Palmas**. Verónica del Hoyo, *Key Account Manager de* **AXIS** - **Fortalecimiento de la seguridad en la inspección de contenedores tras la implantación de un Sistema Global Centralizado de Imágenes** Santiago Ramos, *Sales manager - sector público de* **Excem Technologies** - **El reto de ciberseguridad en puertos** Alberto Alonso, *Product manager* **Tecosa** - **Las amenazas submarinas en las infraestructuras críticas.** Eduardo Ruiz Pérez, *Responsable Comercial y Desarrollo de Negocio Mercado Civil y Seguridad de* **SAES**

PANEL: EXPERIENCIAS COMPARTIDAS EN EL ÁMBITO DE LA SEGURIDAD

12:30-13:30	- Sandra Yunta, *General Manager and PFSO.***Terminal Cruceros de Barcelona** - Cristina Hermoso, *Inspectora jefa del grupo de entry and exit system de* **Policía Nacional** - José Ángel Astillero Fuentes, *TCOL* **Guardia Civil, SERVICIO DE COSTAS Y FRONTERAS**
13:30	**Clausura. Francisco Toledo Lobo,** *Presidente de* **Puertos del Estado**

INSCRIPCIÓN GRATUITA

Patrocina

AXIS COMMUNICATIONS · EXCEM TECHNOLOGIES · SAES · TECOSA

Víctor Alberto Gil Perdomo
Jefe de Seguridad Corporativa de la
Autoridad Portuaria de Santa Cruz de Tenerife

"El modelo de seguridad de los puertos insulares tiene que ser muy ágil para que no se retrasen las operaciones"

Por Enrique González Herrero / Fotos: AP Santa Cruz de Tenerife

La Autoridad Portuaria de Santa Cruz de Tenerife gestiona un total de seis puertos cuya principal característica es el elevado volumen de tráfico de pasajeros. No en vano, los habitantes de las islas dependen de los barcos para desplazarse entre localidades. Una particularidad que los diferencia de otros puertos como los de la Península. Por eso, el responsable de seguridad del organismo, Víctor Álberto Gil, considera necesario que la normativa de estos entornos se adapte a circunstancias como esta para conseguir conciliar la seguridad con la agilidad del tránsito.

¿Cuál es el volumen de tráfico marítimo de pasajeros y carga que soporta la Autoridad Portuaria de Santa Cruz de Tenerife?

En 2019 estábamos moviendo en torno a 12 millones de toneladas de mercancías de todo tipo y más de seis millones de pasajeros. Una cifra muy significativa era pasaje en régimen de crucero, cuyo el volumen estaba en torno al millón de pasajeros anualmente, lo que suponía algo más de 500 escalas. El sector, obviamente, ahora está casi parado, con lo cual el año 2020 no fue indicativo.

De la Autoridad Portuaria de Santa Cruz de Tenerife dependen seis instalaciones. En Tenerife están adscritos el Puerto de Santa Cruz de Tenerife, el de Granadilla y el de Los Cristianos. En la isla de La Palma tenemos el Puerto de Santa Cruz de la Palma. En La Gomera, gestionamos el Puerto de San Sebastián de La Gomera. Y en Valverde, en la isla de Hierro, tenemos el Puerto de la Estaca. En definitiva, son los puertos de interés general de la provincia de Santa Cruz de Tenerife.

¿Cómo estructuran la función de seguridad para dar cobertura a todos esos puertos?

Tenemos una estructura multidisciplinar y multipuerto. Toda la seguridad y protección dependen de la Dirección de la Autoridad Portuaria, a través del área de Desarrollo Operativo. Por un lado, está la seguridad corporativa, la que yo represento, que vela porque todos los parámetros y políticas de seguridad de los diferentes puertos respondan en una misma línea. Después, tenemos en cada puerto un oficial de protección, que es también el jefe de zona portuaria. Es decir, entendemos que la seguridad debe ir de la mano de la explotación, con lo cual, en esa estructura descentralizada que tenemos, quien lleva la explotación o las operaciones también

se hace cargo de toda la estructura de protección y autoprotección, incluyendo la propia policía portuaria.

¿Cuáles son las amenazas de seguridad a las que han de hacer frente habitualmente y cuáles las más preocupantes?
Coyunturalmente tenemos el problema de la migración. Estamos sufriendo una fuerte presión migratoria de África y ese es el principal problema ahora. Conocedores de este drama que estamos viviendo en territorio insular, estamos destinando muchos recursos, tanto humanos, como materiales y económicos. Porque no solo se trata de la recepción y la atención de los migrantes, sino que cuando las personas salen del recinto portuario, al final quedan las embarcaciones, lo que requiere trámites ulteriores que consumen muchos recursos.

Aparte, también tenemos los habituales incidentes en torno al recinto portuario; por ejemplo, la intrusión, el robo, los actos vandálicos, etcétera.

¿Cómo están abordado la pandemia del Covid-19 para continuar su actividad con garantías de seguridad?
Cuando el virus llegó tan precipitadamente, creamos un Plan de Reacción para tratar de mantener los servicios propios de la Autoridad Portuaria, lo cual se consiguió con mucha voluntad por parte de todos los empleados. Por otro lado, implantamos el teletrabajo en los casos necesarios. También reorganizamos los servicios, sobre todo en el caso de la policía portuaria, que es nuestra primera línea en el puerto y un pilar fundamental.

Se ha hecho un esfuerzo importante de reorganización, acompañado de la implantación de las herramientas que permiten el teletrabajo. Esto requirió también un esfuerzo importante por parte de nuestros compañeros del área de Sistemas de Información y Telecomunicaciones.

Terminal de cruceros del Puerto de Santa Cruz de Tenerife.

¿Cuáles son las principales diferencias entre los puertos canarios y los de la Península desde el punto de vista de la seguridad?
Los territorios insulares que abarca la Autoridad Portuaria de Tenerife tienen una característica que siempre repetimos: que el tráfico que se genera en nuestros puertos es como un metro o un tren de cercanías de un territorio peninsular. Nosotros nos movemos entre las principales ciudades de la provincia a través de las infraestructuras portuarias.

Es por ello que el concepto de seguridad se aproxima mucho a ese modelo. Tiene que ser un modelo muy ágil en el que no se retrasen las operaciones en embarque y desembarque. Estamos hablando de buques que cargan y descargan el pasaje, los vehículos y su mercancía en 20 minutos, con lo cual difiere bastante de otro concepto de puerto donde no se genera esa alta frecuencia de tráfico.

Esto significa que les perjudica el modelo general de seguridad para los puertos. ¿Cree que debería adaptarse la normativa para los territorios insulares?
En el caso de lo de los territorios insulares, y por el tipo de operativa y de tráfico de alta frecuencia, efectivamente hay que adaptarlo. La normativa está pensada para puertos en los cuales existen unas horas de embarque, de desembarque, así como espacios grandes. En nuestro caso, requiere de unos procedimientos de acceso, verificación y control mucho más ágiles.

Es habitual la comparación de los puertos con los aeropuertos en términos de seguridad. ¿Cree usted que la protección en el entorno portuario debe acercarse más a la de los aeropuertos?
Hay que partir de las diferencias entre un puerto y un aeropuerto. Lo primero en lo que tenemos que fijarnos es la ubicación física del mismo. Los puertos han ido de la mano de las ciudades, éstas han crecido alrededor del puerto. Eso es prácticamente inimaginable en el caso de un aeropuerto, que están en espacios totalmente alejados de los principales núcleos urbanos.

En el caso del aeropuerto, rara vez existirá el concepto aeropuerto-ciudad,

Una de las dársenas del Puerto de Santa Cruz de Tenerife.

si bien en el caso de los puertos es una realidad. Muchas veces el usuario no conoce el límite del puerto ni el de la ciudad, incluso a veces las propias administraciones discrepamos sobre dónde llega cada uno. Es más, a día de hoy es inconcebible que alguien se vaya a pasear al aeropuerto, pero en cualquier ciudad portuaria es común ir a pasear al puerto. Eso hace que el modelo tenga que ser completamente diferente.

El puerto tiene que crecer de la mano de la ciudad. Esa es la principal diferencia entre las dos instalaciones. Eso hace que la normativa deba ser más acorde a esta situación. No debe perseguir tanto el modelo aeroportuario, sino ir hacia un modelo propio en base a las necesidades del entorno portuario. Porque además en el puerto no solo hay barcos, existen muchísimas otras actividades que no son específicas de la operativa portuaria.

¿Qué aspectos cree que habría que reforzar o revisar?

Habría que revisar un poco la normativa sobre todo en materia de protección. Una asignatura pendiente es el famoso Reglamento de Explotación y Policía de los Puertos, que siempre ha estado a punto de salir, pero nunca lo ha conseguido. En ese sentido, aclararía las competencias y funciones de cada uno de los partícipes en todo este modelo de seguridad.

Sería buena la creación de una comisión de trabajo específica, de la cual fuéramos partícipes las autoridades portuarias, donde se trate de adaptar más la legislación, la normativa, los reglamentos, etcétera, a la realidad de los puertos. Es decir, perseguir un modelo de protección atendiendo a la naturaleza de los puertos, las particularidades de cada uno de ellos y las diferentes actividades que se desarrollan.

¿Cómo les afecta a los puertos esa falta de actualización normativa?

Como punto de partida, tuvimos el famoso Código PBIP, luego el Real Decreto el 1617/2007 y tenemos pendiente la publicación de un Reglamento de Explotación y Policía Portuaria, pues el que tenemos es de 1976.

Debería acondicionarse toda esa normativa a la realidad del entorno portuario y sus riesgos. Perseguir el modelo aeroportuario no es la mejor opción, sino que hay que ir específicamente a lo que es el entorno portuario. Por ejemplo, en nuestro caso, como territorio insular, es necesario que se adapte la normativa al tráfico de alta frecuencia de pasajeros.

Uno de los aspectos más sensibles es la inspección de la carga de los buques. ¿Cómo valora los pasos que se han ido dando en los últimos años para la mejora del sistema de inspección?

Es imposible inspeccionar toda la carga, dados los millones de toneladas que se mueven en los puertos. En nuestro caso, nos encontramos además con el problema de la carga de los buques de pasaje, que además llevan vehículos. Imagínese tener que inspeccionar 200 vehículos cada 20 minutos.

En el Puerto de Santa Cruz de Tenerife hemos implantado desde hace unos años un escáner de inspección que, en función de los diferentes circuitos a través de los que viene el contenedor, realiza la inspección aduanera; pero la inspección absoluta de la carga es prácticamente imposible.

> "Perseguir el modelo aeroportuario no es la mejor opción, hay que ir específicamente a lo que es el entorno portuario"

¿Considera que se ha integrado eficientemente la normativa de protección portuaria con la de infraestructuras críticas?

Nos consta el enorme esfuerzo que han realizado Puertos del Estado y el CNPIC [Centro Nacional de Protección de Infraestructuras Críticas] para ello. Aparte los planes de protección de las instalaciones portuarias tenemos el propio plan de protección del puerto, que es el documento eje vertebrador de toda la protección de ese puerto. Si embargo, dicho documento ha estado siempre más orientado a la protección de las personas y los activos físicos; es decir, la propia instalación portuaria y sus bienes, además de las personas.

En el caso de las infraestructuras críticas, la normativa ha profundizado bastante en la protección del dato y de los sistemas de información, con lo cual se han creado los planes de protección específicos de las instalaciones portuarias. Puertos del Estado, CNPIC y otros organismos han creado un anexo para la protección de la infraestructura crítica del puerto. Eso es muy positivo porque simplifica mucho toda la estructura documental que generamos alrededor de la protección de los puertos.

Además de los escáneres para la inspección de equipajes, ¿cuáles son las tecnologías más empleadas en los puertos en materia de seguridad?

Tenemos implantados varios subsistemas de control de accesos, mediante automatización de los mismos, para tener identificados a los usuarios a través de sus credenciales. En función de su permiso pueden acceder a unas zonas u otras. Tenemos una fuerte implantación de estos sistemas con tecnologías de proximidad, lectores de matrículas, etcétera.

Por otro lado, también tenemos una fuerte implantación en materia de circuito cerrado de televisión, que se visiona desde la sala de control de la Policía Portuaria y el Centro de Coordinación de Servicio de Tráfico Marítimo, o incluso desde las diferentes jefaturas de zona de los oficiales de protección. Tenemos desplegadas más de 200 cámaras entre los cinco puertos.

Padecemos, no obstante, una fuerte deficiencia en cuanto a número de medios humanos en el caso de la Policía Portuaria, que tratamos de suplir haciendo uso de las nuevas tecnologías.

Jesús A. Teva Córdoba
Responsable de Autoprotección de la Autoridad Portuaria de Tarragona

José Luis Díez Basora
Director de Dominio Público y Protección Portuaria de la Autoridad Portuaria de Tarragona

Sostenibilidad, digitalización y transparencia, ejes de innovación en seguridad del Port de Tarragona

Seguridad y sostenibilidad son eslabones inseparables de una misma cadena. No podemos por tanto disociar una de otra cuando diseñamos la política de seguridad integral de la organización, ya que ésta ha de estar alineada con las líneas estratégicas de la empresa, en la que la sostenibilidad y el compromiso con los objetivos de desarrollo sostenible son una realidad.

La Autoridad Portuaria de Tarragona cuenta con un Plan de Sostenibilidad que recoge el compromiso de la organización para reducir el impacto ambiental del Port de Tarragona en el territorio para el período 2020-2030. El plan recoge 23 objetivos a cumplir a través de la aplicación de más de 80 acciones que abarcan los ámbitos de la sostenibilidad ambiental, el crecimiento sostenible y el compromiso social.

La Ley de Puertos establece la obligatoriedad por parte de las autoridades portuarias de controlar el cumplimiento de la normativa que afecta a los sistemas de seguridad y protección ante acciones terroristas y antisociales, contra incendios y de prevención y control de las emergencias, en los términos establecidos por la normativa sobre protección civil y lucha contra la contaminación marina.

Lo anterior se plasma a través de diferentes planes de emergencia que, en general, analizan las instalaciones portuarias, sus riesgos y los medios materiales y humanos de los que se dispone. Asimismo, describen cómo se organizan los mismos en caso de que sea necesario actuar en situaciones de emergencia por parte del personal de la autoridad portuaria y sus equipos especializados de intervención. También recogen las herramientas de coordinación con otras administraciones en el marco de la normativa vigente de aplicación, así como las actuaciones necesarias a seguir en caso de activación de planes de ámbito superior.

En este sentido, la política de seguridad integral de la organización no es ajena a lo anterior, ya que, tal y como se recoge en el Plan de Seguridad del Operador, la misma refleja los conceptos, principios, responsabilidades y objetivos en materia de seguridad. Sus resultados permitirán garantizar a la Autoridad Portuaria de Tarragona la libertad de acción necesaria en función de sus necesidades, prestando especial atención a los principios de apoyo y responsabilidad de la alta dirección, convergencia de las diferentes disciplinas de la seguridad, gestión de la seguridad de la información y aumento de la cultura de seguridad de todo el personal del puerto.

Esta política persigue garantizar la efectiva protección del personal perteneciente a la Autoridad Portuaria de Tarragona, así como de cualquier otro que se encuentre en la zona de influencia de las infraestructuras e instalaciones gestionadas por la misma. Igualmente garantiza la protección de los bienes y servicios que presta, de aquellos afectos al tráfico portuario y de las actividades comerciales portuarias ante las agresiones internas y externas que pudieran sobrevenir.

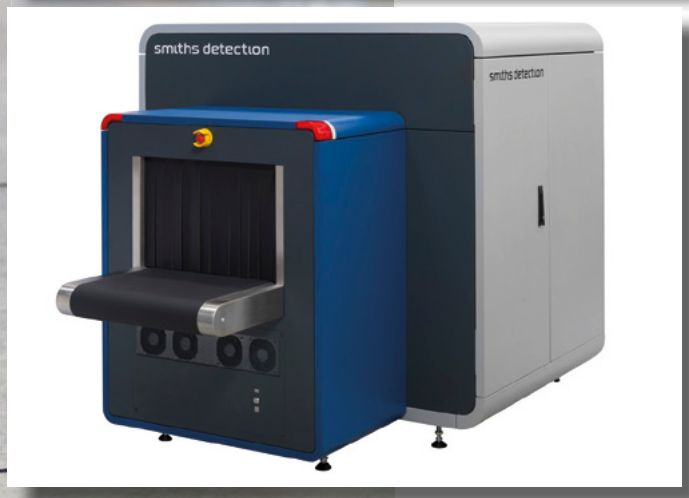
Función transversal

Vemos cómo las acciones estratégicas en este sentido conllevan, por un lado, el apoyo y responsabilidad de la alta dirección de la organización, la transversalidad y convergencia de las diferentes

TECOSA

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

www.tecosa.es



Innovación al servicio de la seguridad

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

Excelencia en calidad y servicio post-venta.

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

disciplinas de la seguridad (física, ciberseguridad, laboral, medioambiental, industrial, emergencias y operativa marítimo-terrestre); y por otro, la promoción de la cultura de seguridad en el seno de la organización que se haga extensiva a todo el personal en el marco de sus competencias y funciones, que mejore el conocimiento de los aspectos relacionados con la seguridad y la minimización de riesgos.

Podemos comprobar, por tanto, el amplio espectro de ámbitos relacionados con la seguridad. Esto hace más relevante la transversalidad y convergencia de las actuaciones relacionadas con la misma, al objeto de dotar de coherencia a la política estratégica de la empresa. Todo ello, sin ser ajena a los elementos de sostenibilidad que dotarán a la misma de una eficacia sostenida en el tiempo con una relación coste-beneficio controlada y que permita la generación de sinergias entre los diferentes sistemas.

Para plasmar lo anterior de manera eficaz, es necesaria una estructura funcional jerarquizada, transversal y dinámica, que favorezca la toma de decisiones eficientes y alineadas con la estrategia de la organización. En ese sentido, es necesaria la existencia de comités y órganos decisores en el marco de la seguridad que, en el caso de la Autoridad Portuaria, son el comité consultivo de protección del puerto, el comité de seguridad integral o el comité de seguridad y salud. Dichos comités, junto con el consejo de navegación y puerto o el comité de servicios portuarios, son los coordinadores de decisiones en el ámbito de la seguridad que afectan a la organización.

Actuación en emergencias

En el ámbito de las emergencias, son diversos los planes que pueden activarse: plan de seguridad específico, plan de autoprotección, plan interior marítimo o plan de protección portuaria. Cada uno de ellos está regulado por una normativa diferente, con estructuras de dirección de emergencia a veces distintas, que hacen necesario un elevado esfuerzo de coordinación de las actuaciones y la toma de decisiones. Estamos hablando, además, de un entorno de elevada complejidad operativa y funcional de las instalaciones marítimo-terrestres, lo que pone en valor la potenciación de prácticas, ejercicios y simulacros periódicos que mejoran la eficiencia de posteriores actuaciones.

En relación con lo anterior, la Autoridad Portuaria de Tarragona ha elaborado un manual básico de actuaciones en emergencias que pretende ser una herramienta de ayuda sencilla que permita a las personas con responsabilidad en el marco de las actuaciones en emergencias, coordinando las decisiones en el marco de los diferentes planes de emergencia.

Los esfuerzos en la formación del personal que forma parte de los equipos de intervención especializados y que tienen funciones recogidas en diferentes planes incidirán muy positivamente en la gestión de la seguridad. Queda incluido el personal cuyas funciones aparencen en planes tanto de la Policía Portuaria, como de los Parques Químicos de Seguridad o Bomberos de la Generalitat de Catalunya, así como de otras áreas funcionales de la Auto-

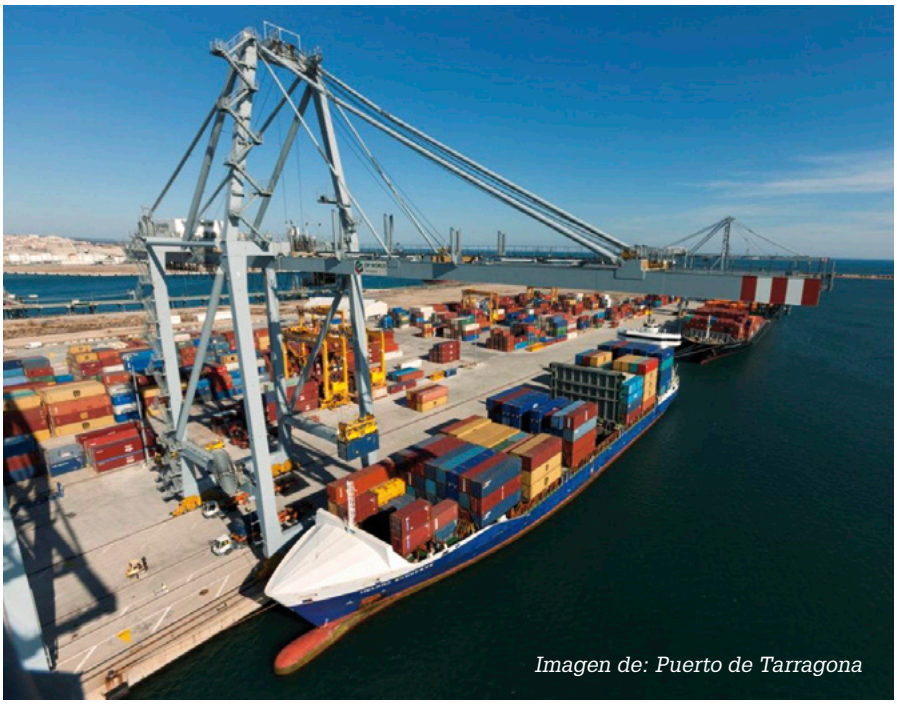


Imagen de: Puerto de Tarragona

> Es necesaria una estructura funcional jerarquizada, transversal y dinámica, que favorezca la toma de decisiones eficientes

ridad Portuaria enfocadas a un mayor conocimiento del entorno portuario, sus riesgos específicos y los medios disponibles, tanto en el ámbito terrestre como marítimo.

Por otro lado, la Autoridad Portuaria de Tarragona cuenta con gran cantidad de medios materiales de extinción de incendios, dotaciones de los equipos de intervención, control de la contaminación marina accidental, y sistemas de seguridad física y lógica de última generación. Este último es un campo en el que existe una constante innovación e implementación de sistemas cada vez más eficientes, que permite implementar procesos de mejora continua que, además, son objeto de auditorías internas y externas que permiten renovar diferentes certificaciones.

Centros de control

Una parte esencial del sistema de seguridad del Port de Tarragona es el Centro de Control y Vigilancia (CCV), desde el que se centralizan los sistemas de monitorización y control de los diferentes ámbitos de la seguridad. Dicho centro coordina las actuaciones en emergencias junto con el Centro de Control y Salvamento (CCS). El primero se complementa con los sistemas SCADA de control de las redes de abastecimiento de agua, contra incendios y suministro eléctrico, así como estaciones de lectura y control de diferentes parámetros medioambientales o de almacenamiento de mercancías peligrosas y control de tráfico marítimo, esenciales en la gestión de la seguridad y la mejora de la sostenibilidad del sistema en su conjunto.

Existen otros proyectos que permitirán continuar los procesos de mejora continua en el ámbito de la seguridad, siempre de la mano de la sostenibilidad, como ejes estratégicos de la organización. Estos son: la próxima implantación de un sistema de comunicación masivo para los diferentes usuarios internos del recinto portuario, la continua ampliación de las redes contra incendios existentes y la mejora de sus sistemas de control y señalización, la digitalización de procesos, el uso de drones en actividades operativas o de control de emergencias, la continua implementación de políticas comunicativas transparentes, así como el hecho de seguir potenciando el trabajo colaborativo con la comunidad portuaria y diferentes grupos de interés del territorio.

Videovigilancia para garantizar una navegación **fluida en el Puerto de Las Palmas**

Pedro Navalpotro
Key Account Manager en Axis Communications

El Puerto de Las Palmas está conectado con más de 380 puertos de todo el mundo a través de 30 líneas marítimas. Además, recibe más de un millón de pasajeros cada año en los distintos cruceros con escala en Gran Canaria. En cuanto al transporte de mercancías, desde él se gestionan 16 millones de toneladas de tráfico de contenedores y es punto clave para la organización de eventos de carácter mundial.

La Autoridad Portuaria de Las Palmas gestiona toda una serie de puertos en el Océano Atlántico que sirven de nexo de una amplia red de comunicaciones entre distintos continentes. Por ello, tal como afirma José Ramón Ansó, CTO del Grupo Gemed, empresa instaladora de las cámaras de Axis Communications en el puerto canario, resulta vital que las actividades que se realizan en estas infraestructuras críticas se gestionen de forma segura y adecuada. Esto incluye la videovigilancia remota en todos los puertos (en concreto, cinco puertos en tres islas), lo que permite que tanto el vídeo en directo como el grabado sean fácilmente accesibles.

> La seguridad portuaria nos lleva a asumir distintos desafíos, entre ellos la conectividad, las redes y la gestión de los diferentes dispositivos

Los puertos son como pequeñas ciudades y, en este caso, la ciudad es el Puerto de Las Palmas, que se extiende por varias islas. Como en todas las urbes, su crecimiento es un área que requiere mucha atención. Actualmente, el Puerto de Las Palmas está ampliando el espigón de La Esfinge, mientras que Lanzarote y Fuerteventura también están agrandando sus puertos.

Factor crítico

La seguridad se convierte de esta forma en un factor crítico. En este sentido, el centro de control del puerto es responsable de coordinar todos los aspectos de la seguridad. Y para ello necesita mantener canales de comu-

nicación constantes con todas las instalaciones existentes en diferentes enclaves estratégicos. La autoridad portuaria tiene que garantizar la seguridad 24 horas al día, siete días a la semana y 365 días al año. De esta forma asegura la protección continua de sus instalaciones y de las personas, así como de los materiales y mercancías que circulan por ellas.

El Puerto de Las Palmas cuenta con una tecnología de iluminación avanzada con amplio rango dinámico, *lightfinder* e IP optimizados. Las cámaras de las que dispone ofrecen gran maniobrabilidad, ya que giran 360 grados y tienen un zoom de largo alcance. Concretamente, cuenta con 130 cámaras domo PTZ, 25 cámaras de caja fija, tres cámaras domo fijas y cuatro unidades del grabador Axis Camera Station S1132, controlables con dispositivos de última generación como los mandos *joystick* y *jog dial*.

La seguridad portuaria nos lleva a asumir distintos desafíos, entre los que destacan la conectividad, las redes y la gestión de los diferentes dispositivos en entornos marinos exigentes. Por ello, configurar y proteger adecuadamente la seguridad de los dispositivos IoT (Internet de las Cosas, por sus siglas en inglés) no es una opción, sino una obligación.

Esto, unido a que los puertos son entornos meteorológicamente hostiles, nos lleva a que cualquier equipo que se haya instalado tiene que cumplir una serie de requisitos para garantizar la calidad en las grabaciones.

Por ejemplo, el tema de la corrosión es clave, mientras que los fuertes vientos también deben ser contrarrestados con un sistema de estabilización de imagen. Por este motivo, todos sus dispositivos instalados cuentan con la tecnología más innovadora, así como con potentes sistemas de estabilización electrónica de la imagen, tecnología de compresión ZipStream, tecnología SharpDome y la funcionalidad Speed Dry, que sacude la cámara para limpiarla de gotas de agua y sal marina, permitiendo siempre la mejor visibilidad.

Cualquier equipo que se haya instalado en un puerto tiene que cumplir una serie de requisitos para garantizar la calidad de las grabaciones

Herramientas

Axis Communications también dispone de una serie de herramientas para gestionar el día a día y optimizar los equipos instalados, lo que permite agilizar los tiempos de reacción en el mantenimiento. Estas herramientas se actualizan continuamente a través de *firmware* y de distintas actualizaciones. Todo esto posiciona a la compañía como líder especializado en materia de seguridad y videovigilancia, respondiendo eficazmente a las necesidades de sus clientes.

Tal como indica Jesús Ramírez, jefe del Departamento de Informática y Nuevas Tecnologías de la Autoridad Portuaria de Las Palmas, "los dispositivos Axis que hemos instalado cumplen estos requisitos y nos permiten no solo obtener imágenes estables, sino también almacenarlas en sistemas que no ocupan demasiado espacio en disco. Además, la función de búsqueda inteligente de los dispositivos Axis hace que nuestros operadores dediquen mucho menos tiempo a la recuperación de imágenes que con la solución anterior. Esto contribuye a mantener los costes totales de funcionamiento realmente bajos y nos hace sentir bastante satisfechos con la inversión realizada".

Nuevas tendencias y soluciones **en seguridad portuaria**

Luis Rolandi Torquemada
Gerente de
Target Tecnología

La importancia de los puertos marítimos en la sociedad y en la economía es indudable. De hecho, desde el inicio de la crisis del coronavirus, apenas ha decrecido su nivel de actividad en cuanto al transporte de mercancías. Es más, se ha visto colapsado en algunos momentos por la necesidad de modificar ciertos protocolos o incluso de tratar las mercancías o la gestión de personas de acuerdo con las nuevas exigencias.

El sector logístico debe mantener su actividad para garantizar el suministro de bienes a la población y a las empresas. Especialmente, para el abastecimiento a la red sanitaria y a establecimientos distribuidores de productos de protección (geles, mascarillas, equipos de protección individual…) y de bienes de primera necesidad.

Además de su importancia para el transporte de mercancías y personas, los puertos tienen un papel relevante en la seguridad nacional y europea al tratarse de puntos de control fronterizo. El riesgo de ataques terroristas o de actividades delictivas es muy alto en este tipo de instalaciones y, por tanto, requieren de estándares de seguridad vanguardistas y actualizados.

Las instalaciones portuarias son las infraestructuras críticas más numerosas de nuestro país, repartidas a lo largo de sus más de 8.000 kilómetros de costas. Su excepcional tamaño y complejidad, así como el elevado volumen de carga que transita por ellas, han supuesto un reto para garantizar su protección, al cual Target Tecnología siempre ha aportado sus soluciones a la altura de la necesidad.

No obstante, existen nuevas amenazas a las que deberán hacer frente para garantizar las cadenas de suministros y los flujos comerciales. Pero ¿están preparados los puertos marítimos para este nuevo escenario?

Nuevos retos

La crisis sanitaria y social que estamos viviendo a nivel mundial nos obliga a enfrentarnos a nuevos retos. La mejora de la seguridad en los puertos, sin penalización del comercio o las actividades portuarias, es el objetivo número uno de estas infraestructuras críticas.

Igualmente, las nuevas tecnologías están ganando protagonismo y tienen mayor impacto, tanto en la prevención como en la mitigación de posibles incidentes o amenazas que puedan atentar contra instalaciones, mercancías o personal. Sin duda, este último está posicionándose en el centro de un modelo de gestión que prioriza la experiencia del usuario.

Dentro de estas tendencias surge el "*Smart Port*" o los "Puertos 4.0", los cuales tendrán que valorar nuevas amenazas digitales, además de las ya existentes. La evolución inteligente de los puertos no solo consiste en modernizar las infraestructuras, sino que también repercute en la operativa y en todos los actores del entorno portuario, tanto público como privado.

Para la protección de los trabajadores del puerto y de sus visitantes, se integran nuevas soluciones para el control de accesos y gestión de personas, donde se prioriza la inspección *contactless*. En estos nuevos entornos se presentan sistemas de control de acceso biométricos, combinado con *software* de presencia y gestión, los cuales permiten realizar una detección de temperatura, reconocimiento de la palma, detección de mascarilla y reconocimiento facial. Estos mismos sistemas se integran con la gestión del aforo en tiempo real, el cual se ha convertido en una prioridad para gestionar espacios cerrados con un nivel de aforo máximo.

Desinfección

Para garantizar que los activos y bienes que pasan a diario por los puertos de

www.alerting24.com

ALERT24 Communication Suite

Mass notification system and crisis management

Incidentes, Continuidad, Amenazas, Riegos, Crisis, Reputación, Simulacros

SaaS 100% y on-premise
Disponible para España, UE, LATAM, EEUU

ALERT24 es una solución específica, confiable, para la comunicación, coordinación de equipos y gestión de la información frente a los riesgos, incidentes y crisis en cualquier tipo de organización

Permite mejorar los procesos definidos durante las diferentes fases de una crisis o para continuidad de negocio

Facilita el análisis para la mejora continua de estos procesos, recopilando datos durante la planificación, prevención, simulacros y activación de cada incidente

Escanear QR para promoción

VOIDSISTEMAS
www.void.es

alert24

nuestro país no se conviertan en propagadores del virus, se han desarrollado recientemente soluciones de desinfección contra el coronavirus (u otros virus que puedan llegar más adelante). Existen tecnologías para la desinfección de pequeña y mediana paquetería, maletas e incluso maquinaria que son altamente eficaces e inocuas para el ser humano.

Target Tecnología, consciente de ello, ha apostado por la tecnología ultravioleta (UV-C), que permite eliminar virus, hongos y mohos de todo tipo de objetos a través de equipos portátiles y en un tiempo de exposición muy reducido. También los pasamanos y las escaleras mecánicas, que son elementos que tienen un riesgo alto de contagio, se pueden desinfectar con este sistema. Incluso los carritos portamaletas, las bandejas u otros objetos de alto uso en este tipo de instalaciones son aptos para su desinfección con luz ultravioleta.

El ozono es otro de los grandes aliados para desinfectar objetos y superficies en recintos cerrados. Con una eficacia del 99,9 por ciento, se trata de un sistema sencillo y económico tanto en su instalación como en su mantenimiento.

En el caso de los vehículos que llegan a través de ferris, una de las soluciones más eficaces para garantizar la seguridad son los túneles higienizadores, que a través de un sistema de rociado hidráulico son capaces de higienizar y desinfectar el exterior de los vehículos de manera rápida e inocua.

Prevención

Como hemos indicado anteriormente, la seguridad es fundamental no solo para proteger las mercancías legítimas, sino también para prevenir los delitos y los ataques terroristas.

Una de las tecnologías que sin duda despuntará en materia de seguridad durante este año 2021 serán los drones para videovigilar los recintos portuarios. Equipados con cámaras, los drones autónomos y cautivos permitirán garantizar el correcto flujo de mercancías y ayudarán a detectar posibles actuaciones delictivas en zonas de difícil acceso para el personal de seguridad, ofreciendo garantías en la velocidad de respuesta y análisis de la situación.

En contrapartida, los drones utilizados de forma ilegítima o temeraria por parte de ciertos usuarios podrían presentar una amenaza y un riesgo para la instalación portuaria. Es aquí donde los C-UAS, o sistemas de detección, mitigación y control, entran en acción para salvaguardar la seguridad de dichas infraestructuras.

También las barreras contra vehículos suicidas serán tendencia en este año, y formarán parte del equipamiento habitual de seguridad para los puertos de nuestro país. Gracias a su sistema de fácil despliegue y traslado, garantizarán el bienestar de todas las personas que transitan a diario por el puerto, evitando escenarios desagradables con los que nos hemos encontrado en los últimos años.

Paquetes sospechosos

Y en relación con paquetes sospechosos, los sistemas móviles con equipamiento de rayos X integrado ofrecen grandes ventajas en la operativa aeroportuaria. Estos son de gran ayuda para inspeccionar estas posibles amenazas en cualquier ubicación del puerto.

Target Tecnología analiza de manera continua los nuevos retos y las nuevas tendencias en seguridad para las instalaciones portuarias, por lo que es capaz de ofrecer las mejores soluciones para garantizar la seguridad en este nuevo escenario. Durante más de 25 años hemos colaborado con los puertos españoles, aportando nuestra experiencia para ofrecer soluciones siempre a la vanguardia tecnológica y a la altura de las nuevas amenazas. Por ello, siempre es nuestra prioridad dar las mejores soluciones adaptadas a las necesidades y peculiaridades de cada uno de los puertos de nuestra geografía.

Gestión de Cuadrantes

FICHAJE DE ENTRADAS Y SALIDAS

CONTROL DE ACTIVIDAD

C/María Zambrano 26
Oficina 3
28981 Parla
Madrid

MILSON
INGENIERÍA

www.milson.es
info@milson.es
+34 644 383 016
+ 34 686 079 578

Víctor Carlos Rubio Faure

Jefe de la División de Protección Portuaria del Puerto de Huelva

"La mayor dificultad a la que se enfrenta un puerto en cuanto a riesgos es el control de la lámina de agua"

Por Juanjo S. Arenas. / Fotos: Puerto de Huelva.

Casi 30 millones de toneladas de mercancía y 2.381 escalas. Estas fueron las cifras más reseñables sobre la actividad del Puerto de Huelva en 2020, aunque han descendido respecto al año anterior debido al coronavirus. Una actividad frenética que debe realizarse con todas las garantías a nivel de seguridad. Al frente de la seguridad física de este puerto se encuentra Víctor Carlos Rubio, quien comenta cómo es la gestión de esta instalación desde el punto de vista de la protección.

El Puerto de Huelva se encuentra entre los siete de mayor volumen de tráfico de España. ¿Cuáles son las instalaciones con la que cuenta concretamente? ¿Qué volumen de mercancía maneja y cuántos buques recibe al cabo del año?

El Puerto de Huelva dispone de cuatro muelles de uso público, destinados a mercancía general, graneles sólidos, mercancía rodada y contenedores. Concesionados, hay una terminal de graneles sólidos y nueve terminales, pantalanes para graneles líquidos y una monoboya de descarga de crudo.

En el pasado ejercicio se manipularon 29,9 millones de toneladas de mercancía, aproximadamente un 11 por ciento menos que en 2019. El motivo de esta bajada es, principalmente, la caída de las importaciones de crudo y del consumo de refinados por las razones que todos conocemos. Sin embargo, la variación no ha sido tan pronunciada como en otros puertos. Nos encontramos en quinta posición en el sistema portuario estatal por volumen de mercancías.

Respecto a los buques recibidos, en 2020 tuvimos 2.381 escalas.

La gestión de la seguridad física del Puerto de Huelva se ubica en la División de Protección Portuaria que usted dirige. ¿Cómo está organizado el departamento y de quién depende organizativamente?

En este puerto, la División de Protección Portuaria depende funcional y organizativamente del Departamento de Explotación, y este de la Dirección.

De la División cuelgan, podríamos decir, tres pilares. El primero es la administración, actualmente ocupada por una persona dedicada a la revisión de planes, auditorías, planificación de simulacros, etc. y por otra focalizada en

la gestión y admisión de mercancías peligrosas. Otro pilar sería el Centro Portuario de Control de Servicios, que comparte funciones y responsabilidades con la División de Operaciones y Servicios Portuarios. El tercer pilar es la Policía Portuaria.

La seguridad de los sistemas de información del Puerto de Huelva depende del Departamento de Tecnología. ¿Cómo colabora su división con este departamento?

Deberíamos darle la vuelta a la pregunta: ¿cómo colabora el Departamento de Tecnología con la División de Protección Portuaria? En este caso, la colaboración es excelente, ya sea en la redacción, seguimiento y control de proyectos de iniciativa propia de la División o aquellos requeridos por otras administraciones competentes o a la hora de aportar soluciones tecnológicas a cualquier cuestión planteada desde el ámbito de la protección.

Tampoco debemos olvidarnos de la excelente implicación de la División de Conservación, Instalaciones y Operaciones Terrestres y del Área de Infraestructuras a la hora de abordar los proyectos relativos a la protección.

Los puertos han mantenido su actividad en todo momento pese a la pandemia debido a que están categorizados como servicio esencial. ¿Cómo se ha adaptado el Puerto de Huelva a convivir con el coronavirus? ¿Qué medidas de seguridad han implementado al respecto?

La adaptación fue rápida y básicamente organizativa. En lo que respecta a la Autoridad Portuaria, disponemos de una base tecnológica lo suficientemente capaz y protegida para soportar el trabajo no presencial sin ningún problema reseñable.

Los prestadores de los servicios portuarios, prácticos, amarradores y remolcadores encapsularon los turnos al objeto de mantener las tripulaciones y sus relevos estancos. Lo mismo hicieron los operadores de las terminales y la Policía Portuaria.

Por otro lado, cabe destacar que se han prohibido las reuniones presenciales. También se han colocado controles de temperatura en los accesos a las oficinas y dispensadores de desinfectante en todas las entradas, se ha separado mediante señalética el flujo de personas, se han colocado mamparas en los puestos de trabajo presenciales, se ha reducido el número de compañeros por despacho habilitando nuevas dependencias para tal fin, se ha reforzado el servicio de limpieza con la desinfección de los equipos de trabajo y de los vehículos para cada cambio de turno y se ha instaurado el uso obligatorio de mascarillas.

¿Qué otro tipo de operaciones son más complejas de gestionar en un puerto en lo que a términos de seguridad y protección se refiere?

Respecto a la seguridad, hay que tener en cuenta que las operaciones con mercancías especialmente sensibles se realizan en terminales altamente especializadas. Además, en el Puerto de Huelva

no hay interacción entre las terminales para mercancías peligrosas, en nuestro caso pantalanes, con los muelles de uso público. Por tanto, la única complejidad que podríamos mencionar es que depende intrínsicamente de la naturaleza de la mercancía manipulada.

De acuerdo con esto, en el momento que la "mercancía" son personas, se complica la operativa: controles e inspección de transbordo rodado, delimitación de flujos de entrada y salida, segregación entre pasaje a pie y vehículos, delimitación de áreas de preembarque, impermeabilidad con el resto de la instalación portuaria, etc.

En su opinión, ¿cuáles son las principales claves para mantener un puerto seguro?

Puntualizando, para un puerto protegido, destacaría el control exhaustivo de su perímetro y de sus accesos disponiendo de medios de protección físicos eficaces, medidas organizativas y procedimentales; una Policía Portuaria comprometida y formada; una relación fluida con las Fuerzas y Cuerpos de Seguridad del Estado; y un Departamento de Sistemas activo.

Actualmente es impensable hablar de protección sin incluir la ciberseguridad. Por tanto, no nos podemos olvidar de disponer de recursos y, sobre todo, del compromiso institucional que hay en el Puerto de Huelva respecto a la protección integral.

De todos los riesgos a los que se enfrenta un puerto, ¿cuáles le preocupa más?

Si hemos hecho bien la tarea no debería preocuparnos especialmente nada en particular. Y si me preocupara alguno no lo diría abiertamente. Aunque no sería una debilidad indicar que la mayor dificultad que se nos plantea es la vigilancia y control de la lámina de agua.

El Puerto de Huelva es el más extenso de España, con 1.700 hectáreas, y tiene una distribución lineal. Desde la bocana hasta la última instalación portuaria hay unos 21 kilómetros, y está ubicado en el entorno de la confluencia de un complejo sistema de rías y marismas: las de los ríos Odiel y Tinto.

> "Para mantener un puerto protegido, algunas de las claves son controlar su perímetro y accesos y contar con una Policía Portuaria comprometida"

En cualquier instalación, el buque atracado hace de apantallamiento para los sistemas de vigilancia CCTV. En el caso del Puerto de Huelva, las terminales se ubican en la margen izquierda de la ría, siendo la margen derecha desde donde se pudiera vigilar la lámina de agua y el atraque, un parque natural en el que solo hay infraestructura de comunicaciones y de energía en una pequeña franja.

Además de lo anterior, añadiría la dificultad para proteger las áreas de fondeo. Su vigilancia es complicada por su naturaleza. Es inviable mantener un control de acceso y un seguimiento a embarcaciones que no sean de tráfico comercial en un nivel normal de protección.

Teniendo en cuenta todo esto, ¿con qué recursos y tecnologías de seguridad cuenta el Puerto de Huelva? ¿Qué tecnologías tendrán más importancia en el devenir de la protección marítima y portuaria?

Actualmente, y ciñéndonos al núcleo del negocio del puerto, hablamos del Puerto Exterior. Con una longitud de aproximadamente nueve kilómetros, disponemos de diferentes tipos de vallado perimetral y de dos kilómetros de vallado sensible de alta seguridad cuya sensorización antiintrusión está integrada en el propio vallado. Este vallado detecta el corte y la escalada sin necesidad de alcanzar la cumbre del mismo.

El resto del cerramiento está dotado de cable sensor que detecta el corte, la escala o el arrastre, siendo capaz de localizar geográficamente la intrusión con un margen de error de tres metros.

Además de la sensorización del cerramiento, disponemos de un sistema de cámaras que garantiza la total cobertura del perímetro. Este sistema tiene la capacidad de detectar intrusos en cualquier situación de luz, temperatura y condición climatológica; y está formado por cámaras domo con resolución HD y *zoom* óptico para la monitorización y seguimiento y cámaras térmicas con capacidad de reconocimiento de hasta 250 metros con capacidad analítica de vídeo.

El CCTV monitoriza en tiempo real y realiza grabaciones de vídeo continuas bajo demanda o automáticamente mediante la asociación con el sistema de detección perimetral. Asimismo, es capaz de realizar análisis forense de incidencias *a posteriori* y genera una alarma ante un determinado evento mediante la aplicación de los algoritmos de detección de movimiento.

Para la vigilancia, además de las cámaras reseñadas, disponemos de cuatro móviles de tecnología dual, óptica y térmica con un alcance de 2.500 metros.

Para las condiciones más duras.

Esta cámara PTZ de alta resistencia cumple con el estándar militar MIL-STD-810G, lo que garantiza un funcionamiento confiable en condiciones climáticas extremas y puede soportar vientos de hasta 245 km / h (152 mph). Con la carcasa con clasificación IK10 resistente al vandalismo y las clasificaciones IP66 / IP68, puede estar seguro de que la carcasa de la cámara es resistente tanto a condiciones climáticas adversas como a impactos.

- HDTV 1080p con zoom 30x
- IR optimizado de largo alcance (rango de 400 m / 1300 pies)
- Sensor de 1/2 "para alto rango dinámico
- Análisis de AXIS Guard Suite
- Axis Zipstream y Axis Lightfinder

www.axis.com/es/products/axis-q6215-le

AXIS COMMUNICATIONS

Todo el sistema está soportado por anillo perimetral de fibra óptica que garantiza la redundancia en el supuesto de corte de la fibra.

Respecto a las tecnologías que tendrán más importancia en el futuro de la protección marítima y portuaria, creo que el salto cualitativo en cuestiones de seguridad vendrá de la mano de la tecnología 5G, la Inteligencia Artificial y los drones. Esta tecnología abre la puerta a una infinidad de posibilidades. Con las nuevas capacidades de reacción, velocidad, alcance y autonomía de drones híbridos se podrán vigilar zonas remotas, como las áreas de fondeo, caños y marisma. Estas capacidades de comunicación, junto con el desarrollo de la Inteligencia Artificial, podrán crear un modelo de aprendizaje que facilite o simplifique las funciones del operador de los sistemas de vigilancia.

Igualmente, se podrá seguir y gestionar el transporte de mercancías peligrosas o de cualquier otra en tiempo real. Incluso los buques podrán usar esta tecnología para comunicarse entre ellos y con sensores ubicados en las boyas o en cualquier otro sistema de balizamiento. Existen, por tanto, infinidad de posibilidades.

En la anterior Conferencia Sectorial de Seguridad en Puertos, celebrada en 2019, algunos ponentes señalaron la necesidad de modernizar el Real Decreto 1617/2007, por el que se establecen medidas para mejorar la protección de los puertos y del transporte marítimo, y de crear un Comité Nacional de Protección Marítima. ¿Qué opinión tiene al respecto?

> "El salto cualitativo en cuestiones de seguridad portuaria vendrá de la mano de la tecnología 5G, la Inteligencia Artificial y los drones"

Creo que sería un gran avance a la hora de armonizar procedimientos y sistemas de protección para cada tipo de instalación a nivel estatal. Eso sí, siempre que sea lo suficientemente amplia la representación del Comité para que abarque la mayoría de las tipologías de los puertos y existan comités locales con la capacidad suficiente para que puedan afinar los requerimientos a situaciones particulares de cada puerto o instalación.

Aligeraría bastante tanto la carga de trabajo como los trámites para aprobar las revisiones y la actualización de los planes de protección.

Predator Radar

Cámara HD PTZ "todo en uno"

Vigilancia de seguridad y detección de intrusos en grandes superficies

Predator Radar de 360 Vision Technology es una exclusiva cámara HD PTZ con radar integrado "todo en uno", con capacidad para vigilar de forma continua y detectar automáticamente múltiples objetos o personas de forma simultánea.

Predator Radar, es un dispositivo de seguimiento de 360 grados controlado por radar altamente rentable que puede funcionar incluso en condiciones meteorológicas extremas, con una cobertura de 400 metros.

Las prestaciones avanzadas de Predator Radar, lo hacen ideal para aplicaciones de alta seguridad como puertos, protección de perímetros, zonas estériles, fronteras, aeropuertos y emplazamientos militares.

Para obtener más información sobre las soluciones de cámaras radar de 360 Vision Technology, para la seguridad, la protección y la gestión eficaz de sus instalaciones críticas, contacte con Sicuralia hoy mismo.

360VISION TECHNOLOGY

Sicuralia

+34 916 621 688 comercial@sicuralia.com www.sicuralia.com

Tecnología de radar para la **vigilancia de la seguridad**

Mark Rees
Managing Director de 360 Vision Technology

Antonio Pereira
Director técnico de Sicuralia

El fabricante británico 360 Vision Technology fabrica soluciones de videovigilancia líderes en el mercado para supervisar la seguridad y la detección de intrusos. Estas soluciones son distribuidas en España a través de Sicuralia.

Su innovadora tecnología de radar, Radar Predator, puede ser utilizada en aplicaciones de videovigilancia, seguridad y control tales como detección de intrusión, drones en vuelo, conteo de vehículos, monitorización de atascos, pasos a nivel, seguimiento de personas y de vehículos, etc.

Cómo funciona

El radar transmite una señal FMCW para determinar con precisión la posición y el alcance de un objeto, midiendo el tiempo que tarda la energía de radio en ser reflejada y devuelta. De este modo, los sistemas de radar pueden calcular de forma instantánea y precisa la distancia y la posición de un objetivo.

Además, basándose en la cantidad de energía reflejada, se puede calcular una magnitud para cada objetivo que permitirá al *software* incorporado determinar el tamaño exacto y la identidad de los intrusos detectados.

Cámara "todo en uno"

La exclusiva solución compacta Radar Predator de 360 Vision Technology es una cámara PTZ controlada por un radar de 360 grados "todo en uno". Tiene seguimiento automático y capacidad de detectar y vigilar continuamente los objetivos, incluso cuando está enfocada hacia otro lugar.

El sistema integrado Radar Predator utiliza una tecnología de iluminación inteligente de alta calidad e intensidad, dedicando luz blanca para el seguimien-

to visible al ojo humano e infrarrojos para el seguimiento electrónico.

Diseñado para aplicaciones de alta seguridad en las que la detección rápida de objetos o individuos es vital, como puertos, prisiones, fronteras, aeropuertos y emplazamientos militares, Radar Predator puede rastrear múltiples objetivos simultáneamente con 400 metros de cobertura.

Radar Predator está optimizado para una instalación sencilla y rápida, con una configuración mínima. Y gracias a la posibilidad de elegir entre una cámara de videovigilancia HD de muy baja luminosidad y una unidad de radar integradas, no se necesitan servidores ni *software* para su puesta en marcha.

Radar contra videoanálisis

El radar tiene la ventaja de recopilar información de un mapa tridimensional de una escena con alta resolución. Por el contrario, los sistemas basados en la analítica toman decisiones de alarma basadas en una pantalla bidimensional y en píxeles individuales. Por tanto, no son tan precisos a la hora de identificar objetos y de seguir sus movimientos.

Al comparar los precios de las cámaras de vídeo con el coste de las alternativas de radar, es importante tener en cuenta el coste total de instalación y mantenimiento de un sistema. Las unidades de radar cubren una distancia mínima de 400 metros y pueden estar distribuidas. Las cámaras basadas en el análisis de vídeo suelen requerir una separación de entre 60 y 80 metros, lo que significa que se necesitan cinco veces más cámaras de vídeo en comparación con los sistemas de radar para cubrir la misma zona.

Por lo tanto, en cuanto a los costes de infraestructura e instalación, un sistema de radar es más rentable, ya que requiere cinco veces menos cableado, energía, equipos de comunicación y mano de obra para su instalación.

Radar Predator funciona en escenarios de humo, fuego, niebla e incluso en condiciones meteorológicas extremas. Es IP68, manteniendo un máximo grado de funcionalidad y fiabilidad.

Por otro lado, utiliza protocolo ONVIF y es compatible con plataformas PSIM o VMS como Situator, Cayuga, Ocularis, Genetec, Avigilon, Milestone, etc. Dispone, además, de conectividad 4G, 5G y GPRS, y puede ser personalizado mediante color y efectos estéticos y de camuflaje.

En la actualidad, las soluciones de cámaras Radar Predator de 360 Vision Technology contribuyen a la seguridad y a la gestión eficaz de alta seguridad en todo tipo de infraestructuras críticas.

Las amenazas submarinas en las infraestructuras críticas

Eduardo Ruiz Pérez
Responsable comercial y de Desarrollo de Negocio del Mercado Civil y Seguridad de Saes

La preocupación por el desafío que suponen las amenazas asimétricas en el entorno marino para los campos de seguridad y defensa ha crecido internacionalmente. La amenaza de sabotaje a buques amarrados, a puntos de carga de gas e hidrocarburos y a las propias instalaciones portuarias por intrusiones desde la lámina de agua es un riesgo con un alto nivel de impacto para la propia infraestructura.

Hechos como el atentado contra el USS Cole en octubre de 2000 marcaron un antes y un después en la evaluación de estas amenazas. Perpetrado por una lancha que se aproximó al costado del buque fondeado en un puerto que se consideraba seguro, supuso la muerte de 17 miembros de la tripulación. Además, 30 personas sufrieron heridas de diversa consideración, aparte de los desperfectos ocasionados al buque.

Más recientemente, los sucesos de mayo y junio de 2019 en el Golfo Pérsico volvieron a recalcar los efectos de la amenaza asimétrica submarina para el tráfico marítimo. Un primer suceso, en mayo, cuando dos petroleros saudíes resultaron dañados por una aparente acción de sabotaje, se vio seguido por un segundo ataque contra otros dos petroleros (de propiedades noruega y japonesa). Aunque se llegó a mencionar la posibilidad de que el ataque fuera cometido por armamento naval (torpedos o minas navales), las características 'quirúrgicas' del daño hicieron más plausible que se produjera por la acción de minas lapa; un tipo de explosivo que se adhiere mediante imanes al casco del buque por buceadores de operaciones especiales. Esta hipótesis se vio reforzada por la detección, por efectivos de la Marina estadounidense, de dispositivos de este tipo adosados a otros buques.

> Incluso un explosivo improvisado de poca potencia podría ocasionar en un buque amarrado o fondeado daños que afecten a su maniobra

Riesgos del sabotaje

Aun cuando los hechos indicados anteriormente puedan parecer lejanos y ubicados en zonas 'calientes', no se puede desdeñar la amenaza terrorista en el territorio español y europeo.

Incluso un explosivo improvisado de poca potencia podría ocasionar en un buque amarrado o fondeado daños que afecten a su maniobra o que obliguen a su inmovilización en puerto, produciendo riesgos para el propio buque, para la navegación en la dársena afectada o para el bloqueo del punto de atraque.

Los puntos de carga y descarga de gas e hidrocarburos precisan de altos requerimientos de seguridad para evitar el sabotaje de estas instalaciones, por el riesgo de incendio y explosión. También para los enseres y las personas, así como para evitar daños al medioambiente por vertido de hidrocarburos.

Otras instalaciones críticas susceptibles de ser víctimas de la amenaza acuática son las centrales energéticas (tomas de agua de refrigeración), instalaciones *offshore* de gas y petróleo e instalaciones hidroeléctricas.

En resumen, riesgos de daños materiales a buques e instalaciones, daños económicos por la parada de actividad y riesgo para la vida de los operarios de estas infraestructuras.

Otro elemento que considerar en la vigilancia de las instalaciones portuarias y el tráfico marítimo es la actividad del narcotráfico que emplea, cada vez con mayor asiduidad, nuevos medios. Entre estos medios se encuentran cargas adosadas a los cascos de los buques (por

medio de buceadores sin conocimiento de la tripulación), embarcaciones de alta velocidad e incluso embarcaciones semisumergidas (conocidas como narcosubmarinos). Estas actividades entrañan riesgo para el tráfico marítimo y para la operación de las instalaciones portuarias.

La protección

Las amenazas de índole acuático (superficie o submarino) hacen necesario extender a este medio (la **lámina de agua**) la protección que puertos y otras infraestructuras han aplicado a nivel de seguridad perimetral terrestre en consonancia con las normativas de protección de infraestructuras críticas y estratégicas, de ámbito europeo, o de protección de buques e instalaciones portuarias, de carácter internacional.

Para vigilar el acceso marítimo en superficie existen diversos sistemas de protección perimetral que pueden aplicarse directamente o con adaptaciones:

- **Sistemas de videocámaras**: requieren adaptación a la vigilancia de la lámina de agua para evitar, por ejemplo, efectos adversos del oleaje. Tienen una mayor efectividad en zonas de proximidad.
- **Sistemas radar**: originalmente orientados a sistemas de control de tráfico marítimo, suelen presentar mayor cobertura que los sistemas de vídeo, en acimut y distancia, además de mayor ventaja a distancias lejanas.
- **Barreras físicas**: están especialmente diseñadas para detener pequeñas embarcaciones de superficie. Presentan el inconveniente de limitar también el movimiento de embarcaciones autorizadas, requiriendo sofisticados sistemas de puertas móviles o una limitación a áreas concretas.

Para vigilar el acceso marítimo vía submarina, la protección requiere de sistemas menos usuales:

Vehículo de superficie Vendaval de Navantia desplegando sensores submarinos.

- **Barreras de protección submarina**: con ventajas e inconvenientes similares a los anteriormente descritos.
- **Sistemas de inspección de cascos/fondos**: como sonares de barrido lateral, remolcados por buques o incluso por un vehículo submarino no tripulado (USV). Permiten localizar objetos en los fondos marinos, facilitando la detección de obstáculos que puedan afectar a la operación del puerto en sus canales o en las zonas de aproximación o fondeaderos próximos.
- **Sonares de alta resolución**: facilitan la detección de objetos adosados a buques, desplegados desde un medio de superficie (lancha o USV). Tanto en este caso como en el anterior, es importante destacar que mediante técnicas avanzadas de procesamiento de señal se puede detectar automáticamente la presencia de objetos potencialmente peligrosos (cargas que puedan desprenderse o artefactos explosivos).
- **Sonares de detección de buceadores**: son sonares de alta frecuencia diseñados específicamente para la protección contra amenazas submarinas de baja detectabilidad por medios pasivos, como el caso de buceadores, y en entornos de un alto nivel de ruido ambiente. De reducido tamaño, facilitan tanto el montaje fijo a instalaciones estáticas (muelles o plataformas *offshore*) como el despliegue portátil desde buques fondeados o por el costado de buques amarrados a muelles.
- **Vehículos autónomos**: se trata de un elemento complementario que amplía las posibilidades de despliegue de sensores y sonares, permitiendo desplazar estos a una zona más próxima a la amenaza detectada y facilitando su identificación y una posible actuación sobre ella.

La diversidad de sensores de superficie y submarinos necesarios para proteger la lámina de agua invita a su integración en sistemas de seguridad multisensor con características específicas para este medio. Diversas empresas ya están trabajando en estas integraciones para complementar los sistemas de seguridad perimetral de superficie, ampliar su cobertura añadiendo la vigilancia submarina y no dejar ninguna fisura a la seguridad de las instalaciones.

Seguridad integral **en los entornos portuarios**

Víctor M. Hernández Segovia
Director técnico de Eulen Seguridad

Desde tiempos inmemoriales, los puertos marítimos han sido elementos clave en el desarrollo de una sociedad, propiciando su crecimiento económico y comercial y dando satisfacción a las necesidades de suministro de una ciudad. Es evidente que los puertos marítimos, siguen siendo un factor esencial para la sociedad, lejos de mermar su actividad, cada vez cobran más importancia. Hoy en día, el transporte marítimo sigue siendo el medio más eficaz en el traslado de mercancías.

La definición de puerto marítimo queda perfectamente clara en el Real Decreto Legislativo 2/2011, de 5 de septiembre, por el que se aprueba el Texto Refundido de la Ley de Puertos del Estado y de la Marina Mercante. Se denomina puerto marítimo al "conjunto de espacios terrestres, aguas marítimas e instalaciones que, situado en la ribera de la mar o de las rías, reúna condiciones físicas, naturales o artificiales, y de organización que permitan la realización de operaciones de tráfico portuario, y sea autorizado para el desarrollo de estas actividades por la Administración competente".

De lo anterior, es necesario saber qué implica el tráfico portuario. La citada norma lo define como "las operaciones de entrada, salida, atraque, desatraque, estancia y reparación de buques en puerto y las de transferencia entre éstos y tierra u otros medios de transporte, de mercancías de cualquier tipo, de pesca, de avituallamientos y de pasajeros o tripulantes, así como el almacenamiento temporal de dichas mercancías en el espacio portuario".

Más allá del tipo de puerto y atendiendo a su clasificación desde distintos puntos de vista, un puerto marítimo aglutina gran cantidad de infraestructuras y servicios donde distintos actores, públicos y privados, gestionan, explotan y desarrollan las actividades que se prestan desde estos. Algunos de dichos agentes que desarrollan su actividad en mar o tierra pueden ser: prácticos, consignatarios, remolcadores, amarradores, empresas estibadoras, aduanas, astilleros y talleres, cargadores, depósitos comerciales, etc. Además están todos los colaboradores que prestan servicios a los primeros. Estamos ante un gran colectivo, la comunidad portuaria, que engloba la gran variedad de sectores de producción y servicios que desarrollan su actividad en torno a un puerto marítimo.

Lo cierto es que los puertos tienden cada vez más a integrarse en las cadenas logísticas de producción, transporte y distribución, y a convertirse en auténticos centros de valor añadido. De este modo, no solo son parte de la cadena del transporte, sino que forman un entorno productivo y logístico de gran importancia, en el que se desarrollan distintas actividades industriales, turísticas, de negocios, entre otras, que van más allá de las actividades más tradicionales.

Teniendo todo esto en cuenta, a nadie extraña que los puertos sean puntos estratégicos en el actual sistema de producción, de transporte y de comercio nacional y mundial. Como nexo estratégico, es un sector fuertemente regulado.

Amplia regulación

De la normativa específica de seguridad aplicable a puertos marítimos y a las instalaciones portuarias, existen dos normas que actúan como eje sobre el que se sustenta su protección y la disponibilidad de los servicios que presta: el Código Internacional de Protección de Buques e Instalaciones Portuarias (Código ISPS) y la Ley 8/2011, en la que se establecen medidas para la protección de las infraestructuras críticas (Ley PIC). Estas normas, aplicables a todos los puertos, incluyen los campos comúnmente denominados como *safety, security* y ciber. Esto implica que para que la seguridad de un puerto sea realmente eficaz y eficiente debe abarcarse de una forma integral, pudiendo así crear

un cultura de seguridad global en toda la comunidad portuaria y optimizar los recursos y esfuerzos, así como facilitar una coordinación entre todos los agentes involucrados.

Cada puerto tiene unas características que lo hacen diferente a otro y, por tanto, la estrategia de seguridad puede ser distinta. Estas características no solo tienen que ver con aspectos geográficos, orográficos y constructivos, también son diferentes por los servicios que se prestan, por su gestión o incluso por lo avanzados que estén en el ámbito tecnológico respecto a otros. Otra tendencia que afecta a la estrategia de seguridad es la de acercar el puerto a la ciudad; el hecho de que la población sienta que es una extensión más de su localidad está cobrando cada vez más importancia. Para llevar esto a cabo no se puede "bunkerizar" un puerto, se necesitan medidas de protección más transparentes al ciudadano y que en un momento dado se puedan activar para proteger ciertas áreas más críticas.

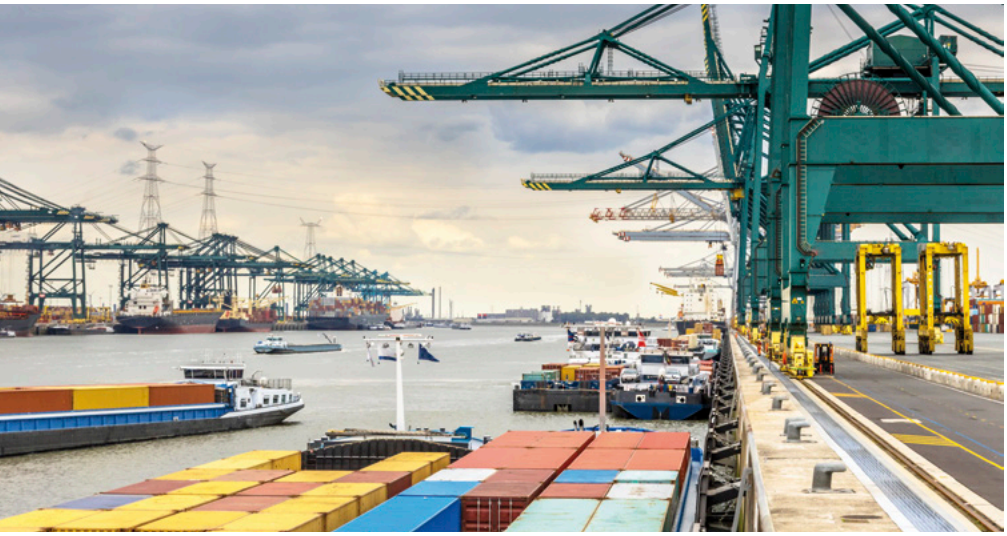
Principios de actuación

Teniendo en cuenta lo anterior, la protección debe adaptarse a cada caso concreto; es decir, a su contexto interno y externo. No obstante, hay una serie de medidas básicas que atienden a una estrategia de seguridad en profundidad sobre la que todos los elementos, en mayor o menor medida, se sustentan. Al final, independientemente de la singularidad de cada puerto, el propósito de todos es hacer de él una infraestructura segura donde la comunidad portuaria pueda operar con todas las garantías de seguridad.

Para ello se pueden seguir los siguientes principios de actuación:

- **Disuasión:** disposición de un conjunto de elementos de protección, varios de ellos visibles, para contribuir a reducir la motivación de los atacantes para materializar las amenazas a las que está expuesto.
- **Prevención:** Dotación de medios para permitir la observación, vigilancia y control de la infraestructura, al objeto de prevenir y evitar el acceso de personas, vehículos y materiales no autorizados al interior de las mismas. Al mismo tiempo, estos sistemas deben permitir el acceso controlado a las distintas zonas del puerto de acuerdo con jerarquías de accesibilidad previamente establecidas.
- **Detección y evaluación:** disposición de medios humanos y técnicos para detectar con antelación cualquier intento de intrusión en la infraestructura, así como para evaluar las condiciones, circunstancias y capacidades de los atacantes.
- **Retardo:** implantación de barreras físicas cuyas características constructivas y de diseño impidan o retarden una intrusión, de modo que el tiempo requerido para que los intrusos puedan alcanzar las áreas críticas sea significativamente superior al tiempo necesario para su localización e interceptación por el servicio de vigilancia propio y el apoyo externo.
- **Respuesta:** conjunto de recursos humanos estructurados jerárquica y funcionalmente y medios organizativos, para proporcionar la capacidad de reacción necesaria, suficiente y proporcionada para impedir los accesos no autorizados, neutralizar los intentos de intrusión en las instalaciones y evitar o dificultar la materialización, con carácter general, las amenazas a las

Hay una serie de medidas básicas que atienden a una estrategia de seguridad en profundidad sobre la que todos los elementos se sustentan



que está expuesto, poniendo a disposición de la autoridad competente, en su caso, a los posibles infractores.

- **Coordinación con las Fuerzas y Cuerpos de Seguridad del Estado (FCSE):** establecimiento de la práctica de coordinación (información, comunicación y petición de apoyo) con las FCSE, tanto en situación de normalidad, prevención, como en situaciones de contingencia.

Medidas de seguridad

Cabe destacar que cualquier estrategia de seguridad, en líneas generales, debe responder a los resultados de un análisis de riesgos realizado de forma correcta, teniendo en cuenta todas las particularidades mencionadas del puerto objeto de análisis, así como las partes interesadas y su cultura en gestión del riesgo. Ahora bien, como medidas de seguridad base se pueden citar las siguientes:

- **Controles de acceso:** son un elemento clave en un sistema de seguridad, que cada día cuenta con mayor implantación cuando se busca controlar y disponer de un registro de las personas que acceden y a qué hora lo hicieron. Además de facilitar un acceso controlado, permite impedir el no autorizado.
- **Seguridad perimetral:** compuesto por medidas pasivas y activas: vallados, CCTV o intrusión, entre otros. Aquí la decisión de optar por unos sistemas u otros ya depende de múltiples factores como pueden ser la extensión, la superficie o área a proteger, la climatología o los recursos disponibles por citar algunos.
- **Vigilancia y respuesta tanto por tierra como por mar:** la presencia física de personal debidamente formado y cualificado para el control, vigilancia y respuesta es una medida de seguridad muy eficaz que responde a todos los principios de actuación mencionados. Tampoco debe olvidarse que un puerto o una instalación portuaria están sujetos a unas amenazas concretas que no se dan en otros sectores como son aquellas que se aprovechan del mar. Por tanto, se deben implantar medidas de seguridad específicas en función del riesgo.
- **Procedimientos y protocolos de actuación para incidentes y emergencias:** que defina quién, qué, cómo, dónde y cuándo se debe actuar ante determinados escenarios, incluyendo aquellos relativos a la coordinación con las FCSE.
- **Un centro de control:** desde donde se controle y coordine todo el sistema de seguridad con sus subsistemas y donde se centralice la gestión y respuesta.

Ciberseguridad

Una cultura de la gestión del riesgo integrada implica que una organización sea dinámica, ya que las amenazas pueden aparecer, cambiar o desaparecer con los cambios en los contextos. Una gestión del riesgo anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna. Esto es fundamental, las amenazas a las que se enfrenta una instalación portuaria han cambiado mucho en los últimos años, y con la incorporación, cada vez más, de nuevas tecnologías, la ciberseguridad desempeña otros ámbitos de control muy importantes.

Las medidas de seguridad en este caso, no difieren de las anteriores. Se requieren controles de acceso a los sistemas, seguridad perimetral de la red ya sea interna o externa, control y vigilancia con una buena gestión de incidencias de ciberseguridad y haciendo uso, por ejemplo, de inteligencia de fuentes abiertas. También se requiere de protocolos y procedimientos aplicados a la ciberseguridad y un Centro de Operaciones de Seguridad (SOC) desde donde, al igual que ocurre en el mundo físico, se controle y coordine todo el sistema de ciberseguridad y se centralice la gestión y respuesta.

Lo cierto es que las instalaciones portuarias en general, ya sea por imperativo legal o como propia mejora en su cultura, han madurado mucho en seguridad. La cantidad de planes de seguridad de deben realizar, implantar, gestionar y mantener, no se pueden sostener sin una visión integral. Por este motivo, en la actualidad se está trabajando en la alineación de criterios entre protección portuaria, seguridad industrial, marítima, mercancías peligrosas, ciberseguridad, ambiental y toda la normativa que los regula.

evento virtual con traducción simultánea español-inglés

X Simposium Seguridad GAP

22, 23 y 24 de marzo

Inscripción gratuita

2021 Año de la cultura en seguridad de la aviación civil

Organiza

Grupo Aeroportuario del Pacífico

SEGURILATAM

Agencia Federal de Aviación Civil México

Colabora

Transportation Security Administration

IATA

ACI Airports Council International

aena

ICAO OACI ИКАО

Fundación Borredá

Patrocina

EXIMCO Protección Perimetral

25 años Grupo SSIA

EULEN Seguridad

INV

NUCTECH

SITA

Trablisa Servicios de Seguridad

Patrocina silver

itisa

LOCSA

Más información:
publicidad@borrmart.es

INSCRÍBETE »

Borrmart Eventos

Joan Bergadá

Director de Seguridad Corporativa de Global Technology

"Los puertos necesitan un cuerpo policial especializado, complementario al concepto de seguridad integral"

Por Enrique González Herrero

Tras más de 25 años en diferentes cuerpos policiales, Joan Bergadá se ha incorporado este año a la consultora Global Technology. Como él mismo señala, desde su nueva posición podrá aportar su experiencia en los proyectos relacionados con la seguridad corporativa de todo tipo de organizaciones. No obstante, su amplio bagaje como jefe de la Policía Portuaria de Tarragona, donde sirvió casi nueve años, le hacen especialmente conocedor de la protección portuaria. Analizamos con él la situación de estos entornos para conocer cuáles son sus principales retos en materia de seguridad.

Hasta el año pasado, usted era jefe de la Policía Portuaria del Puerto de Tarragona. ¿Cómo cambia la perspectiva al pasar a formar parte de una empresa proveedora?

Lo lógico es pensar que hay un cambio de perspectiva, pero en mi caso sigue siendo la misma. Después de más de 25 años asumiendo responsabilidades en el ámbito de la seguridad pública, y además en tres ámbitos diferentes como el de Mossos D´Esquadra, Policía Local en Cambrills y Policía Portuaria, lo veo así. Al final el objetivo es el mismo: la seguridad.

Estar en una consultoría como Global Technology me abre las puertas a vivir un proyecto muy motivador. Una de las cosas que más me motiva es seguir aprendiendo, seguir creciendo profesionalmente. Pero también me va a permitir poner toda la experiencia acumulada en el ámbito portuario a la disposición de administraciones, organizaciones y empresas.

¿Qué tipo de proyectos va a llevar a cabo en Global Technology para los puertos?

Con el desgraciado fallecimiento de Enrique Polanco González, el *core* de Global Technology sufrió un cambio, orientándose al servicio de la ciberseguridad. Pero Enrique Polanco Abarca cree en su empresa, evidentemente, y tiene un proyecto de expansión en varios ámbitos, entre los cuales está el refuerzo de la Dirección de Seguridad Corporativa.

Los servicios que ofrecemos no se alejan mucho de aquello que en su momento dibujó Enrique Polanco padre; es decir, todo lo que es protección del puerto, planes de protección, evaluaciones, apoyo a las instalaciones portuaria, etc. También comprende el ámbito de aplicación de la legislación PIC [protección de infraestructuras críticas], no solo en puertos, sino en cualquiera de los sectores estratégicos reconocidos por la Ley PIC.

Nuestra vocación es acompañar a los clientes en todo lo que haga falta: auditorías, consultoría, apoyo en la implantación de proyectos de seguridad, transformación digital, etc. En definitiva, poner a su disposición todo el conocimiento y experiencia que hemos acumulado durante todo este tiempo.

¿Cuál es el proceso que siguen para elaborar los planes de seguridad que requieren las autoridades portuarias?
Global Technology ya tenía una metodología implantada para realizar los planes, y lo que hemos hecho con mi llegada ha sido procedimentarla. Primero hacemos una propuesta al cliente y, una vez que la acepta y nos contrata, llevamos a cabo un primer intercambio de información, que necesitamos para iniciar la elaboración del plan. A partir de esa documentación, nos desplazamos al puerto para hacer un trabajo de campo en el que comprobamos *in situ* la situación y hacemos un análisis de riesgos y vulnerabilidades.

Luego realizamos un trabajo de gabinete analizando cada uno de los puntos vulnerables que hemos detectado, y empezamos a pensar cuáles son las contramedidas a implementar para paliar de forma rotunda los riesgos.

Una vez lo tenemos, lo plasmamos en un documento y nos reunimos con el cliente. Le presentamos el plan y le indicamos cuáles son sus partes débiles, cuáles son sus puntos fuertes y cuáles son nuestras propuestas de mejora. A partir de ahí, junto con los responsables de protección del puerto, vamos viendo todo y lo plasmamos en los documentos del Plan de Protección del Puerto.

Dada la multitud de planes de Seguridad que tienen que desarrollar los puertos. ¿Es posible integrarlos todos sin que haya contradicciones o carencias?
Ciertamente es una situación compleja de gestionar, pero prefiero utilizar la palabra coordinar en lugar de integrar. Cada plan aborda ámbitos diferentes (ciberseguridad, contaminación marítima, protección portuaria, autoprotección etc.), y además hay planes de superior entidad que vienen dados por el municipio, la autonomía o el Estado.

En este sentido, la normativa PIC ha aportado muy buenas herramientas o soluciones, como pueden ser la identificación de las Políticas de Seguridad y la constitución y desarrollo de los Comités de Seguridad Integral por parte de cada autoridad portuaria. Desde mi punto de vista, son ejes fundamentales en el engranaje de coordinación para cualquier tipo de crisis que afecte a más de un plan a la vez y que se produzca en un puerto. Esto permite el encaje en la gestión de los planes, y admite la posibilidad de mejora continuada en función de cada situación.

> "Es necesario que haya coordinación entre la normativa PIC y el Plan de Protección del Puerto, y que esta sea extensible a todos los puertos, sean o no operadores críticos"

¿Qué aspectos determinan si un puerto es seguro en base a sus riesgos y vulnerabilidades?
Inicialmente hay que identificar los elementos críticos de la instalación portuaria y qué sucesos les pueden afectar. Mediante el análisis y la evaluación de riesgos damos con el conjunto de amenazas y su nivel de vulnerabilidad. De esa evaluación nace el plan de protección, donde se contemplan los recursos, contramedidas, procedimientos, niveles de protección, etc.

Pero tanto o más importante es que exista una política de seguridad bien definida y que se cumpla. Una política en la que prevalezcan las medidas de prevención y de previsión, que sean acordes a las amenazas y riesgos identificados, equilibrando la capacidad de respuesta a los posibles incidentes y su detección.

¿Cuáles diría que son las principales necesidades de los puertos españoles en materia de seguridad?
Como he comentado, creo que el Sistema PIC ha supuesto un buen avance para muchas organizaciones, colaborando en el aumento de la conciencia de la prevención y protección. También ha propiciado la paulatina profesionalización de los equipos directivos de seguridad. Sin embargo, creo que los puertos, a nivel general, continúan con un problema de falta de recursos operativos de seguridad especializados y sin la definición de un modelo concreto al respecto. Esta situación incide directamente en que no se pueda alcanzar la velocidad de crucero que nos exige el contexto actual de seguridad, y poder así situarnos en los niveles de los principales puertos europeos.

¿Cree que los servicios de seguridad privada podrían tener mayor cabida en puertos de la que tienen actualmente? ¿Podrían abordar funciones que hasta ahora no se cubren con este personal?
Creo que la respuesta es susceptible de herir sensibilidades, pero no deja de ser

más que una simple opinión basada en mi experiencia. Pienso que los puertos no tienen que ser diferentes al modelo de gestión de seguridad pública del Estado, donde la seguridad pública y la privada colaboran en casi todos los ámbitos.

Soy consciente que esta opinión puede sentar mal a algunos sectores de la parte social del puerto si solo se analiza superficialmente y no en el contexto más amplio en el que pretendo situar mi respuesta. Yo pretendo ir más allá y situarla en un contexto en el cual los recursos de la Administración no son infinitos, donde el puerto va creciendo, su actividad aumenta y se diversifica y las amenazas, cada vez más complejas, también se multiplican.

Ante este escenario, los puertos necesitan un cuerpo de seguridad especializado, totalmente complementario al concepto de seguridad integral que llevan a cabo las Fuerzas y Cuerpos de Seguridad del Estado. Disponer de este recurso ejecutor de funciones portuarias especializadas, el cual supondría una aportación de valor añadido a la gestión de la autoridad portuaria, también permitiría que la seguridad privada pudiera desempeñar funciones más básicas, pero no menos importantes, como el control de acceso, *handing*, gestión de equipajes, etc.

En términos generales, ¿qué propuestas haría usted para mejorar la seguridad portuaria?

Insisto en que la normativa PIC ha jugado un papel fundamental para mejorar lo que ya se contemplaba en el Real Decreto 1617/2007 sobre medidas de protección portuaria, donde cuestiones muy sensibles desde el punto de vista de la protección, como es la ciberseguridad, no se legislaban.

Dicho real decreto fue un gran avance en su momento, porque incorporó las recomendaciones del Convenio SOLAS convirtiéndolas en obligatorias; pero como

se ha visto, quedaba ámbito de mejora, recogido actualmente en la normativa PIC. Por ejemplo, no se abordaban aspectos fundamentales como las políticas de seguridad, los órganos de gobierno o los comités de seguridad integral.

Numerosas organizaciones no han desarrollado su política de seguridad o han constituido sus comités hasta que no han sido designadas operador crítico. Demostradas las bondades del sistema, creo que cabe hacer un análisis profundo y un esfuerzo en coordinar la normativa PIC con el plan de protección en aquellos puertos que por su naturaleza operativa no han sido designados operadores críticos, y así poder igualar los estándares de protección al conjunto del sistema portuario estatal.

¿Qué tecnologías despuntan actualmente en torno a la seguridad de los entornos portuarios?

En muy poco tiempo hemos visto como en la mayoría de los puertos se ha promovido el cambio al mundo digital. Pero, sin habernos beneficiado todavía de todas las ventajas de ese proceso, el mundo de la seguridad se encamina hacia otro gran cambio donde la Inteligencia Artificial desempeñará un protagonismo esencial. Todas estas permutas han requerido de una buena planificación, justificada en muchas ocasiones por la escasez de recursos humanos, además de una importante inversión económica. No obstante, en términos generales creo que se ha conseguido mejorar la efectividad persuasiva y preventiva del sistema.

Estamos a un pequeño paso de comprobar cómo la seguridad de los puertos empieza a beneficiarse de las ventajas que aporta la Inteligencia Artificial en gestión de sistemas de CCTV, control de acceso con reconocimiento facial, sistemas de reconocimiento de actitudes sospechosas, drones, sonares, etc.

Pero no podemos lanzarnos a este gran cambio sin contar con las personas que lo van a gestionar y que van a operar en estos ámbitos. Todos los componentes que engloban el puerto, tecnología y recursos humanos, tienen que crecer de forma paralela. No conseguiríamos una implementación exitosa de un sistema de seguridad y prevención si no contamos con el crecimiento, no en número, sino en calidad y competencias, de las personas que van a gestionar este nuevo escenario basado en la tecnología.

GLOBALTECHNOLOGY

Consultoría de Seguridad Global e Inteligencia

Seguridad Global
frente a la Amenaza Global

Especialistas en:

- *Planes de Seguridad del Operador*
- *Planes de Seguridad Específicos*
- *Planes de Seguridad Portuaria*

INFRAESTRUCTURAS CRÍTICAS

- **Análisis de Riesgos Globales.** Test de intrusión. Hacking ético.
- **Evaluaciones Integrales de Seguridad.** EPP - EPIP
- **Plan de Seguridad del Operador** PSO.
- **Plan de Protección Específico** PPE.
- **Inteligencia** Preventiva. **Alerta** temprana. **Apoyo** a la decisión.
- **Plan de Protección Portuaria.** PPP - PPIP

www.globalt4e.com

Mejores prácticas y soluciones integrales **de seguridad portuaria**

Jorge Sepúlveda Barrientos
Director de Marketing de Gunnebo Integrated Security

El desarrollo del sector del transporte marítimo, en los últimos años, ha ido acompañado de un importante crecimiento de las infraestructuras portuarias en todo el mundo, tanto en tamaño como en ocupación y tráfico de barcos, personas, vehículos y mercancías.

Como consecuencia, se plantea la necesidad de mejorar las medidas de seguridad y de implementar soluciones con alto contenido tecnológico y que protejan de manera integral las zonas críticas y más vulnerables de estas infraestructuras cada vez más complejas.

En un puerto se desarrollan una gran variedad de actividades según su tipología: de mercancías, pasajeros, industrial, logístico, pesquero, militar y/o deportivo, etc. En ellos, además, coexisten zonas lúdicas, comerciales y distintos emplazamientos administrativos y de representación. En definitiva, se tratan de un gran espacio formado por diferentes áreas con sus propias necesidades de seguridad.

Los últimos avances tecnológicos y la motorización de los procesos han marcado una tendencia hacia la innovación y hacia la incorporación de tecnología en los sistemas de seguridad de las infraestructuras portuarias.

Extensión perimetral

Una de las zonas críticas que requieren especial atención es la extensión perimetral del puerto y de sus accesos, tanto de vehículos como de peatones. En estos accesos es necesario implementar puertas de apertura y cierre rápido que mantengan el flujo dinámico de entradas y salidas de vehículos sin comprometer la seguridad. Estos accesos combinados con cámaras LPR permiten automatizar los procesos de entrada y reducir al mínimo los tiempos de espera.

Además, en áreas más sensibles, para reforzar la protección, se pueden combinar este tipo de puertas con bolardos hidráulicos u obstáculos escamoteables para blindarse contra tentativas de accesos no autorizados con vehículos de alto tonelaje.

Cubrir toda la extensión perimetral es una tarea compleja pero necesaria. Es por eso por lo que las soluciones de videoanálisis con cámaras térmicas brindan a los responsables de la seguridad portuaria información para identificar accesos no autorizados, gestionar de forma inmediata las alarmas y activar las medidas necesarias para reaccionar, en segundos, frente a cualquier intrusión.

El diseño de una estrategia de seguridad integrada y fiable se considera un elemento competitivo que le aporta valor al puerto

De esta manera, y con la implementación de todas estas soluciones, lograremos diseñar una arquitectura física y electrónica muy completa para proteger estos accesos en las zonas perimetrales.

En el interior del puerto identificamos recintos críticos que requieren medidas especiales de alta protección: CPD, salas de comunicaciones, centros de control, etc. De nuevo, la protección física en los accesos a estos recintos es fundamental. Existen diversas tipologías de puertas, esclusas y medidas de compartimentación para proteger estos recintos de diferentes riesgos: explosiones, deflagraciones, incendios y ataques balísticos y físicos.

Seguridad electrónica

Hasta aquí nos hemos centrado en el perímetro y en los accesos tanto perimetrales como internos a recintos críticos. Pero no menos importante es la implementación de soluciones de seguridad electrónica a lo largo de todo el complejo portuario de forma que automaticen y aseguren el cumplimiento de protocolos sin un esfuerzo extra por parte del personal de seguridad. Estas soluciones de seguridad electrónica deben ser rígidas en el cumplimiento de todas las políticas de seguridad y, a la vez, lo suficientemente flexibles para poder modificarlas y adaptarlas a los diferentes entornos de un puerto: desde la gestión de mercancías hasta la seguridad de los pasajeros.

En este sentido, la gestión de llegada de pasajeros y tripulación es un proceso que puede resultar incómodo y significar un incremento notable en el tiempo del personal de seguridad. Las soluciones de control de acceso nos permiten automatizar el alta de personas, integrándose con los diferentes sistemas del puerto. Si añadimos la gestión de los accesos usando las últimas tecnologías en reconocimiento facial, tendremos una solución que garantice y facilite el control de pasajeros.

Hoy en día existen equipos que cumplen la Ley de Protección de Datos sin tener que guardar ningún dato biométrico y mandando un código QR, encriptado e irreversible, con el vector biométrico a la persona dada de alta. Este proceso puede realizarlo el pasajero desde su teléfono móvil, evitando colas y esperas innecesarias.

Por último, no debemos olvidar la importancia de tener un centro de servicios de motorización que esté 24/7 controlando y protegiendo todo lo que sucede en el puerto y en su entorno. La gestión de este centro de control debe de ser manejada por un *software* que centre la atención del personal de seguridad solo en lo importante, en lo que realmente está ocurriendo. Existen plataformas de videoanálisis para centros de control en los que no es necesario visualizar todas las cámaras del recinto al mismo tiempo. Mediante Inteligencia Artificial se muestran únicamente aquellas cámaras en las que está realmente ocurriendo un evento.

Si bien es verdad que cada instalación dentro de una infraestructura portuaria requiere un análisis específico de sus necesidades en cuanto a seguridad y protección, es evidente que se está tomando conciencia y, cada vez más, se están implantando medidas integrales y de alto valor tecnológico. El diseño de una estrategia de seguridad integrada y fiable se considera un elemento clave en la gestión de un puerto y un elemento competitivo que aporta valor a este tipo de emplazamientos, tanto en la protección de sus activos como en la seguridad de los usuarios que transitan por sus instalaciones ofreciendo un entorno fiable y seguro.

El reto de la ciberseguridad **en los puertos**

Alberto Alonso Amores
Security Product Manager de Siemens

España es el país de la Unión Europea con mayor longitud de costa: cerca de 8.000 kilómetros. Además, en 2020 ocupó el undécimo puesto mundial en el Índice de Conectividad de Transporte Marítimo Regular, según las Naciones Unidas sobre Comercio y Desarrollo. En concreto, tres puertos (Valencia, Algeciras y Barcelona) están entre los 30 primeros en este índice. Pese a la caída de un 4,1 por ciento del comercio marítimo mundial provocada por la pandemia del COVID, el sistema portuario español cerró 2020 con algo más de 515,6 millones de toneladas movidas.

Los sistemas de seguridad física en puertos ayudan, sin duda, a que este comercio sea seguro para las personas y los bienes. Se ha avanzado mucho en la implantación de modernos sistemas de videovigilancia que incluyen analíticas de vídeo, así como en sistemas de detección de intrusos y control de accesos con las últimas tecnologías como el reconocimiento facial. Las técnicas de analítica de vídeo forense incluso permiten realizar un seguimiento de la actividad humana y de mercancías.

Amenazas

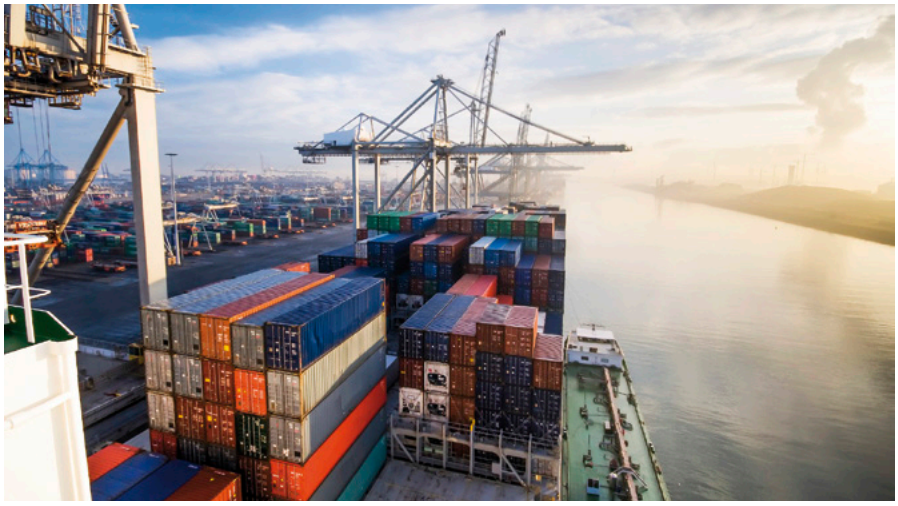
Sin embargo, y según nos recuerda la European Union Agency for Cyber Security, que en los últimos años ha colaborado estrechamente con los responsables de los puertos de la Unión Europea, existen otras amenazas a la seguridad que son más difíciles de ver y que requieren de nuevas medidas de protección.

Uno de los últimos incidentes ocurrió en 2020 en el puerto iraní de Shaid Rajaee. El 9 de mayo vio cómo sus sistemas de control de tráfico de buques, camiones y mercancías caían simultáneamente tras un ataque informático, provocando importantes congestiones del tráfico tanto marítimo como terrestre que se extendieron durante días.

Las motivaciones para estos ataques son diversas, no solo económicas en busca del pago de un chantaje por parte de la autoridad portuaria. Otros motivos van desde el ciberterrorismo hasta los ataques dirigidos entre países con tensiones políticas.

Los efectos de estos ataques pueden ser pérdidas financieras causadas por el bloqueo del puerto, el robo de información o el tráfico ilegal de mercancías y personas. Todo ello, con la consiguiente pérdida de reputación.

Así, aunque mucho se ha avanzado en los últimos tiempos en la ciberseguridad en puertos, siguen existiendo importantes retos que abordar. Entre ellos, la falta de



La ciberseguridad de los puertos es importante para completar la defensa mediante la protección de instalaciones, comunicación y dispositivos

personal formado y preparado para dar respuesta a estas amenazas o problemas presupuestarios para afrontar las medidas requeridas y la complejidad de gestión debido a la gran diversidad de entidades que participan en las operaciones portuarias. Considerando siempre que es necesario encontrar un balance entre la eficiencia del negocio y la seguridad.

En la parte tecnológica, un problema importante en las instalaciones portuarias es el elevado número de sistemas heredados, algunos de ellos con muchos años a sus espaldas, sin disposición de actualizaciones de *software* y con numerosas brechas de seguridad conocidas.

Especialmente críticos son los sistemas industriales compuestos, en gran parte, por controladores PLC que gestionan miles de sensores y actuadores y que han venido considerándose hasta hace no mucho como "cajas negras" que quedaban exentas de las medidas de protección informática.

En los últimos tiempos, estos sistemas tradicionalmente aislados han ido migrando a plataformas convencionales, con Linux o Windows, y se ha ido introduciendo TCP/IP en las redes de control. Esta evolución de los sistemas industriales ha provocado la aparición de una serie de vulnerabilidades que hasta hace poco eran desconocidas en estos entornos.

Para proteger estos sistemas es importante contar con dispositivos específicos orientados a la seguridad informática industrial.

Seguridad informática

Siemens dispone en su porfolio de una gama de productos especialmente diseñados para la seguridad informática en redes industriales. La amplia línea de dispositivos de red de Scallance y Ruggedcom entiende los protocolos de comunicación propios de los sistemas industriales y, a su vez, están preparados para trabajar en entornos hostiles.

Gracias a ellos es posible desarrollar el concepto de protección de célula, basado en el aislamiento mediante *firewalls* industriales de los dispositivos que no disponen de una funcionalidad propia de seguridad de red. Implementando distintas células aisladas y protegidas se reducen significativamente los riesgos de ataques a estos sistemas desprotegidos.

Asimismo, se pueden crear dentro de esta red áreas desmilitarizadas DMZ en las que situar los programas de explotación de la información generada por los sistemas industriales, aislando estos de la más vulnerable red de control. Sin olvidar el uso de cifrado de la información en red mediante IPSec o el cifrado de sistemas de ficheros y bases de datos.

Por otro lado, tan importante como proteger la instalación es reaccionar rápido para evitar nuevas amenazas o responder a ellas. En el portal Siemens-CERT y ProductCERT se publican al momento todas las vulnerabilidades conocidas en los productos de Siemens, así como los parches o procedimientos para su solución.

A su vez, Siemens ofrece servicios de monitorización de vulnerabilidades conocidas como Vilocity, en el que se avisa de los fallos de seguridad publicados de todos los sistemas de cualquier fabricante, herramientas para la búsqueda e identificación de problemas de seguridad como SiESTA y su servicio CustomerCERT, desde donde se ofrece una respuesta rápida ante cualquier incidente en las instalaciones de un cliente.

En definitiva, la ciberseguridad en puertos es un paso importante para completar el concepto de defensa en profundidad mediante la protección de instalaciones, redes de comunicación y dispositivos.

Seguridad en el acceso de pasajeros **con vehículos en el tráfico marítimo**

Julio Martín Hernández
Director Comercial de Excem Technologies

Según el Observatorio del Transporte y Logística en España, a partir de datos del *Anuario Estadístico del Sistema Portuario de Titularidad Estatal* (Puertos del Estado, actualización: diciembre 2019), el número de pasajeros gestionados en 2018 fue de aproximadamente 28 millones. De ellos, alrededor de cuatro millones (un 14,2% del total) adquirieron algún tipo de servicio de embarque de vehículos (los datos incluyen el tráfico comercial de los puertos del Sistema Portuario de Titularidad Estatal y el tráfico portuario de los puertos de las comunidades autónomas no incluidos en dicho Sistema).

Una de las grandes preocupaciones de las empresas del sector es la seguridad en procedimientos como el control de pasajeros a bordo de un buque de cruceros, el embarque o la estancia a bordo hasta su desembarque. Por ello, el desarrollo, investigación e implantación de sistemas de seguridad y control de pasajeros representan un importante capítulo en los gastos de explotación de los buques. El motivo es que los sofisticados elementos de seguridad de última tecnología son requeridos tanto a bordo de los buques como en los puertos, lo cual no solo supone un elevado coste por si mismo, sino que también conlleva costes derivados del personal necesario para su mantenimiento.

Los reguladores

El ámbito de la seguridad marítima está establecido a través de las directrices emanadas de la International Maritime Organization (IMO.) Se trata de una organización técnica con sede en Londres, creada en 1958. En la actualidad la componen 158 Estados miembros y dos miembros asociados. Desde su fundación, su misión consiste en elaborar un cuerpo completo de convenios, códigos y recomendaciones de carácter internacional para ser implantados por todos los Estados Miembros.

El órgano rector de la IMO es la Asamblea, que se reúne con periodicidad bianual. Entre esos periodos de sesiones, actúa como órgano rector un consejo integrado por 32 miembros que elige la Asamblea.

Como mecanismo regulador también se encuentran los Planes de Protección de Instalaciones Portuarias (PPIP), según los cuales los puertos están obligados a elaborar e implantar un plan de protección de todas sus instalaciones.

Sin normas específicas

A pesar de que existen órganos reguladores, hoy en día no hay normas específicas que regulen dichos planes; cada puerto los ejecuta de acuerdo con sus criterios y características propias. Por lo anterior, y con el ánimo de unificar la regulación a nivel internacional, se tomó la decisión de elaborar un instrumento que unifique criterios, pero sin formar parte de SOLAS (1914). Por ese motivo aparecen el Reglamento CE Nº 725/2004, la Directiva 2005/65/CE, el Real Decreto 1617/2007 y la Orden PCI/1188/2018. Estas normas están orientadas a la Administración Marítima (autoridad designada), los buques e instalaciones portuarias de trafico internacional, aunque no se ofrecen soluciones estándares (más allá de obligar a evaluar los riesgos para cada buque y cada instalación).

Cabe mencionar que en la actualidad no existe una regulación consolidada específica para evaluar la vulnerabilidad de los puertos. Por su parte, se espera la elaboración de un instrumento unificado que se presente en el futuro como propuesta para su estudio y posterior puesta en marcha por parte de las autoridades competentes.

Riesgos en buques de pasajeros

Las investigaciones efectuadas por el International Maritime Security (IMS) sobre la importancia de los riesgos en buque de pasajeros, clasifican dichos

buque de pasajeros, clasifican dichos riesgos según la siguiente prioridad: delitos contra las personas y propiedades, tráfico de drogas, polizones, piratería y terrorismo.

Por eso en todos los buques de cruceros existen obligatoriamente diversos planes de actuación donde se desarrollan e implantan acciones dirigidas su aplicación en situaciones excepcionales y de emergencia.

En los accesos al buque se intensifica al máximo el control e identificación de pasajeros. Por ejemplo, al ingreso se dota a todos los viajeros de un documento de identidad magnético en el que figure su fotografía digitalizada. Deberán mostrado a la entrada y la salida del buque.

Asimismo, en los accesos de entrada todos los pasajeros y tripulantes deberán quedar registrados por medio de aparatos de rayos-x detectores de metales, bien manuales o por arcos fijos. Por su parte, la política de autorizaciones a los visitantes ha sido drásticamente limitada y las visitas comerciales han sido totalmente prohibidas.

Inspección de vehículos

En relación con los accesos de vehículos al buque, tal vez el talón de Aquiles de la seguridad actualmente, más allá de la exigencia de la documentación pertinente (como el permiso de conducir, acreditación de la titularidad, además del seguro en vigor y para viajes fuera de la UE, carta verde del seguro, etc.), no existe un control más exhaustivo.

Las inspecciones aleatorias y el uso de unidades caninas se han incrementado con el tiempo siempre que la operativa lo ha permitido. Sin embargo, los grandes flujos de personas, que arriban con una antelación promedia de 90 minutos previos al acceso, sumado a la falta de un protocolo, deja muy poco espacio a un control exhaustivo de los vehículos.

Como mencionó doña Celia Tamarit durante la inauguración de la IV Conferencia sectorial de Seguridad en Puertos de 2019, magníficamente impulsada por la Fundación Borredá y la propia revista *Seguritecnia*, las acciones a medio plazo para fortalecer la seguridad portuaria mediante regulación consistirían en establecer un marco normativo más definido, incluir mecanismos de coordinación, herramientas de planificación y mecanismos de mejora comunes.

Dichas acciones inmediatas partirían del desarrollo tecnológico, la mejora de las directrices para la gestión de las instalaciones portuarias y los sistemas de inspecciones. Basadas en las más avanzadas tecnologías de mercado en material de inspección por rayos X, el sector y la industria, esas acciones deberían ir acompañadas de un procedimiento que asegure el correcto cumplimiento de los estándares de seguridad nacional e internacional, a la par que mantengan niveles aceptables de flujo y cadencia de pasajeros en los accesos al buque.

Para inspeccionar el interior de un vehículo con una carga importante en determinadas situaciones (más concretamente durante el Paso del Estrecho) es necesario pasar de los generadores de rayos X con tensiones de 160kV (los cuales seguimos encontrando en los escáneres de paquetería) a los aceleradores lineales con tensiones de pico desde 2,5MeV hasta 4 MeV. Técnicamente hablando, cabe puntualizar que los aceleradores más comunes hoy en día, de 6 MeV, son capaces de alcanzar penetraciones en acero de hasta 380 milímetros. Para los neófitos en esta materia, es importante mencionar que estas penetraciones mínimas se convierten en un valor fundamental si queremos analizar vehículos tipo VAN o con grandes bultos en el techo de este con elementos muy heterogéneos.

Sobre tecnologías a implementar para fortalecer la seguridad se encuentran la inspección radiológica y la implementación de la doble energía, que permiten distinguir materiales orgánicos e inorgánicos en las imágenes a través de una escala de colores y facilita al operador la identificación de los objetos al conocer no sólo su forma, sino también su naturaleza.

Sin abandonar el marco de la seguridad, no debemos dejar de lado lo crucial que es para un puerto la agilidad en sus

servicios, y en ningún caso despreciar cada minuto de retraso, pues supone, además de un coste monetario, una pérdida de imagen de marca tanto del puerto como de sus terminales.

Tiempo de escaneo

En este sentido surge la necesidad de minimizar los tiempos de escaneado y ayudar al objetivo ideal de controlar el cien por cien de la carga sin perder operatividad. En respuesta a esta carencia, los fabricantes diseñan una solución propia y exclusiva para la inspección de vehículos como es el escaneado rápido (el cual nos permite escanear hasta 300 vehículos por hora), en donde el conductor deposita el vehículo en una zona de espera para que un robot mueva y distribuya el vehículo para su posterior escaneado y valoración positiva o negativa de la carga.

Está en nuestra mano asimilar los sistemas de inspección como inversiones con retorno real y no como un simple gasto para satisfacer las necesidades de otros organismos públicos. Son varios los beneficios que nos ofrecen los escáneres de vehículos: seguridad, modernidad, prestigio y un incremento del tráfico de pasajeros.

Ahondado en los obstáculos que frenan la agilidad en los procesos de inspección, se entiende que es imprescindible ayudar al operador a tomar decisiones acertadas rápidamente, y éste es el siguiente paso hacia un escaneado más cuantioso. Se deben considerar dos vectores sobre los que debemos actuar: formación del operador y ayudas a la detección. Estas pueden ser las líneas sobre las que seguir desarrollando las actuales soluciones, sumando una gestión remota que permita, a su vez, dos mejoras nada desdeñables: por un lado, la optimización del número de operarios, y por otro, dar un tratamiento objetivo a la información obtenida.

En el camino de la evolución tecnológica, cometeríamos un error si fuéramos conformistas limitándonos a mejorar "simplemente" las soluciones existentes. Es por ello que debemos ampliar el foco de nuevas perspectivas dentro de la inspección.

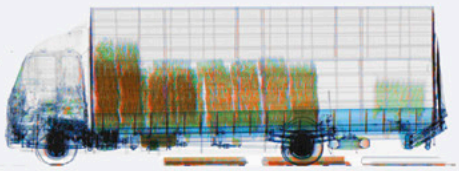
Para finalizar, vale la pena poner énfasis en la importancia de la comunicación entre puertos y proveedores de tecnología. Hoy en día, éstos tienen la posibilidad de seguir la evolución tecnológica de la mano de los propios fabricantes. Como en cualquier mercado, la transparencia y transmisión de la información en forma de requisitos entre el cliente-usuario y el proveedor de tecnología permite a este último ofrecer una respuesta acorde con las necesidades de cada usuario. Es un hecho irrefutable que a un comprador informado le será más fácil exigir a sus proveedores soluciones actuales que faciliten su operativa, haciendo ésta más ágil, segura y moderna, pero, sobre todo, más adaptada a su propio contexto.

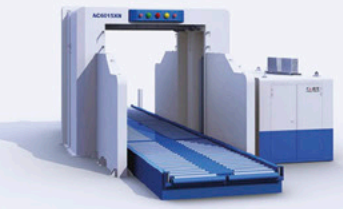
> Es necesario minimizar los tiempos de escaneado de vehículos y conseguir controlar el cien por cien de la carga sin perder operatividad

EXCEM TECHNOLOGIES

EXPERIENCIA, TECNOLOGÍA Y SERVICIO

Líderes en sistemas de **seguridad portuaria**





- Escáneres para inspección no intrusiva de contenedores
- Monitorización de radiación
- Filtros de seguridad completos
- Equipos de inspección de rayos X de paquetería, equipaje y carga
- Integración de sistemas, VMS/PSIM
- Sistema de detección y neutralización de UAS (antidrones)
- Soluciones de ciberinteligencia

excemtech.com

@excemtech

Seguridad privada **en instalaciones portuarias**

Eduardo Téllez Ruiz
Director de Operaciones de Pycseca Seguridad

Al hablar de seguridad privada en entornos portuarios, debemos situarnos para contextualizar la actividad a la que hacemos referencia. Según el Real Decreto Legislativo 2/2011, de 5 de septiembre, por el que se aprueba el Texto Refundido de la Ley de Puertos del Estado y de la Marina Mercante, "un puerto es el conjunto de espacios terrestres, aguas marítimas e instalaciones que, situado en la ribera del mar o de las rías, reúna condiciones físicas, naturales o artificiales y de organización que permitan la realización de operaciones de tráfico portuario y autorice la actividad la autoridad competente".

La página oficial de Puertos del Estado nos indica, por otro lado, que "por ellos pasan cerca del 60 por ciento de las exportaciones y el 85 por ciento de las importaciones, lo que representa el 53 por ciento del comercio exterior español con la Unión Europea y el 96 por ciento con terceros países. Además, la actividad del sistema portuario estatal aporta cerca del 20 por ciento del PIB del sector del transporte, lo que representa el 1,1 por ciento del PIB español. Asimismo, genera un empleo directo de más de 35.000 puestos de trabajo y de unos 110.000 de forma indirecta".

Prolijo marco normativo

El marco normativo que afecta a los puertos es innumerable, lo que hace de ellos un espacio, como mínimo, peculiar. A estos entornos afecta el mencionado Texto Refundido de la Ley de Puertos del Estado y de la Marina Mercante, la Ley de Costas, la Ley de Evaluación Ambiental, la Orden FOM/3769/2007 que establece el procedimiento integrado de escala de buques en puertos de interés general, etc.

En lo que se refiere a la seguridad privada, les afecta la Ley 5/2014, de 4 de abril, de Seguridad Privada; el Real Decreto 130/2017, de 24 de febrero, por el que se aprueba el Reglamento de Explosivos; el Real Decreto 989/2015, por el que se aprueba el Reglamento de artículos pirotécnicos y cartuchería; la Ley y Reglamento de Minas; el Reglamento Nacional del Transporte de Mercancías Peligrosas por Carretera, Ferrocarril y vía aérea; y el Real Decreto 2364/1994, por el que se aprueba el Reglamento de Seguridad Privada.

A todo esto, debemos añadir varias normas internacionales, como son el Convenio SOLAS (Convenio internacio-

nal para la seguridad de la vida humana en el mar) o el famoso Código ISPS (Código para la protección de los buques y de las instalaciones portuarias). Esta normativa da pie a la creación de las figuras de Oficial de Protección de Instalaciones Portuarias (OPIP), Oficial de Protección del Buque (OPB) y Oficial de Protección de Compañía Marítima, (OPCM). Tampoco podemos olvidarnos del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, donde los puertos forman parte del Catálogo Nacional de Infraestructuras Estratégicas. Ambas normas son muy interesantes al dejar la puerta abierta a la figura del Director de Seguridad.

La seguridad privada

Vista la extensa normativa que afecta a puertos y a las actividades que realiza el personal de seguridad privada, cabe mencionar que existen dos programas de formación específica (de especialización) homologados por el Ministerio del Interior para realizar los servicios en puertos y buques. Estos son los de "Servicio de Vigilancia en Puertos" y "Servicio de Vigilancia en Buques".

Dado que la seguridad pública es competencia exclusiva del Estado y que existe un deber de cooperación, coordinación y auxilio a las Fuerzas y Cuerpos de Seguridad, como norma general los controles de identificación que se llevan a cabo dentro de la instalación portuaria serán realizados por el Cuerpo Nacional de Policía; es decir, el control del tránsito de personas, pasaportes, DNI y normativa de extranjería. También realizan controles los agentes de la Policía Portuaria o el personal de seguridad privada, siempre bajo la supervisión de la autoridad competente.

La Guardia Civil asume el control de los embarques, tanto de las mercancías,

como de los equipajes o la paquetería que transporten los viajeros y las tripulaciones. Igualmente, sus agentes desempeñan cualquier otra función de las recogidas en el control del resguardo fiscal. Para esta función también cuentan con el apoyo del personal de seguridad privada, especialmente en el control y transporte de material explosivo, armas, etc.

Dicho esto, debemos tener en cuenta que la Ley de Seguridad Privada trata de encauzar todos los casos en los que la protección y seguridad de determinadas personas y bienes cuente con el concurso de organizaciones y personas distintas de las incluidas en las estructuras administrativas policiales.

Únicamente pueden quedar fuera del ámbito de aplicación de la Ley de Seguridad Privada actividades como las citadas por la disposición adicional primera del Reglamento de Seguridad Privada. Estas pueden calificarse como inherentes a la autoorganización de las empresas o comunidades de bienes, siempre que no supongan una evidente intromisión en los servicios o actividades expresamente reservadas en la Ley de Seguridad Privada, como recoge el artículo 5 sobre "Actividades de seguridad privada" y el artículo 8 "Principios rectores".

Actualmente, el personal de seguridad privada viene realizando una gran cantidad de servicios. Muchos de ellos son poco conocidos, lo cual no significa que no sean importantes. Básicamente, dichos servicios se podrían clasificar en:

- Control de accesos a instalaciones portuarias (vigilantes de seguridad).
- Control de accesos a buques (vigilantes de seguridad).
- Control y vigilancia de recintos portuarios (vigilantes de seguridad).
- Vigilancia de polizones en buque atracado (vigilantes de seguridad).
- Vigilancia y control de explosivos o materias peligrosas (vigilantes de explosivos).
- Dirección de Seguridad de la instalación portuaria o compañía marítima (Director de Seguridad).

> La seguridad privada realiza gran cantidad de servicios en puertos. Muchos de ellos son poco conocidos, pero también son importantes

En definitiva, la seguridad privada forma parte esencial de la actividad y el correcto funcionamiento de los puertos en España.

¿Cómo puede la gestión de vídeo ser soporte **para la seguridad, la logística o las** operaciones en los puertos?

Jaime Durbán
Vertical Specialist EMEA de Milestone Systems

Un puerto no es una instalación donde el vídeo tenga un alcance totalmente definido. Como suele ocurrir en multitud de infraestructuras críticas, sabemos que uno de los principales motivos para instalar cámaras es querer tener ojos por toda la instalación. Ahora bien, las posibilidades y servicios que nos ofrece una red de cámaras desplegada, con la correspondiente analítica de vídeo, va mucho más allá que la mera videovigilancia.

Resulta evidente que una solución de *software* de gestión de vídeo (VMS, por sus siglas en inglés) ayuda a supervisar toda la zona de un puerto desde una ubicación central u otros puestos de control desplegados por las instalaciones. Esto proporciona un mejor conocimiento de la situación, permitiendo una detección mucho más rápida de eventos inusuales y accidentes. Los operadores pueden iniciar una acción de mitigación inmediata con una respuesta temprana que limita el impacto del incidente.

> Una solución de 'software' de gestión de vídeo ayuda a supervisar un puerto desde una ubicación central u otros puestos de control

Sin embargo, como introducía, una plataforma abierta permite alimentar la instalación con diversas tecnologías, como la analítica de vídeo. Y toda la infraestructura se beneficia enormemente de ello reutilizando la red desplegada, las cámaras, los puestos de operador, centros de control y resto de recursos ya contemplados para una supervisión inicial. Hablamos no solo de seguridad o de ver incidentes; hablamos de gestión de operaciones portuarias, logística y almacenamiento, así como de documentación, control y registro. Hablamos de dotar a una instalación que graba imágenes de mucha más inteligencia que nos permita no solo disponer de ojos en la instalación, sino también de tener una tecnología capaz de decidir cuándo un incidente es relevante y presentárnoslo. Una plataforma de vídeo abierta ya no aporta "ojos" solamente; aporta una "mente" capaz de tomar decisiones que aporte un valor mucho más amplio.

Para ello es importante contar con un buen sistema de vídeo que cumpla con unos mínimos requisitos de mantenimiento, visualización de vídeo en tiempo real, funcionamiento sencillo y capacidad de integrar fácilmente una variedad de componentes ya instalados y de próxima instalación: nuevos servidores, cámaras o, por ejemplo, software de análisis. Además de disponer de una interfaz sencilla, o al menos intuitiva, transmisiones rápidas, amplio almacenamiento y optimización en el número de cámaras requeridas.

Gestión de vídeo óptima

La monitorización es una cuestión muy relevante en un lugar donde una gran cantidad de empresas están depositando y almacenando sus mercancías. Poder ofrecer, por ejemplo, a los clientes imágenes en tiempo real que les permita comprobar el estado de su mercancía tiene un valor añadido de negocio muy importante, sumado al valor práctico de

Webinars

Soluciones Tecnológicas

Expertos

OPEN WEEK

SOLUCIONES POSTCOVID

OPEN SECURITY DAY — LUNES SECURITY

OPEN CYBERSECURITY DAY — MARTES CYBERSECURITY

OPEN SAFETY DAY — MIÉRCOLES SAFETY

OPEN FACILITY DAY — JUEVES FACILITY

OPEN CLEANING DAY — VIERNES CLEANING

PRÓXIMO OPENWEEK DEL 19-23 DE ABRIL ¡APÚNTATE!

#JUNTOS SOMOS PARTE DE LA SOLUCIÓN

Borrmart Eventos — Apostamos por los eventos digitales. Por responsabilidad

gestión de estas cargas que ello conlleva de cara a los operarios.

Es decir, hablamos de poder monitorizar, incluso desde un *smartphone*, áreas de miles de metros cuadrados de almacén con un sistema que permita al puerto ampliar su cartera de servicios. Esto le ofrece un plus de confianza al cliente, quien tendrá acceso visual directo a su mercancía. Todo ello, con la tranquilidad de que ha llegado, nunca mejor dicho, a buen puerto y de que se encuentra en todo momento en perfecto estado.

De nuevo hablamos de aspectos más allá de la seguridad. Y siguiendo por esta línea, gracias a sencillas integraciones se pueden implementar nuevos usos al vídeo, como por ejemplo que el *software* permita a la empresa portuaria enviar a sus clientes un enlace con su respectivo nombre de usuario y contraseña para verificar su carga. Desde un ordenador o dispositivo móvil podrían comprobar, entre otros detalles, el estado de su mercancía, cuándo ha entrado en el almacén, por qué puerta o si se ha movido.

Nuevos desarrollos, que suelen surgir bajo demanda, han permitido también que se ponga a disposición una licencia para la aplicación móvil de este sistema. De esta manera, los operarios puedan grabar vídeos desde un dispositivo móvil y enviarlos directamente al servidor de la solución para que el vídeo sea accesible a los usuarios autorizados.

Así se cubren puntos ciegos que inicialmente no formaban parte de la red de cámaras, aumentando la operatividad y la flexibilidad del sistema. Dado el caso, si un operario abre un contenedor y observa que la mercancía está dañada o en mal estado, puede grabar un vídeo en su teléfono y enviarlo por el sistema de gestión de vídeo para mostrar en tiempo real el estado de la mercancía cuando llegó al almacén.

Muchos puertos que cuentan con este sistema de gestión de vídeo están estudiando la posibilidad de añadir analíticas como la lectura de matrículas para el análisis y seguimiento de contenedores, la agilización del flujo de tráfico dentro del complejo, la localización de la carga o el recuento de camiones.

La tecnología abierta y las soluciones flexibles permiten acompañar al cliente al tiempo y al ritmo que necesita, escalando en paralelo a los recursos disponibles o necesidades que vayan surgiendo.

Casos prácticos

Aquí en España, hace ya cinco años que la Autoridad Portuaria de la Bahía de Algeciras decidió implementar un sistema de CCTV muy ambicioso, principalmente en el uso y rendimiento que querían sacarle al vídeo en la instalación en cuestión de analíticas de vídeo.

Cuando leí el pliego y los requisitos de analíticas del Puerto de Algeciras, supe enseguida que formaríamos una alianza muy fuerte a lo largo de los años. Los requisitos en cuanto a analíticas eran altos y variados, incluso algunos contaban con el futuro avance de la tecnología de los algoritmos. Ese siempre fue precisamente nuestro punto fuerte como plataforma de gestión de vídeo: nuestro ecosistema de *partners*, una comunidad de analíticas que a lo largo de los años va enriqueciendo nuestro porfolio sin límites.

Hoy en día seguimos en contacto para ver distintas tecnologías que se puedan implementar para solucionar los problemas que se van descubriendo en el desarrollo de sus actividades.

Otro ejemplo lo tenemos en el Puerto de Amberes (Bélgica), que se enfrenta diariamente a numerosos retos operativos en torno a problemas medioambientales. Accidentes muy habituales son las fugas de petróleo de los buques durante el repostaje o el choque de estos contra el muelle o el muelle de las esclusas. Unas colisiones que causan daños que deben ser reparados.

La detección precoz de los vertidos de petróleo es vital para minimizar el impacto en la vida vegetal y animal y para informar sobre el cumplimiento de la normativa. Y, por su parte, la capacidad de documentar los incidentes de impacto de los buques en los puertos y los daños derivados resulta muy importante para la resolución de conflictos.

Panasonic i-PRO: solución con protección IP66 y anticorrosión para entornos marítimos

Alejandro Ramón
Regional Sales Manager Nordic and Southern Europe Total Security Solutions de Panasonic System Communications Europe

Los modelos WV-S6532LNS y WV-X6533LNS, especialmente indicados para entornos cercanos al mar, incorporan un potente *zoom* óptico de 22x y 40x respectivamente para una videovigilancia sin iluminación.

Pertenecientes a la serie i-Pro Extreme de Panasonic, ambas cámaras de exterior cuentan con certificación IP66 para soportar condiciones atmosféricas cambiantes y contra la corrosión, así como protección antivandálica IK10, para su aplicación en entornos cercanos al mar, como puertos, muelles, etc.

Principales características

Visibilidad extrema: estos modelos PTZ con infrarrojos incorporan un potente *zoom* óptico 22x (para la cámara WV-S6532LN) y de 40x (WV-X6533LN) para una vigilancia de 360 grados a una distancia de 100 a 350 metros sin iluminación.

Para captar las imágenes en prácticamente total oscuridad y a larga distancia, estos dispositivos incorporan un estabilizador inteligente para el zoom que reduce las vibraciones para una imagen *full* HD consistente y sin distorsión.

Revestimiento ClearSight: su cubierta con revestimiento especial (ClearSight) es resistente al agua, las manchas y la acumulación de polvo. Además, habilita la captura de imágenes nítidas 24/7 incluso en entornos lluviosos, reduciendo la necesidad de un mantenimiento periódico.

Deshumidificación y descongelación: la captura nítida de imágenes está garantizada gracias a su sistema de descongelación integrado en la parte frontal de la cubierta y a su tecnología de deshumidificación para evitar la formación de condensación dentro de la cámara en caso de variaciones bruscas de temperatura.

Compresión extrema: estos dispositivos de videovigilancia integran la tecnología Smart Coding de Panasonic para reducir el consumo de ancho de banda y de almacenamiento con compresión H.265. A ello se le suma la función Auto VIQS, que reduce el volumen de datos al gestionar de forma óptima y automática solo las zonas de la imagen con movimiento.

Analítica extrema: estas cámaras PTZ incluyen la licencia y funcionalidad i-VMD (detección inteligente de movimiento de vídeo) para notificar alarmas al centro de operaciones cuando existen cambios en las imágenes frente a los parámetros de normalidad establecidos en una primera instancia, facilitando la operativa en la gestión.

Seguridad extrema de los datos: además de la encriptación de datos y las comunicaciones, los nuevos PTZ i-PRO de Panasonic proporcionan un acceso seguro a la red entre dispositivos de confianza a través de la certificación de dispositivos, pudiendo evitar amenazas de ataques cibernéticos avanzados.

Con la incorporación de estos nuevos modelos en la gama i-PRO Extreme, Panasonic continúa atendiendo a las necesidades de los diferentes mercados verticales, al mismo tiempo que lidera el actual crecimiento del mercado de analíticas de Inteligencia Artificial en la propia cámara.

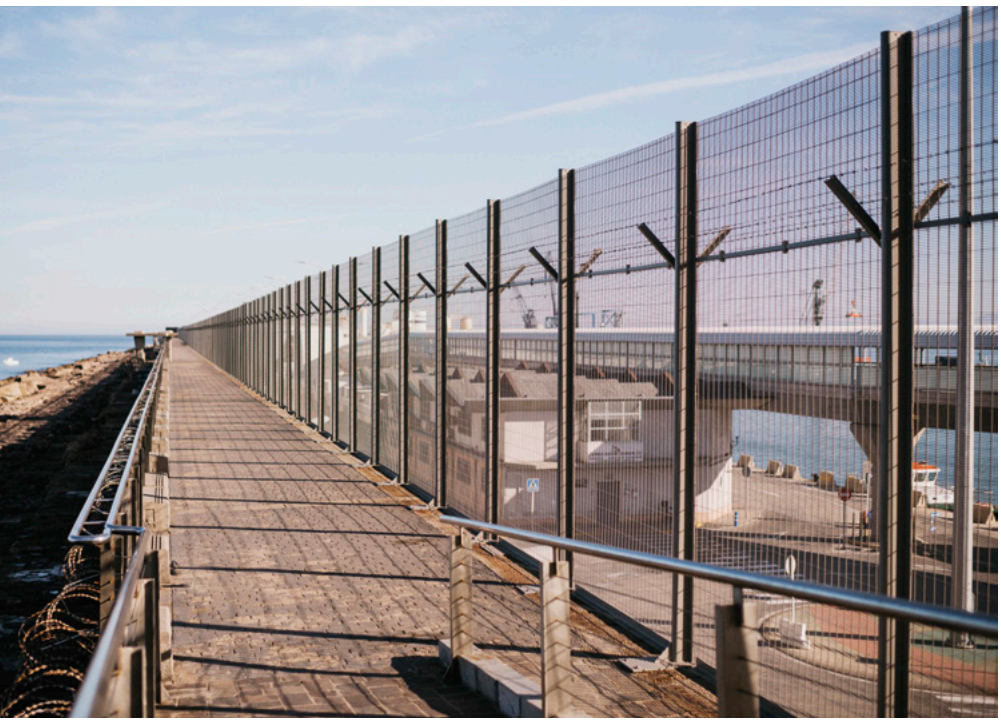
Betafence ofrece la mejor solución perimetral **para zonas críticas en puertos marítimos**

Sebastián Petidier Navajas
Sales Manager Iberica de Betafence

Ángel Díaz
Director Comercial de Sicuralia

Seguridad perimetral, contención y control de accesos son los principales puntos críticos para la autoridad portuaria que demandan sistemas de seguridad integral y con garantía anticorrosión. No obstante, bien para retrasar y detectar una intrusión o para controlar el acceso, se necesitan productos y tecnologías en las que se pueda confiar.

El control de accesos y la detección son elementos cruciales en el concepto de seguridad de Betafence. El hecho de poder permitir o rehusar el acceso al recinto de personas o vehículos, pero también de detectar, identificar y prohibirles el paso a intrusos no deseados, permite determinar en todo momento quién o qué se halla en el recinto.



Todos los productos Betafence se distinguen por su fiabilidad y su seguridad. Por ejemplo, la gama Securifor es la absoluta ganadora en la categoría "demora". Este sistema total integra resistentes paneles de seguridad y tres posibilidades de postes.

Estos vallados son difíciles de penetrar o de trepar debido a su fina malla de 76,2 por 12,7 milímetros y al espesor de su alambre. Al mismo tiempo, ofrecen una excelente visibilidad (esencial para la vigilancia por cámaras) y una larga durabilidad frente a la corrosión.

Securifor hace posible variar el nivel de seguridad. El usuario puede optar por diferentes alturas y grados de dificultad a la intrusión dependiendo del modelo seleccionado.

Los paneles Securifor son sometidos a tratamientos anticorrosión, lo que garantiza una larga vida en entornos altamente salinos, como los puertos marítimos. Los paneles son galvanizados con zinc puro al 99 por ciento acorde a Z3 de la norma EN 1179, con

Vallado perimetral de seguridad anti-escalado con detección integrada

BETAFENCE
a PRÆSIDIAD brand

Securifor®

IP-READY PoE

VALLADO DE ALTA SEGURIDAD ANTI ESCALADO - VPA

Ante las necesidades de seguridad especiales en puertos, Betafence y Sicuralia han desarrollado una solución conjunta de vallado anti escalado con detección electrónica incorporada.
El producto seleccionado ha sido el modelo Securifor de Betafence, tanto es su versión "flat" como "2d". Dotados de una trama de 76,2 mm x 12,7 mm que impide el escalado, favorece la visibilidad a través de él, lo que permite una perfecta integración con sistemas de video vigilancia CCTV.
La integración de los vallados de Betafence con los sensores de Sicuralia proporcionan las mejores soluciones de alta seguridad para los perímetros de instalaciones de alto riesgo, garantizando un mayor nivel de disuasión, mayor tiempo de retardo de la intrusión y una alta fiabilidad en la detección e identificación de intrusos, con garantía contra la corrosión.

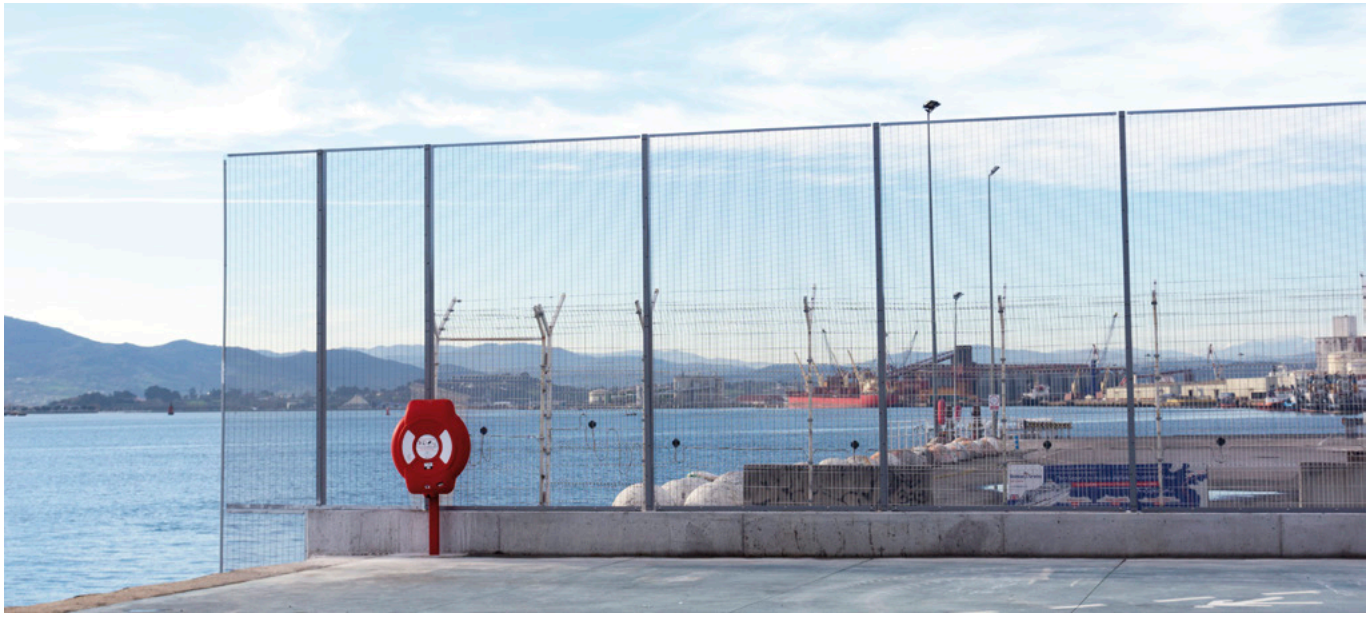
Sicuralia

SIOUX 3.0 CIAS

www.betafence.es
www.sicuralia.com

info.spain@betafence.com
comercial@sicuralia.com

+34 947 269 711
+34 916 621 688



un recubrimiento mínimo de 25 gramos por metro cuadrado. Posteriormente se plastifican con un espesor mínimo de 100 micras de poliéster libre de plomo y cadmio.

El espesor es la media de 10 muestras tomadas en un panel. Opcionalmente, para ambientes muy corrosivos, se puede optar por una mayor protección mediante acabado Zincalú Ultra más doble capa de poliéster. Así se puede garantizar, en este caso, hasta 10 años de garantía contra la oxidación en cualquier tipo de ambiente salino.

De hecho, el ambiente salino de los puertos hace peligrar el recubrimiento de los paneles, ocasionando manchas de óxido que afean y disminuyen la vida del vallado. En Betafence, los paneles que forman el vallado perimetral son sometidos a rigurosas pruebas de calidad para garantizar la resistencia del poliéster utilizado en el recubrimiento a niebla salina siempre acorde a la norma ISO 9227.

> Los vallados Securifor son una plataforma perfecta para soportar y complementar sensores de seguridad perimetral, cámaras de videovigilancia y radares de Sicuralia

Control de accesos

Sin duda, un punto crítico para las autoridades portuarias es el control de accesos. Betafence ofrece soluciones para completar el cierre perimetral con productos de control de accesos que se integran perfectamente con el vallado. Unas soluciones fabricadas siempre bajo el marco del certificado CE.

En este sentido, cabe destacar, además de las tradicionales puertas abatibles y correderas con rail, los sistemas de puertas Cantilever, correderas sin rail, así como el nuevo sistema de puertas de apertura rápida Faldivia.

Los vallados Securifor son una plataforma perfecta para soportar y complementar sensores de seguridad perimetral, cámaras de videovigilancia y radares de Sicuralia.

La simbiosis entre ambas tecnologías da lugar a sistemas de protección perimetral altamente eficaces que garantizan una alta capacidad de retardo y disuasión, a la vez que proporcionan alertas tempranas que identifican la posición exacta del intruso.

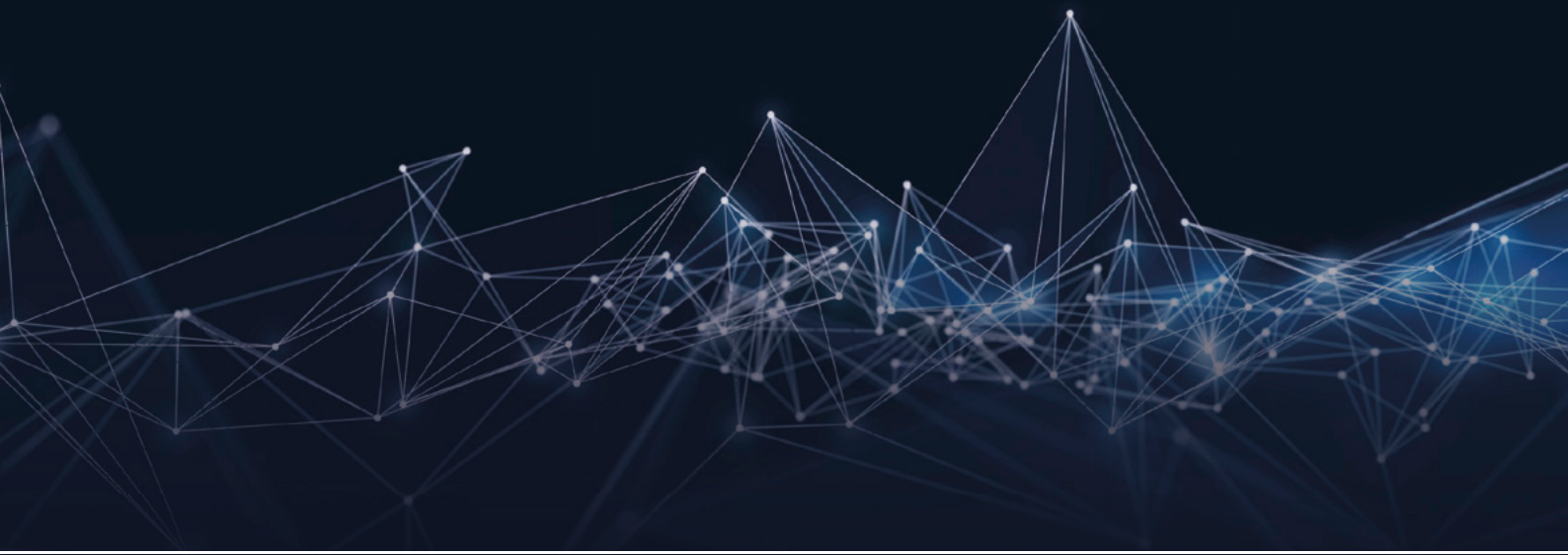
Las soluciones de seguridad integrales aportadas por Betafence y Sicuralia están integradas con las plataformas de seguridad más populares del mercado, como Qognify, Cayuga, Ocularis o Situator. Un hecho que hace que los vallados Securifor sean no solo elementos pasivos de cierre perimetral, sino que pasen a formar parte activa de los sistemas integrados de gestión y control de seguridad de las infraestructuras críticas.

SOMOS LA **REALIDAD** **DIGITAL** QUE NECESITAS

+ 5.000 inscritos a nuestros Webinar y eventos digitales
+ 15.000 inscritos a nuestra Newsletter semanal
+ 20.000 seguidores en redes sociales
+ 225.000 descargas de Seguritecnia Digital en Kiosko Pro
+ 500.000 visitas a **www.seguritecnia.es**

SEGURITECNIA es miembro de Google Editor Program

Súmate a **SEGURITECNIA**
REVISTA DECANA INDEPENDIENTE DE SEGURIDAD



Si no te ven no existes

Monoculares y prismáticos térmicos de T8Tech: **un paso más**

Vicente Bort
Socio fundador de T8TECH

Mejorar la eficiencia en la vigilancia es clave para optimizar los recursos con los que contamos y focalizar los esfuerzos en acciones que reportan unos mejores resultados.

Cada vez más, la tecnología se alía con nosotros para aportar herramientas dotacionales a nuestros vigilantes que les reportan claras mejoras en sus trabajos de control y observación.

La visión térmica –diurna y nocturna– ahorra una enorme cantidad de tiempo en los trabajos de vigilancia, dado que permiten identificar fuentes de calor (personas o barcos) en multitud de entornos con un rápido barrido.

Así, los monoculares y prismáticos térmicos de T8Tech, con rangos de reconocimiento entre 500 metros y 12 kilómetros, tienen los máximos estándares de calidad. Su uso es sencillo, y cuentan con altas prestaciones y una innumerable gama de modelos que se adaptan a cualquier entorno o necesidad de vigilancia u observación.

Además, todos los dispositivos de T8Tech, con capacidad de hacer fotos y grabar vídeo almacenable en una tarjeta insertada cada equipo, tienen *bluetooth*. Este se vincula a una aplicación de la marca con el objeto de optimizar las diversas funcionalidades y almacenar datos segmentados por fecha y hora.

Dar un paso más en la vigilancia significa aliarse con los nuevos productos y soluciones tecnológicas que nos permiten optimizar los tiempos de respuesta, preservar los espacios y maximizar la detección anticipada.

Principales características

Entre las principales características de los monoculares y prismáticos térmicos de T8Tech se encuentran la optimización del tiempo de servicio y la captación de intrusión a kilómetros de distancia. Todo ello, con la última tecnología.

Estos equipos sirven para la captación térmica de personas, vehículos, etc., tanto de día como de noche, en alta mar, costas, grandes instalaciones de vigilancia (centrales eléctricas, cetros comerciales, aeropuertos…), instalaciones críticas en general, fincas privadas y términos municipales.

Sus clientes potenciales son empresas de seguridad, Fuerzas y Cuerpos de Seguridad del Estado o Ejército, ya que su función es prevenir y detectar robos, intrusismo, migrantes y furtivos.

T8TECH.COM 2021

VIGILANCIA

Utiliza la tecnología para optimizar los servicios de vigilancia

La visión térmica te ayudará a ser más eficiente, con captación de imágenes a kilómetros de distancia

IR516B

Guide sensmart t8tech.com

Control de potencia, contraste y brillo
Diseño ergonómico
Rastrea puntos calientes
Toma de fotos y videos

TrackIR Handheld

Guide sensmart t8tech.com

Imagen nítida y delicada
Cómodo a la vista
7 modos de escena
Anti fuga de luz
Resistencia IP66

Contáctanos
www.t8tech.com
607 078 263
info@t8tech.com

El transporte de seguridad en España: parte **consustancial de la seguridad privada**

La Fundación Borredá ha puesto en marcha una serie de encuentros digitales bajo el nombre "El *Zoom* de la Fundación Borredá". Cada evento, exclusivo para sus colaboradores, socios protectores, patrocinadores y amigos, se centrará en un tema de interés para la seguridad. La primera tertulia, desarrollada el 3 de febrero, tuvo como protagonista al transporte de seguridad.

POR JUANJO S. ARENAS

"El *Zoom* de la Fundación Borredá". Bajo este nombre, la entidad sin ánimo de lucro desarrollará una serie de eventos digitales el primer miércoles de cada mes. Estos encuentros, promovidos por sus socios protectores, analizarán diversos aspectos de la seguridad e identificarán fortalezas y oportunidades de cada uno de ellos.

Así lo explicó **Ana Borredá**, presidenta de la Fundación Borredá, durante la primera tertulia, que tuvo como protagonista al transporte de seguridad. **César Álvarez**, coordinador de Proyectos de la Fundación y encargado de moderar el debate, dividió el encuentro en tres bloques: situación actual del sector privado en transporte y distribución de objetos, transporte de efectivo y oportunidades en un futuro próximo.

Situación actual

El primer encargado de explicar la situación del transporte de seguridad en la actualidad fue **Eduardo Cobas**, gerente de Aproser. En concreto, este profesional se centró en los duros momentos que vive dicho sector en tiempos de pandemia: "El transporte de fondos se encuentra en una situación complicada debido a la llegada de la digitalización. Por ejemplo, su volumen de paradas ha disminuido más de un 50 por ciento y el movimiento del efectivo un 60".

A ello le sumó algo que, a su juicio, es un "ataque frontal injustificado" al dinero en efectivo: el hecho de que se relacione el pago en metálico con la transmisión del virus y el fraude.

Precisamente sobre este último elemento, el del fraude, se pronunció **Alejandro Corominas**, consejero delegado de Loomis. El representante de esta empresa de transporte de seguridad aseguró que "la cantidad de fraude producido con el efectivo es muy pequeño respecto al mundo electrónico, según la Agencia Tributaria". De hecho, Corominas explicó que fue la propia Agencia la que trasladó a los operadores que su principal preocupación radica en el entorno digital. "La palabra fraude hay que unirla a los defraudadores, no a la herramienta en sí", sentenció el portavoz de Loomis haciendo alusión al dinero físico.

Por otro lado, el comisario principal **Manuel Yanguas**, jefe de la Unidad Central de Seguridad Privada (UCSP) de la Policía Nacional, ofreció una serie de datos sobre las empresas que desempeñan el transporte de efectos peligrosos y valiosos en la actualidad. En particular, tal y como enumeró el representante del organismo policial, actualmente se encuentran registradas en España 1.586 empresas dedicadas a estas prácticas. De ellas, cinco cuentan con la autorización exclusiva para transportar objetos valiosos y 44 para trasladar explosivos.

Transporte de fondos

La legislación sobre transporte de fondos también fue objeto de debate en la tertulia. Al respecto se pronunció Eduardo Cobas, de Aproser, quien declaró que,

según el borrador del nuevo Reglamento de Seguridad Privada, las operaciones de transporte quedarían fuera del amparo de la Ley, por lo que "se produciría una liberalización del sector".

Por su parte, Manuel Yanguas justificó lo que expone el proyecto de borrador: "En cierto modo, había una controversia porque existían numerosos intereses confrontados: de las empresas autorizadas para el transporte de fondos, objetos valiosos, etc. Por otro lado, también se encontraba el Banco de España, que en cuestión de transporte de efectivo tiene sus propias normas. El problema era que no todo el mundo estaba de acuerdo con lo que se proponía en ese momento".

En otro orden de cosas, el teniente coronel **José Enrique Cordobés**, de la Unidad de Protección y Seguridad de la Guardia Civil, explicó a la audiencia a qué se dedica su unidad. "Nos encargamos de proteger edificios e instalaciones públicas y centros penitenciarios. También realizamos escoltas, conducciones y traslados de seguridad de presos. Por ejemplo, en 2020 llevamos a cabo 284 escoltas, 36 menos que el año anterior. La mayoría de ellas se desarrollaron en el ámbito terrestre, aunque también las realizamos por vía marítima y aérea", comentó.

Santiago Sanz (Secretaría de Estado de Seguridad).

Manuel Yanguas (Policía Nacional).

Nuevas oportunidades

A continuación, **Santiago Sanz**, del Gabinete de Coordinación y Estudios de la Secretaría de Estado de Seguridad, fue el encargado de abrir el debate sobre las nuevas oportunidades surgidas para el transporte de seguridad. Y, cómo no, centró su intervención en el transporte de la vacuna del COVID-19.

Todo ello porque, según explicó este profesional, las compañías dedicadas al almacenamiento y distribución del embrión de la vacuna sufrieron intentos de ciberataques para dañar los sistemas de frío, la cadena de suministro, etc. "La vacuna es un activo a proteger, y como tal se han elaborado planes de seguridad. Pero son las Fuerzas y Cuerpos de Seguridad del Estado quienes llevan a cabo su protección integral en nuestro país", explicó Sanz.

Un campo, por tanto, en el que no estaría inmiscuida la seguridad privada, a pesar de los argumentos de Manuel Yanguas para que esta adquiriera un papel protagonista en el proceso. "He propuesto que la seguridad privada realice el transporte y custodia de la vacuna, pero aún no he recibido respuesta", afirmó al respecto el comisario principal de la UCSP.

La próxima tertulia virtual de la Fundación Borredá, que se celebrará de la mano de su socio protector Deloitte, se centrará en la reciente publicación del Reglamento NIS. Este evento se llevará a cabo el 3 de marzo a las 17:00 horas y contará con la participación de varios expertos en la materia.

José Enrique Cordobés (Guardia Civil).

Alejandro Corominas (Loomis).

Eduardo Cobas (Aproser).

La Seguridad Privada clama por incluir a sus profesionales en la segunda fase de vacunación

El Observatorio Sectorial de Seguridad Privada ha reclamado la inclusión de los profesionales del sector entre los grupos incluidos en la segunda fase de la estrategia de vacunación contra el COVID-19. El órgano considera que este personal deberían recibir el compuesto, de la misma manera que lo harán otros colectivos como la Guardia Civil, Policía Nacional, Bomberos o profesionales de Protección civil, entre otros.

El Observatorio solicita expresamente que "bien simultáneamente, bien una vez haya finalizado el proceso de vacunación de los profesionales de la seguridad pública, se integre a los profesionales de la seguridad privada entre los considerados como preferentes en el proceso de vacunación". Todo ello, agrega, "en beneficio último de los ciudadanos y en atención a su desempeño esencial en esta crisis sanitaria".

La entidad lo argumenta en base a que la estrategia de vacunación incorpora una categoría denominada Grupo 6, que comprende a los colectivos en activo con una función esencial para la sociedad. Entre ellos se encuentran las "Fuerzas y Cuerpos de Seguridad, Emergencias y Fuerzas Armadas". "Una relación que comprende, en términos genéricos, lo que podría denominarse servicios de seguridad y emergencias", apunta el Observatorio.

La nueva web de la Policía Nacional habilita un espacio para la seguridad privada

La Policía Nacional cuenta desde el 20 de enero con una nueva página web en la que ha habilitado un espacio directo para acceder a Red Azul, su programa de colaboración con la seguridad privada. Los profesionales de este sector podrán acceder a través de este enlace a toda la información relativa a los procedimientos administrativos, así como a los requisitos para las acreditaciones de profesores de centros de formación. Este espacio da acceso también al área restringida del programa Vigila.

La nueva web se enmarca en el proceso de transformación digital de la Policía Nacional. Uno de sus principales objetivos es mejorar la accesibilidad y facilitar los trámites que se llevan a cabo ante la Policía Nacional.

El *site* cumple esos objetivos también con los profesionales de la seguridad privada, que podrán realizar gestiones y obtener información de interés.

La UE fortalecerá su mecanismo de protección civil frente a catástrofes

La Presidencia del Consejo y los representantes del Parlamento Europeo alcanzaron, el 8 de febrero, un acuerdo provisional sobre una propuesta para fortalecer el mecanismo de protección civil de la Unión Europea. Estas reglas permitirían a los países de la Unión estar mejor preparados frente a los desastres naturales y provocados por el hombre. El sistema pretenden facilitar la respuesta rápida cuando ocurra un suceso de este tipo, incluso si afecta a varios Estados miembros a la vez.

Estas propuestas también tratan de solucionar las lagunas que existen en relación con el trasporte y la logística y, en caso de urgencia, adquirir capacidades adicionales de rescEU.

Asimismo, la Comisión Europea definirá y desarrollará los objetivos de la Unión de resiliencia ante desastres en el ámbito de la protección civil. Estos objetivos no vinculantes se establecerán en las recomendaciones de la Comisión y se basarán en escenarios actuales y prospectivos.

El acuerdo alcanzado establece la financiación del mecanismo de protección civil en el contexto del marco financiero plurianual 2021-2027, que alcanzará los 1.263 millones de euros.

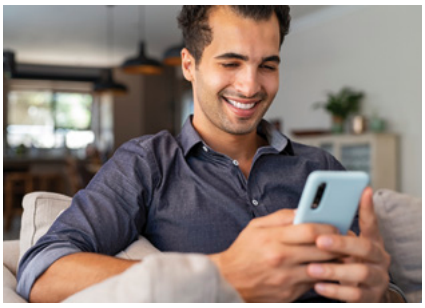
La ciberseguridad crecerá hasta llegar a los 1.324 millones de euros en 2021

El mercado de la ciberseguridad en España crecerá un 8,1 por ciento este año respecto a 2020. En concreto, alcanzará los 1.324 millones de euros. Así lo ha puesto de manifiesto IDC Research España. Además, esta compañía señala que el 37 por ciento de las empresas españolas van a establecer mecanismos para gestionar la identidad de dispositivos y usuarios. Y que el 36 trabajará en la privacidad de los datos y cumplimiento. Un 35 por ciento, por su parte, se enfocará en la concienciación y cultura de seguridad.

Asimismo, entre las tendencias en inversión más significativas para este año que destaca IDC se encuentran la automatización y orquestación de ciberseguridad para el 39 por ciento de las empresas y la simplificación del marco de seguridad para el 32.

En este sentido, la firma cree que, para 2023, el 55 por ciento de las inversiones en ciberseguridad corporativa se realizarán en marcos unificados de ecosistemas y plataformas de seguridad.

La consultora considera que 2021 será el escenario de la evolución hacia un nuevo paradigma de seguridad, pasando de seguridad de red a en la nube.



Los móviles, protagonistas de la estrategia de ciberseguridad del 87% de los CISO

Cerca de nueve de cada diez responsables de Seguridad de la Información (CISO) de la región EMEA afirman que los dispositivos móviles se han convertido en el centro de sus estrategias de ciberseguridad. Así lo pone de manifiesto el último estudio realizado por Ivanti.

Además, según este documento, el 80 por ciento de estos profesionales afirma que las contraseñas ya no son un medio eficaz para proteger los datos corporativos. El motivo, tal y como explican desde Ivanti, es que los ciberdelincuentes se dirigen cada vez más a los trabajadores remotos y a los dispositivos móviles.

Otro de los retos a los que hace mención el estudio son los dispositivos. El 40 por ciento de los CISO reconoció que los trabajadores usan sus propios dispositivos para acceder a los datos corporativos. Y un tercio de estos empleados utiliza aplicaciones no autorizadas para acceder a dichos datos.

En cuanto a las medidas de ciberseguridad, el 93 por ciento de los CISO afirmó que disponían de soluciones eficaces para realizar el cambio al teletrabajo al comienzo de la pandemia. Aunque el 92 también declaró que necesitaron medidas adicionales de seguridad para habilitar a los teletrabajadores y hacer frente a las amenazas.

El Congreso licita su ciberseguridad por más de tres millones de euros

El Boletín Oficial del Estado publicó, el 18 de febrero, el anuncio de licitación de los servicios integrales de ciberseguridad gestionada en régimen de 24x7 de la Mesa del Congreso de los Diputados. El valor estimado de este concurso es de 3.304.748,24 euros para los próximos cuatro años.

Las compañías que así lo deseen podrán presentar sus ofertas o solicitudes de participación hasta las 14:00 horas del 29 de marzo.

El principal criterio de adjudicación será el económico (50% de la ponderación). Aunque desde el Boletín se destacan otros: la formación y concienciación en seguridad de la información, el servicio de gestión y configuración de seguridad y respuesta ante incidentes, el sistema de controladores de entrega de aplicaciones y protección de aplicaciones web, el sistema de gestión de identidades, el sistema de gestión de la seguridad de la información, el sistema de monitorización y gestión de eventos e información de seguridad, el sistema de protección ante *malware* para servidores y *endpoints*, el sistema de protección perimetral de red y el sistema de soporte remoto a usuarios y control de cuentas privilegiadas.

Magnum presenta un amplio catálogo de botas para profesionales de la seguridad y las Fuerzas Armadas

Magnum ha anunciado varios lanzamientos de modelos de botas para profesionales de la seguridad y las Fuerzas Armadas. Se trata de modelos robustos, cómodos y transpirables que cuentan con certificados de calidad y resistencia. Todas las botas están fabricadas en Europa. Las más destacadas son:

Elite 8.0 Waterproof: es una bota con corte de piel flor y nylon hidrófugos, que cuenta con una membrana impermeable y transpirable Dri-Tec®. Dispone de lengüeta acolchada forrada para protección del empeine y collar antifricción. Asimismo, cuenta con un estabilizador trasero y zona de absorción de impacto en el talón. La plantilla es recambiable de PU y la planta antiperforación. Posee un nivel de resistencia al deslizamiento SRC y está certificada en EN ISO 20347.

Wolf 8.0 Side Zip: también dispone de un corte de piel flor y nylon, con forro antihumedad y cremallera lateral. El cierre es con cordones con ojales y anillas de PVC, además de contar con estabilizador trasero. Incorpora zona de absorción de impacto en el talón, plantilla recambiable de PU y cambrillón termoplástico. El piso está fabricado en caucho de carbono y la entresuela es de PU. La bota está certificada con EN ISO 20347.

Fox 8.0 Leather Waterproof: se trata de una bota corte de piel flor y nylon hidrófugos, forro antihumedad, membrana impermeable y transpirable Dri-Tec®, así como cierre de cordones con ojales y anillas de PVC. La lengüeta es acolchada y está forrada para protección del empeine. Posee estabilizador trasero, zona de absorción de impacto en el talón y plantilla recambiable de PU. La entresuela es de plástico y el piso de caucho carbono. Cuenta con el certificado EN ISO 20347.

Fox 6.0 Waterproof: tiene las mismas prestaciones de confort y resistencia que el modelo anterior, si bien en este caso varía el diseño en cuanto a su altura.

Fox 8.0 Desert Waterproof: está bota tiene corte de serraje y nylon hidrófugos, con membrana impermeable y transpirable Dri-Tec®. Sus demás prestaciones son idénticas a los otros modelos.

Elite 8.0 Waterproof.

Wolf 8.0 Side Zip.

Fox 8.0 Leather Waterproof.

Fox 6.0 Waterproof.

Fox 8.0 Desert Waterproof.

SEGURLEX CONSULTORES & COMPLIANCE ABOGADOS es un bufete multidisciplinar que abarca todos los ámbitos jurídicos (fiscal, civil, mercantil, laboral, administrativo …) y consultoría, con especialización añadida en:

- Vigilancia y gestión legal de Riesgos Reputacionales
- Inteligencia
- Seguridad Integral
- Seguridad Privada
- Infraestructuras Críticas
- *Compliance*
- Servicios externos de canales de denuncias para empresas
- Protección de datos (implantación, evaluaciones de impacto, auditorías y servicios de DPO)
- Asesoramiento, medidas de prevención, control y gestión contra el blanqueo de capitales
- Adecuación a sujetos obligados de la Ley de Igualdad Laboral
- Prevención de riesgos laborales

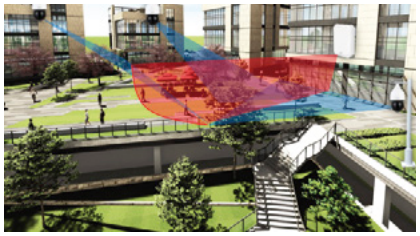
Contamos con *software* de gestión propio para auditorías on line

www.segurlex.com.es

C/ Don Ramón de la Cruz, 68 - 2° dcha
28001 Madrid España
Tel.: +34 91 401 88 74
info@segurlex.com.es

WORLD COMPLIANCE ASSOCIATION
MIEMBRO ASOCIADO

Solución de protección perimetral basada en radar de Dahua



Este producto de **Dahua** proporciona una monitorización de amplio rango, con una gran precisión y adecuada para todos los climas. De hecho, incluye el seguimiento de trayectoria de la persona, así como el del vídeo relacionado. Por tanto, es una solución de monitorización y de protección perimetral muy completa, precisa e inteligente.

La solución se basa un algoritmo inteligente de radar de alta precisión. El propio radar es capaz de determinar si el objetivo es un humano o un vehículo. Y es que mediante el estudio de RCS, la tasa de falsas alarmas es inferior al 0,5 por ciento. De este modo, no se producen errores, solo activará la alarma un evento de intrusión claro. Además, esta novedad cuenta con un ángulo de detección de hasta 120-90 grados, realizando un seguimiento de la trayectoria del objetivo de ultra alta precisión.

Cámaras de seguridad Wisenet XNF-9010RV y XNF-9010RVM de Hanwha Techwin

Hanwha Techwin ha realizado dos incorporaciones a su gama de cámaras Wisenet X, que cuentan con el *chipset* Wisenet7. Se trata de las cámaras de seguridad de 360 grados **Wisenet XNF-9010RV** (en la imagen) y **XNF-9010RVM** con 12 megapíxeles, ambas con iluminación IR integrada. Ambas cámaras disponen de corrección de distorsión integrada. Asimismo, ofrecen una variedad de modos de visualización alternativos, que incluyen vista panorámica única, panorámica doble y cuadrante.

Un PTZ digital permite a los usuarios desplazarse, inclinarse y acercarse electrónicamente a zonas específicas para tener una vista más detallada y, al mismo tiempo, continuar supervisando la vista completa de 360 grados. Además de ofrecer una potente herramienta para disuadir y detectar la actividad delictiva, las dos cámaras están equipadas con aplicaciones especializadas en inteligencia comercial que permiten a los usuarios sacar mucho más partido de sus sistemas de videovigilancia. Los mapas de calor, el conteo de personas y el análisis de vídeo para la gestión de colas ayudan a las empresas y al comercio minorista a identificar oportunidades para incrementar la productividad, comprender mejor el comportamiento de los clientes y mejorar la experiencia del mismo.

Versión mejorada de la plataforma SmaaS de Sensormatic para combatir la pérdida desconocida

Sensormatic Solutions ha actualizado la **plataforma SmaaS** (Shrink Management as a Service) con nuevas capacidades para ayudar a los minoristas a mejorar sus estrategias de prevención de pérdida desconocida. En concreto, esta plataforma gestiona los dispositivos y realiza un análisis predictivo que optimiza al personal y mejora las ventas.

SMaaS cuenta con una interfaz móvil optimizada y una navegación intuitiva. Ambos elementos posibilitan que los usuarios accedan a esta plataforma desde cualquier lugar y con cualquier dispositivo. Además, rastrea los patrones de ocupación definidos por el minorista. Así, estos pueden identificar los momentos de mayor tráfico para gestionar el personal y los clientes. Algo que también ayuda a cumplir las normas sanitarias.

SMaaS proporciona también un gran control de los dispositivos de circuito cerrado de televisión. Y permite a los usuarios visualizar clips de vídeo de las alarmas asociadas a eventos.

MARZO

V Conferencia Sectorial de Seguridad en Puertos

2 de marzo. En digital

Este evento abordará numerosas cuestiones de interés encaminadas a mejorar la protección en el ámbito portuario de la mano de varios profesionales especializados.

SEGURITECNIA
REVISTA DECANA INDEPENDIENTE DE SEGURIDAD

www.fundacionborreda.org

Milipol Qatar 2021

Del 15 al 17 de marzo

Esta feria internacional para la seguridad nacional y la defensa civil en el Medio Oriente contará con ponentes internacionales. Dichos profesionales tratarán la ciberseguridad, las nuevas tecnologías, las emergencias y la gestión de crisis.

www.milipolqatar.com

Simposium internacional de GAP

Del 22 al 24 de marzo. En digital

El Grupo Aeroportuario del Pacífico (GAP) y la revista *Segurilatam* celebrarán este evento para estudiar las últimas novedades sobre la seguridad en la aviación civil internacional.

SEGURILATAM

www.aeropuertosgap.com.mx/es

ABRIL

IV Encuentro sobre Seguridad e Investigación Privada

15 y 16 de abril. En digital

En este evento, actores de la seguridad e investigación privada presentarán las sinergias necesarias para afrontar los retos del sector. Borrmart llevará la secretaría técnica.

SEGURITECNIA
REVISTA DECANA INDEPENDIENTE DE SEGURIDAD

detcamp.com

Open Week 2021

Del 19 al 23 de abril. En digital

Tras el éxito de la primera edición, todas las cabeceras del Grupo Borrmart (*Seguritecnia, Red Seguridad, Formación de Seguridad Laboral, Seguridad Laboral Latam, Limpiezas, Facility Management and Services* y *Segurilatam*) volverán a sumar esfuerzos y sinergias en la organización de una semana digital que convocará a todas sus audiencias. El programa se desarrollará en sesiones diarias en directo y en contenidos audiovisuales permanentes a través de una web *app*.

SEGURITECNIA · Red Seguridad · Seguridad Laboral · facility · Limpiezas · SEGURILATAM

www.borrmart.es

MAYO

Tactical Edge 2021

12 y 13 de mayo. En digital

Diversos expertos presentarán temas relacionados con la ciberseguridad, desde la concienciación hasta nuevas soluciones tecnológicas utilizando Inteligencia Artificial y *Machine Learning*. La pasada edición trató el futuro de los *appliance* de WAF.

tacticaledge.co

IV Encuentro Profesional de la Seguridad en la Distribución, Logística y Comercio

18 de mayo. En digital

El reto que está suponiendo la distribución de la vacuna del COVID-19 en toda España será su principal eje temático. La anterior edición, celebrada en 2019 y que abordó esta temática desde el punto de vista físico y cibernético, trató la seguridad en el ámbito del *retail* desde múltiples vertientes: pérdida desconocida, procedimiento de denuncias, nuevos hábitos del consumo y colaboración, entre otras.

SEGURITECNIA
REVISTA DECANA INDEPENDIENTE DE SEGURIDAD

www.seguritecnia.es

1er Semestre 2021 Nº 49

Calificación Cepreven de

Empresas de Prestación de Servicios en Prevención y Seguridad

Relación de Empresas Calificadas

List of Qualified Companies

calificación cepreven

Período de Vigencia del Listado: 01/01/2021 a 30/06/2021

Aparición del próximo Listado incluyendo, en su caso, nuevas Empresas: **01/07/2021**

Lista actualizada en Internet: **www.cepreven.com**

¿Qué es la Calificación Cepreven?

La Calificación Cepreven es un sistema **complementario** de las exigencias oficiales, para contribuir a la mejora de la calidad y eficacia de las instalaciones de seguridad contra incendio.

Supone que la empresa instaladora, que **voluntariamente** decida incorporarse a la Calificación, respeta las **Reglas del Comité Europeo de Seguros (CEA)** para Evaluación y Calificación de Empresas Instaladoras de Sistemas de Seguridad contra Incendio y/o Robo y el Procedimiento español complementario.

El **Comité de Calificación,** en sus diferentes áreas, está integrado por representantes del sector asegurador, representantes de las empresas calificadas, usuarios y organismos competentes, y gestionado por **CEPREVEN**, que tramita los expedientes, asume la gestión técnica y realiza el seguimiento de las decisiones adoptadas.

Los controles "in situ" se llevan a cabo periódicamente por Verificadores autorizados, cuyos informes son puestos en conocimiento del Comité de Calificación, como apoyo técnico de la propuesta de decisiones a formular por el mismo, por lo que la presente relación es una referencia esencial para proyectistas, usuarios y entidades aseguradoras.

El Procedimiento trata de contribuir a que se respeten las adecuadas condiciones de proyecto y diseño, montaje, recepción y mantenimiento de las instalaciones.

Mediante un **sistema de verificaciones y controles** se pretenden evaluar de forma continuada los siguientes factores relacionados con las empresas peticionarias: Estabilidad, competencia técnica de su personal, fiabilidad de sus procedimientos y calidad de sus servicios de mantenimiento y posventa.

What is the Qualification Procedure?

It is a quality and efficiency control to improve our Fire Protection Installations, which means that those Listed Companies comply, in a continuous and supervised way, with the CEA Rules for Installers Firms of Security Systems or Firefighting Systems and its corresponding Spanish Procedure.

This List could be an essential reference for designers, specifiers and users, as well as a guide for the insurance industry.

The Listed Companies are checked, on a regular basis, through inspections of already erected systems choosed among the completed ones, which enable the Fire Protection Company to maintain its presence on the Qualification List.

¿A quién beneficia?

A los Usuarios y Asegurados: La Calificación de empresas está fundamentalmente concebida para informar a los usuarios en general y especialmente a los asegurados. Proporciona una referencia sobre las empresas especialistas en PCI que, habiendo decidido someterse voluntariamente al Procedimiento de Calificación, han superado satisfactoriamente los controles externos establecidos en el mismo.

A los Aseguradores: Constituye un elemento de gran utilidad para los Aseguradores ya que, dentro de sus misiones, además de la tradicional indemnización de los daños y perjuicios derivados de los siniestros, se encuentra la de asesorar a sus clientes en materia de prevención y protección. Las entidades aseguradoras disponen, con la calificación, de un elemento de referencia útil para el conocimiento del nivel de protección de los riesgos asegurados.

A los Instaladores e Ingenierías: Igualmente, la Calificación Cepreven resulta de interés para los propios instaladores e ingenierías calificadas como testimonio de su competencia, consecuencia de los controles a que se someten.

Calificaciones otorgadas a las empresas

ENTIDAD	Detección / Extinción								SCH	Pasiva			Ingeniería			
ARCE CLIMA, S.L.	♦	♦	♦													
CABALLERO SEGURIDAD, S.L. (Calificación otorgada para la Comunidad Valenciana)	■	■	■			■										
CATALANA DE SEGURETAT I COMUNICACIONS, S.L.	♦	♦	♦													
CHUBB PARSI, S.L.	♦	♦	♦													
COMERCIAL DE MATERIALES DE INCENDIOS, S.L.	♦	♦	♦	♦	♦	♦	♦	♦								
CONEJERO INSTALACIONES CONTRA INCENDIOS, S.L.			♦													
CONTROL IGNÍFUGO SOLUCIONES AVANZADAS, S.A.										♦	♦	♦				
COTEIN FIRE, S.L.	♦	♦	♦													
COTTES Fire & Smoke Solutions, S.L	♦	♦	♦						♦							
CV INSTALACIONES, S.L.	♦	♦														
CYMSA, CONTRATAS Y MANTENIMIENTO, S.A.		♦	♦													
DANMUR INSTALACIONES, S.L.	♦	♦	♦													
EIVAR OBRAS E INGENIERÍA, S.A.	♦	♦	♦		♦	♦		♦								
ENESA CONTINENTAL, S.L.										♦	♦	♦				
ENGIE	♦	♦	♦	♦	♦	♦		♦								
ESPARPLANT													♦	♦		
EXIA PROTECCIÓN CONTRA INCENDIO, S.L.	♦		♦													
FIRE CONSULT, S.L.	♦	♦	♦	♦	♦	♦		♦								
FUEGO DIEZ, S.L (Calificación otorgada para la Comunidad Valenciana)		■	■							♦	♦	♦				
GRUPO EUROFESA	♦	♦	♦													
GUIPONS, S.L.	♦															
IALEC, S.L.	♦	♦	♦			♦										
IBEREXT, S.A.	♦	♦	♦	♦	♦	♦		♦		♦	♦	♦				
JOMAR SEGURIDAD, S.L	♦	♦			♦	♦										
MANIX INTEGRAL, S.L.	♦		♦													
MECÁNICAS BOLEA, S.A.	♦			♦	♦	♦		♦								
MEISA	♦		♦	♦	♦	♦		♦								
MONTAJES INDUSTRIALES LLECA, S.A.	♦			♦	♦	♦		♦								
ONDOAN, S.COOP.	♦	♦	♦	♦	♦	♦		♦								
PACISA	♦	♦	♦	♦	♦	♦	♦	♦								
PCI CLIMA, S.L.		♦	♦	♦												
PEFIPRESA	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦		♦				
PIMEXA Protección contra Incendios, S.L.U.	♦	♦			♦			♦								
PREFIRE, S.L.	♦	♦	♦		♦				♦							
PROSEGUR ESPAÑA, S.L.	♦	♦	♦	♦	♦	♦	♦	♦					♦	♦	♦	
RG SYSTEMS																♦
SECURITAS SEGURIDAD ESPAÑA, S.A.	♦	♦	♦													
SIEMENS, S.A.	♦	♦	♦	♦	♦	♦	♦	♦								
SOLER PREVENCIÓN Y SEGURIDAD	♦	♦	♦	♦	♦	♦		♦								
STAR PROYECTOS Y MONTAJES, S.L.U.	♦	♦	♦													
SURIS, S.L.	♦	♦	♦													
TECHCO SECURITY, S.L.	♦	♦	♦	♦	♦	♦	♦	♦								
TÉCNICAS Y PROYECTOS IGNÍFUGOS, S.A. (TEPROSOL)										♦	♦	♦				
TESEIN, S.A.	♦	♦	♦													
TP CONTRA INCENDIO Y SEGURIDAD	♦		♦													

Las Empresas Calificadas disponen de un Sistema de Garantía de Calidad implantado y certificado según la Norma ISO 9001 cuyo alcance cubre la totalidad de los servicios que deben prestar estas empresas.

El área geográfica para la que se concede la Calificación abarca la totalidad del territorio nacional, salvo mención expresa.

♦ Ámbito Nacional ■ Ámbito Limitado

Calificaciones otorgadas a las empresas

ENTIDAD	Detección / Extinción								SCH	Pasiva			Ingeniería			
ARCE CLIMA, S.L.	♦	♦	♦													
CABALLERO SEGURIDAD, S.L. (Calificación otorgada para la Comunidad Valenciana)	■	■	■			■										
CATALANA DE SEGURETAT I COMUNICACIONS, S.L.	♦	♦	♦													
CHUBB PARSI, S.L.	♦	♦	♦													
COMERCIAL DE MATERIALES DE INCENDIOS, S.L.	♦	♦	♦	♦	♦	♦	♦	♦								
CONEJERO INSTALACIONES CONTRA INCENDIOS, S.L.			♦													
CONTROL IGNÍFUGO SOLUCIONES AVANZADAS, S.A.										♦	♦	♦				
COTEIN FIRE, S.L.	♦	♦	♦													
COTTES Fire & Smoke Solutions, S.L	♦	♦	♦						♦							
CV INSTALACIONES, S.L.	♦	♦														
CYMSA, CONTRATAS Y MANTENIMIENTO, S.A.		♦	♦													
DANMUR INSTALACIONES, S.L.	♦	♦	♦													
EIVAR OBRAS E INGENIERÍA, S.A.	♦	♦	♦		♦	♦		♦								
ENESA CONTINENTAL, S.L.										♦	♦	♦				
ENGIE	♦	♦	♦	♦	♦	♦		♦								
ESPARPLANT													♦	♦		
EXIA PROTECCIÓN CONTRA INCENDIO, S.L.	♦		♦													
FIRE CONSULT, S.L.	♦	♦	♦	♦	♦	♦		♦								
FUEGO DIEZ, S.L (Calificación otorgada para la Comunidad Valenciana)		■	■							♦	♦	♦				
GRUPO EUROFESA	♦	♦	♦													
GUIPONS, S.L.	♦															
IALEC, S.L.	♦	♦	♦			♦										
IBEREXT, S.A.	♦	♦	♦	♦	♦	♦		♦		♦	♦	♦				
JOMAR SEGURIDAD, S.L	♦	♦			♦	♦										
MANIX INTEGRAL, S.L.	♦		♦													
MECÁNICAS BOLEA, S.A.	♦			♦	♦	♦		♦								
MEISA	♦		♦	♦	♦	♦		♦								
MONTAJES INDUSTRIALES LLECA, S.A.	♦			♦	♦	♦		♦								
ONDOAN, S.COOP.	♦	♦	♦	♦	♦	♦		♦								
PACISA	♦	♦	♦	♦	♦	♦	♦	♦								
PCI CLIMA, S.L.		♦	♦	♦												
PEFIPRESA	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦		♦				
PIMEXA Protección contra Incendios, S.L.U.	♦	♦			♦			♦								
PREFIRE, S.L.	♦	♦	♦		♦				♦							
PROSEGUR ESPAÑA, S.L.	♦	♦	♦	♦	♦	♦	♦	♦					♦	♦	♦	
RG SYSTEMS																♦
SECURITAS SEGURIDAD ESPAÑA, S.A.	♦	♦	♦													
SIEMENS, S.A.	♦	♦	♦	♦	♦	♦	♦	♦								
SOLER PREVENCIÓN Y SEGURIDAD	♦	♦	♦	♦	♦	♦		♦								
STAR PROYECTOS Y MONTAJES, S.L.U.	♦	♦	♦													
SURIS, S.L.	♦	♦	♦													
TECHCO SECURITY, S.L.	♦	♦	♦	♦	♦	♦	♦	♦								
TÉCNICAS Y PROYECTOS IGNÍFUGOS, S.A. (TEPROSOL)										♦	♦	♦				
TESEIN, S.A.	♦	♦	♦													
TP CONTRA INCENDIO Y SEGURIDAD	♦		♦													

Las Empresas Calificadas disponen de un Sistema de Garantía de Calidad implantado y certificado según la Norma ISO 9001 cuyo alcance cubre la totalidad de los servicios que deben prestar estas empresas.

El área geográfica para la que se concede la Calificación abarca la totalidad del territorio nacional, salvo mención expresa.

♦ Ámbito Nacional ■ Ámbito Limitado

Relación de Entidades Aseguradoras Adheridas

Las Entidades adheridas al Programa de Calificación desarrollan un Plan de Actuación que comprende la difusión de los listados, la toma en consideración de las Empresas Calificadas, la posible denuncia de deficiencias observadas por sus servicios de inspección y la solicitud a sus asegurados de los certificados emitidos por la Empresa Instaladora Calificada.

- ALLIANZ COMPAÑÍA DE SEGUROS Y REASEGUROS S.A.
- ASEFA, S.A. DE SEGUROS Y REASEGUROS
- AXA SEGUROS GENERALES, S.A. DE SEGUROS Y REASEGUROS
- BILBAO, C. A. DE SEGUROS Y REASEGUROS
- CAJA DE SEGUROS REUNIDOS, COMPAÑÍA DE SEGUROS Y REASEGUROS, S.A. (CASER)
- ESPAÑA, S.A. COMPAÑÍA NACIONAL DE SEGUROS
- GENERALI ESPAÑA, S.A. DE SEGUROS Y REASEGUROS
- HDI GLOBAL SE SUCURSAL EN ESPAÑA
- HELVETIA COMPAÑÍA SUIZA, S.A. DE SEGUROS Y REASEGUROS
- LIBERTY SEGUROS, COMPAÑÍA DE SEGUROS Y REASEGUROS, S.A.
- METRÓPOLIS, S.A. COMPAÑÍA NACIONAL DE SEGUROS Y REASEGUROS
- MGS SEGUROS Y REASEGUROS, S.A.
- MUSSAP, MUTUA DE SEGUROS Y REASEGUROS, APF
- MUTUA TINERFEÑA, MUTUA DE SEGUROS Y REASEGUROS APF
- OCASO, S.A. COMPAÑIA DE SEGUROS Y REASEGUROS
- PELAYO MUTUA DE SEGUROS Y REASEGUROS, APF
- PLUS ULTRA SEGUROS GENERALES Y VIDA, S.A. DE SEGUROS Y REASEGUROS
- PREVENTIVA, COMPAÑIA DE SEGUROS Y REASEGUROS, S.A.
- REALE SEGUROS GENERALES, S.A.
- SANTA LUCÍA, S.A. COMPAÑÍA DE SEGUROS Y REASEGUROS
- SEGURCAIXA ADESLAS, S.A. DE SEGUROS Y REASEGUROS
- SEGUROS CATALANA OCCIDENTE, S.A. DE SEGUROS Y REASEGUROS
- SEGUROS LAGUN ARO, S.A.
- ZURICH INSURANCE P.L.C.

Cada una de las Empresas Calificadas dispone de diplomas individualizados por tipo de calificación, que pueden ser solicitados por las Entidades Aseguradoras o personas interesadas.

El otorgamiento de la correspondiente Calificación tiene como función facilitar, tanto a los Aseguradores como a los usuarios, el conocimiento y selección de aquellos instaladores que, en los controles y verificaciones previas, hayan acreditado un adecuado nivel en sus prestaciones, con una finalidad, por tanto, exclusivamente asesora, informadora y de orientación, pero sin que ello constituya en ningún caso a CEPREVEN ni al Comité de Calificación en garantes del correcto funcionamiento o de la calidad de los equipos instalados.

calificación cepreven

Asociación de Investigación para la Seguridad de Vidas y Bienes
Centro Nacional de Prevención de Daños y Pérdidas
Av. del General Perón, 27 - 28020 MADRID - Tel.: 91 445 75 66 - Fax: 91 445 71 36
www.calificacioncepreven.com

Directorio

- Alarmas
- Área jurídica en seguridad
- Armas de Fuego
- Asociaciones
- Auxiliares de servicio y control de accesos
- CCTV
- Centrales receptoras
- Centrales recepción de alarmas
- Centro de formación
- Cerraduras y cilindros
- Controles de acceso
- Detección de incendios
- Detección volumétrica
- Empresas instaladoras de sistemas
- Equipos de inspección de rayos X
- Equipos y dotaciones para empresas de vigilancia
- Ingeniería de seguridad
- Instalaciones detección y extinción de incendios
- Instalación y mantenimiento de sistemas protección contra incendios
- Instalaciones de sistemas de seguridad
- Mantenimiento de extintores e instalaciones fijas contra incendios
- Proteccion contra incendios
- Proteccion de infraestructuras críticas
- Seguridad electrónica
- Seguridad integral
- Sistemas de alarma con verificación por vídeo
- Sistemas analógicos de protección contra incendios
- Software de gestión para la seguridad
- Software de ingeniería de seguridad
- Soluciones integradas de seguridad electrónica
- Telecomunicaciones
- Tratamiento de efectivo
- Vigilantes de Seguridad

ALARMAS

Fundada en 1966

INSTALACIONES A SU MEDIDA
C/ Antoñita Jiménez, 25
28019 - MADRID
Tel.: 91 565 54 20
Fax: 91 565 53 23
E-mail: seguridad@grupoaguero.com
Web: www.grupoaguero.com

ALARMAS, ASISTENCIA Y SEGURIDAD S.L

Parque Empresarial Campollano, Avenida 3ª, nº 16, Nave nº 27
02007(Albacete)
Tel.: 967 101 058
E-mail.:info@aasseguridad.es

BOSCH SECURITY AND SAFETY SYSTEMS

SOLUCIONES GLOBALES DE CCTV - IP- INTRUSIÓN - INCENDIO - MEGAFONÍA - EVACUACIÓN POR VOZ - CONGRESOS

OFICINAS CENTRALES Y DELEGACIÓN ZONA CENTRO
Avda. de la Institución Libre de Enseñanza, 19
28037 MADRID
Tel.: 914 102 011
Fax: 914 102 056

DELEGACIÓN ZONA ESTE
C/ Sancho de Ávila, 80
08018 BARCELONA
Tel.: 91 410 40 80

DELEGACIÓN ZONA NORTE
Tel.: 676 600 612

DELEGACIÓN ZONA SUR
Tel.: 648 19 08 04

E-mail: es.securitysystems@es.bosch.com
Web: www.boschsecurity.es

CCTV, INTRUSIÓN, CONTROL DE ACCESOS, INCENDIO

www.bydemes.com

San Fructuoso 50-56
08004 Barcelona (España)
Tel.: 934 254 960 / 934 269 111
Fax: 934 261 904
bydemes@bydemes.com

ALMACEN BARCELONA:
Motors 348-358, Pol. Ind. Gran Vía Sur
08908 Hospitalet de Llobregat. (BARCELONA)
Tel.: 934 254 960 - Ext. 303
(Almacén) y 301 (Tienda)
almacenbcn@bydemes.com

MADRID
Avda. Somosierra 22, Nave F, Planta 1 Inferior
28703 San Sebastián de los Reyes. (MADRID)
Tel.: 917 544 804
madrid@bydemes.com

CANARIAS
Carretera del Norte 113
35013 Las Palmas de Gran Canaria
Tel.: 928 426 323
Fax: 928 417 077
canarias@bydemes.com

BY DEMES PORTUGAL
Rua Fernando Namora 33, 2º-I
4425-651 Maia, Porto (Portugal)
Tel.: +351 932 220 421
portugal@bydemes.com

RISCO GROUP IBERIA, S.L.

C/ San Rafael,1
28108 - Alcobendas (MADRID)
Tel.: 91 490 21 33
Fax: 91 490 21 34
E-mail: sales-es@riscogroup.com
Web: www.riscogroup.es

TECNOALARM

C/ Vapor 18 (Pol. Ind. El Regàs)
08850 Gavà (BARCELONA)
Tel. +34 936 622 417
Fax: +34 936 622 438
www.tecnoalarm.es

TINOCO SISTEMAS

R.D.G.S.E. Nº 758 EL 13/11/1985

- Sistemas de Alarmas
- Circuito Cerrado de Televisión
- Protección Contra Incendios
- Control de Accesos

OFICINA TÉCNICA:
C/ Manuel Villalobos, 37
41009- Sevilla
Tel.: 954 350 052
Fax.: 954 430 005

SEDE SOCIAL:
C/ Fray Luis de Granada, 1
41009- Sevilla
Tel.: 954 217 236
Fax.: 954 430 005
E-mail.: info@tinocosistemas.com
Web: www.tinocosistemas.es

ÁREA JURÍDICA EN SEGURIDAD

SEGURLEX CONSULTORES & COMPLIANCE

C/ Don Ramón de la Cruz, 68 - 2 Dcha.
280001 Madrid. ESPAÑA
Tel.: +34 91 401 88 74
www.segurlex.com.es
info@segurlex.com.es

ARMAS DE FUEGO

DEFENSA Y SEGURIDAD

SHOT MADRID S.L.

Juan de Urbieta, 22.
Tels.: 91 552 43 57 / 91 433 24 42
Fax: 91 552 98 22
28007 MADRID
www.tiendashoke.es
info@tiendashoke.es

ASOCIACIONES

ACAES

Viladomat 174
08015 Barcelona
Tel.: 93 454 48 11
Fax: 93 453 62 10
E-mail: acaes@acaes.net

ASOCIACIÓN ESPAÑOLA DE INGENIEROS DE SEGURIDAD (AEINSE)

C/. San Delfin nº4 (Local calle)
28019 MADRID
Tel.: 660 09 60 68
Web: www.aeinse.es

A.E.S. ASOCIACIÓN DE EMPRESAS DE SEGURIDAD

C/ Alcalá , 99 2ª A
Tel: 91 576 52 25.
Fax: 91 576 60 94
28009 MADRID

ASOCIACIÓN PROFESIONAL DE COMPAÑIAS PRIVADAS DE SERVICIOS DE SEGURIDAD

C/ Princesa 43 - 2º Izda.
Tel.: 91 454 00 00
Fax: 91 541 10 90
28008 MADRID
E-mail: aproser@aproser.es
Web: www.aproser.es

SOCIEDAD ESPAÑOLA DE DERECHO DE LA SEGURIDAD

C/ Don Ramón de la Cruz, 68
Tel.: 670 77 02 99
28001 MADRID
Web: www.derecho-seguridad.org
E-mail: info@derecho-seguridad.org

Federación Empresarial Española de Seguridad

C/ Vizcaya 4, Local
28045 MADRID
Tel.: 91 554 21 15
Web: www.fes.es
E-mail: fes@fes.es

TECNIFUEGO

Asociación Española de Sociedades de Protección contra Incendios

C/ Doctor Esquerdo 55, 1ºF
28007 MADRID
Tel.: +34 914 361 419
Fax: +34 915 759 635
Linkedin: http://www.linkedin.com/groups/

AUXILIARES DE SERVICIO Y CONTROL DE ACCESOS

COYMA SERVICIOS GENERALES, S.L.

SERVICIOS DE PREVENCIÓN, MANTENIMIENTO Y EXTINCIÓN DE INCENDIOS, SERVICIO DE BOMBEROS

Sede Operativa:
Avda. Olivares nº 17 - P.I. El Pibo
41110 Bollullos de la Mitación (SEVILLA)

Sede Social:
Plaza del Punto, 1º Dcha.
21003 (HUELVA)
Tel.: 902 194 814
Fax: 954 002 319
Web: www.controlymantenimiento.com
E-mail: gerencia@gruporomade.com

FORCE 1 GENERAL SERVICES, S.L.

SERVICIOS DE PORTERÍA, CONTROL DE ACCESOS Y MANTENIMIENTO

Sede Operativa:
Avda. Olivares nº 17 - P.I. El Pibo
41110 Bollullos de la Mitación (SEVILLA)

Sede Social:
Plaza de la Aceituna nº 1- Local 8
41960 Gines (SEVILLA)
Tel. 902 194 814
Fax: 954 002 319
Web: www.forceonegeneralservices.com
E-mail: gerencia@gruporomade.com

CCTV

ADI GLOBAL DISTRIBUTION

OFICINA Y ALMACÉN CENTRAL
Avda. de Italia, 7- P.I. CT Coslada
28821 Coslada (MADRID)

DELEGACIONES
Madrid, Bilbao, Barcelona, Valencia, Sevilla y Lisboa
188 oficinas en todo el mundo
Dpto. Comercial: 91 419 17 20
Soporte Técnico: 91 419 17 10
Web: www.adiglobal.com/es
E-mail: infospain@adiglobal.com

AXIS COMUNICATIONS

Vía de los Poblados, 3. Edif. 3, planta 1
Parque Empresarial Cristalia
28033 (MADRID)
Tel.. 91 803 46 43
Fax: 91 803 54 52
E-mail: info-es@axis.com
Web: www.axis.com/es

BOSCH

SOLUCIONES GLOBALES DE CCTV - IP- INTRUSIÓN - INCENDIO - MEGAFONÍA - EVACUACIÓN POR VOZ - CONGRESOS

BOSCH SECURITY AND SAFETY SYSTEMS

OFICINAS CENTRALES Y DELEGACIÓN ZONA CENTRO
Avda. de la Institución Libre de Enseñanza, 19
28037 MADRID
Tel.: 914 102 011
Fax: 914 102 056

DELEGACIÓN ZONA ESTE
C/ Sancho de Ávila, 80
08018 BARCELONA
Tel.: 91 410 40 80

DELEGACIÓN ZONA NORTE
Tel.: 676 600 612

DELEGACIÓN ZONA SUR
Tel.: 648 19 08 04

E-mail: es.securitysystems@es.bosch.com
Web: www.boschsecurity.es

GRUPO QUANTUM DISTRIBUCION GLOBAL, S.L.

C/ Can Milans, 51 P.I. Can Milans
08110 Montcada i Reixac. (BARCELONA)
Tlfno.: 935 726 218
E-mail: comercial@grupoquantum.es
Web: www.grupoquantum.es

CCTV CENTER

Parque Tecnológico
C/ Alexander Graham Bell, nº 6.
Tel.: 96 132 11 01
Fax: 96 132 11 08
46980 Paterna (VALENCIA)
E-mail: comerciales@cctvcentersl.es

CCTV, INTRUSIÓN, CONTROL DE ACCESOS, INCENDIO

www.bydemes.com

San Fructuoso 50-56
08004 Barcelona (España)
Tel.: 934 254 960 / 934 269 111
Fax: 934 261 904
bydemes@bydemes.com

ALMACEN BARCELONA:
Motors 348-358, Pol. Ind. Gran Vía Sur
08908 Hospitalet de Llobregat. (BARCELONA)
Tel.: 934 254 960 - Ext. 303
(Almacén) y 301 (Tienda)
almacenbcn@bydemes.com

MADRID
Avda. Somosierra 22, Nave F, Planta 1 Inferior
28703 San Sebastián de los Reyes. (MADRID)
Tel.: 917 544 804
madrid@bydemes.com

CANARIAS
Carretera del Norte 113
35013 Las Palmas de Gran Canaria
Tel.: 928 426 323
Fax: 928 417 077
canarias@bydemes.com

BY DEMES PORTUGAL
Rua Fernando Namora 33, 2º-I
4425-651 Maia, Porto (Portugal)
Tel.: +351 932 220 421
portugal@bydemes.com

DAHUA IBERIA S.L.

Avda. de la Transición Española, 24,
28108 Alcobendas
Tel: +34 917 64 98 62
Web: www.dahuasecurity.com/es/
E-mail: sales.iberia@dahuatech.com

PELCO INC.

Avda. Bruselas 15, Pt. 2
28108 Alcobendas (MADRID)
Tel.: +34 910766800
Web: www.pelco.com
E-mail: pelco.iberia@pelco.com

CENTRALES RECEPTORAS

D.G.P. N.º 597
R.D.G.S.E. nº 597 de fecha 15-7-1985

CENTRAL
Polígono Industrial «El Montalvo II»
C/ Honfria, 30-32
37008 SALAMANCA
Tel.: 902 191 010
Fax: 923 19 05 05
E-mail: vasbe@vasbe.com

DELEGACIONES
MURCIA
Avda. Teniente Montesinos nº 8
Torre A, 4ª planta, oficina 13
30100 MURCIA

VALLADOLID
Edificio Gran Villas Norte
C/ Sajambre (local)
47008 VALLADOLID

CENTRALES RECEPCIÓN DE ALARMAS

CENTRO ESPECIAL DE RECEPCIÓN Y CONTROL DE ALARMAS, S.A.

Número de Homologación: 2970

C/ Bruselas, 16-A. Parque Európolis
28232 Las Rozas (MADRID)
Tel.: 902 180 644
Fax: 91 637 22 73
Web: www.cerca.es
E-mail: cerca@cerca.es

RECEPCIÓN Y CONTROL DE ALARMAS S.L.

Empresa inscrita en la Dirección General de Policía con el n.º 2.572, del día 14 /02/1996

Zamora, 45-47, ático 1.ª
Tel.: 93 242 45 50
C.R.A.: 902 184 184 (24h.)
08005 BARCELONA
Web: www.recepcionycontrol.com
E-mail: info@recepcionycontrol.com

PYCSECA seguridad

Autorizada por la Dirección General de Seguridad con el nº 914
Con fecha 3 de julio de 1986

MADRID
Isabel Collbrand 10-12 28050 Madrid
Tel.: 91 358 97 77
madrid@pycseca.com

BARCELONA
Padilla 228 3ª Planta 08013 Barcelona
Tel.: 93 231 04 12
barcelona@pycseca.com

ALICANTE
Capitán Hernández Mira 1 03004 Alicante
Tel.: 96 524 93 03
alicante@pycseca.com

PALMA DE MALLORCA
Almirante Oquendo 8 07014 Palma de Mallorca
Tel.: 971 71 98 01
palma@pycseca.com

VALENCIA
Nicolás Estévanez 5 46018 Valencia
Tel.: 96 354 04 40
valencia@pycseca.com

MURCIA
Pio XII 47 Bajos 30012 Murcia
Tel.: 968 34 47 70
murcia@pycseca.com

MÁLAGA
Pico de las palomas port. 11 local 45 29004 Málaga
Tel.: 952 36 39 44
malaga@pycseca.com

SEVILLA
Parsi 13 nº 28 41016 Sevilla
Tel.: 954 67 21 72
sevilla@pycseca.com

A CORUÑA
Avd. Ernesto Che Guevara nº 15B 15172
A Coruña
Tel.: 981 658 194
galicia@pycseca.com

TELÉFONO ATENCIÓN CLIENTES
902 153 397

CENTRO DE FORMACIÓN

ASOCIACIÓN DE INVESTIGACIÓN PARA LA SEGURIDAD DE VIDAS Y BIENES

Centro Nacional de Prevención de Daños y Pérdidas
Av. del General Perón, 27- 5º
Tels.: 91 445 7566 • 91 445 7381
Fax: 91 445 7136
28020 MADRID
E-mail: formacion@cepreven.com
www.cepreven.com

SERVICIOS TÉCNICOS CEPRETEC, S.L. GRUPO CEPREVEN

Av. del General Perón, 27- 5º
Tel.: 91 593 0208
Fax: 91 594 2703
28020 MADRID
E-mail: cepretec@cepreven.com
www.cepreven.com

CETS

CENTRO DE ESTUDIOS DE TÉCNICAS DE SEGURIDAD

SEDE SOCIAL
C/ Segundo Mata, 6.
Edificio Estación
28224 Pozuelo de Alarcón - MADRID
Tel.: 91 351 56 29
Fax: 902 366 044
Web: www.formacioncets.com
E-mail. cets@formacioncets.com

CENTROS DE FORMACIÓN
C/ Segundo Mata, 6.
Edificio Estación
28224 Pozuelo de Alarcón (MADRID)

C/ Teide nº3, planta baja
28703 San Sebastián de los Reyes (MADRID)

ROMADE GRUPO CORPORATIVO S.L.

Homologado por el Ministerio del Interior
Formación Específica de Seguridad Privada

Sede Social:
C/ Doctor Duarte Acosta, nº 7
11500 El Puerto de Santa María (Cádiz)

Centro Formación:
Avda Olivares nº 17- P.I. El Pibo
41110 Bollullos de la Mitación (SEVILLA)
Tel.: 902 194 814
Fax: 954 002 319
Web: www.gruporomadeformacion.com
E-mail: gerencia@gruporomade.com

CERRADURAS Y CILINDROS

STRONGPOINT

Avda. de los Reyes,15
28770 Colmenar Viejo. (MADRID)
Tel.: +34 91 847 50 39
Web: www.strongpoint.es
E-mail: info.es@strongpoint.com

CONTROLES DE ACCESO

CCTV, INTRUSIÓN, CONTROL DE ACCESOS, INCENDIO

www.bydemes.com

San Fructuoso 50-56
08004 Barcelona (España)
Tel.: 934 254 960 / 934 269 111
Fax: 934 261 904
bydemes@bydemes.com

ALMACEN BARCELONA:
Motors 348-358, Pol. Ind. Gran Vía Sur
08908 Hospitalet de Llobregat. (BARCELONA)
Tel.: 934 254 960 - Ext. 303
(Almacén) y 301 (Tienda)
almacenbcn@bydemes.com

MADRID
Avda. Somosierra 22, Nave F, Planta 1 Inferior
28703 San Sebastián de los Reyes. (MADRID)
Tel.: 917 544 804
madrid@bydemes.com

CANARIAS
Carretera del Norte 113
35013 Las Palmas de Gran Canaria
Tel.: 928 426 323
Fax: 928 417 077
canarias@bydemes.com

BY DEMES PORTUGAL
Rua Fernando Namora 33, 2º-I
4425-651 Maia, Porto (Portugal)
Tel.: +351 932 220 421
portugal@bydemes.com

DETECCIÓN DE INCENDIOS

ALARMAS, ASISTENCIA Y SEGURIDAD S.L

Parque Empresarial Campollano, Avenida 3ª, nº 16, Nave nº 27
02007(Albacete)
Tel.: 967 101 058
E-mail.:info@aasseguridad.es

CCTV, INTRUSIÓN, CONTROL DE ACCESOS, INCENDIO

www.bydemes.com

San Fructuoso 50-56
08004 Barcelona (España)
Tel.: 934 254 960 / 934 269 111
Fax: 934 261 904
bydemes@bydemes.com

ALMACEN BARCELONA:
Motors 348-358, Pol. Ind. Gran Vía Sur
08908 Hospitalet de Llobregat. (BARCELONA)
Tel.: 934 254 960 - Ext. 303
(Almacén) y 301 (Tienda)
almacenbcn@bydemes.com

MADRID
Avda. Somosierra 22, Nave F, Planta 1 Inferior
28703 San Sebastián de los Reyes. (MADRID)
Tel.: 917 544 804
madrid@bydemes.com

CANARIAS
Carretera del Norte 113
35013 Las Palmas de Gran Canaria
Tel.: 928 426 323
Fax: 928 417 077
canarias@bydemes.com

BY DEMES PORTUGAL
Rua Fernando Namora 33, 2º-I
4425-651 Maia, Porto (Portugal)
Tel.: +351 932 220 421
portugal@bydemes.com

CONTROL DE ACCESOS E INTEGRACIÓN DE SISTEMAS DE SEGURIDAD

Parque Tecnológico de Álava
C/ Albert Einstein, 34
01510 Miñano Mayor (ÁLAVA)
Tel.: 945 29 87 90
Fax: 945 29 81 33
E-mail: comercial@dorlet.com
Web: http://www.dorlet.com

DORMAKABA ESPAÑA S.A.

C/ María Tubau, 4 Torre A- 2Pl
28050 Madrid
Tel.: +34 902 244 111
www.dormakaba.com

ZKTECO EUROPE

Carretera de Fuencarral 44. Edificio 1. Planta 2
28108 Alcobendas (Madrid)
Tel.: 91 653 28 91
Fax: 91 6593200
www.zkteco.eu

C/ de la Ciència 30-32
08840 Viladecans (BARCELONA)
Tel: +34 93 371 60 25
info@detnov.com
www.detnov.com

DELEGACIÓN CENTRO
C/ La Granja 30 bajo
Tel.: 91 919 79 69
28108 Alcobendas (Madrid)

TECNOFIRE

C/ Vapor 18 (Pol. Ind. El Regàs)
08850 Gavà (BARCELONA)
Tel. +34 936 622 417
Fax: +34 936 622 438
Web:www.tecnofiredetection.com

DETECCIÓN VOLUMÉTRICA

CCTV, INTRUSIÓN, CONTROL DE ACCESOS, INCENDIO

www.bydemes.com

San Fructuoso 50-56
08004 Barcelona (España)
Tel.: 934 254 960 / 934 269 111
Fax: 934 261 904
bydemes@bydemes.com

ALMACEN BARCELONA:
Motors 348-358, Pol. Ind. Gran Vía Sur
08908 Hospitalet de Llobregat. (BARCELONA)
Tel.: 934 254 960 - Ext. 303
(Almacén) y 301 (Tienda)
almacenbcn@bydemes.com

MADRID
Avda. Somosierra 22, Nave F, Planta 1 Inferior
28703 San Sebastián de los Reyes. (MADRID)
Tel.: 917 544 804
madrid@bydemes.com

CANARIAS
Carretera del Norte 113
35013 Las Palmas de Gran Canaria
Tel.: 928 426 323
Fax: 928 417 077
canarias@bydemes.com

BY DEMES PORTUGAL
Rua Fernando Namora 33, 2º-I
4425-651 Maia, Porto (Portugal)
Tel.: +351 932 220 421
portugal@bydemes.com

EMPRESA INSTALADORA DE SISTEMAS

SOLUCIONES PROFESIONALES DE SEGURIDAD

www.invisec.com
902365629

EQUIPOS DE INSPECCIÓN DE RAYOS X

C/ Basauri nº 10-12, Urb. La Florida
Ctra. de la Coruña, Aravaca
Tel.: 91 566 22 00
Fax: 91 566 22 05
28023 Madrid
E-mail: cotelsa@cotelsa.es
Web: www.cotelsa.es

EXCEM TECHNOLOGIES

Paseo de la Castellana, 93 Planta 9
280246 Madrid
Tel.: +34 91 417 46 20
Fax: +34 91 417 46 30
E-mail: comercial@excem.com
Web: www.excem.com

TARGET TECNOLOGÍA S.A.

Ctra. De Fuencarral, 24
Edificio Europa I, portal 1, planta 3ª
28108 Alcobendas (MADRID)
Tel.: 91 554 14 36
Fax: 91 554 45 89
E-mail: info@target-tecnologia.es
Web: www.target-tecnologia.es

TECOSA

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

Division Building Technologies
Ronda de Europa, 5
28760 Tres Cantos - MADRID
Tel.: +34 91 514 75 00
Asistencia Técnica: 902 199 029
www.tecosa.es

EQUIPOS Y DOTACIONES PARA EMPRESAS DE VIGILANCIA

DEFENSA Y SEGURIDAD SHOT MADRID S.L.

Juan de Urbieta, 22.
Tels.: 91 552 43 57 / 91 433 24 42
Fax: 91 552 98 22
28007 MADRID
www.tiendashoke.es
info@tiendashoke.es

INGENIERÍA DE SEGURIDAD

Telefónica
INGENIERÍA DE SEGURIDAD

Homologada por la D.G.P.
con Nº 600 a fecha 19-01-1985

Ramón Gómez de la Serna 109-113, bajo posterior
Tel.: +34 902 10 43 53
28035 Madrid (ESPAÑA)
E-mail: tis.clientes@telefonica.es
www.telefonica.com/ingenieriadeseguridad

INSTALACIONES DETECCIÓN Y EXTINCIÓN DE INCENDIOS

INV

INV SEGURIDAD
R.D.G.S.E. nº 2888

✓ Sistemas de Seguridad
✓ Protección contra incendios

Domicilio Social
C/ Tomás Redondo nº 2 Planta 5
Edificio Indobuilding
28033 MADRID
Tel.: 902 112 777
Fax: 91 763 09 33
Web: www.invseguridad.com
E-mail: cliente@invseguridad.com

Techco security

Inscrita en el Registro de Empresas de la Dirección de Seguridad del Estado con n.º 2979 de fecha 22-05-01

Domicilio Social
C/ Barbadillo, n.º 7
Centralita: 91 312 77 77
Fax: 91 329 25 74
28042 Madrid. ESPAÑA.
Web: www.techcosecurity.com

INSTALACIÓN Y MANTENIMIENTO DE SIST. PROTECCIÓN CONTRA INCENDIOS

pefipresa
Protección integral contra incendios

INSTALACIÓN Y MANTENIMIENTO DE SISTEMAS DE PROTECCIÓN CONTRA INCENDIOS

PEFIPRESA, S.A.
C/ San Cesáreo, 22
28021 Madrid
Tfn: 91 710 90 00
Fax: 91 798 04 96
Web: www.pefipresa.com
E-mail: info.madrid@pefipresa.com

INSTALACIONES DE SISTEMAS DE SEGURIDAD

FORCE-1 SECURITY System

CIASIPROIND, S.L.
Inscrita en GPD con nº 3598 con fecha de 17/03/2009

Sede Operativa:
Avda. Olivares nº 17 - P.I. El Pibo
41110 Bollullos de la Mitación (SEVILLA)

Sede Social:
Avda. Castilleja 16, local 1
41110 Bollullos de la Mitación (SEVILLA)
Tel.: 902 194 814
Fax: 954 002 319
Web: www.forceonesystem.com
E-mail:gerencia@gruporomade.com

INV

INV SEGURIDAD
R.D.G.S.E. nº 2888

✓ Sistemas de Seguridad
✓ Protección contra incendios

Domicilio Social
C/ Tomás Redondo nº 2 Planta 5
Edificio Indobuilding
28033 MADRID
Tel.: 902 112 777
Fax: 91 763 09 33
Web: www.invseguridad.com
E-mail: cliente@invseguridad.com

Techco security

Inscrita en el Registro de Empresas de la Dirección de Seguridad del Estado con n.º 2979 de fecha 22-05-01

Domicilio Social
C/ Barbadillo, n.º 7
Centralita: 91 312 77 77
Fax: 91 329 25 74
28042 Madrid. ESPAÑA.
Web: www.techcosecurity.com

PROTECCION CONTRA INCENDIOS

aguilera GRUPO
detección, control y extinción de incendios

GRUPO AGUILERA

SEDE CENTRAL
C/ Julián Camarillo, 26 - 2ª Planta
28037 MADRID
Tel: 91 754 55 11 - Fax: 91 754 50 98

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

DELEGACIÓN GALICIA
C/ José Luis Bugallal Marchesi Nº 9, 1º B
15008 A CORUÑA
Tel: 98 114 02 42 - Fax: 98 114 24 62

DELEGACIÓN CATALUÑA
C/ Rafael de Casanovas, 7 y 9
SANT ADRIA DEL BESOS
08930 BARCELONA
Tel: 93 381 08 04 - Fax: 93 381 07 58

DELEGACIÓN LEVANTE
Tel: 628 92 70 56 - Fax: 91 754 50 98

DELEGACIÓN ANDALUCIA
C/ Industria, 5 Ed. Metropol 3, 3ª Planta,
Mod.17. P.I.S.A.
41927 M. del Aljarafe SEVILLA
Tel: 95 465 65 88 - Fax: 95 465 71 71

DELEGACIÓN CANARIAS
C/ San Paolo, 17 - Pol. Ind, El Sebadal
35008 LAS PALMAS DE GRAN CANARIA
Tel: 928 24 45 80 - Fax: 928 24 65 72

SIEMENS

Siemens S.A.
Division Building Technologies

Área Fire Safety
Ronda de Europa, 5
28760 Tres Cantos (MADRID)
Tel.: 91 514 80 00
Fax: 91 514 07 01
www.siemens.es/buildingtechnologies

Tecnofire DETECTION

TECNOFIRE

C/ Vapor 18 (Pol. Ind. El Regàs)
08850 Gavà (BARCELONA)
Tel. +34 936 622 417
Fax: +34 936 622 438
Web:www.tecnofiredetection.com

PROTECCION DE INFRAESTRUCTURAS CRÍTICAS

grupo control seguridad

GRUPO CONTROL EMPRESA DE SEGURIDAD S.A

Domicilio Social
Avenida Somosierra, 12
28700 San Sebastián de los Reyes - MADRID
Tel: 902 26 22 22
Web: www.grupocontrol.com
E-mail: info@grupocontrol.com

ELECTRÓNICA SUBMARINA
SAES

SAES
SOCIEDAD ANÓNIMA DE ELECTRÓNICA SUBMARINA

Sede Cartagena
Ctra. de la Algameca, s/n
30205 - Cartagena (Murcia)
Tel.: 968 508 214
Fax: 968 507 713
Web: www.electronica-submarina.com
E-mail: saes@electronica-submarina.com

Sede San Fernando
Ctra. de la Carraca s/n
11100 - San Fernando (Cádiz)
Tel.: 956 801 048
Fax: 956 892 872
Web: www.electronica-submarina.com
E-mail: saes@electronica-submarina.com

SEGURIDAD ELECTRÓNICA

Ingloba Seguridac

INNOVACIÓN GLOBAL DE SEGURIDAD, S.A. (INGLOBA)

SEGURIDAD ELECTRÓNICA, INGENIERÍA, INTEGRRACIÓN, INSTALACIÓN Y MANTENIMIENTO DE SISTEMAS DE SEGURIDAD Y P.C.I.

C/ Pierre Curie, 17.
Parque Empresarial La Garena
Álcala de Henares (MADRID)
28806 MADRID
Tel. 91 877 41 01. Fax: 91 877 67 90
Web: www.inglobaseguridad.com
E-mail: cac@inglobaseguridad.com

SEGURIDAD INTEGRAL

60 años
AGÜERO

Fundada en 1966
INSTALACIONES A SU MEDIDA

C/ Antoñita Jiménez, 25
28019 - MADRID
Tel.: 91 565 54 20
Fax: 91 565 53 23
E-mail: seguridad@grupoaguero.com
Web: www.grupoaguero.com

Autorizada por la D.G.P. Nº 2329

CONTROL SYSTEM SEASA

OFICINA PRINCIPAL
C/ Virgen de Lourdes, 4
28027 MADRID
Tel.. 91 326 70 66
Fax: 91 326 70 84
E-mail: css@controlsystemseasa.com
Web: www.controlsystemseasa.com

C/ Basauri nº 10-12, Urb. La Florida
Ctra. de la Coruña, Aravaca
Tel.: 91 566 22 00
Fax: 91 566 22 05
28023 Madrid
E-mail: cotelsa@cotelsa.es
Web: www.cotelsa.es

IMAN SEGURIDAD S.A.

R.D.G.S.E. nº 2.227

https://www.imancorp.es
comercial@imancorp.es

SAN FERNANDO DE HENARES (MADRID)
C/Blas de Otero, 11-13
Tel.: 911 421 184

TARRAGONA
c/ Josep Pont i Gol, 3
Tel.: 977 271 000

TERRASSA (BARCELONA)
C/Unió, 24
Tel.: 937 809 577 / 937 847 111

Dpt. Instalaciones
C/Holanda, 253 (Bl. 5, Local 13)
Tel.: 937 832 686

VALENCIA
Avda. Pío XII, 1 (Esc. 3 P1)
Tel.: 963 479 354

INV SEGURIDAD

R.D.G.S.E. nº 2888

✓ Sistemas de Seguridad
✓ Protección contra incendios

Domicilio Social
C/ Tomás Redondo nº 2 Planta 5
Edificio Indobuilding
28033 MADRID
Tel.: 902 112 777
Fax: 91 763 09 33

Web: www.invseguridad.com
E-mail: cliente@invseguridad.com

Autorizada por la Dirección General de Seguridad con el nº 914
Con fecha 3 de julio de 1986

MADRID
Isabel Collbrand 10-12 28050 Madrid
Tel.: 91 358 97 77
madrid@pycseca.com

BARCELONA
Padilla 228 3ª Planta 08013 Barcelona
Tel.: 93 231 04 12
barcelona@pycseca.com

ALICANTE
Capitán Hernández Mira 1 03004 Alicante
Tel.: 96 524 93 03
alicante@pycseca.com

PALMA DE MALLORCA
Almirante Oquendo 8 07014 Palma de Mallorca
Tel.: 971 71 98 01
palma@pycseca.com

VALENCIA
Nicolás Estévanez 5 46018 Valencia
Tel.: 96 354 04 40
valencia@pycseca.com

MURCIA
Pio XII 47 Bajos 30012 Murcia
Tel.: 968 34 47 70
murcia@pycseca.com

MÁLAGA
Pico de las palomas port. 11 local 45 29004 Málaga
Tel.: 952 36 39 44
malaga@pycseca.com

SEVILLA
Parsi 13 nº 28 41016 Sevilla
Tel.: 954 67 21 72
sevilla@pycseca.com

A CORUÑA
Avd. Ernesto Che Guevara nº 15B 15172 A Coruña
Tel.: 981 658 194
galicia@pycseca.com

TELÉFONO ATENCIÓN CLIENTES
902 153 397

Instalación y mantenimiento de sistemas de seguridad

SAIMA SEGURIDAD S.A.

R.D.G.S.E. nº 2463 de fecha 2/11/1994

Sede Social
Avda. Valgrande, 12
28108 Alcobendas. (MADRID)
Tel: 91 661 68 92
E-mail: saima@saimaseguridad.com

SISTEMAS ANALÓGICOS DE PROTECCIÓN CONTRA INCENDIOS

SOLUCIONES GLOBALES DE CCTV - IP- INTRUSIÓN - INCENDIO - MEGAFONÍA - EVACUACIÓN POR VOZ - CONGRESOS

BOSCH SECURITY AND SAFETY SYSTEMS

OFICINAS CENTRALES Y DELEGACIÓN ZONA CENTRO
Avda. de la Institución Libre de Enseñanza, 19
28037 MADRID
Tel.: 914 102 011
Fax: 914 102 056

DELEGACIÓN ZONA ESTE
C/ Sancho de Ávila, 80
08018 BARCELONA
Tel.: 91 410 40 80

DELEGACIÓN ZONA NORTE
Tel.: 676 600 612

DELEGACIÓN ZONA SUR
Tel.: 648 19 08 04

E-mail: es.securitysystems@es.bosch.com
Web: www.boschsecurity.es

Honeywell Life Safety Iberia

HONEYWELL LIFE SAFETY IBERIA

C/ Pau Vila, 15-19
08911 Badalona (Barcelona) ESPAÑA
Tel.: **902 03 05 45**
Tel. Internacional: (+34) 93 24 24 236
Fax: (+34) 934 658 635
Web: www.honeywelllifesafety.es
E-mail: infohlsiberia@honeywell.com

NOTIFIER by Honeywell

Honeywell
MORLEY IAS FIRE SYSTEMS

ESSER by Honeywell

Honeywell Life Safety Iberia

Oficinas centrales
C/ Pau Vila, 15-19
08911 Badalona - BARCELONA
Tel.: **902 03 05 45**
Tel. Internacional: (+34) 93 24 24 236
Fax: (+34) 934 658 635

Web: www.honeywelllifesafety.es
E-mail: infohlsiberia@honeywell.com

Representación comercial en:
Barcelona, Madrid, Bilbao, Sevilla, Valencia, Mallorca, Galicia y Lisboa

SOFTWARE DE GESTIÓN PARA LA SEGURIDAD

MILSON INGENIERÍA S.L.

C/ María Zambrano, 26. Oficina 2
28981 Parla (MADRID)
Tel:. +34 686 079 578
Web: www.milson.es
E-mail:info@milson.es

Gestiona3w
Una nueva forma de Trabajar

GESTIÓN REMOTA S.L.

C/ Barquillo 49. Madrid
28004 (MADRID)
Tel: 91 545 40 44
Web: www.gestiona3w.com
E-mail: info@gestiona3w.com

SOLUCIONES INTEGRADAS DE SEGURIDAD ELECTRÓNICA

TECOSA

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

Division Building Technologies
Ronda de Europa, 5
28760 Tres Cantos - MADRID
Tel.: +34 91 514 75 00
Asistencia Técnica: 902 199 029
www.tecosa.es

TELECOMUNICACIONES

ALAI SECURE

La solución de seguridad M2M definitiva para las comunicaciones de su CRA
www.alaisecure.com

Oficinas centrales
Condesa de Venadito 1, planta 11
28027 Madrid
Tel.: 902 095 196
Fax: 902 095 196
E-mail: comercial@alai.es

TRATAMIENTO DE EFECTIVO

LOOMIS SPAIN, S.A.

Inscrita en el Registro de Empresas de la Dirección de Seguridad del Estado con n.º 2903 de fecha 31-03-00

Domicilio Social
C/. Ahumaos, 35-37
P.I. La Dehesa de Vicálvaro
28052 (MADRID)
Tel.: 91 743 89 00
Fax: 91 775 22 18
Web: www.loomis.com

VIGILANTES DE SEGURIDAD

Nº homologación D.G.P. 3589 - 25/02/2009

ALCOR SEGURIDAD.

C/ Estrella 4-8 Entlo. B
27400 Monforte de Lemos
(LUGO)
Tel.: 902 996 967
Fax: 901 707 282
www.alcorseguridad.com

Registro D.G.S.E: con el nº 1536 – 11-05-1989

GRUPO TRES PUNTO UNO

Ronda de Pitágoras, 1 NV. 106
Polígono Empresarial El Pilar
28806 Alcalá de Henares (MADRID)
Tel: 91 879 63 99 - 91 879 63 84
Fax: 91 883 78 18
E-mail: 3p1@grupo3p1.com
Web: www.trespuntouno.com

ARIETE SEGURIDAD, S.A.

D.G.S.E. nº 2617 de fecha 9-7-1996

C/ Industrias, 51
Pol. Ind. Urtinsa II
Tel.: 91 643 12 14
Fax.: 91 643 45 81
28923 Alcorcón (MADRID)
Web: www.arieteseguridad.com
E-mail: info@arieteseguridad.com

FISSA SEGURIDAD Y VIGILANCIA SLU

C/ Esquiladores, 231, nave 3
Polígono Industrial Las Capellanías
10001 CÁCERES
Tel.: 927 10 29 00 - 927 21 34 82
Web: www.grupofissa.com

MEGA - 2 SEGURIDAD, S.L.
M2

Nº HOMOLOGACIÓN 3247

C/ Maestro Alonso, 24 local
28028 MADRID
Tel.: 91 354 12 92
Fax: 91 355 58 51
E-mail:mega2@mega2seguridad.com
Web: www.mega2seguridad.com

GRUPO RMD SEGURIDAD, S.L.

Central de alarmas propia
Inscrita en DGP con el nº 729 con fecha de 25/09/1975

Sede Central:
Avda. Olivares nº 17 - P.I. El Pibo
41110 - Bollullos de la Mitación (SEVILLA)
Tel.: 902 194 814
Fax: 954 002 319
Wen: www.grupormd.com
E-mail: gerencia@gruporomade.com

PYCSECA seguridad

Autorizada por la Dirección General de Seguridad con el nº 914
Con fecha 3 de julio de 1986

MADRID
Isabel Collbrand 10-12 28050 Madrid
Tel.: 91 358 97 77
madrid@pycseca.com

BARCELONA
Padilla 228 3ª Planta 08013 Barcelona
Tel.: 93 231 04 12
barcelona@pycseca.com

ALICANTE
Capitán Hernández Mira 1 03004 Alicante
Tel.: 96 524 93 03
alicante@pycseca.com

PALMA DE MALLORCA
Almirante Oquendo 8 07014 Palma de Mallorca
Tel.: 971 71 98 01
palma@pycseca.com

VALENCIA
Nicolás Estévanez 5 46018 Valencia
Tel.: 96 354 04 40
valencia@pycseca.com

MURCIA
Pio XII 47 Bajos 30012 Murcia
Tel.: 968 34 47 70
murcia@pycseca.com

MÁLAGA
Pico de las palomas port. 11 local 45 29004 Málaga
Tel.: 952 36 39 44
malaga@pycseca.com

SEVILLA
Parsi 13 nº 28 41016 Sevilla
Tel.: 954 67 21 72
sevilla@pycseca.com

A CORUÑA
Avd. Ernesto Che Guevara nº 15B 15172
A Coruña
Tel.: 981 658 194
galicia@pycseca.com

TELÉFONO ATENCIÓN CLIENTES
902 153 397

ILUNION Seguridad

R.D.G.S.E. nº 1747 de fecha 16-4-1990

SEDE CENTRAL
C/ Albacete 3
28027 (MADRID)
Tel. 91 453 82 00 · Fax 91 453 82 22.
E-mail: comercial.facilityservices@ilunion.com
Web: seguridad.ilunion.com

DELEGACIONES

ALICANTE
C/ Bono Guarner, 16 – Bajo · 03005 Alicante
Tel.: 96 592 10 23 · Fax: 96 592 41 76.
E-mail: comercial.facilityservices@ilunion.com

ALMERÍA
Quinta Avenida Nº 85, Bajo. Colonia los Ángeles.
04008 Almería. Tel. y Fax: 950 25 39 30
E-mail: comercial.facilityservices@ilunion.com

BARCELONA
C/ Motores, 300-304 · Pol. Industrial Gran Vía Sur · 08908 Hospitalet de Llobregat (Barcelona)
Tel.: 93 216 29 00
Fax: 93 216 29 02 / 93 216 29 04
E-mail:comercial.facilityservices@ilunion.com

BILBAO
Ribera de Axpe, nº11, edificio D1 - Dpto. 107
48950, Erandio (Vizcaya)
Tel.: 94 413 22 84 / 94 413 26 80
Fax: 94 446 42 19.
E-mail: comercial.facilityservices@ilunion.com

BURGOS
C/ San Pablo nº 12C, planta 1ª, letra I (Burgos).
E-mail: comercial.facilityservices@ilunion.com

CÁDIZ
C/ Callejón del Blanco s/n · 11008 Cádiz
Tel.: 956 25 61 51.
E-mail: comercial.facilityservices@ilunion.com

CEUTA
C/ Fructuoso Miaja Sánchez 2, 1ºB
51001 Ceuta · Tel. y fax: 956 51 65 60.
E-mail: comercial.facilityservices@ilunion.com

CIUDAD REAL
C/ Ronda de Ciruela 5, portal 5, Ofic. 4B
13004 Ciudad Real.
E-mail: comercial.facilityservices@ilunion.com

CÓRDOBA
C/ Doctor Manuel Ruiz Maya, 8
Edif. Anexo ONCE – 4ª Plta · 14004 Córdoba
Tel.: 957 41 10 22 · Fax: 957 41 04 76.
E-mail: comercial.facilityservices@ilunion.com

GRAN CANARIA
C/ Pi y Margall, 62 y 63 - Bajo
35006 Las Palmas de Gran Canaria
Tel. y Fax: 928 23 26 67 / 928 29 32 59 ·
Tel. y Fax: 928 29 37 33 / 928 29 32 59
E-mail: comercial.facilityservices@ilunion.com

GRANADA
C/ Motril, Edificio Monte Alayos – 1ª Planta
Pol. Industrial Juncaril · 18220 Albolote (Granada)
Tel.: 958 26 02 51 · Fax: 958 26 21 08
E-mail: comercial.facilityservices@ilunion.com

HUELVA
C/ San Ramón, 37 · 21006 Huelva
Tel.: 959 27 14 64 · Fax: 959 23 55 37.
E-mail: comercial.facilityservices@ilunion.com

JAÉN
C/ Esteban Martínez Ramírez, 2 – 4º A
Edificio Borja · 23009 Jaén
Tel.: 953 26 38 73 · Fax: 953 26 39 65.
E-mail: comercial.facilityservices@ilunion.com

JEREZ DE LA FRONTERA
C/ Lancería, 7 – Local 39 Of. 2 ·
11403 Jerez de la Frontera (Cádiz)
Tel. y Fax: 956 16 80 02.
E-mail: comercial.facilityservices@ilunion.com

LA CORUÑA
C/ José Luis Bugallal Marchesí, 9 – bajo ·
15008 La Coruña
Tel.: 981 23 28 67 / 981 23 49 57 · Fax: 981 15 18 66
E-mail: comercial.facilityservices@ilunion.com

LUGO
C/ San Roque, 71, Entresuelo dcho. · 27002 Lugo
Tel.: 699 507 045 . Fax: 981 15 18 66
E-mail: comercial.facilityservices@ilunion.com

MADRID
Avda. de Burgos, 31 · 28036 Madrid
Tel.: 91 384 07 10
Fax: 91 384 07 22 / 91 384 07 36 / 91 384 07 29 .
E-mail: comercial.facilityservices@ilunion.com

MÁLAGA
C/ Monseñor Oscar Romero, 4 - Bajo · 29006 Málaga
Tel.: 95 265 28 29 · Fax: 95 265 28 33.
E-mail: comercial.facilityservices@ilunion.com

MÉRIDA
Pol. Industrial El Prado. Grupo 20 · Nave 15
Apdo. 449 · 06800 Mérida (Badajoz)
Tel.: 924 37 40 96 / 924 37 07 33 · Fax: 924 37 05 58.
E-mail: comercial.facilityservices@ilunion.com

MURCIA
Avda. Ciudad de Almería, 37-39 Bajo
30010 Murcia · Tel.: 968 34 08 70 / 968 22 14 59
Fax: 968 34 19 85 / 968 21 52 25.
E-mail: comercial.facilityservices@ilunion.com

OVIEDO
C/ López del Vallado, 8-10 Edif. Vetusta
33010 Oviedo
Tel.: 985 20 80 12 · Fax: 985 20 41 08
E-mail: comercial.facilityservices@ilunion.com

PAMPLONA
Avda. Marcelo Celayeta, bajo · 31004 Pamplona.
E-mail: comercial.facilityservices@ilunion.com

SALAMANCA
C/ Arroyo de Santo Domingo, 29 - Bajo
37001 Salamanca
Tel.: 923 26 44 45 · Fax: 923 26 45 99.
E-mail: comercial.facilityservices@ilunion.com

SAN SEBASTIÁN
C/Etxaide, 14 (Edificio Once)
20005 San Sebastián (Guipúzcoa)
Tel.: 943 44 40 56 · Fax: 943 44 40 57.
E-mail: comercial.facilityservices@ilunion.com

SANTANDER
C/ Fernández de Isla 14 B-3ª planta
39008 Santander
Tel.: 942 31 13 14 · Fax: 942 36 13 91.
E-mail: comercial.facilityservices@ilunion.com

SEVILLA
C/ Laminadora 21
Parque Pol. Industrial La Negrilla · 41020 Sevilla
Tel.: 95 426 06 06
Fax: 95 451 13 39 / 95 425 77 69 / 95 467 10 32
E-mail: comercial.facilityservices@ilunion.com

TENERIFE
C/ Volcán Elena, 26 - Los Majuelos ·
38108 San Cristóbal de la Laguna
(Santa Cruz de Tenerife)
Tel.: 922 15 12 65 · Fax: 922 24 05 18
E-mail: comercial.facilityservices@ilunion.com

TOLEDO
Seguridad y Servicios Auxiliares. Crtra. De Ocaña,
s/n · 45007 Toledo · Tel. y Fax: 925 23 44 19.
E-mail: comercial.facilityservices@ilunion.com

VALENCIA
C/ Franco Tormo, 3-5 · 46007 Valencia
Tel.: 96 378 91 00 / 96 377 78 88/79 81 IS)
Fax: 96 378 97 72
Fax: 96 377 01 93 / 96 378 86 60
E-mail: comercial.facilityservices@ilunion.com

VALLADOLID
C/ Ferrocarril, 2 · 47004 Valladolid
Tel.: 983 39 50 11
Fax: 983 39 45 14 / 983 20 51 79.
E-mail: comercial.facilityservices@ilunion.com

VIGO
C/ Venezuela 10, 1º C · 36203 Vigo (Pontevedra)
Tel.: 986 48 19 10 · Fax: 986 41 56 03
E-mail: comercial.facilityservices@ilunion.com

VITORIA
C/ Pintor Mauro Ortiz de Urbina, 3 – puerta 16
01008 Vitoria (Álava) Tel. y Fax: 945 21 98 83.
E-mail: comercial.facilityservices@ilunion.com

ZARAGOZA
C/ Julián Sanz Ibáñez, 42 · 50017 Zaragoza
Tel.: 976 35 51 51 · Fax: 976 28 31 94 .
E-mail: comercial.facilityservices@ilunion.com

VENEZUELA
Avda. Ernesto Blohm. Chuao. Torre Diamen
Piso 5. Caracas (Venezuela) · Teléfonos: 00582
1261453 78 / 85 · Fax: 00582 127 534579

RESET SEGURIDAD Y VIGILANCIA, S.L.
REG. D.G.P. Nº 4456 . 30/09/2019
ÁMBITO NACIONAL
Auxiliares control de accesos y Planes de seguridad
Virgen de Lourdes, 10. Local 1. 28027 MADRID
Tel.: 91998548 · www.resetseguridad.com
E-mail: comercial@resetseguridad.com

i3Seguridad
Seguridad Privada
Autorizada RNSP N.º 4211
Anteriormente Rexsecur Seguridad Global

Gobelas, 17 (Urb. La Florida) - 28023 Madrid
Tel.: +34 910 687 699
E-mail: info@i3seguridad.com
Web: www.i3seguridad.com

rexsecur GROUP

Seguridad Privada
Servicios Auxiliares
Facility Services
Sistemas de Seguridad
Proyectos e Infraestructuras

C/ Gobelas, 17 1ºA (Urb. La Florida)
28023 Madrid
Tels.: 918 319 393
902 365 949 (24 Horas)
Fax: 902 89 49 25
E-mail: rexsecur@rexsecur.es
Web: www.rexsecur.es

VASBE

D.G.P. N.º 597

R.D.G.S.E. nº 597 de fecha 15-7-1985

CENTRAL
Polígono Industrial «El Montalvo II»
C/ Honfria, 30-32
37008 SALAMANCA
Tel.: 902 191 010
Fax: 923 19 05 05
E-mail: vasbe@vasbe.com

DELEGACIONES:

MURCIA
Avda. Teniente Montesinos nº 8.
Torre A, 4ª planta, oficina 13.
30100 MURCIA

VALLADOLID
Edificio Gran Villas Norte
C/ Sajambre (local)
47008 VALLADOLID

Loomis

Líder mundial en gestión de efectivo

LOOMIS

Especialista en **gestión de efectivo**

www.loomis.es

Managing **cash** in society.

VISIBILITY

agencia digital

VISIBILITY

La agencia que revoluciona el marketing digital

Te ayudamos a vender más
Comunicando. Fidelizando. Visualizándote

Servicios: redes sociales, SEO y conversión CRO, email marketing, webs, e-commerce y marketplaces, Facebook y programática, planificación en medios digitales de Google.

Grupo Borrmart S.A.
C/ Don Ramón de la Cruz, 68 - 6º. 28001. Madrid. Tel.: 911976047. visibility@borrmart.es