CUADERNOS DE SEGURIDAD

Núm. 320 • MARZO 2017 • 10 euros

PUNTOSEGURIDAD.com

Ciberseguridad

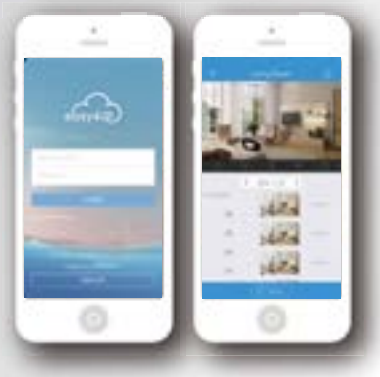
Seguridad en la Industria

II CONGRESO NACIONAL DE JEFES DE SEGURIDAD

II Congreso Nacional de Jefes de Seguridad

Hogar Seguro, Vida inteligente

Activado por Easy4ip Cloud



App Store

Google play

easy4ip

Puerta / Entrada

- Desvío de llamadas de las visitas al teléfono móvil
- Desbloqueo de puertas por control remoto
- Alarma de detección de movimiento

Perimetro

- Sensores PIR alimentados por batería
- Amplia cobertura inalámbrica
- Alarma de detección de movimiento

Monitor para bebé

- Conversación de dos vías
- Video en directo

CE FC RoHS ISO 9001:2000

DAHUA IBERIA

Juan Esplandiú 15-1B-28007 Madrid, SPAIN

Tel: +34 917649862

Fax: +34 917649862

E-mail: sales.iberia@global.dahuatech.com

- Captura más detalles con la cámara de 3MP
- Vigilancia y reproducción en tiempo real 24/7
- Audio bidireccional
- Mensaje de activación de alarma (detección de movimiento y detección de sonido)

Modelos recomendados

C15/35	A15/35	HFW1120/1320S-W	HDBW1120/1320E-W	VTO2111D-WP/VTH5221D	Sensor de alarma & panel

Security Forum 2017
17 - 18 May 2017 Barcelona
Booth: 037

II CONGRESO NACIONAL DE JEFES DE SEGURIDAD

BARCELONA
05.04.2017

COACB

Salón de Actos del Colegio Oficial de
Agentes Comerciales de Barcelona

AJSE

Peldaño

Más información e inscripciones:

www.congresojefesdeseguridad.com info@congresojefesdeseguridad.com +34 914 768 000

CIBERESPIONAJE, CIBERDELINCUENCIA...

La ciberseguridad, protagonista de 2017

La sociedad en general –y el entramado empresarial del país en particular– tiene ante sí un gran desafío: la seguridad del ciberespacio. Hoy en día, a nadie le son ajenos términos como ciberespionaje, ciberdelincuencia, ciberterrorismo, hacktivismo..., acciones delictivas que pueden llegar a poner en peligro el normal funcionamiento de nuestra sociedad, su economía y futuro desarrollo.

¿Estamos preparados para responder a un ciberataque? ¿Sabemos cómo actuar y minimizar estos riesgos que traspasan fronteras? ¿Qué papel debe jugar la concienciación y formación en prevención de los usuarios?

Nos encontramos ante un nuevo escenario y, tal como hemos reiterado en diferentes ocasiones desde estas mismas páginas, es necesario unificar criterios y normativas entre todos los agentes sociales implicados con el fin de generar mecanismos y soluciones que hagan frente a este nuevo tipo de amenazas.

Estas son algunas de las reflexiones que se recogen en el tema En Portada de este número, donde destacados profesionales analizan desde distintas perspectivas las tendencias en las amenazas y ciberataques, así como los instrumentos para su prevención y, en su caso, los recursos para responder activamente a las ciberamenazas. No cabe duda que, como apunta uno de los expertos en páginas interiores: «La ciberseguridad será en 2017 un reto para todos donde prevenir, además de defendernos, será lo más eficaz».

Esos nuevos retos y desafíos de la seguridad en el ciberespacio serán también analizados durante la celebración de Security Forum (17 y 18 de mayo en Barcelona), que dedicará una jornada completa a analizar los desafíos de la ciberseguridad, con intervenciones sobre ramsonware y otros programas cuya función es dañar un sistema o causar un mal funcionamiento. Asimismo, se abordará el papel del CISO en las empresas, o la coordinación estatal ante la Directiva NIS, entre otros temas de interés. Por quinto año consecutivo, Security Forum –que al cierre de esta edición, ya contaba con más del 75% de la zona expositora contratada– pretende mantener su posición como evento de referencia para los profesionales de la seguridad, ofreciendo el mejor escenario para el networking, la innovación y el debate, que contribuyan a reforzar el tejido empresarial de un sector en continuo avance.

Previamente, el próximo 5 de abril, también Barcelona acogerá el II Congreso Nacional de Jefes de Seguridad, un encuentro organizado por PELDAÑO y la Asociación de Jefes de Seguridad de España (AJSE), que tiene entre sus objetivos prioritarios crear un foro de debate en torno las necesidades y los retos a los que se enfrenta la figura del Jefe de Seguridad.

En esta segunda edición, la jornada se desglosará en diferentes ponencias y mesas de debate donde se abordarán las nuevas tecnologías y su aplicación al ámbito de la seguridad, el presente y futuro de la industria de la seguridad, sus diferentes actividades, así como los últimos avances en sistemas de gestión de vídeo desde el punto de vista del operador y el jefe de Seguridad, entre otros temas.

© Photobank – stock.adobe.com

ARTÍCULOS:

CUADERNOS DE SEGURIDAD

www.puntoseguridad.com

Nº 320 • MARZO 2017

Peldaño

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

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

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

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

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

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

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

60 SEGURIDAD EN LA INDUSTRIA

79 SEGURIDAD

88 CS ESTUVO ALLÍ

90 ACTUALIDAD

100 EQUIPOS Y SISTEMAS

114 UN CAFÉ CON...

ABRIL 2017- Nº 321

EN PORTADA

SEGURIDAD EN PUERTOS


© Nienwland Photrography / Shutterstock

La tecnología, en su aplicación a las instalaciones portuarias, concretamente al ámbito de la seguridad, se encuentra en una dinámica de cambio constante, todo ello encaminado a conseguir una adecuada eficacia y optimización en cuanto a todos y cada uno de los recursos utilizados. Es necesario reconocer que la modernización y el desarrollo tecnológico que ha experimentado el sistema portuario español ha contribuido a disminuir el catálogo de riesgos asociado a la actividad portuaria. De cualquier forma al hablar de seguridad, no podemos olvidar la aprobación en los últimos años de diferentes normativas: Código PBIP, Directiva Europea 2005/65/CE, entre otras, así como la entrada en vigor en 2011 de la Ley 8/2011, de 28 de abril, por la que se establecían las medidas de protección de infraestructuras críticas, donde los puertos se encuentran dentro de uno de los 12 sectores estratégicos, ésta tiene su objetivo principal en todo lo relacionado con los actos antisociales y, dentro de ellos, como protagonista indiscutible el terrorismo.


© HQuality / Shutterstock

SISTEMAS DE CONTROL DE ACCESOS

Los sistemas de control de accesos son ya un elemento fundamental de un sistema de seguridad en general, ya que tienen como función primordial permitir o cancelar el paso a un espacio protegido con determinados riesgos. Hoy en día asistimos a un constante crecimiento y avance de este tipo de sistemas, y de una manera más espectacular de aquellos que conocemos como de lectura biométrica. Este tipo y otros son cada día más demandados por los usuarios que se plantean seleccionar un adecuado sistema de control de accesos que cubra sus necesidades.

La tecnología es el elemento primordial de este tipo de sistemas cuyas características y funcionalidades avanzan continuamente, adaptándose a las necesidades de los usuarios.

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

ÍNDICE DE EMPRESAS CITADAS EN ESTA EDICIÓN

EMPRESA	PAG.	TELÉFONO	WEB
ALAI SECURE	53	902095195	www.alai.es
ALDIR	105	914690111	www.aldirsa.com
BITDEFENDER	101	932189615	www.bitdefender.es
BOSCH SECURITY SYSTEMS	105	902121497	www.boschsecurity.es
BUNKER	100	913316313	www.bunkerseguridad.es
BY DEMES GROUP	73,93,104	934254960	www.bydemes.com
CISCO	103	900987190	www.cisco.com
II CONGRESO JEFES DE SEGURIDAD	4	914768000	www.congresojefesdeseguridad.com
DAHUA	2ªcub,102	865718768883	www.dahuasecurity.com
DETNOV	91	933716025	www.detnov.com
DICTATOR	67	937191314	www.dictator.es
DORLET	35	945298790	www.dorlet.com
ELEVENPATHS	26	914830815	www.11paths.com
ESET	42	962913348	www.eset.es
EULEN SEGURIDAD	20, 91	902355366	www.eulen.com/es/seguridad
GENAKER	74, 90	932422885	www.genaker.net
HANWHA TECHWIN EUROPE	25, 92,100	916517507	www.hanwha-security.eu
HIKVISION	4ªcub, 17	917371655	www.hikvision.com
HIWATCH	90	917371655	
HOCHIKI	92,1	441634260133	www.hochikieurope.com
INNOTEC SYSTEMS	40	917281504	wwwinnotecsystem.com
INTEL SECURITY	52	913478500	www.intelsecurity.com
KASPERSKY	31,32	913983752	www.kaspersky.es
MNEMO	28	914176776	www.mnemo.com
MORSE WATCHMANS	84	1159671567	www.morsewatchmans.com
PELCO by SCHNEIDER ELECTRIC	45,101	916245617	www.pelco.com
P.S.A GROUP	89	693603444	www.psagroup.es
PYD SEGURIDAD	99	918475039	www.pydseguridad.es
PYRONIX	11	917371655	www.pyronix.com
SAFIRE	49		www.safirecctv.com
SECURE & IT	34	911196995	www.secureit.es
SECURITAS	93	902100052	www.securitas.es
SECURITY FORUM	3ªcub	914768000	www.securityforum.es
SEGURIDAD INTEGRAL CANARIA	37	902226047	www.seguridadintegralcanaria.com
SETELSA	27	942544354	www.setelsa.net
SOFTGUARD	103	910100400	www.softguard.com
SOPHOS	46	913756756	www.sophos.com
STRONGPOINT	99	918475039	www.strongpoint.com
TECOSA	97	915147500	www.tecosa.es
TREND MICRO	38	913697030	www.trendmicro.es
TYCO IF & S	77,94	916313999	www.tyco.es
VIVOTEK	104	886282455282	www.vivotek.com
WESTERN DIGITAL	23	615235013	www.wdc.com
WHITAN ABOGADOS	54	965210307	www.whitanabogados.com

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

ÍNDICE DE ANUNCIANTES

EL ENCUENTRO PROFESIONAL SE CELEBRA EL PRÓXIMO 5 DE ABRIL EN BARCELONA

II Congreso Nacional de Jefes de Seguridad: retos y objetivos

La jornada es organizada por PELDAÑO y la Asociación de Jefes de Seguridad de España

Nuevas tecnologías aplicadas a la seguridad, seguridad a nivel internacional, o el presente y futuro de la industria de la seguridad, todo ello desde el prisma de la figura del Jefe de Seguridad, serán algunos de los temas que se abordarán en el II Congreso Nacional de Jefes de Seguridad que, organizado por PELDAÑO y la Asociación de Jefes de Seguridad de España, se celebrará en Barcelona el próximo 5 de abril.

EL encuentro, que tendrá lugar en el Colegio de Agentes Comerciales de Barcelona, tiene entre sus objetivos identificar y valorar los nuevos retos a los que se enfrenta el Jefe de Seguridad, así como analizar la perspectiva de futuro de esta figura profesional.

El encuentro, en su segunda edición, tiene entre sus fines prioritarios crear un foro de debate y análisis que reúna al sector de la Seguridad en una jornada de trabajo, en la que se analizará de forma exclusiva la figura del jefe de Seguridad en el entorno normativo actual y futuro, entre otros temas.

Dirigido a jefes de Seguridad, directores y responsables de la Seguridad de entidades públicas y privadas, profesionales de empresas de seguridad, así como a miembros de las Fuerzas y Cuerpos de Seguridad, la jornada se desglosará en diferentes ponencias y mesas de debate en las que se abordarán temas sobre las nuevas tecnologías y su aplicación al ámbito de la seguridad, el presente y futuro de la industria de la seguridad, sus diferentes actividades y los últimos avances en sistemas de gestión de vídeo desde el punto de vista del operador y el jefe de Seguridad, entre otros temas.

Para finalizar se procederá a la entrega de los II Premios AJSE a la Seguridad Privada, en las categorías de: Premio Emprendedor del año; Premio Empresa Responsable; Premio Dedicación al Sector; Premio Tecnología de Seguridad, y Premio AJSE de Honor.

Doscientos profesionales

El I Congreso Nacional de Jefes de Seguridad se celebró hace ahora casi dos años, donde doscientos profesionales avalaron el éxito de un encuentro en el que se abordaron los nuevos retos a los que se enfrentaba el Jefe de Seguridad ante la nueva realidad legislativa, y otros aspectos como la cualificación profesional, la responsabilidad corporativa penal de la empresa de Segruidad y el Jefe de Seguridad, entre otros. ●

Detector Volumétrico de Exteriores de Triple Tecnología y Anti-masking

Pyronix
HIKVISION

XDH10TT-AM

Características

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

Para recibir más información, regístrese aquí

EL ENCUENTRO SE CELEBRARÁ EL 17 Y 18 DE MAYO EN BARCELONA

Las empresas, de nuevo con Security Forum

El ministro del Interior, Juan Ignacio Zoido, inaugurará el evento profesional

Las empresas del sector siguen reservando su espacio en el área de exposición de Security Forum 2017. A dos meses para la celebración del salón, los empresarios del sector –al cierre de esta edición, más del 75% de la zona expositora se encontraba ya reservada– vuelven a confiar en un formato que pretende mantener su posición como evento de referencia para los profesionales de la seguridad. Además, la organización da las últimas pinceladas al programa de expertos que formará parte de las intervenciones y ponencias con las que articulará el Global Day y Ciber Day, que en esta edición será conducido por la periodista Pilar García Muñiz, presentadora de la I Edición del Telediario TVE.

CONSOLIDADO ya como un espacio de networking, esta nueva edición sigue apostando por la innovación y los nuevos valores empresariales en el sector de la Seguridad. Y es que Security Forum volverá a convertirse en un evento ágil, flexible y orientado a la innovación y desarrollo, que sigue respondiendo una edición más al espíritu emprendedor y audaz que caracteriza a las empresas y profesionales del sector de la Seguridad, y que apuesta por reforzar el tejido empresarial de un sector en continua evolución, que demanda nuevos escenarios de plataformas de negocio e intercambio de conocimiento.

El encuentro contará de nuevo en esta edición con una zona de exposición con áreas sobre CCTV, integración de sistemas, seguridad física, seguridad lógica, control de accesos, IP/REDES...; paneles de expertos, con charlas de transferencia tecnológica entre las empresas que aportan soluciones tecnológicas y los profesionales

Ficha técnica

Fechas: 17 y 18 de mayo de 2017.

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

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

Periodicidad: Anual.

Carácter: Exclusivamente profesional.

Organiza: Peldaño.

Áreas de Exposición:

- CCTV.
- Integración de sistemas.
- Seguridad lógica.
- Control de accesos.
- IP/redes.
- Protección contra robo e intrusión.
- Protección contra incendios.
- Ciberseguridad.

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

de la gestión, consultoría e instalación de sistemas; etc.

Global Day y Ciber Day

Y respecto al Congreso, cabe destacar que se desglosará en dos sesiones diferenciadas:

– **Global Day:** la primera jornada estará dedicada a la seguridad global. Los asistentes podrán descubrir desde una visión multidisciplinar aspectos y temáticas de gran interés a través de mesas de debate y ponencias sobre «Comunicación no verbal y análisis de conductas sospechosas como herramienta para el Director de Seguridad»; «Vigilados por defecto»; «Realidad virtual aplicada a Seguridad», o «Las nuevas guerras del Siglo XXI».

– **Ciber Day:** la segunda jornada se centrará en la ciberseguridad. Temas como la robustez de los sistemas profesionales de CCTV frente a ciberataques, «Hacking & Cibersecurity for fun and profit» o mesas de debate sobre «Ponga un CISO en su empresa» y «La coordinación nacional ante la Directiva NIS» centrarán el análisis de esta edición.

Además, aún sigue abierta la fecha de recepción de los premios Security Forum, que pretenden promover y potenciar la investigación, el desarrollo y la innovación de la industria de la seguridad en España, a través del reconocimiento a los responsables de proyectos actuales de investigación en materia de seguridad, y a aquellos proyectos de carácter significativo ejecutados, que puedan ser modelo y escaparate internacional del amplio potencial de nuestra industria.

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

Premios Security Forum 2017

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

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

La dotación de los premios será:

• **Premio Security Forum I+D+i:**

–Primer Premio: cheque valorado en 3.000 euros + trofeo conmemorativo.

–Finalista: Trofeo conmemorativo.

• **Premio Security Forum al Mejor Proyecto de Seguridad:**

–Primer Premio: Trofeo conmemorativo.

–Finalista: Trofeo conmerativo.

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

*Fotos: **Xavi Gómez***

MIGUEL ÁNGEL ABAD. JEFE DEL SERVICIO DE CIBERSEGURIDAD Y OCC DEL CENTRO NACIONAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS. CNPIC

Retos de la **inteligencia artificial** en el ámbito de la seguridad

ES sabido que la inteligencia artificial puede mejorar la eficiencia de sistemas autónomos, y que su aplicación es tan amplia que abarca casi cualquier aspecto de nuestra vida cotidiana que podamos imaginar. Desde mecanismos de ayuda a toma de decisiones a sistemas predictivos, pasando por la identificación automática de imágenes, voz o datos, la inteligencia artificial puede ayudar tanto a empresas como a ciudadanos en sus labores cotidianas.

Sistemas basados en inteligencia artificial han sido por ejemplo implementados para el desarrollo de vehículos inteligentes, robots, sistemas de recomendación, drones, sistemas de ventas, campañas de marketing, y otros tantos. Sin embargo, no siempre se realza la utilidad que puede llegar a tener la inteligencia artificial en el mundo de la seguridad, o bien cuando se hace se presupone la existencia de sistemas que no requieren en absoluto la intervención humana. Si bien existen ya sistemas en el mundo de la seguridad que implementan mecanismos basados en técnicas de inteligencia artificial, como puede ser por ejemplo la detección de objetos sospechosos en imágenes grabadas por CCTV, existe una rama de la inteligencia artificial denominada aprendizaje automático que puede aportar, y ya empieza a hacerlo, grandes posibilidades a los sistemas de prevención y detección de vulnerabilidades y amenazas.

© Mopic/shutterstock.

Aprendizaje automático

Cuando hablamos de aprendizaje automático, debemos diferenciar aquellas técnicas que basan su evolución en la mejora basada en datos ya existentes y adecuadamente procesados, de aquellas que evolucionan de forma autónoma, sin necesidad de requerir con carácter previo datos para acometer un proceso de entrenamiento imprescindible para su funcionamiento; las primeras son las denominadas técnicas de aprendizaje supervisado, mientras que las segundas son las técnicas de aprendizaje no supervisado. Los sistemas basados en aprendizaje supervisado nos sirven para implementar por ejemplo sistemas de detección de intrusiones, de reconocimiento de voz y texto, o detección de fraude, que requerirán una fase de entrenamiento previa para ser eficaces; es decir, requieren de la exis-

tencia de una batería de datos que reflejen las distintas formas de intrusión, los distintos tipos de voz y texto, idiomas relacionados, etc. Por otro lado, los sistemas basados en aprendizaje no supervisado serán de utilidad para la identificación y agrupación de patrones similares, convirtiéndose por tanto en una gran ayuda en las tareas de clasificación, categorización o tipificación de eventos en una primera instancia, sin necesidad de requerir una batería de datos previos relacionados.


© Vectorfusionart/shutterstock.

La unión hace la fuerza

Si bien tradicionalmente se usan ambas técnicas de forma diferenciada, en el campo del aprendizaje automático es igualmente aplicable el refrán de que «la unión hace la fuerza», y por tanto la conjunción de técnicas de aprendizaje supervisado y no supervisado podrá mejorar nuestras capacidades de identificación de nuevas formas de amenaza, lo cual es sin duda de especial relevancia en el ámbito de la seguridad. Pero para ello, es fundamental contar con un buen equipo de analistas que sean capaces de gestionar la información que se obtiene de las distintas implementaciones de técnicas de aprendizaje automático. La figura del analista es probablemente la más olvidada a la hora de tratar e implementar este tipo de sistemas, lo que en muchos casos da como resultado un sistema inoperativo por la incapacidad de gestionar de forma oportuna la información disponible.

Quizás el nombre dado a estas áreas de conocimiento («inteligencia artificial» y «aprendizaje automático»), pueda llevar a pensar en sistemas totalmente autosuficientes, que con un componente casi mágico son capaces de alimentarse de toda la información disponible en su entorno, para proveer información predictiva de utilidad directa para el usuario final. Sin embargo, no debemos olvidar que el factor humano es no solo necesario sino imprescindible a día de hoy, tanto para gestionar los sistemas de aprendizaje como para determinar su utilidad.

Poniendo un ejemplo más concreto, un sistema basado en aprendizaje no supervisado podría identificar formas de amenaza no catalogadas hasta ese momento, agrupando aquellas que tienen un comportamiento similar. Como se puede imaginar, esta información sería de mucha utilidad para retroalimentar sistemas de aprendizaje supervisado destinados a la identificación de intrusiones, pero este trasvase no se puede llevar a cabo de forma automática, sino que requiere de una labor previa de análisis que consistiría en:

- Identificar aquellos parámetros que conforman el patrón de comportamiento de un conjunto de amenazas (protocolos utilizados, conexiones realizadas, tiempos, usuarios, latencia, cadencia de las comunicaciones, etc.), partiendo para ello de todo el conjunto de parámetros identificado por las técnicas de aprendizaje no supervisado.
- Determinar cuáles de esos parámetros identifican de forma exclusiva un tipo de amenaza, para lo cual se pueden emplear técnicas de análisis estadístico.
- Asociar (de forma manual) cada grupo de amenazas a una categoría ya existente o crear una nueva (denegación de servicio, botnet, ransomware, etc.).

Como vemos, esta labor de análisis es la que realmente llega a conjugar el aprendizaje no supervisado con el supervisado, es decir, de una agrupación apriorística de la información tratada por el sistema, el analista es capaz de asociar cada agrupación con un tipo de amenaza de forma que puede retroalimentar el mecanismo de aprendizaje supervisado, trayendo consigo un nuevo entrenamiento del sistema. Con ello, se consigue disponer de un sistema actualizado a la evolución de las amenazas que van apareciendo a lo largo del tiempo. No obstante, debemos ser conscientes de que esa actualización dependerá mucho de las capacidades, experiencia y eficiencia del analista para procesar la información existente. Es por ello que la antedicha labor de análisis no se entiende a día de hoy sin la implicación del personal humano que conforman los equipos de analistas de información, que suman a las capacidades de optimización y detección automática de los sistemas informáticos implicados aquellas capacidades de expe-

riencia y congruencia que solo una persona puede aportar.

Por otra parte, cabe resaltar las mejoras que se han producido en los últimos años en la gestión de grandes cantidades de datos, lo que se ha dado a conocer como «big data». Estas mejoras han redundado sin duda en una optimización de los procesos de aprendizaje automático, y será difícil encontrar en el futuro mecanismos de aprendizaje que no se basen en técnicas de «big data» como herramienta de pre-procesamiento de la información. Pero al igual que en el caso anterior, es imprescindible el factor humano para asegurar que la optimización de las técnicas de «big data» es la apropiada, y que el dimensionamiento de los sistemas es el adecuado.

Inteligencia artificial, en avance

Con todo, podemos concluir que la inteligencia artificial continúa su imparable avance en nuestras labores cotidianas relacionadas con las nuevas tecnologías, y se atisba que en el ámbito de la seguridad lo hará con un impulso tan extraordinario como necesario. Sin embargo, no debemos olvidar que para que un sistema basado en técnicas de inteligencia artificial sea eficiente, se requiere la constitución de un equipo humano que disponga de las oportunas capacidades de análisis, tanto para gestionar el sistema como para certificar que su funcionamiento es el apropiado, llevando a cabo aquellas acciones que sean necesarias para optimizarlo cuando se requiera. El asumir que un sistema basado en técnicas de inteligencia artificial es lo suficientemente inteligente como para sustituir a un humano es algo que solo resulta en la inoperatividad del sistema, con el consiguiente perjuicio que ello conlleva tanto a nivel reputacional como económico. El adjetivo «artificial» que se incluye en el término debe servirnos como recordatorio de que al fin y al cabo por detrás todo está implementado en máquinas, sí, pero desarrollado por personas. Se podrá avanzar en autonomía, pero seguirá siendo imprescindible un rol de supervisor del sistema que solo puede aportar un humano.

© Maskin/Makabushutterstock.

«Es necesario reorientar los sistemas hacia entornos de computación en tiempo real, es decir, que sean capaces de gestionar lo que se conoce como stream mining»

En cualquiera de los casos, a pesar de la evolución de la inteligencia artificial y del aprendizaje automático como caso particular, quedan aún determinados retos que es necesario acometer para implementar sistemas con un mayor valor añadido. En particular, destacaría la necesidad de reorientar los sistemas hacia entornos de computación en tiempo real, es decir, que sean capaces de gestionar lo que se conoce como «stream mining» (grandes cantidades de datos que deben ser procesados en tiempo real y de forma eficiente), agilizando los procesos de entrenamiento en los sistemas supervisados, y de adaptación al entorno en los no supervisados; otro reto sería abordar el desarrollo de sistemas que sean capaces de superar la ausencia de datos «etiquetados», que son precisamente los que se utilizan para entrenar sistemas supervisados; y por último, destacaría la necesidad de evaluar la viabilidad y el impacto que tendría un ataque o disrupción al propio núcleo que implementa la inteligencia artificial. Hemos visto que los sistemas basados en inteligencia artificial pueden ser de utilidad en el ámbito de la seguridad, pero ¿hasta qué punto están protegidos para identificar ataques dirigidos a ellos mismos?.

A buen seguro tendremos respuesta para muchos de estos asuntos a corto plazo, vistos los avances en la materia. ●

HIKVISION

ÚNASE A LA REVOLUCIÓN
INSTALE EASY IP 3.0

Hikvision ofrece un sistema profesional de videovigilancia completo, innovador y rentable: Easy IP 3.0. Fácil de instalar, de configurar y de manejar. Controle en todo momento las distintas zonas de su establecimiento, para tener la seguridad de que está protegido. Disfrute de las ventajas que ofrece la nueva vigilancia IP, únase a la revolución 3.0.

Características principales:

- Menor consumo de ancho de banda/HDD con H.265+
- LEDs EXIR 2.0 para una mejor iluminación
- Amplia gama, desde 1 MP hasta 8 MP (4K)
- Tecnología Darkfighter para baja iluminación
- VCA (*Video Content Analysis*)
- Auto-focus, lentes monitorizadas
- Protección a la intemperie (IP67)
- Protección anti-vandálica (IK10)

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

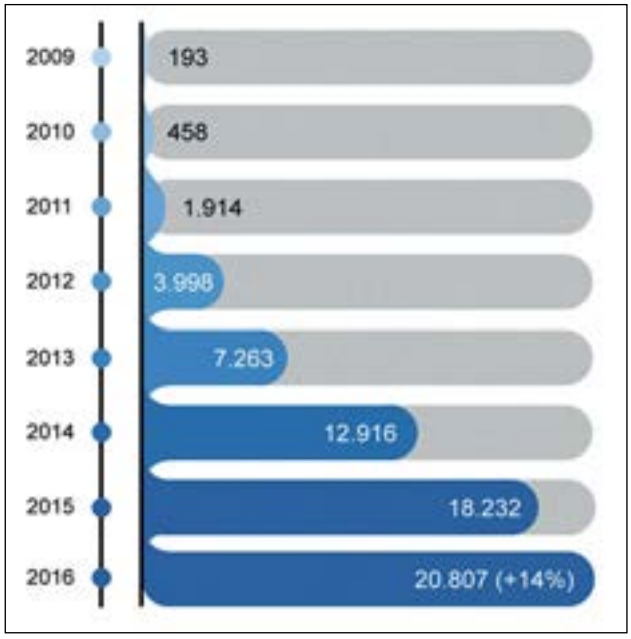
CCN-CERT

CCN-CERT y la necesidad de un sistema de protección nacional del ciberespacio

EL denominado ciberespionaje (tanto político como industrial promovido por Estados o por organizaciones privadas), la ciberdelincuencia organizada, el ciberterrorismo, el hacktivismo o la nueva amenaza del ciberyihadismo ponen en riesgo el normal funcionamiento de nuestra sociedad, de su economía y de su desarrollo futuro, y se han convertido en la amenaza más importante para los intereses nacionales y la seguridad nacional. Ante esta situación, la Capacidad de Respuesta a Incidentes del Centro Criptológico Nacional, CCN-CERT, aboga y trabaja por un sistema de protección nacional encaminado a reducir los riesgos y amenazas, propiciar la coordinación y comunicación entre todos los agentes implicados, preservar la información clasificada y sensible, evitar la interrupción de servicios y defender el patrimonio tecnológico español.

La interrupción y toma de control de los sistemas de una Administración Pública; el secuestro y cifrado de los archivos de un equipo con la exigencia del pago de un rescate (ransomware); la sustracción, publicación o venta de información sensible, los ataques con herramientas «ad hoc» y perfectamente dirigidos a través de Amenazas Persistentes Avanzadas (APT –Advanced Persistent Threat-); los ataques DDoS (Denegación de Servicios Distribuido); la intrusión en todo tipo de dispositivos, con especial hincapié en los equipos móviles (con un grado de protección mucho menor); el robo y suplantación de identidad, el sabotaje o la infección por código dañino distribuido a través de correo electrónico, páginas web o redes sociales, son algunos de los incidentes que, diariamente, se producen en el ciberespacio español.

Fig. 1 Evolución de los ciberincidentes gestionados por el CCN-CERT



Ante la intensidad y sofisticación de estos ciberataques, y de acuerdo a la normativa y legislación vigente, el CCN-CERT tiene responsabilidad en la gestión de ciberincidentes que afecten a sistemas del Sector Público, a empresas y organizaciones de interés estratégico para el país y a cualquier sistema clasificado. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques, y a afrontar de forma activa las ciberamenazas.

Para ello, desde su creación en el año 2006, ha venido proporcionando herramientas y servicios de ciberseguridad que aportan valor al conjunto y mejoran nuestras defensas en el ciberespacio. Elaboración de guías y estándares de seguridad (Guías CCN-STIC[1]), la generación de avisos y vulnerabilidades (informes de amenazas, código dañino, técnicos y mejores prácticas[2]), la formación y concienciación de los profesionales, la respuesta rápida ante los

ciberataques y el intercambio de información (incidentes y ciberamenazas) son los cinco pilares en los que descansa esta actividad. En este sentido, conviene reseñar que la diferente normativa desarrollada en los últimos años obliga al intercambio de información de ciberincidentes:

• RD 3/2010 que regula el Esquema Nacional de Seguridad (ENS). En su artículo 36 se habla de la notificación al Centro Criptológico Nacional de aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados (esta actividad se puede automatizar con el empleo de la herramienta LUCIA[3] de gestión de ciberincidentes).

• Instrucciones de la Secretaría de Estado para la Seguridad en el caso de las Infraestructuras Críticas.

• Nuevo Reglamento Europeo de Protección de Datos.

• Nueva Directiva NIS.

No debemos olvidar tampoco el papel del CCN-CERT como principal interlocutor español en los foros internacionales en los que se dirimen cuestiones de ciberseguridad, y en donde se comparte información de alto valor e imprescindible para una buena gestión de ciberincidentes.

Principales retos

El reto más importante sigue siendo, por tanto, detectar estas amenazas cuanto antes y proceder a su neutralización, reforzando la capacidad de prevención y protección en todas las instancias del Estado (ciudadanos, empresas y administraciones públicas), desplegando y coordinando sistemas de alerta que mejoren la facultad de detección y vigilancia. Al mismo tiempo, es preciso reforzar las capacidades de inteligencia para la identificación de los atacantes, determinación de sus objetivos y la difusión y compartición de la información obtenida.

No es una tarea sencilla y se necesitan recursos específicos dedicados a esta actividad en los organismos públicos y privados. Unos recursos dirigidos a la concienciación y formación de los usuarios; la incorporación de políticas y procedimientos en los procesos de decisión; la utilización de tecnología y productos de seguridad certificados, y la implementación verificada en cada una de las fases de diseño/desarrollo/implementación y mantenimiento de cualquier sistema.

De estos retos se derivan otros desafíos para los organismos públicos y privados, tales como la necesidad de aumentar el intercambio de información casi en tiempo real; conseguir una mayor colaboración entre las entidades públicas y privadas, así como alcanzar un equilibrio, siempre difícil, entre privacidad y seguridad (manteniendo el ritmo de la evolución tecnológica). ●

«El reto más importante sigue siendo detectar estas amenazas cuanto antes y proceder a su neutralización»


© Liu Zishan/shutterstock

1.- En estos momentos existen 268 Guías CCN-STIC compuestas por 364 documentos (https://www.ccn-cert.cni.es/guias.html).

2.- https://www.ccn-cert.cni.es/informes.html

3.- LUCIA es una herramienta desarrollada por el CCN-CERT para gestionar ciberincidentes y cumplir con el Esquema Nacional de Seguridad: https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/lucia.html

PABLO BLANCO ÍÑIGO. JEFE DE LA UNIDAD DE CIBERSEGURIDAD DE EULEN SEGURIDAD

Tendencias en las **amenazas** de la **ciberseguridad**

SIN duda, estamos viendo cambios a una velocidad vertiginosa que se suceden en una progresión que nunca habríamos podido imaginar. Con los últimos acontecimientos sufridos con la denegación de servicio distribuida más grande que se conoce –aunque parece que ya se nos ha olvidado a todos o lo vemos muy lejano–, se ha vivido el récord en tráfico generado para hacer un ataque contra un objetivo concreto y, a nosotros, sólo nos queda hacernos las siguientes preguntas: ¿cómo podemos luchar contra esto?, ¿estamos preparados?, ¿qué será lo próximo?

Los riesgos y las consecuencias de las ciberamenazas son las mismas que en negocios tradicionales: la indisponibilidad de servicios esenciales, fraude, robo de activos, etc., pero los vectores de ataque han variado hasta límites inimaginables. Este hecho, sumado al anonimato de los cibercriminales, que han encontrado un medio para perpetrar sus ataques con una percepción de impunidad gracias a su ocultación en lugares donde no se puede aplicar el derecho, dado las lagunas legales existentes en el ámbito internacional –como por ejemplo cuando se trata de procesar ciertas acciones ilícitas que se encuentran en jurisdicciones con arreglos de extradición limitados o inexistentes–, hacen que nos encontremos en una situación complicada y con incertidumbre de cómo y cuándo se va a producir el siguiente ataque, y quién va a perpetrarlo.

La ciberseguridad es actualmente uno de los temas principales dentro de la agenda de las Juntas Directivas y Comités de Dirección, tanto de las principales compañías a nivel mundial como de las Administraciones Públicas. Los incidentes de seguridad, la fuga y robo de información y el fraude tecnológico, son noticias relevantes en cualquier medio de comunicación de manera diaria. Las consecuencias de este tipo de acciones para las organizaciones pueden ser significativas en su cuenta de resultados y su reputación. Con el cambio de la naturaleza, complejidad y magnitud de los ciberataques, así como el aumento de ritmo de éstos, se hace casi imposible gestionar estos riesgos de una manera adecuada sin un enfoque holístico y metódico.

Para prepararnos sobre lo que viene, lo fundamental es conocerlo y prevenirlo, siempre bajo un contenido estratégico, táctico y con un marco global de actuación actual y prospectiva.

Como premisa principal, cabe resaltar que la tecnología es un medio esencial para el funcionamiento de la sociedad en general: un fenómeno como la conexión de todo a Internet, o «Internet de las Cosas» es una realidad que está en nuestro día a día y resulta imparable. Sin embargo, la fácil adquisición de sensores de todo tipo, con precios cada vez más bajos, hace que cada vez estén más extendidas estas prácticas y se facilite a los ciberdelincuentes que alcancen sus objetivos. De la misma manera, la configuración por defecto, las vulnerabilidades implícitas en los dispositivos, incluso la falta de una legislación internacional o el hecho de que los propios gobiernos no castigan ni persiguen los delitos perpetrados por medios tecnológicos, ponen en peligro el bienestar de las empresas y de los ciudadanos.

Aunque la tendencia de las amenazas se caracteriza por la utilización de los dispositivos tecnológicos, gracias a su automatización y su amplitud en los ataques, las ciberamenazas provenientes de factores humanos pueden desencadenar el terror, el caos y la destrucción en un país, entendido éste como la ciudadanía, empresas e intereses.

Los grupos terroristas continúan aspirando a llevar a cabo actividades cibernéticas perjudiciales contra los ciudadanos, gobiernos y empresas. Se considera que, aunque la capacidad técnica de estos grupos es habitualmente baja, el impacto, el terror y el miedo que provocan sus actuaciones es desproporcionadamente alto: las destrucciones más simples permiten a los grupos terroristas y sus seguidores atraer la atención de los medios e intimidar a sus víctimas.

La evaluación actual es que los ataques terroristas físicos, en lugar de cibernéticos, siguen siendo la prioridad de los grupos terroristas para el futuro inmediato. A medida que una generación cada vez más informática se involucra en el extremismo, potencialmente intercambiando mejores habilidades técnicas, se prevé un mayor volumen de actividad y más sofisticada. De la misma manera, aumentará el potencial de surgimiento de un número de actores extremistas y solitarios capacitados, al igual que el riesgo de que una organización terrorista intente reclutar a una persona con experiencia establecida.

Los terroristas, probablemente, usarán cualquier capacidad cibernética para lograr el máximo efecto posible, de manera similar a como ocurre en el ámbito tradicional de sus actuaciones: siguiendo el principio de oportunidad, aprovecharán las opciones que tengan según aparezcan, primando la necesidad de impactar en la sociedad que sufre el atentado frente a posibles cálculos estratégicos de largo recorrido. Por lo tanto, incluso un aumento moderado de la capacidad terrorista puede constituir una amenaza significativa para los gobiernos, empresas y ciudadanos. Como señalan los expertos, el problema es la dependencia en infraestructura tecnológica que hemos desarrollado, lo que se traduce en una gran vulnerabilidad: quien quiera ejercer daño sólo


© Shutterstock.

tiene que penetrar o golpear el ciberespacio, física o virtualmente. Y ahí radica la gran dificultad de la ciberdefensa, pues los criminales sólo necesitan tener éxito una vez en sus ataques a alguno de los infinitos puntos clave de nuestros sistemas tecnológicos.

Hacktivistas

Los grupos hacktivistas están descentralizados, muy organizados y orientados a las cuestiones sociales. Forman y seleccionan sus objetivos en respuesta a quejas percibidas, introduciendo técnicas de vigilancia y monitorización continua en muchos de sus casos. Mientras que la mayoría de la actividad cibernética hacktivista es de naturaleza principalmente contestataria (reivindicando derechos, promulgando ideas políticas o quejas de la sociedad en general, haciendo uso de los fallos de seguridad de las entidades o sistemas gubernamentales), los hacktivistas más capaces podrán infligir un daño mayor y duradero a sus víctimas, causando un perjuicio en el sentido más amplio de la palabra. Por ejemplo, en el caso de las empresas, un ataque hacktivista puede acarrear importantes problemas como la pérdida de confianza de los clientes o la pérdida económica y reputacional consiguientes.

Los ataques hacktivistas caen siempre dentro de alguna de las siguientes categorías: ataques de DDoS, con los que intentan denegar los servicios web de una empresa o institución; los defacements, que consisten en la modificación de aspectos visuales de los sitios web de los objetivos en el punto de mira; y el robo y posterior filtrado de información privada y confidencial.

La principal característica de estos grupos es que sus acciones siempre están basadas en un principio, justo o no, que pretenden defender. Por ejemplo, han sido muy sonadas las operaciones de Anonymous, quizá el grupo hacktivista más famoso del mundo, contra el Estado Islámico y su brazo propagandístico online (en Twitter sobre todo): los hackers que se sumaron a Anonymous en las operaciones #OpCharlieHebdo primero, y #OpISIS después, se encontraron con un adversario más duro de lo que esperaban, porque el Estado Islámico cuenta con su propio equipo de expertos dedicados a la defensa de sus activos cibernéticos.

Cibercriminales

Los cibercriminales son personas que pueden tener perfiles muy distintos pero que en todos ellos existe un objetivo común, perpetrar sistemas informáticos ajenos para la consecución de un fin del que obtengan alguna ventaja, ya sea de tipo económico, reputacional, o de desprestigio para el afectado.

Este grupo de amenazas se contextualiza de varias formas interrelacionadas con la actividad delictiva que les ocupa:

• **Crímenes ciberdependientes**: crímenes que sólo pueden cometerse mediante el uso de dispositivos de tecnología de la información y las comunicaciones (TIC), en los que los dispositivos son la herramienta para cometer el delito y el objetivo del delito.

• **Crímenes cibernéticos**: crímenes tradicionales que pueden ser aumentados a escala o alcance mediante el uso de computadoras, redes informáticas u otras formas de TIC.

Gran parte de los crímenes cibernéticos más graves, principalmente el fraude, el robo y la extorsión, continúan siendo perpetrados principalmente por grupos de delincuencia organizada con nacionalidad conocida e identificada, con muchos de los servicios delictivos del mercado alojados en esas ubicaciones. No obstante, existen grupos que emanan de ubicaciones que antes no se podían imaginar y que debe tratarse como una creciente preocupación.

Cabe destacar que los ciberdelincuentes son los principales responsables del desarrollo y despliegue del malware, que infecta de manera automática y con ámbito masivo a PC y smartphones, así como cualquier elemento que esté conectado a Internet o tenga la capacidad de conectarse. Los ataques realizados por estos medios son cada vez más agresivos y conflictivos, como lo demuestra el creciente uso de ransomware y amenazas de denegación de servicio distribuida (DDoS) por extorsión.

Hace apenas unas semanas podíamos leer en los periódicos que «la ciberdelincuencia está hoy más activa que nunca, los ataques informáticos y el fraude económico a través de la tecnología alcanzan un grado de sofisticación hasta ahora inimaginable. El resultado es que las actividades ilícitas a través de Internet pueden llegar a alcanzar un impacto económico de un billón de euros al año en el mundo, según estimaciones del Instituto Nacional de Ciberseguridad (Incibe) o, lo que es lo mismo, el equivalente al PIB de un país como España. Fuentes policiales aseguran que esta actividad supera al narcotráfico en lucro. En cambio, las inversiones en ciberseguridad en el planeta se estima que alcanzan los 70.000 millones de euros.»


© Welcomia/Shutterstock.

Un ejemplo de ciberdelincuencia que ha saltado a las televisiones y periódicos de todo el mundo es el robo y filtrado de información confidencial del Partido Demócrata estadounidense por parte de hackers patrocinados por Rusia, cuyo objetivo era influir en las elecciones norteamericanas y ayudar a la victoria del candidato republicano Donald Trump. En esta misma línea, EEUU y su Comunidad de Inteligencia ha señalado con insistencia que países como China utilizan los ciberataques de manera frecuente para obtener información de gran valor. Los propios EEUU, de donde emanan hasta un 45% de los ataques cibernéticos a nivel global no pueden esconder que ésta es una herramienta de uso habitual por varios agentes, los Estados entre ellos.

«Insiders»

Las amenazas internas siguen siendo un riesgo cibernético para las organizaciones. Los empleados desleales o maliciosos, que en muchas ocasiones son empleados de confianza de las organizaciones y tienen acceso a sistemas y datos críticos, representan una gran amenaza para el bienestar de la compa-

Presentamos el Programa de almacenamiento para Videovigilancia myWD™ para Certified Resellers

WD®, líder mundial en soluciones de almacenamiento, presenta el programa de Partners Certificados destinado a revendedores de almacenamiento para vigilancia, proveedores de servicios e integradores de sistemas.

Dicho programa ha sido diseñado específicamente para reconocer y ayudar a nuestros partners del canal de distribución que están en condiciones de ofrecer una excelente experiencia al cliente con productos de videovigilancia de WD en el punto de venta. El programa es una solución integral que ofrece ventajas exclusivas e información útil disponible de inmediato para aumentar sus ingresos y su rentabilidad.

Consulte todas las ventajas e inscríbase hoy mismo en http://event.mywd.com/SurveillanceSpain

myWD™ PARTNER PROGRAM

ñía. Estos actores pueden causar daños financieros y de reputación a través del robo de datos sensibles y propiedad intelectual. También pueden representar una amenaza cibernética destructiva si utilizan su conocimiento privilegiado, o el acceso, para facilitar o lanzar un ataque para interrumpir o degradar servicios críticos en la red de sus organizaciones o borrar datos de la red.

Igualmente preocupantes son aquellos empleados internos que accidentalmente causan daño cibernético al hacer clic inadvertidamente en un correo electrónico de phishing, conectar un USB infectado a una computadora o ignorar los procedimientos de seguridad y descargar contenido inseguro de Internet. Aunque no tienen la intención de dañar deliberadamente a la organización, su acceso privilegiado a sistemas y datos significa que sus acciones pueden causar tanto daño como una información privilegiada maliciosa. Estas personas suelen ser víctimas de la ingeniería social pudiendo, sin saberlo, proporcionar acceso a las redes de su organización o llevar a cabo instrucciones de buena fe que beneficien al delincuente.

«Script kiddies»

Los llamados «guionistas» –individuos generalmente menos calificados que usan guiones o programas desarrollados por otros para realizar ataques cibernéticos– no se consideran como una amenaza sustantiva para la economía o la sociedad en general, pero sí como una tendencia que puede causar perjuicios bajo el paradigma de los cisnes negros. Estos actores tienen acceso a guías de hacking, recursos y herramientas en Internet, y debido a las vulnerabilidades encontradas en los sistemas orientados a Internet utilizados por muchas organizaciones, las acciones de «script kiddies» pueden, en algunos casos, tener un impacto desproporcionadamente perjudicial en una organización afectada.

Incumplimiento de normativa

El cumplimiento de las normativas y buenas prácticas en materia de Ciberseguridad ha sido y sigue siendo, incluso a día de hoy, una asignatura pendiente para muchas organizaciones.

Las motivaciones que llevan a las empresas o a sus empleados a la falta de rigor en el cumplimiento de la normativa interna y legal suelen ser de diversa índole, donde se incluye, pero no se limita, a la desinformación acerca de los costes reales de implantación de las medidas marcadas en el diseño de los controles, falta de concienciación y en otras ocasiones falta de percepción de los beneficios que aporta para la organización el cumplimiento de la normativa aplicable.

En definitiva, algunas organizaciones y sus empleados perciben que el cumplimiento normativo y legal es un factor que retrasa su operativa, y no pueden pensar el riesgo al que están expuestos tanto a nivel de falta de confidencialidad, integridad y disponibilidad de la información que tratan. Por ejemplo, las consecuencias del incumplimiento del Nuevo Reglamento Europeo de Protección de Datos, donde se advierte que la multa por incumplimiento puede llegar a ascender a 20.000.000 de euros o el 4% del volumen de facturación global anual de la organización, sin tener en cuenta en esta cuantiosa cantidad el coste por la degradación de la imagen de la compañía, la vulneración de los derechos de clientes, empleados y proveedores, con los consiguientes riesgos legales, como por ejemplo el cese de la actividad o incluso el cierre del establecimiento.

Por todo lo anterior, se puede concluir que las personas, con independencia de las tendencias o de los paradigmas que se planteen a nivel tecnológico o legislativo, son la principal amenaza del pasado, presente y futuro, y representan un riesgo real para nuestra prosperidad y la seguridad colectiva. ●


© Maksin Kabakou/Shutterstock.

Contactos de empresas, p. 9.

WISENET
SAMSUNG

WISENET X series

eXcepcional rendimiento

- **X**2. Duplica la velocidad de procesamiento de vídeo para un rendimiento extraordinario
- **X**3. Triplica la memoria aumentando la capacidad de análisis de vídeo y audio
- Almacenamiento e**X**tra. Medio terabyte de memoria incluida
- e**X**cepcional Amplio Rango Dinámico (WDR) con 150 db, el más potente del mundo
- e**X**clusivo sistema de compresión que optimiza el ancho de banda en hasta un 99%

eXperimente ahora www.WisenetX.com

Hanwha Techwin

YAIZA RUBIO. ANALISTA DE INTELIGENCIA. ELEVENPATHS

Errores de configuración y metadatos: las asignaturas pendientes

EN los últimos años, las empresas han sufrido una clara orientación al mundo digital. La aparición de nuevas amenazas contra sus sistemas con el objetivo de acceder a su información está a la orden del día. Sin embargo, de acuerdo al informe de tendencias en vulnerabilidades publicado recientemente por ElevenPaths, las compañías son cada día más conscientes de que su infraestructura tecnológica puede sufrir ataques independientemente del sector.

Los datos totales

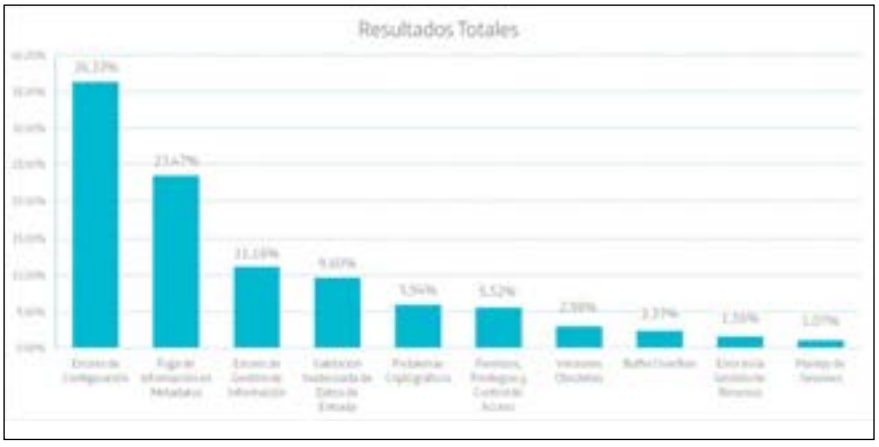
Las categorías de vulnerabilidades que más se han identificado en 2016 pertenecen a errores de configuración (36,33%), a fugas de información en metadatos (23,47%), a errores de gestión de la información (11,16%), a validaciones inadecuadas de datos de entrada (9,60%) y a problemas criptográficos (5,94%). **(Gráfico 1)**

En general, se aprecia un descenso en la mayoría de las categorías si las comparamos con informes de años anteriores, salvo los errores de configuración que han aumentado en un 21,97%. En este sentido, la mayoría de servicios no poseen la protección adecuada en los servicios web, pudiendo habilitar ataques de *content spoofing.* En concreto, en su inmensa mayoría, los errores suelen corresponder a una incorrecta implementación de la cabecera HTTP, permitiendo el uso de mecanismos como *crossorigin* o ataques de *clickjacking*.

Por otro lado, aunque existe un descenso de las vulnerabilidades concretas debidas a la fuga de información en metadatos, siguen siendo una parte fundamental de los errores detectados con un 23,47% de los resultados globales. Las organizaciones lo siguen pasando por alto, quizás debido a que no están ligados de forma directa a brechas de información ni son consideradas vulnerabilidades críticas por fabricantes ni por proveedores de seguridad. Esto provoca, por un lado, una falta de preocupación sobre los metadatos y, por otro, una falta de concienciación sobre los riesgos que entrama la exposición de esta información.

Y, por último, respecto a los errores de gestión de información, el 40% de estos pertenecen a fugas de información sobre las respuestas del servidor y que hacen referencia a la revelación de información sensible por errores de la aplicación. Los errores principales son debidos a comentarios de desarrolladores en el código de respuesta, una configuración inadecuada del servidor o de la aplicación o diferencias en las respuestas de la página. Las recomen-

Gráfico 1



daciones son bastante claras al respecto: es necesario eliminar los comentarios dentro del código antes de liberarlo públicamente, y también vigilar el diseño de las aplicaciones a la hora de la respuesta en base a la validez de los datos de entrada, poniendo especial foco en proteger información como número de tarjetas de crédito.

Por sector de actividad y por región

En el sector de telecomunicación y tecnología se destaca la cantidad de errores de configuración llegando incluso a doblar al resto de sectores. Respecto al sector público, este ha disminuido los errores por fugas de información, pero todavía este esfuerzo es insuficiente ya que el 61,97% de sus errores proceden de esta categoría. Y, por último, es reseñable la falta generalizada por parte del sector de la educación de medidas generalizadas de implementación de medidas de seguridad de la información en sus sistemas. **(Gráfico 2)**

Por su parte, existe un intercambio de posiciones en errores de configuración y fuga de información en metadatos entre las regiones de LATAM y EMEA. En LATAM se mantiene un nivel similar al del periodo 2014-2015 (45,17%) al que unimos los errores de gestión de información (14,39%) para reforzar la cantidad de información sobre el reconocimiento, que puede ser recopilada por atacantes usando técnicas de *fingerprinting* y *footprinting*, junto con el análisis de metadatos.

Pero, en cambio, permisos, privilegios y control de acceso contaban en el periodo 2014-2015 con un porcentaje representativo en la región de EMEA (4,99%), y actualmente ha empeorado teniendo un 7,41% de sus errores debidos a esta categoría.

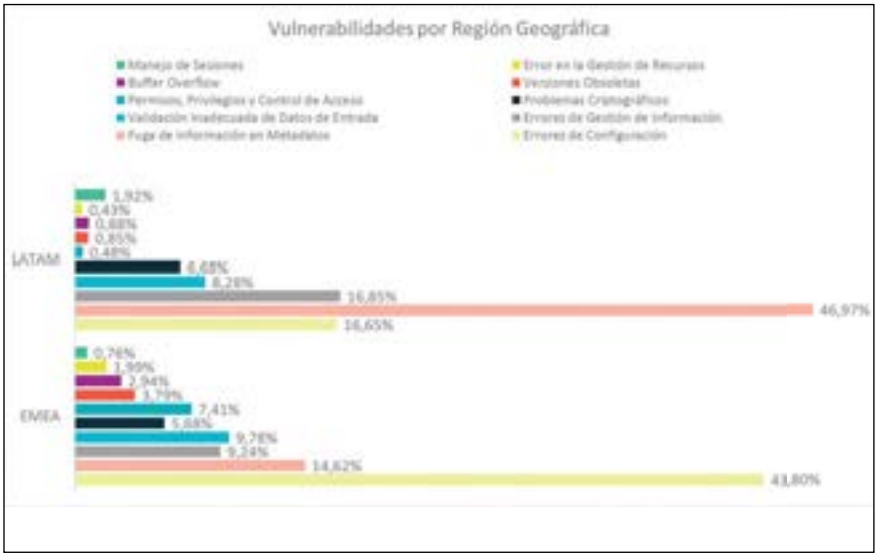


Gráfico 2

Cada día, más conscientes

De forma generalizada, existe un descenso de la mayoría de las categorías de vulnerabilidades. Sin embargo, todavía existe una falta de cuidado en la gestión de información que es accesible desde Internet: ficheros con información sensible, información del servidor, metadatos, copias de seguridad, entre otros. Independientemente del punto de vista utilizado, el análisis de los datos arroja un elevado número de vulnerabilidades de este tipo.

Fotos: *ElevenPaths*

INMACULADA PARRAS. DIRECTORA DE MARKETING Y COMUNICACIÓN DE MNEMO ESPAÑA

Los **retos** de la **ciberseguridad** en España

Lo único seguro es que todos los sistemas son potencialmente vulnerables.

HEMOS finalizado el año 2016 sin que no pasara día con una referencia a la ciberseguridad en los medios de comunicación. Nos han llegado noticias de ataques de toda índole y se ha convertido, como en otras ocasiones, en un mensaje al que no le damos la suficiente importancia, tanto a nivel personal como profesional: «esto es muy difícil que me pase a mí».

Sólo cuando bajamos al detalle nos damos cuenta de que lo «ciber» nos invade y que todo ello está rodeado de una seguridad que no tiene. Niños con exceso de horas de móvil, acosados, sin referente familiar en este sentido en la mayoría de los casos, protegidos por una pantalla de plasma, para lo bueno y para lo malo.

Y esto no ha hecho nada más que empezar. Las generaciones venideras llevarán en el ADN profesional la «picardía» aplicada a lo digital, lo que trascenderá a las organizaciones e, incluso, a los delitos.

La dificultad de prevenir los ataques cibernéticos pone de manifiesto que las organizaciones no están contemplando la ciberseguridad del mismo modo que sus atacantes. Las motivaciones de éstos están muy lejos de la percepción de riesgo de las empresas. El mensaje de que una gran empresa compite con una pequeña por volumen ha demostrado no ser cierto. ¿El motivo? Muy sencillo. No se trata de volumen sino de agilidad. La empresa ágil se come a la inmóvil, pues en seguridad esto se eleva a la enésima potencia. La ágil además ha de pensar con la mentalidad del atacante, que no descansa, es imaginativo y sus intereses son dispares, desde el económico, pasando por la notoriedad y llegando al perjuicio por el perjuicio.

Por otro lado, la velocidad en el desarrollo de nuevos productos y su disponibilidad prácticamente inmediata para los consumidores hacen que aún los criterios de ciberseguridad no sean tenidos en cuenta por las empresas, a la hora de poner a disposición de sus clientes finales dispositivos de telemedicina, SmartTV's, vehículos, drones y otros muchos elementos que de un día para otro han pasado a formar parte de nuestra vida cotidiana.

La percepción de que todo está conectado con todo ya supera la ficción, aunque no nos demos cuenta. Un motivo por el cual la seguridad en la conectividad será la clave para la tecnología en los años venideros.

Pero realmente, ¿somos conscientes de lo que nos rodea? Hoy en día podemos presenciar cómo la actividad social tiene a las redes sociales como elemento clave en algunos estilos políticos, y cómo algunos individuos las utilizan como una herramienta para generar actividad e información per-

judicial para algunos individuos en particular y para la influencia social en general. La delgada línea entre el ciberactivismo y el cibervandalismo está ahí, pero en muy poco tiempo se comenzará a percibir que esto ya no es inocuo, porque legalmente, cada vez son más los recursos para perseguir estas iniciativas y las herramientas para probar estas acciones y perseguirlas serán más ágiles y contundentes.

Proteger nuestros dispositivos móviles

¿Para qué sirven las recomendaciones que vemos frecuentemente sobre cómo proteger nuestros dispositivos móviles? No quiero imaginarme cómo contárselo a un usuario que no puede vivir sin Whatsapp o a los más pequeños, niños y adolescentes que siendo nativos digitales, utilizan dispositivos y tecnología como cualquier sencillo electrodoméstico, sin ver implicaciones o consecuencias más allá.

Y es que, ¿cómo incorporamos dispositivos de telemedicina a nuestro día a día?, ¿con qué criterio de seguridad descargamos aplicaciones móviles? Damos por hecho que lo que llega a los consumidores es seguro, cuenta con la seguridad apropiada, las empresas habrán trabajado en ello o habrán invertido lo suficiente, pero la realidad es otra. Las empresas reducen el tiempo de puesta en el mercado para sus consumidores en el menor tiempo posible, y al menor coste posible y ello incluye la seguridad.

Cuando abordamos procesos de preventa con potenciales clientes de nuestras soluciones de seguridad, nos encontramos con ese escenario, los servicios son caros, los presupuestos inexistentes o sencillamente las empresas cuentan con servicios justos para «cubrir el expediente». ¿Cómo abordar este escenario? Si las brechas de seguridad están ahí, si la seguridad 100% no existe, y las amenazas están más resueltas que nunca a hacerse patentes. ¿Qué van a hacer las empresas que, por defecto, van por detrás de los atacantes? ¿Y nuestras infraestructuras críticas? Los servicios han de ser más inmediatos y estar disponibles para evidenciar en todo momento la adaptación al medio, facilitando la evolución e incorporando elementos inteligentes que permitan a las organizaciones tomar las decisiones que van a ser estratégicas para ellas, tanto en momentos de crisis como en cualquier situación aunque no existan amenazas.

> «La ciberseguridad será en 2017 un reto para todos donde prevenir, además de defendernos, será lo más eficaz»

En este sector, la incertidumbre es compañera de viaje y trabajar con ella forma parte de cómo cada cual andará el camino. El desarrollo tecnológico proporciona grandes oportunidades en todos los mercados y para todos los usuarios, pero también incrementa la exposición de personas y organizaciones, aumentando el número de amenazas en organizaciones que no están preparadas para enfrentarse a éstas.

La ciberseguridad será en 2017 un reto para todos donde prevenir, además de defendernos, será lo más eficaz. Uno de tantos ejemplos son los dispositivos IoT; muchos de los ataques ocurridos hace unos meses a Dyn o Yahoo, entre otros, han demostrado que dispositivos como smartphones, dispositivos de telemedicina conectados por Bluetooth en servicios alojados en la nube, no siempre cuentan con una seguridad total. Su popularidad, uso generalizado y sus bajos costes, no permiten actualizaciones cuando se identifican vulnerabilidades en dichos dispositivos.

Desde Mnemo proponemos atajar estos retos desde una visión de la prevención en seguridad basada en cuatros puntos de apoyo:

La adaptación constante (seguridad adaptativa): un sistema inmunitario eficaz es aquel capaz de adaptarse para poder reconocer y hacer frente a la amenaza, de manera que nos permita estar en **evolución constante (seguridad evolutiva)**: ¿cuál es el mayor reto que plantea hoy cualquier amenaza? Su constante evolución. Y todo lo anterior de forma realmente **inteligente (seguridad inteligente)**, porque hemos de saber elegir la mejor solución cuando nos encontramos cara a cara con un problema y, habitualmente, estos momentos no son ni reflexivos ni los mejores para la improvisación. Finalmente, si combinamos los tres elementos anteriores, conseguiremos que la **seguridad** sea realmente **estratégica** para las organizaciones porque conoceremos en qué nivel de riesgo se encuentra la organización y qué medidas debe tomar, convirtiendo la seguridad en un proceso clave e integrado en la organización que debería poder llevarse a cabo de forma natural.

La integración de todos estos elementos permite flexibilizar y hacer más eficiente la gestión de la seguridad. No todas las organizaciones tienen los recursos necesarios para dar cobertura a los requerimientos de seguridad que hoy exigen los mercados y la tecnología. Por ello, consideramos que la seguridad de una organización no es importante, es innegociable.

Los nuevos modelos de servicios y negocio, cada vez más abiertos y conectados, generan gran contenido y calidad de datos que debemos proteger. Por este motivo, convertimos la ciberseguridad en un principio básico en el diseño de cualquier elemento de la organización. La información de una organización es un valor incalculable.

> «La seguridad en la conectividad será la clave para la tecnología en los años venideros»

Herramientas adaptadas a los riesgos en cada momento

Para racionalizar los esfuerzos, una organización ha de disponer de herramientas que se adaptan a los riesgos en cada momento, porque éstos cambian de forma permanente. De hecho, la tendencia se dirige a soluciones en modo servicio, disponibles incluso bajo demanda que permitan encontrar de forma dinámica las respuestas precisas en cada momento.

Asimismo, es preciso automatizar e inyectar en los sistemas existentes la información obtenida de las acciones correctoras, ya que en ocasiones los sistemas no evolucionan por falta de actualización. Cuando automatizamos estos procesos cambiamos la forma de trasladar la seguridad a toda la organización.

Por último, un aspecto fundamental para las organizaciones es la concienciación y formación de todos sus componentes. Cuantos más esfuerzos se realicen en este sentido, más efectiva será la prevención. Los ejercicios prácticos con diferentes colectivos de las organizaciones, en función de los diferentes perfiles y responsabilidades, son garantía de seguridad. Además estos ejercicios deben estar adaptados a las características del negocio y personalizados en base a la madurez de cada organización.

En resumen, seguridad adaptativa, evolutiva, inteligente y estratégica, claves para incorporar la seguridad de forma transversal en una organización. ●

Fotos: *Mnemo*

Contactos de empresas, p. 9.

Kaspersky® Anti Targeted Attack

Detecta ataques dirigidos y amenazas avanzadas que el software de seguridad tradicional no puede reconocer

- Identifica rápidamente ataques dirigidos contra redes corporativas
- Combina análisis de objetos y de actividades para ofrecer detección avanzada
- Proporciona una visibilidad mejorada tanto a nivel de red como de endpoint
- Investigación de incidentes efectiva usando la inteligencia más avanzada
- Fácil escalado para cubrir redes de IT complejas y en crecimiento

Saber que eres el objetivo y reaccionar antes de que sea demasiado tarde

kaspersky.es

KASPERSKY lab THE POWER OF INTELLIGENCE

ALFONSO RAMÍREZ. DIRECTOR GENERAL. KASPERSKY LAB IBERIA

Cuando un 1% supone **pérdidas millonarias**

ACTUALMENTE, las empresas han de hacer frente a un panorama de ciberamenazas complicado. Han de «lidiar» con factores externos e internos, que dificultan la labor de aquellos dedicados a mantener la seguridad de las empresas. Entre esos factores externos nos encontramos, por ejemplo, con amenazas que utilizan vulnerabilidades básicas, con el temible factor humano, ataques a terceros (pequeños proveedores), que entran a formar parte de la cadena de un ataque y nos alcanzan de lleno o con lo que se ha denominado Cibercrime as a Service. Como factores internos, por mencionar solo algunos, podríamos destacar la sofisticación de los sistemas TI, que redunda en una falta de visibilidad y de información operacional, o simplemente la falsa sensación que crea disponer de una seguridad perimetral. Seguridad perimetral que, en muchos casos, está sobrevalorada. Y todo esto es solo una pequeña muestra de los peligros que acechan a las empresas, ya sean grandes, medianas o pequeñas. No hay objetivo pequeño.

A todo esto, y por si la situación no fuera lo suficientemente compleja, los ataques dirigidos irrumpen en todo este ecosistema de forma sigilosa y tremendamente dañina. Como su propio nombre indica, una de estas amenazas puede no ser detectada en meses; en realidad 214 días de media, casi un año. Este tipo de ataques son, efectivamente, procesos «vivos» y pueden tardar años en completarse y nunca llegar a descubrirse.

Tal vez pueda consolar el hecho de que este tipo de amenazas solo representan un 1% de todos los ataques; imponiéndose así una pregunta: ¿Cuál es entonces la ventaja de invertir en una protección para una probabilidad de ataque tan pequeña?

Es cierto que los ataques dirigidos pueden suponer solo el 1% de todos los ataques, pero las pérdidas que puede causar un único ataque pueden ascender a 2,5 millones de dólares en grandes empresas y 84.000 dólares en pequeñas y medianas empresas. Cifras nada despreciables y que deberíamos tener presentes.

Llegados a este punto, se impone la necesidad de revisar nuestro concepto de seguridad, de examinar y analizar qué estrategia de seguridad necesito en mi empresa para lograr acercarnos lo más posible a una seguridad total. Algo que como bien sabemos no es posible; aunque sí podemos intentar aproximarnos.

Hoy en día, las empresas centran la mayoría de sus esfuerzos en implementar una seguridad preventiva. De hecho, entre un 80 y 90% de las inversiones se destinan a la prevención. Y, a pesar de ser una inversión muy importante, muchos de los ataques logran penetrar estas defensas tradicionales. El resto, ese 20-10% de inversión es el que se reserva para la predicción, detección y respuesta ante amenazas e incidentes. Ese pequeño porcentaje es el que puede marcar la diferencia y en el que, estamos convencidos, va a equilibrar la balanza a nuestro favor.

Efectivamente, teniendo en cuenta el panorama anteriormente descrito, las soluciones de seguridad tradicional, centradas principalmente en la prevención, ya no son suficientes ni adecuadas para dar respuesta eficaz a todos estos ciberataques. Y prevemos que los porcentajes de inversión cambiarán en los próximos años, adaptándose a un nuevo enfoque que dé respuesta a las amenazas actuales.

> «Hoy en día, las empresas centran la mayoría de sus esfuerzos en implementar una seguridad preventiva»

En Kaspersky Lab, nuestra visión de la seguridad se basa en cuatro pilares fundamentales: prevenir, detener, responder y precedir. Se trata de un enfoque centrado en «inteligencia», un enfoque que va mucho más allá de la prevención de amenazas. Hablamos de aplicar conocimiento, de inteligencia, innovación no solo a la prevención que, como hemos visto, ya no es eficaz por sí sola, sino a todo el ciclo de vida de la seguridad.

Por ello, es necesario una solución como Kaspersky Anti Targeted Attack Platform, que proporciona la monitorización en tiempo real del tráfico de red, combinado con el análisis de seguridad de objetos y el análisis de comportamiento de EndPoints, proporcionando una visión detallada de lo que está pasando en la infraestructura de TI de una empresa. Al correlacionar eventos de múltiples capas, incluyendo la red, los EndPoint y el panorama global de amenazas, Kaspersky Anti Targeted Attack Platform ofrece una detección «en tiempo real» de amenazas complejas y ayuda a realizar investigaciones retrospectivas. Kaspersky Anti Targeted Attack Platform es parte de un enfoque adaptativo e integrado para la seguridad empresarial.

Fotos: Kaspersky

Contactos de empresas, p. 9.

FRANCISCO VALENCIA. EXPERTO EN CIBERSEGURIDAD.DIRECTOR GENERAL DE SECURE & IT.

Móviles y APT, objeto de **mayor impacto en 2017**

ESPAÑA es uno de los países más castigados por los ciberataques (es el tercer país que más impactos sufre, solo por detrás de Estados Unidos y Reino Unido). Poco a poco, empresas y usuarios van tomando conciencia de la importancia que tiene la seguridad de la información, pero aún queda mucho por hacer. Por este motivo, es interesante hacer balance de lo que ha ocurrido en el año que acaba de terminar pero, sobre todo, analizar la situación de cara a 2017.

Conviene recordar que -desde hace una década- a las empresas y organismos que trabajan en la prevención de ciberdelitos se les ha multiplicado el trabajo. Hay un dato muy llamativo: solo hasta septiembre de 2016 se reportaron unos 90.000 ataques, el doble que en todo el año 2015. Los números van a seguir al alza. Pero, ¿cuál va a ser la tendencia el próximo año?

Previsiones para 2017

En primer lugar se prevé que en 2017 haya una mayor incidencia de ciberataques, que serán masivos y más rápidos. Esto se debe a que los ciberdelicuentes buscan la alta rentabilidad, es decir, obtener información y dinero a muy corto plazo. Además, conviene destacar que se van a incrementar muchísimo los impactos en móviles.


© Lightspring / Shutterstock

También van a aumentar considerablemente las Amenazas Persistentes Avanzadas (APT), que irán dirigidas sobre todo al sector industrial. Uno de los motivos por los que se van a disparar los ataques en entornos industriales es que los cibercriminales se han dado cuenta de que son fácilmente atacables, debido a su obsolescencia tecnológica. Se han adaptado redes de nueva generación a sistemas muy antiguos, que son tremendamente vulnerables y, además, es muy difícil protegerlos porque la actualización es complicada.

Desde hace un tiempo, el concepto Internet de las Cosas (IoT, del inglés Internet of Things) está revolucionando el mundo. La conexión de objetos de la vida cotidiana con Internet va a suponer también una gran transformación en el mundo de la empresa. Por supuesto, a esta evolución van aparejadas nuevas amenazas que afectarán a entornos donde no hay un humano detrás, por ejemplo, los vehículos conectados a la Red.

En cuanto a los ciberdelincuentes, seguro que estarán más organizados en torno a bandas terroristas o de cri-


© GlebStock / Shutterstock

men organizado. Y, por supuesto, van a seguir utilizando las TIC para financiar el tráfico de armas, el de drogas o el de personas.

Además, la incertidumbre social y política siempre tiene efectos en el mundo de la ciberseguridad. Aspectos como el brexit o la victoria de Donald Trump en Estados Unidos generan una inestabilidad que provoca el auge de entidades que intentan conseguir información a través de cualquier medio.

La nueva normativa europea de Protección de Datos

En el ámbito del cumplimiento legal también debemos estar atentos a los cambios. La rapidísima evolución tecnológica y la globalización han planteado nuevos desafíos para la Protección de los Datos de Carácter Personal, de ahí la necesidad de crear un nuevo Reglamento Europeo de Protección de Datos.

Según la UE, esta reforma pretende que los ciudadanos recuperen el control de sus datos personales y trata de garantizar, en todo el territorio, unos estándares de protección mayores y adaptados al entorno digital.

Aunque entró en vigor el 25 de mayo de 2016, empezará a aplicarse el próximo 25 de mayo de 2018, por tanto, seguimos sujetos a la actual Ley Orgánica de Protección de Datos de nuestro país. Pero, la Agencia Española de Protección de Datos recomienda que se utilice este periodo transitorio de dos años para llevar a cabo una adaptación progresiva a las nuevas normas.

Entre las novedades del nuevo Reglamento se encuentra la ampliación del ámbito de aplicación territorial. Hasta ahora, estaba dirigido a responsables o encargados del tratamiento de datos (empresas, asociaciones, autónomos

o profesionales independientes) establecidos en la Unión Europea. Pero, en la nueva norma se amplía a aquellos no establecidos en la UE que realicen tratamientos a ciudadanos europeos, derivados de una oferta de bienes o servicios, o como consecuencia de una monitorización y seguimiento de su comportamiento. Esto permite que la normativa sea aplicable a empresas que podían hacer tratamiento de datos de personas en la Unión Europea, pero que se regían por reglamentos de otros lugares que no siempre ofrecen el nivel de protección del reglamento europeo.

La norma prevé que las organizaciones implanten la figura del Data Protection Officer (responsable de protección de datos), que deberá tener una formación adecuada, así como conocimientos en Derecho y Protección de Datos. Se encargará de: informar y asesorar a los empleados que lleven a cabo tratamiento de datos; monitorizar los procedimientos establecidos en su organización, certificando que se adaptan a la normativa sobre protección de datos; y cooperar con las autoridades nacionales de protección de datos. En este punto, hay que tener en cuenta que se ha eliminado la necesidad de notificar los ficheros ante las distintas agencias nacionales de protección de datos.

Por otro lado, las compañías que traten datos de carácter personal estarán obligadas a notificar a la autoridad de control competente cualquier tipo de brecha grave de seguridad. ¿Cuándo debe notificarse? Tan pronto como el responsable de tratamiento sepa que se ha producido esa violación en la seguridad, y sin que transcurran más de 72 horas desde que ha tenido constancia de ella. Por cierto, con el nuevo Reglamento no basta con informar a las autoridades, también es necesario comunicar al interesado la brecha de seguridad en el caso de que pueda suponer un alto riesgo para sus derechos o libertades.

Como hemos dicho, la nueva norma trata de que los ciudadanos tomen el control de sus datos. En este sentido, refuerza la necesidad de que se dé un consentimiento claro y afirmativo sobre el tratamiento de los datos personales. No sirve que se haga por defecto (que pongamos casillas ya marcadas, o nos basemos en el silencio o la inacción).

Además, cualquier persona tendrá derecho a que su información sea eliminada de los proveedores de servicios de Internet cuando lo desee, siempre y cuando quien posea esos datos no tenga razones legítimas para retenerlos. Y, si solicita a una compañía de Internet que elimine sus datos personales, la empresa deberá remitir la petición al resto de entidades que puedan haberlos replicado.

En cuanto a los datos especialmente protegidos, esta categoría se amplía a la información genética, biométrica, las creencias filosóficas o la orientación sexual.

Por cierto, la nueva normativa establece que los menores de entre 13 y 16 años (cada país podrá establecer la edad mínima) necesitarán permiso de sus padres para poder abrir cuentas en redes sociales como Facebook, Instagram o Snapchat. Es decir, para poder hacer el tratamiento de datos personales de un menor, las entidades deberán contar con la autorización de los padres o tutores. Además, el responsable de tratamiento deberá esforzarse para verificar que ha sido así.

Estos son solo algunos de los aspectos que recoge la nueva normativa, pero hay más. Y, si como ciudadano puede ser interesante conocer el nuevo Reglamento de Protección de Datos, en el caso de tener una empresa es absolutamente necesario que estés al tanto de los cambios.

Las empresas y su apuesta por la ciberseguridad

Para los usuarios los ciberataques son un inconveniente, pero para las empresas se pueden convertir en un gran problema: incalculables pérdidas económicas, robo de información, sanciones por incumplimiento legal, daño a la reputación, etc.

Por este motivo, es importante que las compañías apuesten por la ciberseguridad como una inversión de futuro y se pongan en manos de expertos. Los ciberdelincuentes mejoran sus técnicas, pero las empresas que trabajamos para prevenir estos delitos también avanzamos en nuestra tarea. ●

Fotos: *Secure&IT*

Contactos de empresas, p. 9.

SEGURIDAD

SEGURIDAD INTEGRAL CANARIA SA

Líderes en **Seguridad**

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

ISO 9001 · ISO 14001 · OHSAS 18001

T 902 226 047

www.seguridadintegralcanaria.com

JOSÉ BATTAT. DIRECTOR GENERAL DE TREND MICRO IBERIA

El papel de la **ciberseguridad** en el proceso de **transformación digital**

ESTAMOS inmersos en un momento de grandes cambios -políticos, económicos, sociales, geográficos, medioambientales, tecnológicos, de modelos de negocio…- que colocan en una encrucijada a las organizaciones de hoy en día. Este cambio en el orden de las cosas supone evolucionar y, a su vez, tener capacidad de adaptación. Hasta aquí no hay nada nuevo, pues sería como aplicar la teoría de Darwin al terreno empresarial, y todos sabemos cómo concluye: transformarse o morir, desaparecer.

Bajo esta premisa, y centrándonos en el ámbito de las tecnologías, se observa que el ritmo que imprime la innovación tecnológica es muy rápido; a veces incluso excesivo, y en plazos tan cortos que es complicado de asimilar; especialmente desde que Internet se democratizara y permitiera nuevos desarrollos que han pasado a formar parte imprescindible de nuestro día a día. La sociedad ha sabido abrazar esos cambios con rapidez y adaptarse al nuevo panorama de la economía digital y los entornos hiperconectados. No ocurre lo mismo con las empresas, que deberían tomar como ejemplo esa precocidad y establecer una estrategia digital clara para sobrevivir.

Pero al igual que nos resguardamos cuando llueve, lo mismo deben hacer las organizaciones: contar con una estrategia de ciberseguridad inteligente, proactiva, multicapa y global, que actúe como un gran paraguas que proteja y defienda al negocio en todos los niveles. Sin seguridad, y ante el grado de exigencia de los mercados, concebir un negocio a futuro es harto complicado, por no decir que es inviable, especialmente teniendo en cuenta el panorama de las ciberamenazas actual. Al igual que las empresas son más globales, también lo son los peligros que las acechan y quienes están detrás de las amenazas. Los ciberdelincuentes son uno de los grupos que mejor se adaptan y adoptan la transformación digital. Su persistencia y flexibilidad a la hora de modificar las amenazas y los métodos de ataque cada vez que se lanza un parche o se crea una solución, hace que las empresas deban estar preparadas para actuar en consecuencia; pues las organizaciones deben esperar ser objeto de ataques en algún momento de su vida.

¿Está preparada su empresa para responder ante un ciberataque? ¿Sabe cómo actuar y minimizar los riesgos? ¿Es consciente de a qué se enfrenta y qué se está jugando? Los cibercriminales están en todas partes, viendo y esperando a su nueva víctima. Con Internet accesible con solo tocar un botón, caer en la trampa del ransomware, ser víctima de una estafa tipo BEC (Business Email Compromise) o encontrarse con los dispositivos plagados de malware es más fácil que nunca. Las consecuencias pueden ser fatales.

El ransomware, ese malware que secuestra, bloquea, cifra e impide el acceso a los datos y sistemas a sus propietarios, y que obliga a las víctimas a pagar un rescate, es capaz de paralizar a cualquier organización, no importa su tamaño o sector. En 2016 se convirtió en un auténtico tsunami y todo apunta a que seguirá siendo una de nuestras peores pesadillas a corto y medio plazo, ya que los ciberdelincuentes han encontrado en esta amenaza una fuente de ingresos efectiva, fácil y constante.

Por hacernos una idea de la magnitud de lo que estamos hablando, solo durante los meses de enero y junio de 2016 se detectaron y bloquearon más de 80 millones de amenazas de ransomware y se identificaron 79 nuevas familias, frente a las 29 de todo 2015. Esto supuso un aumento del 179%. Y todo esto solo en seis meses.

Tanto las nuevas como las viejas variantes, que están diseñadas para atacar la red en cualquiera de sus niveles, causaron a las empresas unas pérdidas económicas totales que se estiman en más de 209 millones de dólares en el período al que nos referimos de 2016. La epidemia de ransomware también afectó a nuestro país. Según un estudio de Opinium Research, el 41% de las empresas españolas se ha visto afectada por el ransomware en los últimos dos años, y un 22% lo ha estado en más de una ocasión. Otro dato alarmante tiene que ver con la tendencia a sucumbir al pago del rescate, algo que los profesionales de la seguridad rotundamente desaconsejamos, en tanto que no representa ninguna garantía de recuperación de la información y restablecimiento de la situación. En este sentido, si bien en España la mayoría de las compañías son conscientes de esta amenaza, todavía son demasiadas las que ceden a las demandas de los cibercriminales, pues el 52% de las organizaciones infectadas pagó el rescate por temor a enfrentarse al bloqueo total de sus sistemas informáticos y a la pérdida de datos altamente confidenciales, el impacto en su imagen corporativa y las pérdidas económicas.

Más vale prevenir que curar

El ransomware puede entrar en una organización sin ser detectado por cualquier pequeño resquicio que no esté vigilado. Se distribuye principalmente a través de exploit kits, patrones de ingeniería social y correos electrónicos de spam y phishing. Cuando el destinatario abre el archivo adjunto malicioso o accede a un enlace comprometido, el malware se descarga en el sistema del usuario. Aquí se desencadena todo, por lo que es necesario tener una visión clara y control centralizado de lo que ocurre en la red, en el endpoint, a nivel del gateway web y

© Den Rise / Shutterstock

de email, así como en el servidor. Se trata de aplicar una defensa efectiva contra las nuevas formas de amenazas, que combine múltiples capas de seguridad con inteligencia avanzada de amenazas a nivel global, soluciones técnicas configuradas de forma apropiada teniendo en cuenta las mejores prácticas, personal preparado y una sólida base educativa y de formación de los empleados; algo que ayudará a prevenir los ataques de ransomware desde el primer momento. Por supuesto, y de forma complementaria, se requiere una solución segura de backup.

Resolviendo las incógnitas de la ecuación: adaptar la seguridad a cada caso

Pero no nos quedemos aquí, sigamos evolucionando. Como vemos, los desafíos de seguridad son enormes: amenazas más sofisticadas y dinámicas, usuarios con comportamientos cada vez más arriesgados y falta de visibilidad de los diferentes sistemas de seguridad. Cada problemática y cada amenaza necesitan sus técnicas de protección específicas, pero somos conscientes de que no podemos exigir a las empresas un sinfín de soluciones que en muchos casos no sabrán para qué sirven y cuándo aplicar en cada momento. Al contrario, debemos ofrecer soluciones ágiles, que simplifiquen procesos y sean efectivas. ¿Pero cómo?

La aplicación de la inteligencia artificial y el aprendizaje automático a la tecnología nos han permitido alcanzar un nuevo estadio en la lucha contra el cibercrimen. La combinación de técnicas de protección intergeneracionales frente a amenazas impulsada por la aplicación de high fidelity machine learning, permite poner en marcha la tecnología adecuada en el momento oportuno, eliminando brechas de seguridad y elevando la protección ante las amenazas del presente y del futuro para puntos de conexión y usuarios, y con mínimo impacto en el rendimiento de los procesos, como es el caso de la tecnología XGen.

La nueva Era marcada por la transformación digital viene acompañada por una revolución de la industria de la ciberseguridad, donde se amplía el enfoque y el radio de acción apostando por un diseño multigeneracional y perfectamente integrado, basado en una arquitectura que pueda trascender los límites de la tecnología, las amenazas y los comportamientos de los usuarios.

Ahora, vuelva a preguntarse: ¿está preparado su negocio para el futuro? ●

Contactos de empresas, p. 9.

MIKEL RUFIÁN ALBARRÁN. RESPONSABLE DE CIBERINTELIGENCIA; Y **PABLO BURGOS**. CONSULTOR DE CIBERINTELIGENCIA (I+D+I). INNOTEC SYSTEM

Ciberinteligencia: conocer para decidir correctamente

La incorporación de capacidades de Ciberinteligencia puede suponer un incremento de la rentabilidad de las organizaciones de hasta un 26%; sin embargo, en España, la apuesta por esta actividad es aún incipiente con respecto a otras grandes economías. Potenciar su desarrollo es imprescindible para maximizar las oportunidades que ofrece el nuevo entorno digital, valorar y mitigar los riesgos y lograr una posición ventajosa en el mercado.

Con la globalización, la digitalización y la conectividad, organizaciones de todo tipo de sectores se enfrentan al reto de identificar y aprovechar las oportunidades que ofrece el salto al mundo digital, así como las amenazas y los riesgos del ciberespacio.

En este sentido, las organizaciones están dedicando actualmente cada vez mayores recursos al examen de su entorno, con el fin de disponer de información útil y de calidad que les ayude en sus decisiones estratégicas, tácticas u operativas, con tres objetivos fundamentales: prevenir riesgos y amenazas, minimizar el impacto de las acciones de los competidores y lanzarse a la conquista de nuevas oportunidades en el ciberespacio.

Encontrar la forma de transformar sus estructuras, en muchos casos obsoletas, para hacerlas ciberinteligentes es el principal desafío al que se enfrentan las empresas e instituciones hoy en día.

Pero... ¿Qué es la Ciberinteligencia?

Es el producto obtenido tras aplicar a la información del ciberespacio distintas técnicas de análisis que permitan su transformación en conocimiento, de forma que resulte útil a la hora de tomar decisiones con el menor nivel de incertidumbre posible, siguiendo el ciclo de Ciberinteligencia **(Fig. 1)**:

1. **Dirección y planificación**: Establecimiento de los requisitos y planificación de las acciones.

2. **Recolección:** Recopilación de datos en bruto a través de las fuentes de información que hayan sido definidas en el proceso de planificación.

3. **Transformación**: Conversión de los datos en bruto obtenidos en formatos procesables y manejables que permitan su tratamiento y análisis.

4. **Análisis y producción**: Los datos tratados son procesados, enriquecidos, analizados y evaluados para extraer un producto de Ciberinteligencia, capaz de satisfacer las necesidades de la organización.

5. **Difusión**: Transmisión de la Ciberinteligencia producida en las fases anteriores y presentada en un formato fácilmente entendible a todos los niveles.

6. **Evaluación**: Valoración y retroalimentación de todo el proceso para su reevaluación y la mejora continua de todo el ciclo.

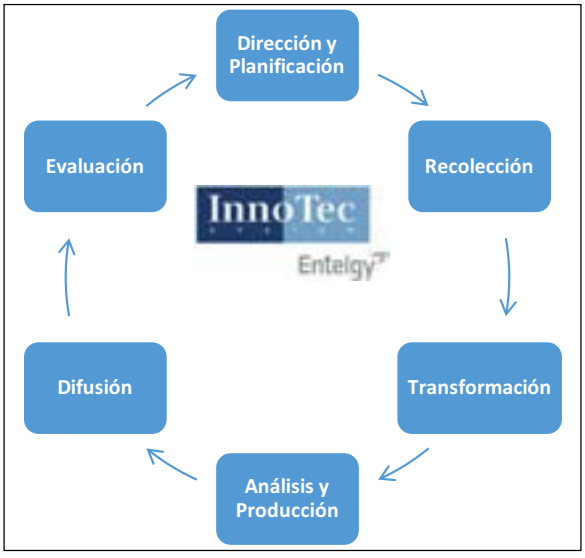


Fig.1. Rufián Albarrán, Mikel (2011). Guía profesional de Ciberinteligencia. Madrid

Con el fin de proporcionar un modelo preventivo y la mayor seguridad posible para una organización, los proveedores de servicios o células propias de Ciberinteligencia deben reunir los siguientes requisitos: **(Fig. 2)**

- Capacidad de explotación de las fuentes de información del ciberespacio.
- Cibercapacidades tecnológicas propias (Desarrollo I+D), que permitan reducir la dependencia externa de la organización en materia cibernética.
- Transformación de la información en inteligencia mediante un

Fig. 2. Rufián Albarrán, Mikel (2015). Manuel. Guía de Ciberinteligencia. Madrid Innotec System

equipo multidisciplinar con formación y habilidad en técnicas de análisis de inteligencia (Intelligence Analysis) y ciencia de datos (Data Science), para ejecutar análisis complejos de datos estructurados y no estructurados en plataformas y grandes volúmenes de información (Big Data) y de valor (Smart Data).

• Identificación de posibles violaciones a la identidad digital o propiedad intelectual, como puede ser el robo o falsificación de la documentación de uso interno.

• Conocimiento para evadir ataques a través de datos sospechosos y/o escondidos.

• Respuesta efectiva y rápida a situaciones de crisis.

• Comunicación en diferentes idiomas, ya que los ataques pueden provenir de cualquier parte del mundo.

• Servicio ininterrumpido 24x7, debido a que los atacantes suelen aprovechar los horarios de inactividad para realizar sus operaciones.

• Capacidad de ciberinvestigación (Detectives Digitales y Forense Digital) para la obtención y aportación de información con metodología forense.

• Elaboración de alertas tempranas e informes detallados para comunicar debidamente y con el objeto de reducir la incertidumbre en el proceso de toma de decisiones.

• Medidas de ciberdefensa para la protección de amenazas contra identidades digitales o contra infraestructuras de las organizaciones públicas o privadas.

El componente humano, factor clave

Aunque se empleen recursos informáticos para la producción de Ciberinteligencia, el análisis y la interpretación siguen siendo actividades esencialmente humanas. El analista de Ciberinteligencia es un especialista en la valoración, la integración, el análisis y la interpretación de la información en el ciberespacio para su conversión en conocimiento.

Carencia de cultura de Ciberinteligencia

Desafortunadamente, en España el desarrollo de estas unidades de Ciberinteligencia en la organización es reciente y nos encontramos aún lejos de los países precursores que son, además, las economías más competitivas.

Talento hay para ello, y es necesario apoyar y potenciar la Ciberinteligencia Nacional para salvaguardar la soberanía en el ciberespacio, compartiendo dicha Ciberinteligencia entre la comunidad, siempre y cuando sea oportuno.

La Ciberinteligencia no es un gasto, sino una inversión. Las organizaciones que la han incorporado son más competitivas, obtienen mayores beneficios y superan a sus homólogas en tres ámbitos clave: ingresos, rentabilidad y valoración del riesgo. Algunos estudios llegan a afirmar que las organizaciones ciberinteligentes son un 26% más rentables que sus competidoras. ●

Fotos: *Innotec System*

Contactos de empresas, p. 9.

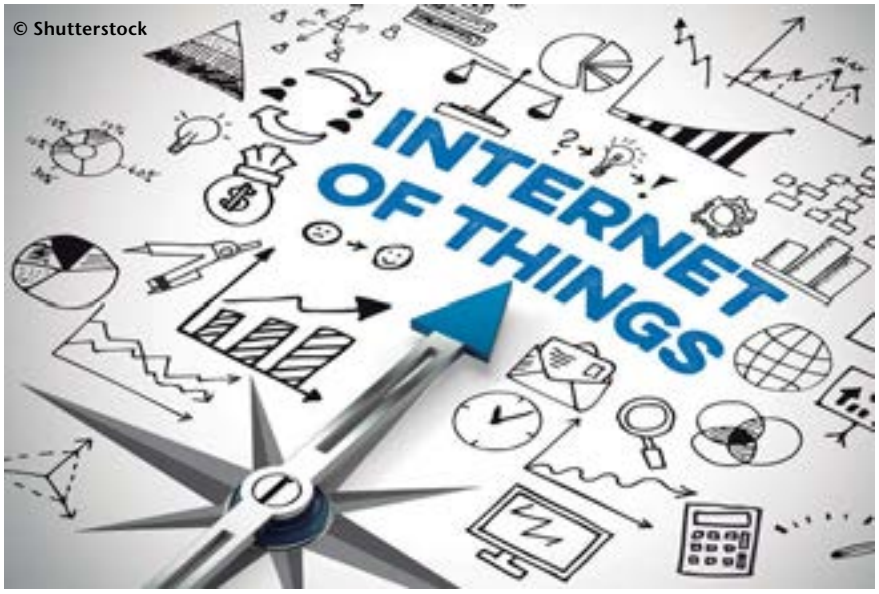
JOSEP ALBORS. DIRECTOR DEL LABORATORIO DE ESET ESPAÑA

La **amenaza** está en todas partes

HACE más de veinte años los Wet Wet Wet versionaban la canción de Reg Presley para cantar aquello de que el amor está en todas partes. Hoy en día, con la previsión de que en tres años haya entre 30.000 y 50.000 millones de dispositivos conectados en toda suerte de ubicaciones y dispositivos, podríamos decir que es la amenaza la que está en todas partes.

Y es que al analizar el estado y la evolución de la tecnología en la actualidad hay un aspecto que resalta por encima de todo: cada vez existen más dispositivos, más tecnologías y, por lo tanto, un mayor número de desafíos para mantener la seguridad de la información, sea cual sea el ámbito de su implantación. Grandes, pequeñas y medianas empresas tienen muchos motivos por los que deberían establecer férreas políticas de seguridad.

En los últimos años, la infección con códigos maliciosos y los casos de ciberespionaje se han vuelto más preocupantes –con ataques a infraestructuras críticas como el cibersabotaje a centrales eléctricas de Ucrania el año pasado–, más notorios –con conocidas marcas como Yahoo!, Sony, o LinkedIn, e incluso instituciones como el FBI o el Departamento de Homeland Security, reconociendo brechas de seguridad y fugas de información–, y más evidentes para los usuarios de la mano de una tendencia que se ha ido consolidando: el ransomware. Este tipo de malware ha llamado la atención de usuarios de todo el mundo al encontrarse con sus datos o sus sistemas secuestrados por parte de ciberdelincuentes que exigen un rescate para recuperarlos. Pero más allá de esta prominente tendencia, creemos que es preciso hablar de la seguridad en términos más amplios, ya que el éxito del ransomware se combina y no debe hacernos olvidar lo que sucede en diferentes ámbitos con respecto a la protección de la información, sobre todo en un momento en el que la digitalización de servicios y procesos es imparable.



© Shutterstock

En este contexto de smartcities, smartwearables, etc., los dispositivos del Internet de las Cosas (IoT), o más bien su inseguridad, se han posicionado en el centro de la diana en 2016. Sus numerosas vulnerabilidades en materia de seguridad los han convertido en objetivos fáciles para los ciberdelincuentes. El ejemplo más claro es el ataque de denegación de servicio distribuido (DDoS) lanzado desde

miles de dispositivos (principalmente cámaras, routers y dispositivos de grabación de vídeo) a un proveedor de nombres de dominio, que provocó que servicios como Twitter, Netflix, Paypal, Spotify o Playstation Network quedaran inaccesibles durante horas en algunas regiones del planeta.

Este incidente fue un aviso del peligro que supone tener millones de dispositivos conectados a Internet sin apenas protección. Desde entonces, se han producido ataques similares con resultados dispares como la supuesta desconexión de Internet (que al final no fue tal) de Liberia o los ataques a routers de Brasil o Alemania. Lo preocupante es que estos incidentes parecen haber sido meras pruebas y que en 2017 podríamos llegar a ver un ataque a gran escala protagonizado por todo tipo de dispositivos conectados, que dejara sin acceso a Internet a buena parte de la población mundial, algo que tendría graves consecuencias.

Por desgracia, las investigaciones demuestran los preocupantes agujeros de seguridad existentes en estos dispositivos y ante los cuales los fabricantes siguen sin tomar medidas. Por eso, para 2017 el laboratorio de ESET prevé nuevos ataques a estos dispositivos que abarcarán desde dispositivos de uso cotidiano como los routers domésticos, hasta otros menos habituales como los coches conectados. Esto supone un problema para la implantación del Internet de las Cosas, debido a que aumenta la desconfianza de los usuarios en estos dispositivos y se podría retrasar el lanzamiento de novedades hasta que se solucionen los problemas existentes.

Además, hay que tener en cuenta que estos dispositivos no son solo objetivos de los delincuentes sino que también se pueden lanzar ataques desde ellos. La botnet Mirai ha demostrado este 2016 la capacidad que tienen miles de dispositivos vulnerables controlados por un atacante de causar graves daños, y es más que probable que en 2017 veamos más ataques de este tipo.


© Shutterstock

También esperamos oír hablar más de una nueva amenaza como evolución del ransomware con el secuestro de objetos conectados. Podríamos estar ante «el año del jackware». El jackware es el software malicioso que intenta tomar el control de un dispositivo, cuyo objetivo principal no es el procesamiento de datos ni la comunicación digital.

Un buen ejemplo son los automóviles conectados o coches autónomos. Estos vehículos realizan una gran cantidad de procesamiento de datos y de comunicaciones para llevarte desde el punto A hasta el punto B. El jackware funcionaría como una forma especializada de ransomware. Con el ransomware tradicional, como Locky y Cryptolocker, el código malicioso cifra los documentos del equipo y exige el pago de un rescate para desbloquearlos. En cambio, el objetivo del jackware es mantener bloqueado un automóvil u otro dispositivo hasta que pagues el rescate.

El escenario de una víctima de jackware puede ser el siguiente: en una helada mañana de invierno abrimos la aplicación de nuestro automóvil instalada en el teléfono para arrancarlo y calentar el motor desde la comodidad de nuestra cocina, pero el coche no arranca. En cambio, aparece un mensaje en nuestro smartphone diciéndonos que tenemos que entregar X cantidad de dinero para reactivar nuestro vehículo. Afortunadamente (y ponemos énfasis en esto): el jackware, hasta donde sabemos, solo existe en la teoría.

Otro foco potencial de inseguridad es el de la salud y los objetos conectados. En las instituciones sanitarias, donde el acceso rápido a los datos puede ser una cuestión de vida o muerte, el coste de ser atacado por el ransomware crece considerablemente. Los delincuentes lo saben y están apuntando de forma deliberada a las organizaciones médicas.

A medida que la industria médica se vuelve más digital, es mayor la cantidad de profesionales de la salud y los pacientes que comienzan a utilizar dispositivos médicos. Ya no sólo en hospitales y centros médicos sino también en los hogares y nuestro cuerpo de la mano de todo tipo de pulseras y dispositivos diseñados para monitorizar la actividad física. Estos dispositivos suelen estar repletos de información confidencial. Sin embargo, la seguridad y la privacidad, por lo general, son una preocupación secundaria.

Como hemos visto al analizar la tendencia del ransomware, el riesgo de tener información de alta confidencialidad sin una base sólida de seguridad puede ocasionar graves problemas. Sobre todo, si tenemos en cuenta que los dispositivos médicos utilizados en las redes de hospitales pueden ser máquinas grandes y costosas que, con frecuencia, usan sistemas operativos comunes (y con demasiada frecuencia obsoletos) como Windows XP Embedded. A menudo proporcionan un fácil acceso al resto de la red hospitalaria donde se guardan todo tipo de datos confidenciales: información financiera para la facturación, información de identidad para ofrecer seguros médicos, información relacionada con la salud generada por las visitas de los pacientes...

Desde una perspectiva del cibercriminal, estos datos son sumamente lucrativos: tienen el potencial de ser diez veces más valiosos que los detalles de las tarjetas de crédito o débito. Los dispositivos médicos de los hospitales suelen utilizar un sistema operativo similar al que usan los equipos de escritorio, por lo que es posible aplicar la misma tecnología y las mismas técnicas para protegerlos. Sin embargo, si un dispositivo tiene un sistema operativo obsoleto (y potencialmente sin soporte) se le deberá dar una protección adicional significativa. Hasta puede ser preferible mantener la máquina completamente desconectada de todas las redes, aunque aun así se deberá proteger contra amenazas que se puedan propagar por medios extraíbles.

En el caso de los dispositivos médicos y de monitorización de la actividad física o de la salud utilizados en el hogar suelen ser muy pequeños para que se puedan usar o implantar sin resultar intrusivos. La mayoría utiliza sistemas operativos Linux o basados en Linux. Pueden estar conectados a Internet u ofrecer sincronización con un dispositivo móvil o equipo de escritorio; y al igual que los dispositivos que se usan en hospitales, también suelen actualizarse con poca frecuencia... si es que alguna vez el usuario llega a actualizarlos. Si bien es cierto que un dispositivo utilizado por el paciente en su casa no suele almacenar información de tarjetas de pago, puede tener otros datos que a los delincuentes les interesaría robar o modificar, tales como: la dirección de correo electrónico, el nombre de usuario, la contraseña y los datos de GPS, incluyendo la dirección particular o laboral. Además, el dispositivo podría indicar cuándo el usuario está fuera de casa o dormido, facilitando una intrusión física en el hogar.

Un ataque a un dispositivo médico implantado podría permitir que los delincuentes hicieran una serie de cambios a las medidas prescritas, lo que podría causar problemas médicos graves (o incluso mortales). En cuanto a un dispositivo médico personal, es de suma importancia evitar que se use para dañar a los usuarios o comprometer su privacidad. Es evidente que un ataque a una bomba de insulina o un marcapasos con conexión a Internet será significativamente diferente a un ataque a un dispositivo para monitorizar la actividad física. Pero las medidas de seguridad son necesarias puesto que un ataque menor puede ser la antesala de uno mayor.

En conclusión, hay un tema que es transversal a todo tipo de riesgos y amenazas, que es la necesidad, más grande que nunca, de educar a los usuarios, las empresas y los fabricantes para que comprendan los riesgos actuales y futuros, y tomen dimensión de que la era de la conectividad y digitalización implica un cambio de mentalidad. Basta como ejemplo los datos de algunas encuestas realizadas por ESET: solamente el 30% de los usuarios utiliza una solución de seguridad en sus dispositivos móviles, a pesar de que más del 80% reconoce que los usuarios son los que tienen la mayor cuota de responsabilidad al momento de caer en engaños por no tomar consciencia ni educarse sobre las diferentes estafas.

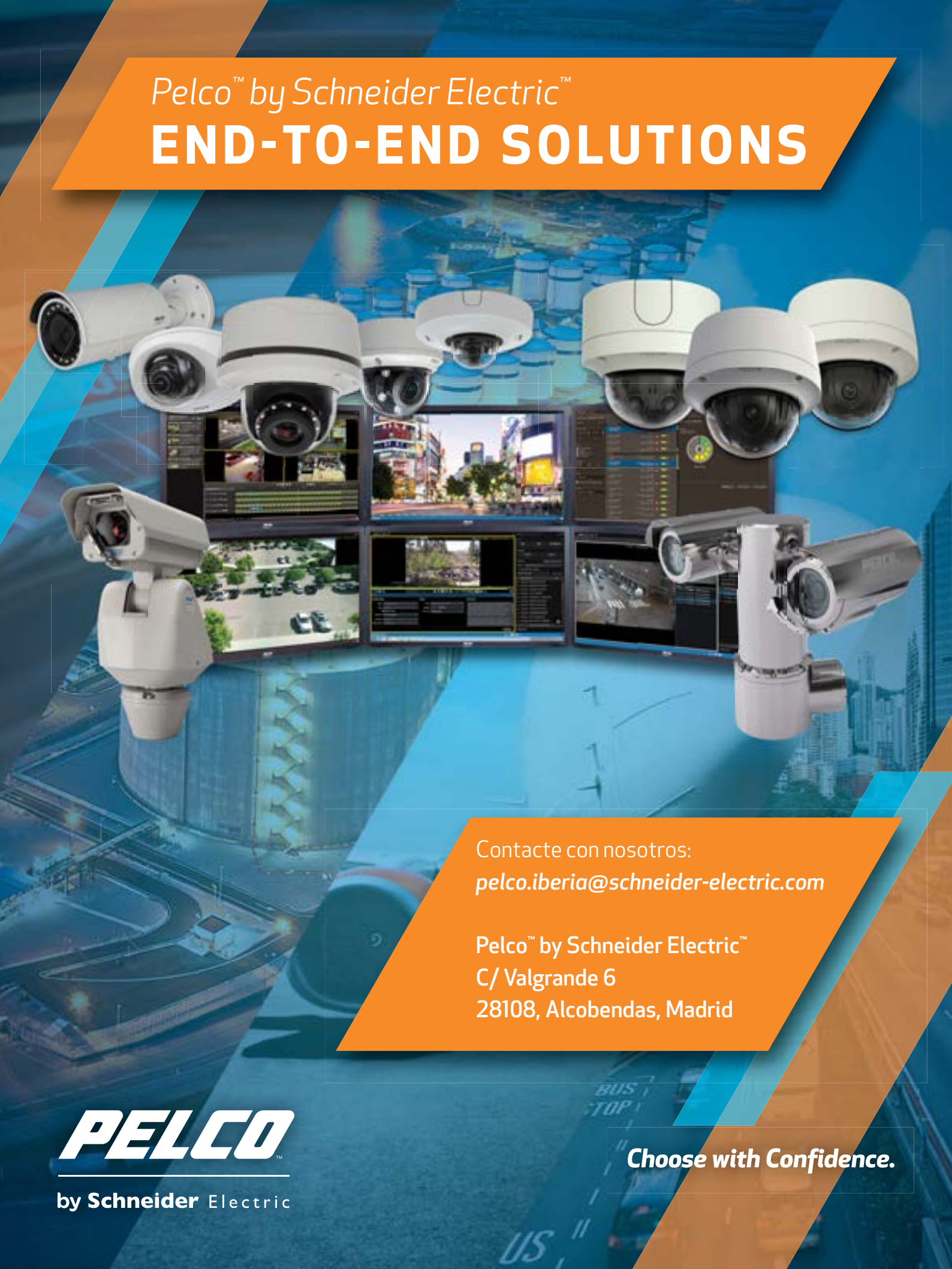
Este tipo de paradojas demuestran que el denominador común en todas las secciones es el factor humano, y debemos seguir trabajando para que las personas dejen de ser el eslabón más débil. De lo contrario, en una sociedad digital híper conectada seguiremos en un escenario con tecnología de última generación pero gestionada con conceptos de seguridad de hace más de 10 años. ●

Fotos: *ESET/Shutterstock*

Contactos de empresas, p. 9.

Pelco™ by Schneider Electric™

END-TO-END SOLUTIONS



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

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

PELCO™
by Schneider Electric

Choose with Confidence.

RUTH VELASCO. MARKETING MANAGER DE SOPHOS PARA ESPAÑA Y PORTUGAL.

Las **12 tendencias** clave en **ciberataques que amenazan en 2017**

EL año 2016 ha estado marcado por el gran número y variedad de ciberataques. Hemos sido testigos desde el potencial destructivo de los ataques DDoS, fruto de la inseguridad de los dispositivos IoT (Internet de Cosas), hasta el presunto hackeo durante las últimas elecciones de los Estados Unidos. A esto se ha sumado el incremento significativo de las filtraciones de datos. Tanto grandes como pequeñas organizaciones, así como los usuarios de cualquier tipo se han visto afectados por pérdidas de información. Y la pregunta que nos hacemos ahora es: ¿Qué nos depara 2017 en cuanto a ciberataques? Desde nuestra compañía hemos analizado y evaluado cómo han impactado los ciberataques de 2016 y hemos identificado las 12 tendencias claves que amenazarán en 2017:

1. Incremento de los ataques destructivos DDos a IoT. En 2016, los ataques de Mirai solo explotaron un pequeño número de dispositivos y vulnerabilidades, usando técnicas básicas de predicción de contraseñas. Para 2017, se espera que los cibercriminales encuentren la manera de ampliar su alcance debido al gran número de dispositivos IoT que contienen un código obsoleto. Es de esperar que se den exploits de IoT, una mayor capacidad de predicción de contraseñas y más dispositivos IoT comprometidos utilizados para ataques DDoS o tal vez para atacar a otros dispositivos conectados a la red.

© Vasin Lee / Shutterstock

2. Sustitución de exploits por ataques sociales dirigidos. Los ataques cada vez son más sofisticados y convincentes, e intentan confundir a los usuarios para que comprometan su propia seguridad. Por ejemplo, es común ver un correo electrónico que se dirige al destinatario por su nombre y afirma que tiene una deuda pendiente que el remitente ha sido autorizado a cobrar. La sorpresa, el miedo o la recaudación de impuestos por parte de autoridades son tácticas comunes y eficaces. Estos ataques de phishing serán cada vez más difíciles de identificar.

3. Infraestructuras financieras bajo mayor riesgo de ataques. Los ataques phishing utilizan información detallada de los ejecutivos de las empresas para engañar a los empleados y que paguen por fraudes o comprometan cuentas. También se esperan

más ataques a infraestructuras financieras críticas, tal como el ataque de instituciones conectadas a SWIFT que costaron al Banco Central de Bangladesh 81 millones de dólares en febrero. SWIFT ha admitido que fueron objeto de otros ataques de este tipo y esperan que haya más, declarando en una carta filtrada a los bancos clientes: «La amenaza es muy persistente, adaptativa y sofisticada, y está aquí para quedarse».

4. Explotación de la infraestructura intrínsecamente insegura de Internet. Todos los usuarios de Internet están a merced de antiguos protocolos, y su ubicuidad los hace casi imposibles de renovar o reemplazar. Estos protocolos están a veces sujetos a graves fallos. Por ejemplo, los ataques contra el BGP (Border Gateway Protocol) podrían interrumpir, secuestrar o desactivar gran parte de Internet. Y el ataque DDoS a Dyn en octubre, que tiró abajo el servicio de DNS y, a su vez, a una parte de Internet, fue uno de los mayores asaltos vistos, y aquellos que se atribuyeron la responsabilidad dijeron que se trataba solo de un simulacro. Los ISP y las grandes empresas pueden tomar algunas medidas como respuesta, pero éstas no pueden prevenir un daño si los individuos o los estados optan por explotar los fallos de seguridad más profundos de Internet.

5. Incremento en la complejidad de los ataques. Los ataques agrupan múltiples elementos técnicos y sociales, y reflejan un examen cuidadoso y continuado de la red de la empresa que será víctima. Los atacantes comprometen varios servidores y endpoints mucho antes de que empiecen a robar los datos o actúen de forma agresiva. Controlados por expertos, estos ataques son estratégicos, no tácticos, y pueden causar mucho más daño. Se trata de un mundo muy diferente a las típicas cargas de malware pre-programadas y automatizadas que se solían ver, siendo ahora más pacientes y evadiendo las detecciones.


© ESB Professional / Shutterstock

«Los ataques cada vez son más sofisticados y convincentes, e intentan confundir a los usuarios para que comprometan su propia seguridad»

6. Más ataques con lenguajes y herramientas de administración integradas. Se observan más exploits basados en PowerShell, el lenguaje de Microsoft para automatizar las tareas administrativas. Como lenguaje de scripting, PowerShell evade las contramedidas centradas en ejecutables. También se ven más ataques que utilizan técnicas de penetración y otras herramientas administrativas que ya existen en la red de la víctima, sin necesidad de infiltrarse y sin levantar sospechas.

7. Evolución del ransomware. A medida que más y más usuarios reconocen el peligro del ransomware, los cibercriminales están explorando otros métodos de ataque. Algunos están experimentando con un malware que vuelve a infectar mucho después de que se pague por rescatar los datos, y algunos están empezando a usar herramientas integradas y sin malware ejecutable, para evitar la detección por código que se centra en los archivos ejecutables. Ejemplos recientes muestran cómo, supuestamente, ofrecen descifrar archivos después de que la víctima haya compartido el ransomware con otros amigos, y esos amigos hayan pagado por liberar sus archivos. Los autores de ransomware también están empezando a usar técnicas distintas de cifrado, por ejemplo, eliminar o dañar los encabezados de los archivos. Y, por último, con el ransomware «antiguo», que sigue estando activo, los usuarios pueden ser víctimas de ataques que no pueden ser resueltos porque el método de pago del rescate ya no sigue activo.

© Profit-Image / Shutterstock

8. Aparición de ataques de IoT personales. Los usuarios de dispositivos IoT en casa no se dan cuenta que sus monitores de bebé son secuestrados para atacar la web de otra persona. Pero, una vez que los atacantes se hacen con un dispositivo en una red doméstica, pueden comprometer otros, como ordenadores portátiles que contienen datos personales importantes. Se prevé que esto suceda más veces, así como más ataques que utilicen cámaras y micrófonos para espiar a los usuarios.

9. Crecimiento de malvertising y corrupción de ecosistemas de publicidad online: el malvertising, que propaga el malware a través de redes de anuncios online y páginas web, ha existido desde hace años. Pero en 2016, vimos que estos ataques ponen de relieve mayores problemas en todo el ecosistema publicitario, como el fraude de clics, que genera clics de pago que no se corresponden con un interés real de clientes.

10. La desventaja del cifrado. A medida que el cifrado se vuelve omnipresente, se ha vuelto mucho más difícil para los productos de seguridad inspeccionar el tráfico, haciendo que para los cibercriminales sea más fácil pasar de forma furtiva a través de las detecciones. Los productos de seguridad tendrán que integrar estrechamente las capacidades de red y de cliente, para reconocer rápidamente los incidentes de seguridad después de que el código se descifre en el punto final.

11. Aumento del enfoque en exploits contra sistemas virtualizados y cloud. Los ataques contra hardware físico (por ejemplo, Rowhammer) plantean la posibilidad de nuevas explotaciones peligrosas contra los sistemas cloud virtualizados. Los atacantes pueden abusar del host u otras máquinas virtualizadas que se estén ejecutando en un host compartido, atacar los privilegios y posiblemente acceder a los datos de otros. Por otro lado, a medida que Docker y todo el ecosistema de contenedores (o «sin servidor») se vuelvan más populares, los atacantes buscarán descubrir y explotar sus vulnerabilidades de esta relativamente nueva tendencia informática.

12. Ataques técnicos contra estados y sociedades. Los ataques tecnológicos apuntan cada vez más a los gobiernos. Hoy en día, las sociedades se enfrentan a la desinformación, noticias falsas y sistemas de votación comprometidos en su seguridad, entre otras amenazas. Por ejemplo, se ha demostrado que los ciberataques podrían permitir a un mismo votante repetir el proceso de votación varias veces de manera fraudulenta, sin ser descubierto. Incluso, si los estados no están involucrados en los ataques contra sus adversarios en las elecciones, la percepción de esta capacidad de vulnerar el sistema democrático es en sí mismo un arma poderosa.

> «A medida que más y más usuarios reconocen el peligro del ransomware, los cibercriminales están explorando otros métodos de ataque»

Un año más, las predicciones de Sophos muestran cómo el cibercrimen es un negocio muy bien organizado, que cada año consigue más beneficios y, que, quienes están detrás de estos ataques y estrategias, emplean cada vez más recursos en conseguir extorsionar a usuarios y empresas para golpearles donde más les duele: robando su información y lucrándose por ello.

Fotos: *Sophos/Shutterstock*

Contactos de empresas, p. 9.

safire

HOTVI - HDCVI - AHD - CVBS

4N1

NUEVAS CÁMARAS ULTRA

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

Encuentra tu distribuidor oficial en:

SAFIRE
www.safirecctv.com
info@safirecctv.com

safire

JAVIER ZUBIETA MORENO. RESPONSABLE DE DESARROLLO DE NEGOCIO DE CIBERSEGURIDAD. GMV SECURE E-SOLUTIONS

Gestión de **vulnerabilidades** en entornos menos evidentes

Descubrir vulnerabilidades vs Gestionar vulnerabilidades

EL tratamiento de las vulnerabilidades es una práctica bien conocida por los departamentos de Ciberseguridad de las organizaciones, se lleva haciendo muchos años y cada vez se refina más y más. Se ha estandarizado un proceso de tratamiento con muchísimo sentido común, que empieza por el descubrimiento, continúa por la depuración y constatación, le sigue la determinación de las acciones correctoras y termina con la información a los afectados, todo ello de forma cíclica para su seguimiento.

Este ciclo puede llegar a ser desesperante, dado que normalmente hay un equipo que descubre las vulnerabilidades, constata que están presentes en el sistema que está analizando e investiga cómo remediarlas. Pero finalmente ese equipo no tiene la capacidad de remediación efectiva, lo que desencadena una serie de tareas adicionales a otros equipos que bastante tienen ya con lo suyo. Como consecuencia, el seguimiento de la evolución de las vulnerabilidades encontradas se convierte muchas veces en una constatación de que todo sigue como estaba y, siendo consciente del riesgo latente, no queda más remedio que desistir en el empeño.

Todo esto es de sobra conocido en las TIC tradicionales, pero la pregunta ahora es: ¿Funciona igual en otros entornos? La no remediación de una vulnerabilidad, ¿incrementa siempre el riesgo?

Veamos dos casos. Vulnerabilidades a nivel de código fuente en Apps o en aplicaciones web, y vulnerabilidades en Entornos Industriales.

©Mozakim/Shutterstock

El caso del código fuente en Apps o aplicaciones web

En este entorno se agudiza más si cabe la criticidad del descubrimiento y de la gestión de vulnerabilidades que en el entorno TIC tradicional.

Es claramente más difícil encontrarlas. Se necesita analizar no sólo el código fuente, sino también su diseño, es decir, un análisis estático de la aplicación. Pero también se analiza la aplicación funcionando, viendo cómo se comporta. Además, las aplicaciones suelen necesitar otros componentes de base, como los servidores de aplicaciones o las máquinas virtuales, cu-

yo código no pertenece a la aplicación y que, lamentablemente, es un vector de entrada muy frecuente. Como consecuencia, otros componentes a añadir en el análisis exhaustivo de nuestra aplicación.

¿Y qué decir tiene de la gestión de las debilidades encontradas en la propia aplicación? Que la dificultad se incrementa sensiblemente, debido a que:

• Si la vulnerabilidad reside en programación insegura, se debe atajar en el mismo código fuente, cuya gestión suele depender de empresas externas.

• Si la vulnerabilidad reside en un componente de base, debe ser resuelto por el proveedor del componente a través de parches, pero los parches hay que instalarlos. Hay que decir que compañías como Microsoft, Apple, Adobe, Oracle, etc., son especialmente diligentes para anunciar vulnerabilidades y publicar parches, aunque también son los que más ataques sufren.

• Si todo lo anterior se dilata mucho en el tiempo, en el caso de aplicaciones web siempre está la posibilidad de implementar una solución WAF (Web Application Firewall), que exige normalmente la involucración de los departamentos de comunicaciones y de ciberseguridad.

Por lo tanto, en este entorno tanto el descubrimiento como la gestión de las vulnerabilidades resulta más complejo que en el TIC tradicional. Afortunadamente, se puede abordar mediante programas de Seguridad en el Ciclo de Vida de las Aplicaciones, que se están implantando en las organizaciones cada vez con mayor frecuencia.

El caso de los Entornos Industriales

Nos referiremos aquí a los Sistemas de Control Industrial y a las Redes OT (Operational Technology).

Harto complicada resulta la tarea del descubrimiento de vulnerabilidades en estos casos. Existe una razón de peso: la disponibilidad de los Sistemas de Control Industrial y de las Redes OT debe ser máxima, absoluta, y todo aquello que perturbe la disponibilidad no se permitirá. Por lo tanto, si el descubrimiento de vulnerabilidades añade latencias, sólo se permitirá en las paradas programadas de mantenimiento del entorno industrial, si fuera el caso. Así que en muchos casos hay que conformarse con análisis tipo «table-top».

Y en el caso de la gestión, también nos encontramos piedras en el camino. Las actualizaciones de software base, como sistemas operativos u otros componentes plataformados, es prácticamente inviable por las razones de disponibilidad anteriormente expuestas. Además, la instalación de software de protección, como antimalware o whitelisting, siempre requiere de la aprobación del fabricante industrial del sistema, por lo que se adivina las situaciones de bloqueo más frecuentes.

Por lo tanto, en los Entornos Industriales se debe vivir con la asunción del riesgo que supone saber que ni se pueden descubrir las vulnerabilidades ni se pueden gestionar con la «facilidad» de los entornos TIC tradicionales.

No todo está perdido, ni mucho menos. De hecho se aplican medidas preventivas y paliativas basadas en las buenas prácticas y no como reacción a un fallo detectado. Por ejemplo, si no puedes actualizar el sistema operativo de un SCADA, al menos implementa todas las medidas de bastionado de ese sistema operativo. Otro ejemplo, si el interfaz web de un concentrador de smartmeters es vulnerable, si no puedes actualizarlo puedes instalar un firewall industrial que lo proteja a nivel de red. ●


© ESB Professional/shutterstock

«El tratamiento de las vulnerabilidades es una práctica bien conocida por los departamentos de Ciberseguridad de las organizaciones»

Contactos de empresas, p. 9.

MARÍA CAMPOS. DIRECTORA REGIONAL DE INTEL SECURITY ESPAÑA

Cómo evitar que la **información** de tu empresa quede **expuesta**

La información es el petróleo de la economía digital. Con la llegada de la digitalización, el volumen de datos en las empresas ha experimentado un crecimiento sin precedentes. Esta ingente cantidad de información que se transmite y almacena es un recurso de gran valor, no sólo para los propietarios de la misma, sino para los ciberdelincuentes que han visto en ella una forma rentable de extorsión.

Especialmente en los últimos meses, hemos visto casos notorios de fugas de información en los que se han visto involucradas empresas y organizaciones de gran relevancia a nivel mundial, poniendo en peligro tanto la información personal de sus clientes o empleados como su reputación o incluso su propiedad intelectual. Por otro lado, la proliferación de nuevos estilos de trabajo móviles y el uso de portátiles y dispositivos móviles fuera del espacio de trabajo ha ampliado el número de canales a través de los cuales se pueden producir pérdidas o robos de datos.

Ante esta situación, vemos cómo la ciberseguridad debe ser una de las principales prioridades empresariales; así lo considera la Unión Europa, que ha publicado un reglamento –que se espera que sea aplicable en 2018– que obliga, precisamente, a que las organizaciones lleven a cabo medidas de seguridad para evitar ciberataques. No en vano, según algunos organismos nacionales, los incidentes de ciberseguridad han aumentado en 200% en el último año, generando pérdidas de más de 13.000 millones de euros,

Ante este contexto y a la luz de las consecuencias de las fugas de información, las empresas deben tomarse muy en serio implementar medidas de seguridad robustas para hacer frente a esta situación. Para ello, considero relevante matizar que la fuga de datos es causada por dos vías: externa e interna. Bien es cierto que la mayor parte de estos incidentes son causados por agentes externos que recurren a múltiples formas y canales para sustraer nuestros datos, la fuga de datos también puede ocurrir de forma interna. Por ejemplo, a través de empleados descontentos que envían información a terceros para su propio beneficio o emails que enviamos con información que no deberíamos haber enviado, e incluso por la pérdida de dispositivos de almacenamiento de información como pendrives.

Por tanto, es recomendable que las organizaciones apuesten por la tecnología adecuada, así como por la implementación de políticas de seguridad; al tiempo que forman y conciencian a sus profesionales sobre los riesgos y responsabilidades en relación a la seguridad de su empresa. Estoy convencida de que, con una integración de estas acciones, las organizaciones serán capaces de reducir notablemente el riesgo de perder datos e información confidencial.

Conciencia sobre el valor de los datos

Por último, en España, estamos viendo cómo poco a poco las empresas están adquiriendo mayor conciencia sobre el valor de sus datos y la importancia de la confidencialidad y privacidad de su información. En este sentido, las organizaciones están comenzando a invertir más en estrategias de protección, cifrado de datos y otros servicios que les ayuden a orquestar la seguridad a través de diferentes dispositivos y entornos.

Queda claro pues, que cualquier organización que gestione datos debe disponer de una estrategia de seguridad férrea y sin fisuras si quiere asegurar la prevención, contención y protección de su información. ●

Contactos de empresas, p. 9.

Alai Secure, primer operador global en Seguridad Telco

Ofrezca a sus clientes un servicio Telco completo, aportando una **capa adicional de seguridad** sobre todas sus comunicaciones.

M2M
IoT

Red
Inteligente

Y ahora también:

ADSL
Privada y Segura

www.alaisecure.com

Alai Secure
Operador global en Seguridad Telco

ANA MARZO. SOCIA WHITAN ABOGADOS

La **ciberseguridad** en el punto de mira de la regulación

TRAS el revuelo que levantó la aprobación de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (Directiva NIS), parece que vivimos una calma que, sin duda alguna, tiene los días contados, si tenemos en cuenta que, la propia norma insta a los Estados miembros a adoptar y publicar, a más tardar el 9 de mayo de 2018, las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la misma.

Mayo de 2018 se presenta como una fecha clave en la que concurrirán, la necesaria aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (RGPD), y la necesaria adaptación de la Directiva NIS, a las normas locales internas.

La Directiva NIS tiene un objeto más técnico que el RGPD, el cual, pese a no tener exactamente como finalidad la seguridad de los datos, desde luego deja bien claro que, sin seguridad, los datos no se pueden tratar por las organizaciones. Por ello, el propio RGPD exige que, con el fin de mantener la seguridad y evitar que el tratamiento de datos personales infrinja los principios básicos del reglamento, el responsable o el encargado evalúen los riesgos inherentes al tratamiento de datos personales y apliquen medidas para mitigarlos. Estas medidas deben garantizar un nivel de seguridad adecuado, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Incluso el RGPD va más allá y exige a los responsables del tratamiento, comunicar «sin dilación indebida», tanto a los interesados como a la autoridad de control, la violación de la seguridad de los datos personales, en caso de que pueda entrañar un alto riesgo para los derechos y libertades de los individuos.

El objeto de la Directiva NIS, es lograr un elevado «nivel común de seguridad de las redes y sistemas de información» dentro de la Unión Europea, en un momento en que tanto el mercado digital como la Administración Electrónica están plenamente consolidados.

No es casualidad haber llegado al punto de tener que regular la ciberseguridad, si tenemos en cuenta que, el mundo digital ha aportado grandes beneficios, pero también ha demostrado tener grandes vulnerabilidades.

Los incidentes de ciberseguridad, tanto deliberados como accidentales, se han incrementado a ritmo alarmante, llegando a perturbar no sólo el suministro de servicios esenciales, que damos por descontados, como el agua, la asistencia sanitaria, la electricidad o los servicios móviles, sino también la Seguridad Nacional de los Estados, como en algunas ocasiones hemos podido apreciar.

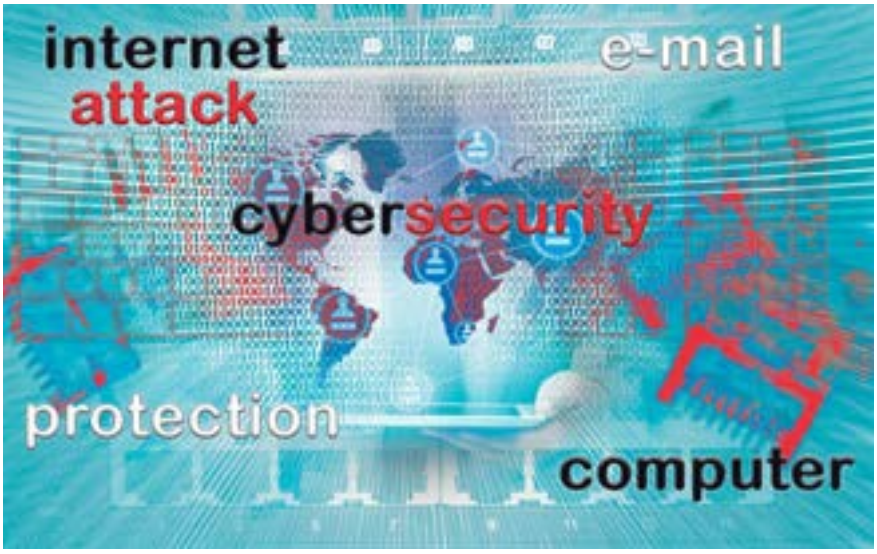
Ello ha hecho difícil establecer los límites entre Defensa, Seguridad y tecnologías civiles, hasta el punto en que, la Unión Europa incluyó la ciberseguridad en su agenda, llegando a establecer de un lado, cuáles deben ser los principios que deben presidir la «política de ciberseguridad» tanto en la Unión Europea como a escala internacional, y de otro lado, las prioridades y medidas estratégicas, todo ello en la denominada «Comunicación conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo, y al Comité de

las Regiones Estrategia de Ciberseguridad de la Unión Europea: un ciberespacio abierto, protegido y seguro». En la misma Comunicación, la Unión Europea aboga por la coordinación entre autoridades competentes en materia de seguridad de redes e información, los cuerpos de Seguridad y la Defensa.

De aquella Comunicación, llegamos a la Directiva NIS para consolidar la seguridad como «un objetivo» que se debe alcanzar a través de tres líneas de trabajo: a) adoptando una estrategia nacional de seguridad de las redes y sistemas de información; b) creando un grupo de cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros; y c) creando una red de equipos de respuesta a incidentes de seguridad informática (llamados «red de CSIRT», por sus siglas en inglés de «computer security incident response teams») para promover una cooperación operativa rápida y eficaz.

Ahora bien, siempre confrontando retos, como el ya legendario de la «seguridad vs privacidad», que el legislador europeo ha reconocido manifestando que, la ciberseguridad solo puede resultar positiva y eficaz si se basa en los derechos fundamentales y libertades enunciados en la Carta de los Derechos Fundamentales de la Unión Europea y en los valores esenciales, y en particular, si se cumple la normativa de protección de datos.

En este punto el RGPD ha aclarado en todo caso que, constituye un interés legítimo del responsable del tratamiento, el tratamiento de datos personales en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información, es decir la capacidad de una red o de un sistema de información de resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que



comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos, y la seguridad de los servicios conexos ofrecidos por, o accesibles a través de, estos sistemas y redes, por parte de autoridades públicas, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad.

Menos ruidosa, pero no por ello menos importante, es la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad y que exige que, cuando los operadores del sector privado presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categoría «Básica», o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías «Media» o «Alta», utilizando los mismos procedimientos que los exigidos en esta Instrucción Técnica de Seguridad para las entidades públicas.

Además, advierte a las entidades públicas contratantes que, es su responsabilidad notificar a los operadores del sector privado que participen en la provisión de soluciones tecnológicas o la prestación de servicios, la obligación de que tales soluciones o servicios sean conformes con lo dispuesto en el Esquema Nacional de Seguridad y posean las correspondientes Declaraciones o Certificaciones de Conformidad, según lo señalado en la presente Instrucción Técnica de Seguridad.

La pregunta que nos deberíamos hacer es, si el sector privado está preparado para afrontar el cumplimiento de los diferentes marcos legislativos que sobre ciberseguridad van apareciendo y regulando los distintos aspectos y sectores, en algunas ocasiones a golpe de certificaciones, creación de nuevos roles internos, adaptaciones tecnológicas, elevadas multas económicas y, en todo caso, bajo criterios de responsabilidad proactiva y rendición de cuentas, a los cuales no estábamos acostumbrados. ●

Fotos: *Shutterstock*

Contactos de empresas, p. 9.

MARIANO J. BENITO GÓMEZ. COORDINADOR CLOUD SECURITY ALLIANCE, CAPÍTULO ESPAÑOL. CISO, GMV SECURE E-SOLUTIONS; **ALDO CARLESSI.** CLOUD SECURITY ALLIANCE, CAPÍTULO PERUANO. CEO EN ATMOSPHERA.CLOUD.COMPUTING*

Una actualización sobre el **estado del arte en seguridad en la nube**

EL concepto de Computación en la Nube, o Cloud Computing, está incorporándose de forma cada vez más frecuente en el lenguaje coloquial, tanto por parte de usuarios particulares como por parte de empresas y organizaciones.

Sin embargo, y como ya apuntábamos en el pasado número de marzo de 2016 de esta revista, «Cuadernos de Seguridad», en nuestro artículo «Luces y Sombras del Estado del Arte de Seguridad en Seguridad Cloud», la adopción (creciente) de estas tecnologías por parte de sus usuarios no se estaba realizando con garantías de seguridad suficientes. Más bien, se dibujaba un panorama en el que la adopción de tecnologías de la Nube y servicios basados en ellas (SaaS, PaaS, IaaS, XaaS, etc.), se estaba realizando sin tener en cuenta las modificaciones en las condiciones de seguridad de los servicios que suponía la migración hacia la Nube de los servicios TI actuales. Lo que suponía que los usuarios de servicios en Nube estaban adquiriendo riesgos para su información sin conocerlos y/o sin valorarlos suficientemente, durante sus procesos de adopción de las tecnologías en la Nube.

El estudio también dibujaba un escenario en el que los proveedores de servicios en la Nube (CSP, Cloud Service Providers) no estaban tampoco respondiendo satisfactoriamente a las demandas y expectativas de seguridad por parte de sus usuarios. Los usuarios de servicios en la Nube tienen expectativas de servicios en la Nube de muy alta seguridad, y aunque rebajan estas expectativas para solicitar requisitos de alta seguridad, su satisfacción final con la seguridad de los servicios recibidos no llega ni siquiera a alta.

Gráfico 1

Estos datos resumen a grosso modo las conclusiones del 3er Estudio del Estado del Arte en Seguridad Cloud[1], publicado en 2015 por los capítulos español[2] y peruano de Cloud Security Alliance. Estudio que se ha continuado en el año 2016, como se presentará a continuación.

Los hallazgos realizados en el año 2015 animaron al grupo de trabajo conjunto de España y de Perú para continuar los trabajos realizados en los estudios anteriores, y producir el Cuarto Estudio del Estado del Arte en Seguridad Cloud[3], con un triple objetivo:

1. Verificar la evolución en el tiempo de los hallazgos más relevantes localizados en los estudios anteriores.

2. Ampliar el ámbito geográfico del estudio, incorporando equipos de analistas e información local de otros mercados hispanohablantes, como por ejemplo Argentina.

3. Ampliar los campos de interés del estudio con aspectos adicionales no contemplados, o contemplados de

forma insuficiente en los estudios anteriores. En particular, se querían analizar ámbitos relacionados con Shadow IT, concienciación de Seguridad por los usuarios de la Nube, y seguridad de la cadena de suministros en la Nube.

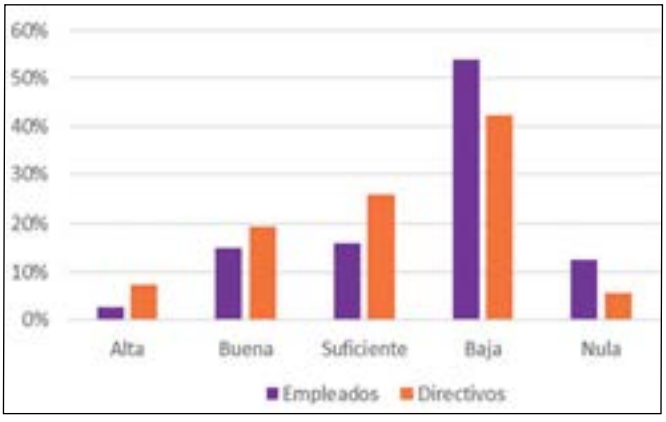
Todos estos objetivos se han cumplido en esta nueva edición del Estudio del Estado del Arte, que está disponible y publicada en https://www.ismsforum.es/ficheros/descargas/iv-cloudsecurity-sota-2016-csa-es-pe-ar-isaca-mad.pdf. Este estudio ha sido desarrollado conjuntamente por los capítulos Español, Peruano y Argentino de Cloud Security Alliance, y por los capítulos de Madrid y de Lima de ISACA, durante los meses de julio a octubre del pasado año 2016.

Comentaremos a continuación algunos de los principales hallazgos efectuados por el estudio, invitando a los lectores a que descarguen y consulten el estudio directamente para ampliar el detalle de los hallazgos realizados y acceder a otros hallazgos, también de interés, pero que no pueden ser analizados en esta contribución.

Principales conclusiones del 4º Estudio

1.- La satisfacción de los usuarios de Nube sigue estando por debajo de sus expectativas y de sus requisitos. **Gráfico 1**

Gráfico 3



Los resultados del año 2017 confirman que se mantiene la situación detectada en años anteriores, con expectativas más altas que los requisitos de seguridad exigidos y satisfacción inferiores a cualquiera de las dos anteriores. Como única novedad, las expectativas en seguridad de los clientes están en los valores menos elevados de todos los estudios, lo que pudiera apuntar a una nueva tendencia en el mercado de los servicios en la Nube.

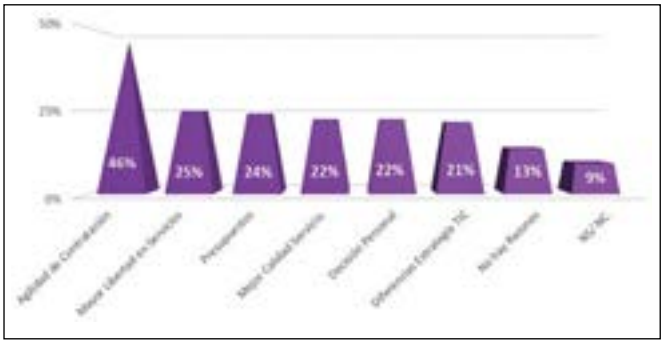


Gráfico 2

2.- Shadow IT. Está ocurriendo en las organizaciones. Porque es más ágil.

El estudio también ha abordado la viabilidad del Shadow IT, es decir, la capacidad de los departamentos No-IT de una organización de contratar y utilizar servicios en la Nube sin la colaboración del departamento IT, e incluso ocultando deliberadamente. En este sentido, se analizaba el fenómeno desde una doble perspectiva:

• En primer lugar se analizaba si el fenómeno de Shadow IT estaba efectivamente ocurriendo en las organizaciones. Así, el 40% de los participantes opinan que ShadowIT no ocurre en las organizaciones (por prohibición o por ser una tarea asignada al departamento de TI). Por el contrario, un 33% cree que el fenómeno existe, bien puntualmente, bien de forma generalizada; y un 20% no tiene una posición clara, bien porque simplemente sospecha que esté ocurriendo pero no lo ha verificado, bien porque no cree que se pudiera detectar.

• En segundo lugar, e independientemente de si el fenómeno está ocurriendo o no, se ha investigado en las causas que podrían justificar este fenómeno. Practicamente todos los participantes identificaban dos razones para hacer uso de Shadow IT. Y de entre todas ellas, hay una razón principal que predomina claramente sobre todas las demás: La agilidad de contratación de servicios en ShadowIT. El resto de razones son seleccionadas por uno de cada cuatro participantes, por lo que no pueden desdeñarse como posible justificación para el uso de ShadowIT.

Por ello, el estudio concluye que el fenómeno de ShadowIT efectivamente está ocurriendo en las organizaciones, debido a la mayor agilidad en el servicio que proporcionan los servicios en la Nube, que se traslada a la agilidad del servicio de las organizaciones a sus clientes. Sin embargo, este fenómeno no se identifica fácilmente ni de forma igual en todos los estamentos de la compañía. Mientras que los niveles de dirección confían en las políticas, procedimientos y recursos corporativos y no detectan el fenómeno, ShadowIT se detecta y asume con más normalidad en otros niveles de responsabilidad dentro de las compañías. **Gráfico 2**

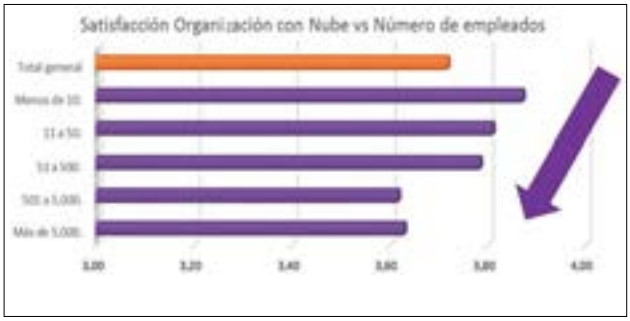


Gráfico 4

3.- Insuficiente concienciación en seguridad en la Nube por parte de las empresas usuarias.

La migración de servicios a entornos de Nube supone cambios en las organizaciones y en sus operativas, sistemas de información, sistemas de control, etc. Y también en el entorno de riesgos y problemas de seguridad a los que debe enfrentarse las organizaciones. La organización y su personal deben ser conscientes de estos cambios, y estar preparados para los mismos, de forma que la migración a la Nube no conduzca a situaciones no deseables e incidentes de seguridad.

Para ello, el estudio ha analizado el grado de concienciación en Seguridad que aplican en sus decisiones a distintos niveles de la organización: Dirección y empleados. Los resultados señalan que se tiene la percepción de que los órganos de dirección de las compañías realizan con más frecuencia análisis de riesgos formales previos a la adopción de servicios en la Nube (uno de cada cuatro), frente a una menor consciencia espontánea o inducida del personal no directivo sobre estos riesgos, que sólo se percibe en uno de cada seis empleados.

En todo caso, la concienciación por parte de ambos niveles se juzga como baja para uno de cada dos directivos y para dos de cada tres no directivos. Estos resultados permiten concluir sin lugar a duda que el grado de concienciación en las organizaciones ante los servicios en la Nube es aún bajo e insuficiente. **Gráfico 3**

4.- La Nube y el tamaño de las empresas usuarias.

Durante el análisis de los datos de base del estudio, se valoraba constantemente la variación de los parámetros analizados en función del sector al que pertenecían las organizaciones, de su ubicación geográfica, de cifra de negocio, etc. Este análisis buscaba identificar las situaciones y circunstancias que podrían caracterizar perfiles de usuarios de servicios en la Nube que no respondieran al escenario general común identificado, o que pudieran ser definitorios de grados de adopción de los servicios en la Nube particulares.

Las actividades de análisis segmentado que se acaban de detallar han ofrecido en realidad escasas conclusiones. Salvo en un caso concreto:

El tamaño de las organizaciones condiciona su satisfacción con los servicios en la Nube. Y condiciona también la respuesta a incidentes que puedan ocurrir en la organización. En general, la satisfacción de las empresas con los servicios en la Nube es inversamente proporcional a su tamaño. Así, las empresas menos satisfechas son las empresas de mayor tamaño, puesto que requieren más información, disponen de más medios para gestionar los servicios recibidos y verificar en primera persona sus servicios en la Nube. Esta situación se detecta de nuevo, y de forma más evidente aún en la gestión y tratamiento de incidentes de seguridad en entorno de Nube. Las organizaciones de menor tamaño tienen menos incidentes de seguridad y de menor impacto que las organizaciones grandes, y además, menos incidentes y de menor impacto que cuando no trabajan en entorno de Nube. Sin embargo, las organizaciones de mayor tamaño sufren más incidentes y de mayor impacto cuando están trabajando en entorno de Nube que cuando están utilizando otro tipo de esquemas de prestación de servicios de TI. Más incidentes y de mayor impacto. Por ello, los beneficios para las empresas grandes de moverse a la Nube existen, pero no están en la gestión de incidentes. **Gráfico 4**

Conclusiones

En conclusión, el Estudio del Estado del Arte confirma que la adecuada seguridad sigue siendo una materia insuficientemente tratada tanto por proveedores como por usuarios, que requiere y va a requerir acciones específicas a presente y a futuro. Algunas de estas acciones serán de concienciación por parte de los usuarios, otras deberán ser abordadas por los proveedores para proporcionar un servicio más satisfactorio y reduciendo número e impacto de los incidentes en sus clientes de mayor tamaño.

El éxito de esta serie de estudios asegura la repetición del mismo en 2017. Les invitamos a que se unan al equipo de analistas para el estudio 2017, contactando con los autores de este artículo. ●

Fotos: *ISMS Forum*

*mjbenito@gmv.com
*aldo@atmosphera.cc

1.- http://www.ismsforum.es/ficheros/descargas/csa-es-pe-2015-estudio-estadodelarte-nube-es.pdf.

2.- www.cloudsecurityalliance.es

3.- https://www.ismsforum.es/ficheros/descargas/iv-cloudsecurity-sota-2016-csa-es-pear-isaca-mad.pdf

INSTITUTO NACIONAL DE CIBERSEGURIDAD

INCIBE: ranking de incidentes de ciberseguridad de 2016

EL Instituto Nacional de Ciberseguridad (INCIBE) ha publicado el ranking de los diez principales incidentes de ciberseguridad producidos en 2016 en todo el mundo y recogidos a través de la Bitácora de Ciberseguridad de INCIBE.

Este ranking se establece teniendo en cuenta criterios de impacto económico, dimensión de las fugas o robos de información en cuanto a usuarios, empresas o instituciones afectadas, daño a la reputación o efectos causados en el ciberespacio a nivel mundial.

En total, se han registrado en la Bitácora 98 «sucesos» de Ciberseguridad, principalmente ataques con robo de información, perpetración de ciberdelitos, infecciones por malware, incidentes que afectaron a Operadores Críticos no nacionales, ciberespionaje e incidentes relacionados con el cifrado de información.

El ranking de los principales «sucesos» de ciberseguridad, que vuelve a poner de manifiesto que ningún sector es inmune a los ataques y que es importante seguir los procedimientos de seguridad, lo encabeza el robo de 81 millones de dólares al Banco Central de Bangladés, perpetrado por piratas informáticos que lograron acceder a los sistemas informáticos del Banco y transferir esa cantidad de dinero a varios casinos de Filipinas. Un error ortográfico en el nombre de uno de los destinatarios levantó las alarmas, evitando así el mayor robo de la historia.

El segundo puesto lo ocupa el robo de unos 64 millones de dólares en bitcoins a la plataforma de intercambio Bitfinex de Hong Kong, el mayor operador mundial de intercambio de bitcoin basado en dólares, lo que provocó una caída de la cotización del bitcoin superior al 23 por ciento.

La tercera posición del ranking es para la publicación de datos de 154 millones de votantes de Estados Unidos.

En cuarto lugar, encontramos la publicación de datos personales de 93 millones de ciudadanos de México, debido a la defectuosa configuración de la base de datos MongoDB utilizada por el Instituto Nacional Electoral de México. En la quinta posición aparece el robo de 1.000 millones de cuentas a Yahoo!. Además de fechas de nacimiento, direcciones de correo electrónico, números de teléfono, contraseñas en MD5, la información robada también contenía preguntas y respuestas de seguridad sin cifrar.

Ocupa el puesto sexto, el robo de 500 millones de cuentas en un ataque, que de acuerdo a la información publicada podría estar respaldado por un estado, ocurrido en a finales de 2014.

En séptima posición aparece el robo de 400 millones de cuentas de Friend Finder Network Inc., compañía que gestiona diferentes páginas de citas. La información robada incluía datos personales, como correo electrónico, patrones de navegación, patrones de compra y orientación sexual de los usuarios.

El octavo puesto es para el mayor ataque de DDoS producido hasta la fecha con dispositivos de Internet de las cosas (IoT). Producido por la botnet Mirai, compuesta por cientos de miles de cámaras IP junto a otros dispositivos IoT, dejó fuera de juego a múltiples servicios de Internet, llegando a afectar a PlayStation Network y Twitter, entre otros.

El noveno lugar de esta clasificación lo ocupa el fallo en la implementación de la pila TCP en sistemas Linux posteriores a la versión de Kermel 3.6.

Cierra este ranking el fallo en los procesadores Qualcomm que permitía acceder a la información cifrada sin que se activaran los mecanismos de borrado. Esta vulnerabilidad afectó aproximadamente al 60% de los móviles Android del mercado.

© StanislauV/Shutterstock

JUAN CARLOS CARRACEDO RUBIO. DIRECTOR DE SEGURIDAD. CAMPOFRÍO ESPAÑA

*«Para Campofrío lo **más importante** **son** sus empleados y, por tanto, su **seguridad**»*

«Cada vez hay más cultura de prevención y seguridad. El punto principal es la concienciación de los trabajadores, para lo cual es necesario una formación continua en esta materia, sensibilizando hacia las consecuencias, el control y comprobación de las tareas que se están realizando y, por supuesto, una implicación directa de la Dirección de la empresa», así lo asegura Juan Carlos Carracedo Rubio, director de Seguridad de Campofrío España, quien durante la entrevista analiza para Cuadernos de Seguridad cuáles son los puntos básicos de la estrategia de seguridad de la compañía, entre otros aspectos.

En un primer acercamiento a la compañía, ¿podría ofrecernos datos concretos de la empresa: historia, áreas de actividad, centros de trabajo, número de empleados?

—Campofrío España, pertenece a Campofrío Food Group, compañía europea líder en el mercado de elaborados cárnicos. Sus productos, que se comercializan bajo sus marcas líderes –Campofrío, Navidul, Revilla y Óscar Mayer, Aoste, Cochonou, Fiorucci, Justin Bridou, Marcassou, Moroni, Nobre, Stegeman, entre otras–, abarcan una gran variedad de categorías y se fabrican y venden en ocho países europeos y en Estados Unidos. Adicionalmente, el Grupo exporta a 80 países a través de distribuidores independientes.

Campofrío Food Group es una subsidiaria de Sigma Alimentos, compañía productora de elaborados cárnicos, lácteos y otros productos refrigerados y congelados, que comercializa a través de marcas bien posicionadas en los mercados donde participa. Sigma opera en 68 plantas y 144 centros de distribución, atendiendo a más de 500.000 clientes en 18 países del norte, centro y sur de América, Europa Occidental y el Caribe. Actualmente Sigma emplea a más de 40.000 personas.

Fábrica de Carnes selectas en Burgos.

Campofrío tiene sus orígenes en Burgos donde fue fundada en 1952. Desde esa fecha su crecimiento ha sido continuo, destacando su expansión internacional, iniciada a principios de los 90, su consolidación en España con la fusión con el grupo Navidul y OMSA Alimentación en el año 2000, y su transformación desde una empresa industrial a una empresa de gran consumo. En la actualidad cuenta con más de 3.000 empleados, 9 plantas de producción, 2 almacenes reguladores, y 21 oficinas comerciales.

—¿Cuál es la estructura e infraestructura del departamento de Seguridad de Campofrío? ¿Cuáles son sus funciones concretas?

—El departamento de Seguridad tiene una total coordinación y colaboración con los distintos departamentos de la Compañía, destacando especialmente los de Recursos Humanos, Jurídico, Sistemas y Manufacturing. Sus funciones en Campofrío son las propias del mismo, es decir, velar por la integridad física de las personas, garantizar la protección de los bienes, valores y patrimonio de la empresa y el normal funcionamiento de los Servicios. Asimismo, otra importante función es la de ser el interlocutor con las Fuerzas y Cuerpos de Seguridad del Estado, cuando se requiera, y la coordinación con las empresas de Seguridad Privada que trabajan en nuestras instalaciones.

—A modo de resumen, ¿podría explicarnos el día a día del responsable de Seguridad de una gran compañía como Campofrío?

—No existe realmente un día a día planificado. Cada día es distinto, aunque por norma general, lo primero que hago es leer los partes recibidos de las distintas fábricas por los servicios de vigilancia que han estado de servicio, analizando las posibles incidencias, de cara a aportar soluciones a las mismas. Por otro lado, mantengo reuniones con proveedores, contacto directo con las diferentes fábricas y con Seguridad Pública.

—¿En qué puntos básicos basa la estrategia de Seguridad de los centros de producción de Campofrío?

—Para Campofrío lo más importante son sus empleados, y por tanto su Seguridad, entendida tanto en su matiz de condiciones laborales, a través de nuestro departamento de Prevención de Riesgos Laborales, como en un significado más amplio, a través del departamento de Seguridad.

La clave de nuestra seguridad en los centros de producción es el excelente trabajo, la dedicación y la involucración de los vigilantes de Seguridad en nuestras plantas, alguno de ellos con antigüedades de más de 25 años. Ellos son los que día a día se relacionan con el personal tanto interno como externo, manteniendo el orden en los accesos a las fábricas, y son los primeros en

Fábrica de Pizzas en Olvega.

detectar conflictos e incidencias en la planta o en los sistemas.

—¿Cuáles considera que son los principales riesgos y amenazas con los que se encuentra un responsable de la Seguridad en instalaciones del tipo de las de Campofrío?

—Para un departamento de Seguridad como el nuestro, una de las prioridades es el control de accesos en nuestras fábricas e instalaciones, así como un sistema de Protección Perimetral de CCTV que detecte cualquier tipo de intrusión en las mismas, de cara a posibles perjuicios, daños o sabotajes.

Tenemos protocolos de actuación ante las diversas situaciones que nos podamos encontrar (Inundaciones, fugas de líquidos, incendios, amenazas, etc.)

—Hoy en día las grandes compañías apuestan por la convergencia de la seguridad como concepto integral, ¿cree que las empresas están preparadas para asumir este nuevo tipo de concepto?

—No es fácil converger en un solo modelo que integre Seguridad Física, Seguridad Lógica y Ciberseguridad.

El valor de los activos, la necesidad de evaluar los riesgos y la constante evolución de las amenazas hacen que debamos trabajar hacia esa concepción global de la seguridad.

En definitiva un análisis integral de los riesgos sería el que nos debe llevar a ese concepto de seguridad integral.

Fábrica de Navidul en Trujillo.

—¿Cuál cree que es el grado de implantación de la cultura de prevención y seguridad en el sector industrial en nuestro país?

—Cada vez hay más cultura de prevención y seguridad. El punto principal es la concienciación de los trabajadores, para lo cual es necesario una formación continua en esta materia, sensibilizando hacia las consecuencias, el control y comprobación de las tareas que se están realizando y, por supuesto, una implicación directa de la Dirección de la empresa.

Asimismo, el número de siniestros, por diferentes motivos, que están ocurriendo en la industria en los últimos tiempos, supone también una mayor concienciación en esta materia y especialmente en sus consecuencias.

—En un mundo globalizado, donde somos objeto de ciberamenazas y ataques virtuales, ¿están las empresas preparadas para hacer frente a estos nuevos riesgos?

—Cada vez estamos mejor preparados; ahora bien, la seguridad completa no existe, hay que evaluar correctamente los riesgos de cada empresa y compartir esa información.

En este mundo donde todo está informatizado y digitalizado, surgen nuevas amenazas que ponen en peligro la seguridad de las empresas (robo de información, robo de clientes, amenazas, extorsiones o falsas informaciones en plataformas digitales que amenazan tu porfolio, etc.), y las empresas deben tener necesariamente unos potentes departamentos de Seguridad, en este caso informáticos.

Por este motivo, es fundamental la integración de los sistemas de Seguridad, tanto la Seguridad Física como la Ciberseguridad. ●

Texto Gemma G. Juanes.
Fotos: Campofrío

JOSÉ JUAN MEAZA IDIRIN. RESPONSABLE DE SEGURIDAD PATRIMONIAL.
BAHÍA DE BIZKAIA GAS. S.L. (BBG)

«El **director de Seguridad** es una figura clave en la **convergencia de la seguridad** desde un punto de vista integral»

«Entendemos la Seguridad Patrimonial desde un punto de vista integral, aglutinando no solamente la Seguridad Física y Lógica, sino también la Seguridad Industrial, la Seguridad de la Información...», así lo asegura José Juan Meaza Idirin, responsable de Seguridad Patrimonial de Bahía de Bizkaia Gas. S.L. (BBG), quien además analiza para Cuadernos de Seguridad la estrategia de seguridad implantada en la compañía, así como su visión profesional sobre la adaptación de las empresas ante las nuevas ciberamenazas, entre otros temas.

EN un primer acercamiento a la compañía, ¿podría ofrecernos datos concretos de la empresa: historia de la compañía, áreas de actividad, centros de trabajo, número de empleados,...?

—Bahía de Bizkaia Gas S.L. (BBG) inicia su actividad en diciembre de 2003, con la misión de suministrar gas natural al País Vasco y áreas limítrofes y reforzar el Sistema Gasista español, atendiendo a los mercados de gas industrial, doméstico y comercial, así como al de generación de energía eléctrica, en condiciones óptimas de Seguridad Integral y Sostenibilidad.

Nuestra actividad se desarrolla en Bizkaia en terreno concesional del Puerto de Bilbao. Con un único centro de trabajo en el municipio de Zierbena y una estructura de 73 personas, damos servicio de descarga, almacenamiento y regasificación de GNL, así como de carga de cisternas y de recarga de buques metaneros.

BBG es la empresa propietaria, cuyos socios son ENAGÁS, con una participación del 50 %, y el Ente Vasco de la Energía (EVE), igualmente con una participación del 50%

Disponemos de un Sistema de Gestión Certificado aplicable a todas nuestras actividades, que integra la Calidad, el Medio Ambiente, la Seguridad y la Salud en el Trabajo, la Prevención de Accidentes Graves, la Seguridad de la Información y la Eficiencia Energética, según las normas ISO 9001, ISO 14001, OSHAS 18001, RD 1254/99 de accidentes graves, ISO 27001 e ISO 50001 respectivamente.

—¿Cuál es la estructura e infraestructura del departamento de Seguridad de Bahía de Bizkaia Gas?¿Cuáles son sus funciones concretas?

—Desde el año 2014 se ha creado un área de Seguridad Patrimonial, con un responsable de Seguridad Patrimonial, que depende directamente del Director General, y se ha designado a la Jefatura de Ingeniería y Sistemas como CISO, siendo a través de dichas figuras que se lleva a cabo la interrelación con el resto de los departamentos de la organización.

Como principales funciones que desarrollamos desde el área de Seguridad están el garantizar el cumplimiento de la Política General de Seguridad, mediante la elaboración de un Plan Director de Seguridad, la implantación de las medidas de seguridad definidas en el mismo, y el reporte del seguimiento de dichas acciones al Comité de Dirección.

Como funciones más concretas, fomentar una cultura de seguridad entre todos los miembros de la organización y potenciar el entrenamiento para situaciones de riesgo mediante la realización de ejercicios prácticos, contribuir en la definición de los mecanismos de respuestas ante incidentes de seguridad, definir las acciones de comunicación interna y de sensibilización, realizar un seguimiento de la legislación actual y adaptar la organización a los cambios que se van produciendo en dicha legislación, proponer acciones encaminadas al control y la mejora continua de la Seguridad Integral, poner en marcha nuevos proyectos, elaborar los procedimientos pertinentes para que las actuaciones redunden en una mejora de la seguridad, y apoyarnos en nuestro sistema de gestión integrado como herramienta para reducir los niveles de riesgo.

Como conclusión nuestra función se resume en desarrollar y gestionar nuestras capacidades para prevenir, detectar, responder y recuperarnos ante posibles incidentes que pudieran poner en riesgo la continuidad de nuestra línea de negocio.

—A modo de resumen, ¿podría explicarnos el día a día del responsable de Seguridad de una gran compañía como BBG?

—El día a día está encaminado a dar fondo y forma a las funciones comentadas en la pregunta anterior, que son muchas y muy variadas, y que responden a las siguientes líneas de actuación.

– **Interacción**: La Seguridad es transversal con todos los departamentos de la empresa, por lo tanto hay una interrelación directa con todas las personas de BBG (reuniones, grupos de trabajo, gestión administrativa, realización de instrucciones de seguridad, etc.) y con otros grupos de interés.

– **Coordinación y comunicación con Organismos Oficiales**: Dentro de los grupos de interés hay que coordinar y gestionar diferentes temas con el CNPIC, el CERTSI, con la OCC, con Cuerpos y Fuerzas de Seguridad del Estado, con la Autoridad Portuaria de Bilbao… Organismos fundamentales para una adecuada gestión de la Seguridad.

– **Apoyo y colaboración con Contratistas**: Es fundamental, igualmente, dar servicio a nuestras contratas y a su personal, así como a las visitas. Debemos marcar las directrices de funcionamiento interno y coordinarlas con el Servicio de Vigilancia, realizando un seguimiento de las incidencias y desarrollando propuestas de mejora.

– **Cumplimiento legislativo**: Además, en el día a día debemos trabajar para cumplir lo dispuesto en la legislación vigente y en las acciones que se derivan de dicha legislación y en las propias de BBG.

En definitiva el día a día es intenso y diferente uno del siguiente.

—¿En qué puntos básicos basa la estrategia de Seguridad de la Planta de Regasificación de BBG?

—La línea estratégica de Seguridad está basada en principios recogidos en nuestra política empresarial.

Dentro de los puntos básicos de nuestra estrategia de Seguridad podemos destacar los siguientes: gestionar la seguridad desde un punto de vista integral; proteger mediante controles humanos, técnicos y organizativos los servicios esenciales prestados por BBG a la sociedad, así como los activos de la organización con el fin de preservar la integridad y la dis-

ponibilidad de dicho suministro; medir la seguridad de los servicios ofrecidos; realizar una gestión efectiva de la LOPD; promover entre las organizaciones colaboradoras la adopción de políticas de Seguridad Industrial, Física, Lógica y de la Información; garantizar la confidencialidad, la integridad y la disponibilidad de la información; participar proactivamente en grupos de trabajo sectoriales para alinear políticas de Seguridad Integral y colaborar con grupos de interés.

Para conseguir estos objetivos nos basamos en unas líneas maestras tales como el compromiso de la Dirección General con la Seguridad; el establecimiento de un organigrama en el que aparecen las figuras directamente relacionadas con la seguridad con unas funciones y responsabilidades establecidas; una metodología de análisis de riesgos como embrión para establecer un Plan Director de Seguridad; la concepción de la Seguridad desde un punto de vista integral; la creación y el funcionamiento de un Comité de Seguridad Integral y la impartición de formación a todos los trabajadores de la plantilla, para concienciar e implantar una política de Seguridad que abarque todos los niveles, con la implicación de todo el personal que formamos parte de BBG.

Quiero destacar, que entendemos la Seguridad Patrimonial desde un punto de vista integral, aglutinando no solamente la Seguridad Física y Lógica, sino también la Seguridad Industrial, la Seguridad de la Información, la formación en diversas materias de todo el personal adscrito a BBG… Entendemos la Seguridad Patrimonial como un factor estratégico que es transversal a todas las áreas y departamentos de BBG. Uno de nuestros objetivos es evitar la interrupción de un servicio esencial. Por ello debemos estar atentos y preparados para evitar cualquier acto malicioso contra nuestras instalaciones o área de negocio, pero no podemos quedarnos ahí, debemos trabajar en todas las áreas. Es de gran importancia tener un mantenimiento adecuado de nuestras instalaciones, un plan de formación adaptado a nuestras necesidades, no solamente desde el punto de vista de la seguridad, que también, sino también en el resto de facetas para disponer del mejor conocimiento posible para operar la planta, de cara a minimizar los errores humanos y a restablecer el servicio en caso necesario con rapidez y garantías; poseer sistemas adecuados y mantenidos de detección y extinción de incendios; contar con el conocimiento y la implantación de los diversos planes de emergencia, estando estos adaptados a nuestra realidad, así como la implantación de distintos procedimientos de actuación ante las distintas casuísticas que puedan darse… La estrategia de Seguridad de BBG, tiene como principales componentes, por una parte su equipo humano que, adecuadamente formado, da respuesta a las necesidades de la organización y de las Administraciones implicadas; por otra parte, el Sistema de Gestión que dota a la organización de procedimientos de actuación garantistas y, finalmente, la implantación de los Sistemas de Protección derivados de la aplicación de nuestro Plan Director de Seguridad.

—¿Cuáles considera que son los principales riesgos y amenazas con los que se encuentra un responsable de la Seguridad en instalaciones del tipo de las de Bahía de Bizkaia Gas, SL?

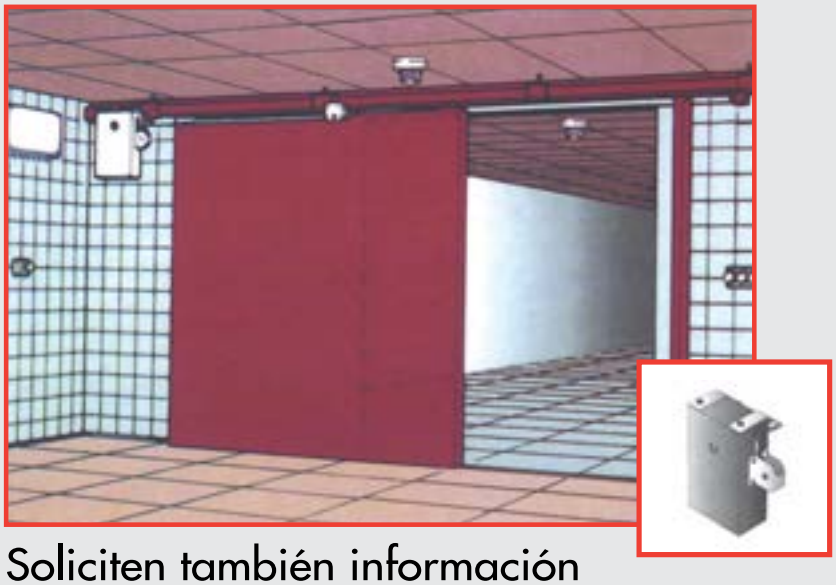
—En estos momentos nuestros riesgos no son distintos de los que pueden tener otras empresas. La irrupción de Internet ha cambiado en pocos años la sociedad y la forma de ver y vivir las distintas situaciones. Ha habido una evolución exponencial en el ámbito de la ciberseguridad como consecuencia directa de la aparición y el desarrollo del ciberterrorismo. Por otro lado, el aumento de la inseguridad como consecuencia de la situación que se está viviendo a nivel internacional afecta a la sociedad en su conjunto y a determinadas empresas del sector industrial en particular.

Hablando de riesgos y amenazas en términos genéricos y conceptuales, desde mi punto de vista, el eslabón más débil de la cadena es la persona (tanto personal propio como subcontratado), por el grado de acceso que tiene a la información y a la propia instalación. Es por ello, muy importante dotarles de la formación necesaria para hacerles conocedores de su grado de responsabilidad en este ámbito.

PROTECCIÓN CONTRA INCENDIOS

Todo del mismo proveedor

Nuestro completo programa ofrece soluciones individuales para la protección pasiva contra incendios, (también antideflagrantes) con:
accionamientos, electroimanes y detectores de humo.



Soliciten también información sobre otras gamas de nuestro programa:

amortiguadores, pistones a gas y cierrapuertas, etc.

Nuestro servicio de asesoramiento colabora con ustedes, incluso para ejecuciones especiales.

DICTATOR Española

C/ Mogoda, 20-24, Polígono Industrial Can Salvatella
• 08210 Barberà del Vallés, Barcelona
Tel. (34 3) 93 719 13 14 • Fax (34 3) 93 718 25 09
www.dictator.es • dictator@dictator.es

Otro de los principales problemas con los que se encuentran las empresas es que, como todos sabemos, un aumento de la seguridad significa una inversión económica. En una inversión asociada a la mejora de la Seguridad, muchas veces es muy difícil de justificar un retorno de la inversión, por lo que finalmente incide directamente en los costes de producción con las dificultades que implica su aprobación. Por ello, partiendo de que debe existir una proporcionalidad entre las medidas de seguridad, armonizada con la eficacia y la eficiencia de las mejoras implantadas, pienso que se debería estudiar la posibilidad de establecer subvenciones para la inversión en la mejora de la Seguridad en las empresas que proporcionan un servicio esencial a la sociedad y que están sujetas a un marco regulatorio, con el objetivo de conseguir unas mayores cotas de Seguridad que de forma general redundarían en beneficio de toda la sociedad

Creo también que, en aras a reducir riesgos y amenazas, sería muy positivo la realización de un marco normativo para que los sistemas de control industrial estén sometidos a unos estándares de seguridad de forma previa a su comercialización

Pero como soy una persona positiva, y centrándome ahora en BBG, quiero aprovechar este punto para hacer hincapié en nuestras fortalezas. La principal, desde mi punto de vista, radica en nuestro tamaño, que aunque a priori pueda resultar una de nuestras debilidades, constituye uno de nuestros puntos fuertes, ya que hace que la comunicación sea fácil y fluida, y que podamos acometer la solución a cualquier imprevisto en un tiempo récord. Somos un equipo que interacciona con rapidez, nuestra elasticidad y flexibilidad nos proporcionan un gran margen de maniobra, de tal manera que una vez puesto en marcha un proyecto, podemos avanzar, retroceder, cambiar de dirección e incluso de sentido sin que la organización se resienta.

Quiero terminar este punto, mencionando la cobertura que nos proporciona trabajar con un sistema de gestión integrado implantado, que nos está facilitando la gestión e implantación de nuestro Plan Director de Seguridad.

—Hoy en día las grandes compañías apuestan por la convergencia de la seguridad como concepto integral, ¿cree que las empresas están preparadas para asumir este nuevo tipo de concepto?

—Hasta no hace mucho tiempo los departamentos de Seguridad integraban la Seguridad Patrimonial como una pequeña parte de un todo, en el que la esencia se encontraba en la Prevención de Riesgos Laborales y en menor medida en la Seguridad Industrial. En los últimos tiempos se está produciendo un cambio cultural en las organizaciones empresariales. Se está tendiendo a la especialización y a la dotación de recursos en el ámbito de la Seguridad Patrimonial, y poco a poco se está extendiendo la idea y la práctica de su desarrollo, desde un punto de vista integral

Las empresas se están preparando y adaptando a los nuevos tiempos porque la Seguridad se ha convertido en un factor estratégico para garantizar la continuidad del negocio o del servicio prestado.

Ha aparecido y se está potenciando la figura del Director de Seguridad, que se está erigiendo como un puntal sobre el que descansa la gestión y la implantación de las políticas de seguridad de las empresas. Es una figura clave en la convergencia de la seguridad desde un punto de vista integral. Tiene una gran proyección y ha llegado para desarrollarse y para quedarse. Una de sus misiones y funciones es la de buscar y encontrar la convergencia entre los diferentes tipos de seguridades que interactúan dentro de una empresa.

Al referirme a esta figura, quiero volver a destacar y a incidir en la transversalidad entre la Seguridad y todas las áreas de las empresas, y de facto con todos los departamentos que la componen.

Otro factor que puede utilizarse como un indicador que mide la madurez de las empresas desde el punto de vista de la Seguridad vista desde una perspectiva integral, es que se está tendiendo entre las grandes empresas industriales, cada vez en mayor medida, a la colaboración público-privada y a la colaboración privada-privada, desde los distintos prismas de la seguridad. Es evidente que si cada una de las partes proporciona todo lo que está en sus manos (medios humanos, materiales, conocimiento,

experiencia, apoyo, información…), estas relaciones van a proporcionar sinergias que redundarán en beneficio de todos. Es necesario comentar y recalcar la importancia de la necesaria relación de confianza que debe existir entre las partes para que este tipo de colaboración dé sus frutos.

—¿Cuál cree que es el grado de implantación de la cultura de seguridad patrimonial en el sector industrial en nuestro país?

—Las empresas están avanzando exponencialmente en la implantación de la Cultura de Seguridad en nuestro país. La legislación, por poner un ejemplo, la Ley 8/2011 y el RD 704/2011, está traccionando en la implantación de una cultura y de sistemas de gestión de la Seguridad en algunas grandes empresas, que a su vez están influyendo en las de su entorno. Esto está haciendo que la implantación de la Cultura de Seguridad esté en un proceso de expansión que avanza sin detenerse. El hecho de que haya un ordenamiento legislativo que marca unas determinadas reglas de juego ha influido considerablemente en la nueva concepción de la seguridad y en su implantación.

Las grandes empresas del sector industrial, están tendiendo al establecimiento de una política de Seguridad con el compromiso implícito de la Dirección, con marcos de gobierno bien definidos, con políticas claras y precisas de Seguridad, y orientadas a la formación y concienciación de todos los integrantes de la empresa.

—En un mundo globalizado, donde somos objeto de ciberamenazas y ataques virtuales, ¿están las empresas preparadas para hacer frente a estos nuevos riesgos?

—Como he comentado anteriormente, las empresas están avanzando en este campo. Estamos asistiendo a un cambio de mentalización y de adaptación al medio. Desde mi percepción, hasta hace relativamente poco tiempo en las grandes empresas, de forma general, los departamentos de Seguridad y de Sistemas eran áreas independientes y prácticamente estancas en las que no había mucha conexión ni excesiva comunicación.

Actualmente, las nuevas formas de ataque se están incrementando exponencialmente por el área ciber. Los departamentos de Sistemas no tienen ya solamente que limitarse a actualizar equipos y mantenerlos relativamente protegidos, sino que tienen que estar preparados para defenderse y reaccionar ante hipotéticos ataques.

La evolución del ciberterrorismo está haciendo que haya que adaptarse a los nuevos tiempos y se está produciendo un cambio sustancial en la forma de trabajar. Este hecho está contribuyendo a que en las empresas estén convergiendo las seguridades Física y Lógica como forma de reforzarse y protegerse.

Los pronósticos apuntan a la integración de miles de profesionales expertos en ciberseguridad en los próximos cinco años, para cubrir el hueco que existe en este campo en estos momentos.

Por lo tanto y como conclusión, pienso que las empresas se están preparando y reforzando para superar con éxito este reto en un plazo relativamente corto.

—¿Qué tipo de formación reciben los trabajadores de BBG en cuanto a Seguridad Patrimonial?

—BBG planifica la formación en Infraestructuras Críticas y Código ISPS, a través de sus Planes de Formación anuales. Así, durante el año 2016 se formaron tanto el Comité de Dirección como las Jefaturas de Turno por considerar prioritarios estos colectivos en un conocimiento tan importante como la seguridad. Para el CISO y equipo de apoyo, se ha planificado la realización de un curso específico adaptado a la realidad de BBG.

Para todo el personal de BBG se va a trabajar en la sensibilización y concienciación en materia de Seguridad durante todo el año 2017, mediante la impartición de formación e información a través de charlas específicas, entrega de trípticos y píldoras informativas, cuyo conocimiento se irá evaluando progresivamente

Asimismo el personal externo responsable de tareas de seguridad patrimonial en nuestras instalaciones, tiene incorporado en su Plan de Formación, acciones formativas adecuadas para las funciones de su puesto.

Texto: Gemma G. Juanes.
Fotos: BBG

DANIEL BERNABÉ FERNÁNDEZ. DIRECTOR REGIONAL DE SEGURIDAD PARA EUROPA, ÁFRICA, MEDIO ORIENTE E INDIA. NISSAN INTERNACIONAL

«*La apuesta de Nissan por la* ***inversión en tecnología punta de seguridad*** *es clave en nuestra estrategia*»

«Solamente con un equilibrio entre los factores técnicos y humanos se puede lograr un plan efectivo de seguridad», así lo asegura Daniel Bernabé Fernández, director regional de Seguridad para Europa, África, Medio Oriente e India de Nissan Internacional, quien además explica para Cuadernos de Seguridad, entre otros aspectos, la estrategia de seguridad de la compañía.

—¿Cuál es la estructura e infraestructura del departamento de Seguridad de Nissan? ¿Cuáles son sus funciones concretas?

—Nissan es un fabricante global de vehículos que vende más de 60 modelos bajo las marcas Nissan, Infiniti y Datsun. La compañía cuenta con unos 175.000 empleados en todo el mundo y operaciones en los cinco continentes. En el año fiscal 2015 vendió 5,4 millones de vehículos.

La importancia que tiene la operación empresarial de Nissan requiere que la compañía se dote de una potente estructura de seguridad, que minimice los riesgos a los que se encuentra expuesta.

Planta Nissan Zona Franca (Barcelona).

El responsable mundial de Seguridad de la compañía se encuentra en Japón. Bajo su supervisión se sitúan tres personas, quienes dirigen la protección y seguridad para las diferentes regiones en las que la compañía lleva a cabo sus operaciones. En mi caso, dirijo las estructuras de seguridad para Europa y AMI (África, Oriente Medio y la India). Otros dos profesionales coordinan las regiones de América y Asia, respectivamente.

Ya en concreto dentro de la región de la que soy responsable, cuatro personas encargadas de otras tantas subregiones me informan directamente acerca de los aspectos de seguridad en el norte y sur de África (desde El Cairo y Pretoria, respectivamente); en Oriente Medio (desde Dubái) y en la India (desde Chennai).

Dentro de dicha región, Nissan cuenta con plantas de producción en países tan culturalmente dispares como son el Reino Unido, España, Rusia, Nigeria, Sudáfrica, Egipto o la India. A través de sus sedes en París (Francia), Rolle (Suiza) y Dubái (Emiratos Árabes Unidos), la

compañía extiende su red de ventas a través de numerosos países, muchos de los cuales están en permanente alerta terrorista o incluso próximos al conflicto armado. Todo lo anterior basta para hacernos una idea del reto que supone el trabajo diario de este departamento. El equipo regional que dirijo cuenta con el personal cualificado para confeccionar y coordinar las políticas de seguridad en dos áreas principales: la protección de las personas y el aseguramiento de los activos. Su posterior aplicación por parte de los equipos de seguridad locales garantiza el mantenimiento de elevados estándares de seguridad y una gestión eficaz de las emergencias.

—A modo de resumen, ¿podría explicarnos el día a día del responsable de Seguridad de una gran compañía como Nissan?

—La verdad es que empieza muy temprano. La mayoría de nuestros equipos se encuentran en países orientales, por lo que la diferencia horaria hace que utilicemos las primeras horas del día en Europa para nuestras videoconferencias o llamadas telefónicas con Chennai, Dubái, El Cairo o incluso con Japón. Básicamente comienzo el día analizando las novedades más importantes que se han producido en cada instalación, y leyendo el informe diario de seguridad que para cada país nos confeccionan analistas externos. A partir de ahí y en función de los diferentes proyectos, mantengo reuniones con los equipos para conjuntamente definir la estrategia.

Por otro lado, y dada la extensión territorial de la responsabilidad de mi departamento, me veo obligado a viajar con mucha frecuencia. Es de vital importancia revisar periódicamente con los equipos locales su nivel de actividad, y mantener las entrevistas de campo necesarias que faciliten el conocimiento necesario para una eficaz valoración de los riesgos y asignación de recursos. Mi trabajo como director regional engloba tanto la aprobación de presupuestos de gastos operativos como la de inversiones, por lo que la proximidad con la gestión de cada uno de los países es necesaria a la hora de tomar decisiones.

—¿En qué puntos básicos basa la estrategia de Seguridad de Nissan en sus plantas de producción?

—Nos centramos especialmente en asegurar un estricto control de los transportes de mercancías desde su llegada a las plantas hasta que los vehículos finalizados abandonan las factorías. También lógicamente en un sistema eficaz de acceso de las personas. Para ello, la apuesta de la compañía por la inversión en tecnología punta de seguridad es clave en nuestra estrategia. En ese sentido, los avances tecnológicos y en comunicaciones nos facilitan concentrar la información de seguridad en un solo punto estratégico, permitiendo así que el control ante emergencias o situaciones de crisis sea mayor y más ágil.

Observamos que muchas empresas están poniendo únicamente en manos de la seguridad electrónica partes importantísimas de su estrategia de futuro, algo que desde mi punto de vista resulta un tanto aventurado.

Solamente con un equilibrio entre los factores técnicos y humanos se puede lograr un plan efectivo de seguridad. Es cierto que los costes son importantes y la tendencia a la reducción de personal de vigilancia está a la orden del día, pero insisto en la importancia que en mi opinión tiene establecer el balance correcto. Un sistema electrónico moderno es el complemento perfecto para el hombre que ha de analizar su información, pero creo que no es prudente dejar la garantía de seguridad de una empresa exclusivamente en los sistemas.

Desde el equipo de Seguridad de Nissan buscamos ese balance perfecto. En concreto, contamos con un sistema mundial de seguridad integrado que gestiona áreas tan importantes como el control electrónico de accesos, el sistema de alarmas o la videovigilan-

cia. Estas prestaciones no hacen que reduzcamos nuestros estándares de formación del personal de seguridad privada.

Por ejemplo, en el caso de España, Nissan mantiene operativo las 24 horas un Centro de Coordinación de Seguridad. Desde aquí es posible monitorizar los sistemas de seguridad, contra incendios y de emergencia de todas las instalaciones que la compañía tiene en diferentes puntos de nuestro país. Paralelamente, las personas que trabajan en este centro han recibido una formación específica que complementa la parte técnica.

—¿Cuáles considera que son los principales riesgos y amenazas con los que se encuentra un responsable de la Seguridad en instalaciones del tipo de las de Nissan?

—A los conocidos y ya tradicionales riesgos asociados a la pérdida de activos a través de la comisión de robos o pequeños hurtos o bien a la intrusión forzada, le añadimos ahora la amenaza terrorista y el robo de información confidencial.

En cuanto al primero de los puntos antes mencionados, la creciente acción terrorista nos obliga a mantener planes de protección muy sólidos. Dichos planes se extienden, no solo a la protección de las instalaciones y de las personas que trabajan en ellas, sino también a los empleados que se encuentran de viaje desde el momento en el que llegan a determinados países considerados de riesgo.

En este sentido, disponemos de herramientas ágiles que nos permiten alertar a nuestros empleados, proveerles de recomendaciones o instrucciones de seguridad de forma inmediata y confirmar que no se han visto afectados por dichos ataques en caso de producirse. Para ello contamos con el apoyo de diversas multinacionales del sector de la seguridad que trabajan sobre la base de las nuevas tecnologías de la comunicación.

Por lo que respecta a la protección de la información confidencial, en nuestro caso se trata de un factor clave para el desarrollo y éxito de nuevos productos. En ese campo se avanza en línea con la creciente competitividad del sector y con el interés de los medios especializados en poner a disposición del ciudadano información de productos que todavía no han sido lanzados al mercado.

Centro de Coordinación de Seguridad de Nissan.

—¿Cuál cree que es el grado de implantación de la cultura de prevención y seguridad en el sector industrial en nuestro país?

—El sector de la automoción es clave en el mundo industrial. España tiene un papel importantísimo en el mismo, no en vano somos uno de los países de Europa con mayor producción de automóviles. Diez marcas diferentes construyen en nuestro país y al menos cinco poseen avanzados centros de diseño, por lo cual, debemos imaginarnos la fuerte implantación, aún hoy creciente, de una conciencia de seguridad y prevención diferente para cada actividad, ya sea diseño, producción o comercialización. No obstante ello, estoy seguro que queda camino por recorrer para tener un sector concienciado plenamente y a ello debemos contribuir con un mayor aumento de la profesionalización y de la formación específica de las personas que trabajan en nuestros departamentos.

—En un mundo globalizado, donde somos objeto de ciberamenazas y ataques virtuales, ¿están las empresas preparadas para hacer frente a estos nuevos riesgos?

—Las compañías multinacionales dedican cada vez mayores recursos y es indudable que la preparación de los profesionales ha mejorado, lo cual garantiza una protección más eficaz. Dicho esto, el reto es incrementar la velocidad en que la tecnología es capaz de minimizar las nuevas amenazas ,y que esta tecnología se encuentre al alcance también de la pequeña y la mediana empresa.

Texto: Gemma G. Juanes.
Fotos: Nissan Internacional

Detectores GUARDALL Performance Line, calificados por BY DEMES GROUP como los mejores del mundo

BY DEMES GROUP lanza la serie de detectores de alta gama GUARDALL Performance Line, bajo su punto de vista, la mejor gama en detección de intrusión del mercado global tanto para aplicaciones residenciales como comerciales.

BY DEMES GROUP, distribuidor líder en material electrónico de seguridad en España, ha presentado la línea de detectores volumétricos de movimiento **Performance Line** de **UTC FIRE & SECURITY,** comercializados bajo la marca **GUARDALL** y destinados a uso residencial y comercial.

La gama **Performance Line** cuenta, por un lado, con una serie de detectores **PIR (PQ15)** y, por el otro, con una serie de detectores de doble tecnología **(DT15).** En primer lugar, la serie **PQ15** está formada por detectores con infrarrojo pasivo volumétrico digital y sensor **QUAD,** el cual proporciona un rendimiento superior. Su instalación resulta rápida y sencilla gracias a la **óptica libre de ajuste** que permite montar entre 2,1 y 2,5 m de altura y proporcionar 15 m de cobertura volumétrica.

Los detectores **PQ15** disponen de **cuatro modos de detección** fácilmente seleccionables (incluyendo el contador de impulsos), lo cual les permite adaptarse a la mayoría de entornos. También disponen de supervisión de **tensión de alimentación, relés** de estado sólido y **tamper** de apertura y pared. Incorporan una **lente varifocal** de alto rendimiento, que no requiere de ajustes y que optimiza el área de detección.

Todo ello sumado a su combinación con el espejo especial para la detección de **ángulo cero,** proporcionan a los **PQ15** una detección excepcional. Además, su diseño basado en microprocesador con algoritmo de procesado de señales, provee una mayor **resistencia a falsas alarmas** (causadas por las variaciones térmicas y picos de ruido).

En efecto, todas estas prestaciones convierten a la serie **PQ15** en la más rentable y atractiva para la protección de locales residenciales y comerciales. Cabe decir que también existe la variante **antienmascaramiento PQ15 AM,** la cual utiliza la tecnología de infrarrojos activa, además de incorporar una resistencia seleccionable de final de línea.

En segundo lugar, la serie de detectores **DT15** incorpora **microondas** de banda X de alta eficiencia y tecnología **PIR,** combinación que da como resultado una mejora en la inmunidad a falsas alarmas. Disponen de **Anti-stealth™**, tecnología exclusiva de **UTC FIRE & SECURITY** que les provee a los mismos de un modo altamente inteligente que analiza con precisión la actividad del **microondas** y del **PIR** y mejora significativamente la detección en condiciones extremas. Gracias a esta tecnología los equipos son capaces, además, de detectar intrusiones por intento de **camuflaje** (neopreno, caja de cartón, paraguas, etc.). Como en la serie **PQ15,**

también se utiliza un espejo especial para mejorar el rendimiento de detección de **ángulo cero.**

Cabe añadir que los detectores **DT15** proporcionan supervisión continua y autoconmutan a una sola tecnología **(PIR o microondas)**, en el caso improbable de fallo en cualquiera de las dos tecnologías. Son igualmente fáciles de instalar gracias a sus **tres LEDs** dentro del sensor y al **ATR autotest** para mantenimientos no presenciales. Además, esta serie también dispone de dos variantes **antimasking** distinguidas por usar tecnología de **infrarrojos activos (DT15 AM)** o tecnología de **microondas (DT15+).**

Toda la gama **Performance Line** cuenta con los certificados de **Grado 2** y todas sus versiones con **antienmascarmiento** con los certificados de **Grado 3.** Para aplicaciones residenciales y comerciales de pequeña escala, **GUARDALL** también dispone de otra línea de detectores volumétricos denominada **Design Line,** la cual cuenta con una serie **PIR** con óptica **Fresnel** y otra serie de doble tecnología **(PIR y Microondas).** Esta gama sigue también una elegante línea de diseño, resultando asimismo rápida y fácil de instalar. Proporciona detección para una amplia variedad de rangos, incluyendo coberturas de hasta **360º** e incluso dispone de detectores con discriminación inteligente de **mascotas** de hasta 35 kg.

El prestigio del fabricante **UTC FIRE & SECURITY** unido a la calidad, fiabilidad y sofisticación de sus productos, hacen de los detectores **Performance** y **Design Line** los equipos más flexibles y efectivos tanto para grandes proyectos como para instalaciones de menor envergadura. Por todo ello, han sido calificados como los "mejores detectores del mundo" por el Director General de **BY DEMES GROUP,** el Sr. Ricardo Rubí, el cual augura un gran éxito en cuanto a su introducción en el mercado nacional.

DAVID VIAMONTE. SALES AND MARKETING DIRECTOR. GENAKER

Evolución de las **radiocomunicaciones** en el sector industrial

La llegada del PTT sobre LTE

Desde la invención de los primeros sistemas de radiocomunicaciones para usos militares y de emergencias, fueron progresivamente adoptados por nuevos segmentos de mercado, como las policías, ambulancias, bomberos, transportes y, eventualmente, los distintos sectores industriales. En la actualidad, sectores como la industria química y petroquímica, alimentaria, siderúrgica, cementera, farmacéutica, son usuarios habituales de distintos sistemas de comunicación, entre ellos sistemas de telefonía inalámbrica DECT (muchos de ellos en fase de sustitución), sistemas de radiocomunicación mediante walkie-talkies, así como soluciones de telefonía fija y móvil, entre otros.

ESTOS sistemas de comunicación walkie-talkie (que, generalmente, agruparemos bajo el acrónimo PMR, Private Mobile Radio) aportan, entre otros, dos principales beneficios respecto a otros sistemas de comunicaciones:

Emisora PMR ATEX vs. Smartphone LTE ATEX con Genaker PTT

a) Instantaneidad. Al pulsar el botón PTT de un walkie-talkie el usuario se pone en contacto de manera inmediata con el resto de usuarios conectados al canal y con el centro de control, facilitando una atención inmediata ante cualquier situación.

b) Comunicación en grupo ágil. Las tecnologías PMR están diseñadas para facilitar la comunicación instantánea entre grupos de trabajo con decenas, centenares o miles de usuarios.

Estas características han hecho de las tecnologías PMR una solución particularmente interesante para el sector Industrial, que a lo largo de los últimos 30 años ha implantado distintos tipos de redes en función de las necesidades y de la evolución de la propia tecnología. Así, a día de hoy podemos encontrar un amplio espectro de escenarios, incluyendo: instalaciones de telefonía fija y DECT, uso de sistemas de walkie-talkie en modo directo sin infraestructura, soluciones basadas en infraestructura PMR analógica (por ejemplo, el sistema MPT-1327 o sistemas «trunking» similares) o sistemas digitales más modernos basados en la tecnología denominada DMR (Digital Mobile Radio).

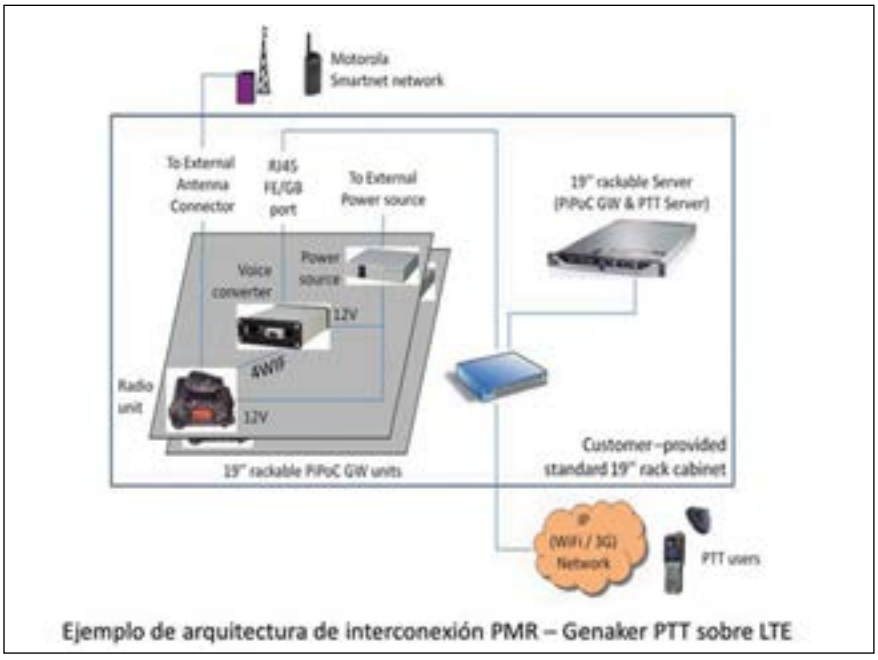
En muchos casos la implantación de este tipo de sistemas requiere el despliegue de infraestructura de red dedicada (repetidores) en cada planta industrial, así como la compra de derechos de uso del espectro radioeléctrico en banda UHF o VHF definidas al efecto. La infraestructura de red permite por una parte dotar de cobertura radio a la planta en cuestión, así como multiplexar las comunicaciones de los usuarios para permitir un uso eficiente del

espectro (mecanismo típicamente denominado «trunking» en este sector).

Nuevos retos para los sistemas de comunicación PMR tradicionales

Este tipo de soluciones PMR ha ofrecido un excelente rendimiento a lo largo de los últimos 30 años, siendo múltiples los sistemas implantados que han alcanzado un elevado nivel de fiabilidad y madurez. No obstante, la evolución de las propias tecnologías de comunicación, así como un acelerado cambio de paradigma en la operativa del sector industrial han dado lugar a algunas limitaciones o nuevas necesidades en el sector, entre las cuales cabe destacar las siguientes:

- El mantenimiento de redes de comunicación dedicadas supone una inversión en recursos propios y mantenimiento, que no tiene una relación directa con el negocio de base de la empresa.
- Los sistemas PMR proporcionan una cobertura local con un radio de algunos kilómetros. Por tanto, la comunicación con usuarios «off site», con la flota de distribución o logística, o la comunicación entre distintas sedes es imposible o requiere del despliegue de infraestructuras adicionales.
- Los sistemas PMR permiten una comunicación de voz instantánea. No soporta otros formatos de comunicación como el intercambio de imágenes, vídeo, formularios, órdenes de trabajo o similares.
- Algunas de las soluciones implantadas en los últimos años están alcanzando su final de vida, siendo necesarias nuevas inversiones para su sustitución por sistemas equivalentes. Adicionalmente, a nivel regulatorio algunas de las frecuencias UHF/VHF actualmente en uso por algunos sistemas PMR deben ser liberadas para nuevos usos que se han definido en dicha banda, forzando por tanto en dichos casos una reconfiguración o migración de los sistemas actualmente en uso.



Ejemplo de arquitectura de interconexión PMR – Genaker PTT sobre LTE

El nuevo paradigma. Las soluciones IP PTT sobre redes LTE y WiFi

En este contexto, hay dos tendencias interesantes en paralelo que cabe analizar. En primer lugar, la progresiva digitalización general de los procesos productivos, la reducción del papel, el uso de equipos electrónicos, PDAs, tabletas industriales, terminales POS, lectores de tags NFC… donde los usuarios reportan la información desde la misma planta, sin necesidad de trabajar con papel. Esta tendencia imparable (en el marco de la iniciativa que se ha empezado a denominar «Industry 4.0») provoca que a día de hoy una buena parte de la operativa industrial dependa de procesos digitales.

En segundo lugar, y en relación con lo anterior, el hecho de que muchos procesos fundamentales estén basados en el intercambio de información digital ha acelerado la implantación de redes de comunicación IP de banda ancha, bien sean sistemas WiFi dedicados o bien redes 3G y 4G desplegadas y reforzadas por los distintos operadores en entornos industriales.

Como consecuencia de todo ello, a día de hoy existen plantas con múltiples redes implantadas y superpuestas, por ejemplo un sistema PMR, una buena cobertura 4G (en muchos casos reforzada y acordada con el operador en un contrato marco de telefonía) y/o una red WiFi desplegada en planta.

A su vez, la aparición de terminales móviles diseñados para usos industriales y la aparición de soluciones PTT (Push-to-Talk) que emulan las comunicaciones walkie-talkie sobre redes WiFi o 4G, permiten a la empresa del Siglo XXI desplegar las nuevas soluciones de comunicaciones del Siglo XXI, permitiendo algunas de las siguientes ventajas:

- Reducción de costes. Ya no es necesario mantener una infraestructura de red PMR propia, así como la inversión en terminales walkie-talkie dedicados únicamente a un servicio de voz, o pagos de frecuencias o proyectos de ingeniería radio.

«Las tecnologías PMR están diseñadas para facilitar la comunicación instantánea entre grupos de trabajo con decenas, centenares o miles de usuarios»

• Convergencia de servicios en un único terminal. Al centralizar las comunicaciones de voz y datos en un único dispositivo se asegura la máxima fluidez en la gestión de la información.

• Comunicaciones ubicuas. Las comunicaciones operativas ya no quedan restringidas a la cobertura de un sistema PMR. Con las nuevas soluciones PTT es posible intercomunicar a usuarios «off-site» con usuarios en planta, intercomunicación entre sedes o comunicación con usuarios de viaje o proveedores ubicados en otros países.

Todo ello, además, manteniendo los dos grandes beneficios de los sistemas de comunicación tradicionales: instantaneidad y comunicación en grupo para coordinar los equipos de trabajo.

En la actualidad múltiples empresas de distintos sectores industriales ya han empezado a implantar sistemas de comunicación PTT sobre redes WiFi y LTE, coexistiendo en algunos casos y sustituyendo en otros a los sistemas PMR tradicionales. En ese sentido, algunas soluciones como Genaker PTT permiten a su vez interconectar ambos sistemas (PMR-PTT) para facilitar una coexistencia temporal de ambos sistemas y una migración progresiva de PMR a PTT.

Un caso particular. El sector Petroquímico

Por último, cabe destacar que la tendencia descrita para el sector Industrial es si cabe más marcada en el sector petroquímico en particular. Efectivamente, debido a la potencial peligrosidad de los procesos en el sector Oil&Gas, es necesario el uso de equipos certificados para funcionar en zonas potencialmente explosivas (equipos certificados ATEX en la UE). Dado lo restringido de este mercado la disponibilidad de soluciones PMR con certificaciones ATEX es más escasa que el mercado PMR general. A modo de ejemplo el sistema más ampliamente desplegado en este sector en los últimos 20 años (la tecnología Smartnet) ha alcanzado ya su final de vida.

En la actualidad los principales actores del sector petroquímico han lanzado iniciativas internas para la migración de sus sistemas de comunicación PMR ATEX hacia soluciones de nueva generación.

En el marco de esta tendencia, Genaker cuenta con múltiples despliegues PTT en entorno petroquímico, y está dando soporte a multinacionales que ya han implantado nuevas soluciones como Genaker PTT en sustitución de los sistemas PMR.

Conclusiones

Las nuevas necesidades del sector industrial han acelerado la adopción de tecnologías y redes digitales basadas en IP. En este escenario, el mantenimiento de redes PMR dedicadas a un servicio de voz únicamente supone unos costes elevados. Actualmente es posible migrar de manera progresiva los sistemas PMR a aplicaciones PTT sobre WiFi y LTE utilizando terminales industriales de alta calidad y manteniendo la instantaneidad de las comunicaciones de los equipos de trabajo. ●

Fotos: Genaker

Contactos de empresas, p. 9.

MANUEL LATORRE. DIRECTOR COMERCIAL. HIGH SECURITY DE TYCO

Integración: presente y futuro de la **seguridad industrial**

La industria es un sector económico clave para la economía española. Según los datos del Instituto Nacional de Estadística (INE), la industria representa el 17,1% del producto interior bruto de nuestro país. Estas infraestructuras tan grandes y costosas llevan asociadas, tanto por los materiales utilizados como por el personal que trabaja en ellas, el concepto de riesgo.

POR ello la seguridad dentro de las industrias debe ser primordial para mantener a los empleados y la producción a pleno rendimiento, a la vez que se consiguen abaratar costes y evitar tiempos de inactividad. De esta forma se garantiza el éxito competitivo del negocio, en un momento donde la competencia global es cada vez más grande y ser el primero proporciona una enorme ventaja en el mercado actual.

Cada industria tiene una necesidad diferente a la que los sistemas de seguridad se deben adaptar. El objetivo principal es reducir al mínimo la incertidumbre. Es imprescindible para toda industria identificar a priori las situaciones de riesgo según los estándares y leyes establecidas, e implementar medidas preventivas según sea el caso. Las plantas químicas son industrias relacionadas con el uso, durante los procesos de producción, de materiales delicados que implican riesgos de incendio. En industrias más convencionales como el sector manufacturero o el agroalimentario el robo de materias primas sigue siendo el riesgo principal a combatir. En el caso de la industria textil la aparición del etiquetado en origen y las tecnologías de gestión de inventario RFID ha supuesto un enorme avance, permitiendo controlar la pérdida desconocida y proteger las prendas desde el proceso de producción. El hurto, la intrusión y el vandalismo contra el material propio son situaciones a las que se enfrentan infraestructuras de servicio público como los aeropuertos. Actualmente, el sector de la alimentación ha sido determinado por el Estado como Infraestructura Crítica, por lo que necesitará desarrollar una planificación donde se plasmen las políticas de seguridad, metodologías y análisis de riesgos, que permitan la protección de unos activos que son especialmente importantes para la prestación de servicios esenciales para la sociedad.

¿De qué manera puede la industria adelantarse y minimizar este tipo de riesgos?: mediante la integración de los sistemas de seguridad. En caso

de producirse una emergencia o un incidente, la unificación de sistemas como el análisis de vídeo de circuito cerrado de televisión (CCTV) de alta resolución, el control de accesos a las plantas, la restricción de zonas sensibles y sistemas de protección, el filtro de autorizaciones o los lectores portátiles para un control total de los procesos de trabajo interno, garantizan una respuesta coordinada que permite una seguridad optimizada y la reducción de costes innecesarios.

Por ejemplo, en una infraestructura con un sistema de seguridad no integrado, cada elemento de seguridad tiene su propio software manejado por un operario diferente. La implantación del PSIM (Physical Security Information Management) permite unificar la gestión de estas plataformas tan diferentes en una sola, simplificando los diversos procesos.

En el supuesto de que hubiera una intrusión y saltase la alarma, el PSIM guiaría al operario posicionando la cámara hacia el punto dónde ha saltado la misma y procedería a avisarle del siguiente paso o a quién llamar. El PSIM permite prescindir de un centro de control con vigilantes que tengan que estar mirando varias pantallas con diferentes subsistemas a la vez y sustituirlo por un solo operador, mientras se realizan servicios de vigilancia en remoto. Alcanzando, de esta manera, un rápida rentabilidad de la inversión (ROI).

Por otro lado, la solución de videovigilancia remota como servicio (VSaaS) permite abordar problemas de seguridad de una forma nueva y efectiva, utilizando vídeo interactivo y audio para observar y monitorizar las instalaciones y el personal 24 horas al día. Por ejemplo, se puede monitorizar el proceso de descarga de un camión mediante el control remoto de los accesos –abriendo y cerrando puertas- o la verificación de imagen. El VSaaS de Tyco integra el control y la gestión de los diferentes sistemas del cliente, incluyendo:

• **Video assist**: Ofrece ayuda personal e inmediata a la organización dando apoyo mediante seguimiento de CCTV. También permite hacer análisis y realizar informes. Así como heatmapping y la posibilidad de contar la gente que entra y sale en el recinto.

• **Auditorías**: Permite realizar chequeos remotos del seguimiento de los procedimientos internos. Por otro lado, hace posible la verificación de indicadores clave de desempeño (KPI).

• **Customer Support:** Permite dar soporte al cliente final en establecimientos desatendidos, como podría ser el caso de gasolineras sin empleados.

• **Revisión técnica de sistemas:** Permite realizar revisiones preventivas de manera remota. Por ejemplo, los responsables de una empresa pueden supervisar en todo momento, mediante el servicio de vídeo, lo que sucede en cualquier localización remota sin necesidad de estar in-situ.

• **Control de Accesos:** Dar soporte para poder reaccionar a tiempo ante eventos de seguridad. Proporcionando una gestión unificada de las credenciales y tarjetas de los trabajadores, regulando la entrada y salida de personas y material.

• **Soporte a logísticas y contratas:** Los sistemas de CCTV ofrecen la posibilidad de apoyar la entrega de material y realizar seguimientos personalizados de transporte de fondos. También permite verificar el trabajo realizado por las contratas de limpieza y mantenimiento de manera remota.

El control integral de todos estos elementos se centraliza en la Central Receptora de Alarmas, que controla durante las 24 horas todos los aspectos relacionados con la seguridad y la gestión de las instalaciones del cliente. Se trata de un servicio personalizado, diseñado a medida de cada cliente y de sus necesidades, que proporciona importantes mejoras en la seguridad, facilita la gestión de los recursos y optimiza la operativa general del negocio, al tiempo que permite importantes ahorros de costes.

La otra gran tendencia actualmente consiste en la integración de la seguridad convencional con la ciberseguridad. Una convergencia que necesita de la unión entre dos sistemas tan diferentes como son los elementos de protección físicos y la seguridad para la programación de servidores y páginas web. Para que la seguridad de estas infraestructuras sea lo más óptima posible, los fabricantes deben contar con socios estratégicos que conozcan el mercado y las dinámicas de la industria, además de contar con los sistemas correctos que garanticen la continuidad del negocio y contribuyan de una forma vital a su éxito competitivo. ●

Fotos: Tyco

Contactos de empresas, p. 009.

ASOCIACIÓN ESPAÑOLA DE DIRECTORES DE SEGURIDAD

AEDS entrega un año más sus Metopas de Honor

Emilio Raduán, al frente de la nueva Junta Directiva

La Asociación Española de Directores de Seguridad (AEDS) celebró el pasado mes de enero su Asamblea General Ordinaria, en la que se aprobaron las cuentas del año 2016, el informe de gestión y se produjo el cambio de la Junta Directiva. El acto finalizó con la tradicional entrega de las Metopas de Honor que cada año concede la Asociación.

EN el encuentro, que tuvo lugar en el Hotel Meliá Castilla de Madrid, el presidente saliente de la Asociación en ese momento, José Antonio Martínez Gómez, dio la bienvenida a los presentes y procedió a la composición de la mesa que quedó constituida por, José Antonio Martínez como presidente, Emilio Raduán como vicepresidente, Ildefonso Polo como secretario, Antonio Avilés como tesorero y Carlos Virumbrales como técnico.

A continuación dio comienzo la Asamblea General Ordinaria con la lectura del acta anterior y resumen de la Memoria de Actividades de 2016.

Seguidamente el tesorero, expuso el Balance Económico de 2016 y los presupuestos para 2017, que fueron aprobados por unanimidad.

Galardonados con las Metopas de Honor, junto a representantes de la AEDS y miembros de las Fuerzas y Cuerpos de Seguridad.

Nueva Junta Directiva de la AEDS.

Acto seguido se procedió a la celebración de la votación de la única candidatura, no habiéndose presentado en tiempo y forma como establece los estatutos de la Asociación otra candidatura alternativa, proclamándose una nueva Junta Directiva, integrada por:

– **Presidente:** Emilio Raduán Corcho.
– **Vicepresidente:** Bernardino Cortijo Fernández.
– **Secretario:** Juan Salvador Roldán García.
– **Tesorero:** Rafael de Castro Pino.
– **Vocal:** Alejandro Gutiérrez Martínez.
– **Vocal:** Javier Herrera Gil.
– **Vocal:** Ángel Antonio Avilés García.
– **Vocal:** Valentín Yebra Fernández.
– **Vocal:** Javier Díaz Maroto.
– **Vocal:** Segundo Pareja Fernández.

Acto seguido, la Asociación Española de Directores de Seguridad (AEDS), procedió a entregar sus Metopas de Honor, que en esta edición recayeron en:

– Julio Camino Burguillos, Inspector, Jefe de Grupo de la Sección de Inspección – UCSP – Comisaría General de Seguridad Ciudadana – Policía Nacional.
– Fernando Alcázar Pérez, Comandante de la Guardia Civil del departamento de Comunicación del SEPROSE.
– Javier Borredá Martín, presidente Ejecutivo de Borrmart y Patrono de la Fundación Borredá.

Fotos: AEDS

RAFAEL SARASOLA. COORDINADOR DEL COMITÉ DE INSTALACIÓN DE PRODUCTOS DE PROTECCIÓN PASIVA. TECNIFUEGO-AESPI

Análisis de **criterios de evaluación y de resistencia al fuego**

En este artículo se estudiará la evaluación y mejora de la resistencia al fuego analizando diferentes casos para que los técnicos puedan tomar decisiones más correctas. Se expondrán partes del CTE que se consideran relevantes y se irán comentando. Hay que tener en cuenta que el CTE debe ser un organismo vivo dado que continuamente se están modificando normas con objeto de asegurar la mejor protección contra incendios e incorporando las nuevas tecnologías.

EL análisis estructural es muy complejo, dado que influyen numerosos factores. El reto de los ingenieros de incendios es lograr la máxima rentabilidad con el menor coste posible facilitando el salvamento de vidas. El dimensionado para la adecuada protección de un bien se refiere para un tiempo determinado (no es ilimitado). La especialización en este campo es muy compleja dado que requiere una experiencia en ensayos y análisis en incendios reales para poder aportar soluciones sólidas que aseguren un buen comportamiento al fuego. La modelización del ensayo suele ser más desfavorable que la realidad, pero el análisis estructural es determinante al objeto de poder definir una solución constructiva. Sin conocimientos sólidos en estructuras es difícil optimizar los resultados, al fin y al cabo, la acción del fuego actúa como una carga adicional, pero con más efectos colaterales que los puramente estructurales.

El establecimiento de escenarios es complicado. La elaboración del código técnico está basado es unos estándares de carga de fuego generales que no siempre responden a la realidad que nos encontramos. Y aún más, el proyecto no puede ser modificado en ningún caso por el usuario de dicho establecimiento, dado que cambiaría las exigencias de comportamiento al fuego.

Cómo se eligen las soluciones de resistencia al fuego

Las soluciones respaldadas con ensayos oficiales tienen una justificación legal clara. Se aplica la norma que está en vigor.

Hay que tener en cuenta que en el código técnico aparecen solamente el número de la norma y a veces no aparece el año de publicación, se supone que los proyectistas deben de utilizar la última norma en vigor que ha salido en el diario de la Comunidad Europea. Adjunto comentarios del código técnico.

Versión de las normas UNE-EN de ensayo que debe considerarse

Las UNE-EN de ensayo o de clasificación, al ser normas de apoyo a normas EN armonizadas de producto publicadas en el Diario Oficial de la Unión Europea, se pueden considerar incluidas entre las de actualización automática conforme a la última versión.

Condiciones de comportamiento ante el fuego de los productos de construcción y de los elementos constructivos

1.- Este DB establece las condiciones de reacción al fuego y de resistencia al fuego de los elementos constructivos conforme a las nuevas clasificaciones europeas establecidas mediante el Real Decreto 312/2005, de 18 de marzo, y a las normas de ensayo y clasificación que allí se indican. No obstante,

cuando las normas de ensayo y clasificación del elemento constructivo considerado según su resistencia al fuego no estén aún disponibles en el momento de realizar el ensayo, dicha clasificación se podrá seguir determinando y acreditando conforme a las anteriores normas UNE, hasta que tenga lugar dicha disponibilidad.

2.- El Anejo G refleja, con carácter informativo, el conjunto de normas de clasificación, de ensayo y de producto más directamente relacionadas con la aplicación de este DB.

Cuando no existe norma clara y hay que aplicar diferentes interpretaciones es cuando pueden llegar los problemas. Hay que justificar la seguridad contra incendios como si fuera una prueba a tamaño real. Cuando los sistemas puedan ser evaluados mediante ensayos con normas internacionales contrastadas, podrían ser aceptados. La aplicación de estas tecnologías requiere una profunda especialización para dar una respuesta técnicamente adecuada a los problemas de obra. El uso a nivel mundial de los equipos multidisciplinares es una constatación que en los grandes proyectos es imprescindible la participación de especialistas expertos en los sistemas. Solo así se realizará un análisis profesional.

Criterios generales de aplicación

Pueden utilizarse otras soluciones diferentes a las contenidas en este DB, en cuyo caso deberá seguirse el procedimiento establecido en el artículo 5 del CTE, y deberá documentarse en el proyecto el cumplimiento de las exigencias básicas. Cuando la aplicación de este DB en obras en edificios protegidos sea incompatible con su grado de protección, se podrán aplicar aquellas soluciones alternativas que permitan la mayor adecuación posible, desde los puntos de vista técnico y económico, de las condiciones de seguridad en caso de incendio. En la documentación final de la obra deberá quedar constancia de aquellas limitaciones al uso del edificio que puedan ser necesarias, como consecuencia del grado final de adecuación alcanzado y que deban ser tenidas en cuenta por los titulares de las actividades.

Cuando se cita una disposición reglamentaria en este DB debe entenderse que se hace referencia a la versión vigente en el momento que se aplica el mismo. Cuando se cita una norma UNE, UNE-EN o UNE- EN ISO debe entenderse que se hace referencia a la versión que se indica, aun cuando exista una versión posterior, excepto cuando se trate de normas UNE correspondientes a normas EN o EN ISO, cuya referencia haya sido publicada en el Diario Oficial de la Unión Europea en el marco de la aplicación de la Directiva 89/106/CEE sobre productos de construcción, en cuyo caso la cita debe relacionarse con la versión de dicha referencia.

Cómo y dónde se ensayan

Los laboratorios acreditados se encargan de realizar las evaluaciones de los productos. Sin embargo a veces resulta complicado analizar los informes y su validez.

Se pueden realizar tanto ensayos a tamaño real o modelizado con las normas UNE-EN.

Laboratorios de ensayo

La clasificación, según las características de reacción al fuego o de resistencia al fuego, de los productos de construcción que aún no ostenten el marcado CE o los elementos constructivos, así como los ensayos necesarios, para ello deben realizarse por laboratorios acreditados por una entidad oficialmente reconocida conforme al Real Decreto 2200/1995 de 28 de diciembre, modificado por el Real Decreto 411/1997 de 21 de marzo.

En la fecha en la que los productos sin marcado CE se suministren a las obras, los certificados de ensayo y clasificación antes citados deberán tener una antigüedad menor que 5 años cuando se refieran a reacción al fuego y menor que 10 años cuando se refieran a resistencia al fuego.

Obligatoriedad de aportar los informes de ensayo

Los fabricantes o suministradores de productos que aún no ostenten el marcado CE solo están obligados a aportar copia del certificado de clasificación, el cual en todo caso debe contener la descripción e identificación completa del producto. Tanto el informe de clasificación como el de ensayo, aunque éste no se entregue, deben ser vigentes conforme a lo que establece este DB SI.

Vigencia de los informes de extensión de la aplicación de los resultados de los ensayos (EXAP)

Los informes de extensión de la aplicación de los resultados de los ensayos (EXAP) deben basarse en la norma aplicable vigente (EN EXAP). Cuando esta no exista, deben basarse en su último proyecto disponible (prEN EXAP) y cuando este tampoco exista, en la experiencia del laboratorio si bien, en este caso, su validez queda al margen del ámbito de aplicación del CTE.

Los informes EXAP basados en la experiencia de un laboratorio se deben anular cuando se disponga de un prEN EXAP. Los informes basados en un prEN EXAP se deben actualizar cuando se disponga de un proyecto posterior o bien de una norma EN EXAP.

Cuando se modifique una norma EN EXAP, los informes realizados conforme a ella se deben anular y revisar de acuerdo a la nueva norma, aunque los informes de ensayo en los que se base el informe EXAP estén en vigor.

Un informe EXAP pierde su vigencia cuando la pierda alguno de los informes de ensayo en los que se basa.

Los informes EXAP los deben elaborar laboratorios acreditados para la realización de ensayos por una entidad oficialmente reconocida.

Cómo se calcula la resistencia al fuego estructural

Se debe saber el comportamiento térmico y estructural del elemento a proteger. Por ejemplo, la temperatura crítica a la que se ha dimensionado la estructura. Si existe una buena coordinación entre el cálculo de estructuras y los de protección al fuego permitirán sin ninguna duda optimizar la solución.

Se pueden realizar con cálculos analíticos, experimentales y por el método basado en comparación con las tablas ya incluidas en el CTE, que es fruto de un estudio que se realizó por el ministerio.

Método experimental

En cuanto a la evaluación experimental de la resistencia al fuego de un sistema constructivo estructural o no, se utilizan las normas UNE_EN. Los ensayos se llevarán a cabo en los laboratorios expresamente autorizados.

Con la introducción del sistema de prueba y la clasificación europea, el laboratorio da dos documentos diferentes:

– **El informe del ensayo**, que contiene una descripción detallada del elemento bajo prueba y las condiciones de preparación. También contiene una descripción precisa de las observaciones que se registran durante el ensayo y la evaluación de los parámetros necesarios para la clasificación (temperaturas más altas, paso de gases calientes, creación de grietas evidentes, el paso de la llama, deformaciones, etc.). Este informe no contiene ninguna indicación de la clasificación.

– **Informe de clasificación**, que contiene una descripción del elemento bajo prueba, el número de referencia del ensayo, la clasificación obtenida, y el campo de la aplicación directa del resultado de la prueba en la que se indican las variaciones admitidas en comparación con la muestra de prueba, sin una evaluación adicional (campo de aplicación directa). Existen normas que introducen los conceptos de «campo de aplicación directa» y de «alcance extendido» del resultado de la prueba.

– **El «campo de la aplicación directo»** del resultado de la prueba, es el conjunto de cambios que puede realizar en el elemento en estudio, sin necesidad de más pruebas o cálculos. Cada informe de calificaciones contiene una cláusula específica en la que se indican las variaciones admisibles.

– **El «alcance extendido»** es el conjunto de cambios en el elemento ensayado que no entran dentro del campo de aplicación directo y que se reconoce como válida por el laboratorio.

Métodos analíticos

Se incluyen varios métodos analíticos.

Anejo B

Tiempo equivalente de exposición al fuego

B.1 Generalidades

1.- Este anejo establece el procedimiento para obtener el tiempo equivalente de exposición al fuego que, según se indica en SI 6, puede usarse como alternativa de la duración de incendio a soportar, tanto a efectos estructurales como compartimentadores. El tiempo equivalente se obtiene teniendo en cuenta las características geométricas y térmicas del sector y el valor de cálculo de la carga de fuego.

2.- En este anejo se indica también la expresión de la curva normalizada tiempo-temperatura definida en la norma UNE EN 1363:2000 y que se utiliza como curva de fuego en los métodos de obtención de resistencias dados en este DB-SI. En la norma (Eurocódigo) UNE EN 1991-1-2:2004 se indican otras curvas de fuego nominales.

B.2 Curva normalizada tiempo-temperatura

La curva normalizada tiempo-temperatura es la curva nominal definida

Cuadro 1.

Coeficiente de ventilación w

Altura de planta (m)	*Superficie relativa de huecos en fachada*				
	0,05	*0,10*	*0,15*	*0,20*	*≥ 0,25*
2,5	*2,6*	*1,8*	*1,3*	*1,0*	*0,9*
3,0	*2,4*	*1,7*	*1,2*	*0,9*	*0,8*
3,5	*2,3*	*1,6*	*1,1*	*0,9*	*0,8*
4,0	*2,2*	*1,5*	*1,1*	*0,9*	*0,8*

Tabla B.1. *Valores de K_c según el material estructural*

Material de la sección transversal	k_c
Hormigón armado	1,0
Acero protegido	1,0
Acero sin proteger	13,7 · O

Tabla 1.

en la norma UNE EN 1363:2000 para representar un modelo de fuego totalmente desarrollado en un sector de incendio. Está definida por la expresión:

$\Theta g=20 + 345 \log_{10} (8 t +1)$ [°C]; (B.1)

siendo:

Θg temperatura del gas en el sector [°C]; y t tiempo desde la iniciación del incendio [min].

La curva normalizada tiempo-temperatura supone, aproximadamente, las siguientes temperaturas:

Tiempo t, en minutos (15 30 45 60 90 120 180 240).

Temperatura en el sector Θg, en °C (740 840 900 950 1000 1050 1100 1150).

B.3 Tiempo equivalente de exposición al fuego

1.- Para elementos estructurales de hormigón armado o acero puede tomarse como valor de cálculo del tiempo equivalente, en minutos:

$t_{e,d} = k_b \bullet w_f \bullet k_c \bullet q_{f'd}$ (B.2)

siendo:

k_b: coeficiente de conversión en función de las propiedades térmicas de la envolvente del sector; que puede tomarse igual a 0,07. El anejo F de la norma UNE EN 1991-1-2:2004 aporta valores más precisos.

w_f: coeficiente de ventilación en función de la forma y del tamaño del sector.

k_c :coeficiente de corrección según el material estructural (**Tabla B.1**).

$q_{f'd}$: valor de cálculo de la densidad de carga de fuego en función del uso del sector, en MJ/m2, obtenida según se indica en el apartado B.4.

2.- El coeficiente de ventilación wf se calcula como:

$w_f = (6/H)^{0,3} \bullet [0,62 + 90(0,4 - \alpha_v)^4 / (1 + bv\, \alpha_h)] \geq 0,5$ [-] (B.3)

siendo:

$\alpha v = A_v/A_f$: relación entre la superficie de las aberturas en fachada y la superficie del suelo del sector, con los límites $0,025 < \alpha v < 0,25$ (B.4) .

$\alpha h = A_h/A_f$:relación entre la superficie de las aberturas en el techo, Ah, y la superficie construida del suelo del sector

$bv=12,5 (1 + 10\, \alpha v - \alpha v^2) \geq 10$ (B.5).

H :altura del sector de incendio [m]

Para sectores pequeños (A_f <100 m^2), sin aberturas en el techo, el coeficiente wf se puede calcular aproximadamente como:

$w_f = O^{-½} \bullet A_f/A_t$ (B.6) siendo:

$O = A_v \sqrt{h} / A_t$ coeficiente de aberturas con los límites $0,02 \leq O \leq 0,20$ [$m^{1/2}$];

At : superficie total de la envolvente del sector (paredes, suelo y techo), incluyendo aberturas [m2];

H: altura promedio de los huecos verticales, [m]

Como aberturas en fachada o en techo se deben considerar los huecos, lucernarios, ventanas (practicables o no) superficies acristaladas y, en general, toda zona susceptible de facilitar la entrada de aire a la zona en la que se desarrolle el incendio.

De forma simplificada, para casos de sectores de una sola planta con aberturas únicamente en fachada, el coeficiente de ventilación w en función de la altura de la planta y de la superficie de dichas aberturas respecto de la superficie en planta del sector, puede tomarse como se refleja en el **Cuadro 1**.

Los valores del coeficiente de corrección kc se toman de la siguiente **Tabla 1**.

Conclusiones Finales

El cálculo es complejo por la cantidad de variables que se dan en la obra que no se pueden reproducir en el laboratorio, los ensayos son solo una modelización que conducen a una simplificación del problema. La única solución exacta sería la realización de ensayos a tamaño real, pero tienen un coste muy grande y solo se pueden hacer en casos muy especiales.

En el comité SC7 de Resistencia al fuego se incluyen todas las normas que están en revisión, y es en los grupos de trabajo donde se definen con detalle los ensayos. Se analizan por subsector de aplicación, para describir los detalles de cada solución constructiva dado que tienen diferentes metodologías de ensayos. ●

Fotos: Tecnifuego-Aespi

FERNANDO PIRES. VP SALES MANAGER AND MARKETING. MORSE WATCHMANS

Cómo mejorar la operatividad del negocio **con un sistema de gestión de llaves**

La información de su uso se puede rastrear, recopilar, clasificar y analizar

En una época anterior, las decisiones empresariales a menudo se hacían basadas en el instinto, partidas de golf, política y muy ocasionalmente en investigación de mercado. Desde entonces, las organizaciones se han alejado de este tipo de comercialización y han adoptado un enfoque más respaldado por las investigaciones y orientado hacia los resultados en los negocios.

HOY en día, las empresas de todos los tamaños y tipos dependen de la investigación, obtenida a través de la minería de datos, para ayudarles a ver el panorama general e identificar tendencias y patrones que pueden ayudar a crear eficiencias operativas. Con el concepto de «Big Data», cada dato (de digital a convencional) es una pieza potencial de información que se puede rastrear, recopilar, clasificar y analizar.

Tomemos como ejemplo el uso de sistemas de gestión de llaves en una organización. Estos sistemas están diseñados para almacenar y controlar el acceso a las llaves mecánicas y otras usadas en una instalación. A las llaves sólo pueden acceder personas previamente autorizadas con un código, una placa y/o una identificación biométrica apropiada. Todas las actividades de acceso se registran automáticamente y, de estos datos, la administración tiene un historial completo de quién eliminó y devolvió qué llave y cuándo. Los datos obtenidos de la grabación automática de la actividad de acceso se pueden utilizar para analizar las tendencias para generar inteligencia valiosa y útil para la seguridad física y las prácticas empresariales.

Rastreo

Por razones de seguridad, las llaves pueden ser controladas de acuerdo con los requisitos (es decir, hora/día disponible, personal, etc.) y la administración puede consultar rápidamente qué llaves no se han devuelto y cuándo cada llave llegará con retraso. Y si una llave no se devuelve al armario según lo programado, se puede enviar una alerta por correo electrónico o texto SMS al personal apropiado para que se puedan tomar medidas inmediatas. Para que la administración de llaves sea aún más conveniente, una aplicación móvil permite a los usuarios autorizados ver una amplia gama de información en directo e in-

teractuar remotamente con el sistema. En caso de un incidente, la administración puede consultar el sistema para obtener detalles específicos, como una lista de todas las transacciones entre ciertas horas o un informe de la hora anterior al incidente. Inmediatamente después de un incidente como el descubrimiento de una pieza dañada o una que falte en un equipo, se puede generar un informe mostrando quién accedió por última vez a la llave en particular. Junto con los datos de auditoría de un sistema de control de acceso, la función de notificación de un sistema de control de llaves proporciona una sólida trayectoria de evidencias.

Recolección y clasificación

Los planificadores incorporados se pueden programar para descargar automáticamente todos los datos a un PC seguro según lo requerido por el usuario, incluyendo en línea como ocurre con las transacciones: periódicamente; diariamente en un momento especificado; semanal con el día y la hora especificados; o mensual con el día y la hora especificados. La entrega de correo electrónico de informes personalizados o estándar se puede programar para cualquier frecuencia o tiempo específico, o se puede acceder mediante una aplicación de teléfono inteligente. Con esta capacidad, la administración puede ordenar y analizar mejor la información para mantener el máximo control de los problemas de acceso y seguridad.

Además, la funcionalidad avanzada permite mejorar el filtrado de usuarios y transacciones, así como la capacidad de crear una plantilla de informe personalizada que proporcione la información y la perspicacia que los usuarios finales deseen, cuando la deseen durante el día o después de horas. Los recursos humanos, por ejemplo, pueden querer un informe de todos los accesos de llaves más allá de las horas regulares. O los requisitos de cumplimiento en un casino pueden requerir la recolección y clasificación de información que detalla la actividad ilegal de puerta y alarma durante un período de 90 días. Software de informes puede ser programados para asegurar que la información es reportable, recuperable y rastreable.

Analizando

Los datos de uso de llaves proporcionan una amplia gama de inteligencia de negocios, que se puede analizar para identificar infracciones de políticas y procedimientos y/o mejoras potenciales. Las tendencias que podrían tardar semanas o meses en detectarse manualmente se pueden ver casi al instante cuando las consultas relevantes se programan en el software de informes. Esta inteligencia altamente específica permite identificar las causas de los problemas en lugar de los síntomas, y permite que la administración adopte contramedidas que ayudarán a prevenir incidentes antes de que ocurran.

Los datos de uso de llaves analizados también pueden señalar otros puntos débiles en una operación. En una gestión de flota, por ejemplo, la falta de una política de rotación de vehículos puede estar causando desgaste indebido en un vehículo que se está utilizando mucho más que otros vehículos. El análisis de los datos de uso de llaves puede identificar el problema con información, como el número de veces que el vehículo es retirado en comparación con otros vehículos de la flota.

La información basada en datos proporcionada por el control de acceso de gestión de llaves de última generación es un recurso que seguirá ganando en valor percibido y real, a medida que las organizaciones se den cuenta de que la tecnología puede ayudar a mejorar las operaciones comerciales y lograr una amplia gama de objetivos empresariales. ●

Fotos: Morse Watchmans

Contactos de empresas, p. 9.

FUNDACIÓN MAPFRE Y APTB PRESENTAN EL ESTUDIO «VÍCTIMAS DE INCENDIOS EN ESPAÑA 2015»

143 personas **pierden la vida** en España por un **incendio**

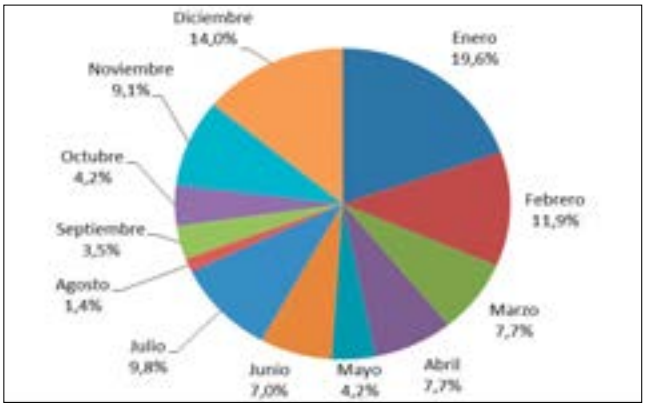
Un 11,7% menos con respecto al año anterior

Entre diciembre de 2016 y enero de 2017 se ha producido en España un 50% más de fallecidos por incendio en el hogar que en el mismo periodo que el año anterior. Durante esos meses, un total de 51 personas han perdido la vida, principalmente como resultado de un descuido con un radiador, brasero o chimenea en el salón de la vivienda, sucedido en más de la mitad de los casos en horario nocturno, entre las 20.00 y las 8.00 horas de la mañana. Por Comunidades Autónomas, la que más víctimas ha registrado en este periodo entre diciembre de 2016 y enero de 2017 ha sido Andalucía, con 10 fallecidos, seguida de Comunidad Valenciana, con 9, y Cataluña y Castilla La Mancha, ambas con 8.

SON los últimos datos de víctimas mortales por incendio que dieron a conocer en Madrid la Fundación MAPFRE y la Asociación Profesional de Técnicos de Bomberos (APTB) en el marco de la presentación del estudio «Víctimas de incendios en España 2015», realizado por ambas entidades con el objetivo de disponer de información precisa sobre las víctimas mortales de incendio y desarrollar acciones preventivas.

Estudio Víctimas de Incendios en España 2015

Según dicho informe, los Cuerpos de Bomberos realizaron en 2015 un total de 136.007 intervenciones por incendios, un 8,1% más que el año anterior. Dicho repunte, tras dos años de caídas, no se ha reflejado en el número de incidentes con víctimas mortales, que en dicho año ascendió a 143 personas, 19 menos que en 2014. Del total de fallecidos, 78 fueron hombres, un 24% menos.



Porcentaje de víctimas mortales por meses

El informe, el único que recoge de forma actualizada y precisa información sobre este tipo de sucesos en España, también destaca la importante reducción en el número de fallecidos entre los menores de 14 años, ya que se ha pasado de 14 víctimas en 2014, que representaban el 8,6% del total de fallecidos, a 6 víctimas mortales en esta franja de edad en 2015, lo que supone el 4,2%.

En el hogar, el número de incendios en 2015 ascendió a cerca de 15.628, lo que representa una media de 43 fuegos diarios, que acabaron con la vida de 110 personas, un 15% menos que el año anterior.

Al analizar el número de fallecidos en viviendas por meses, se produce un patrón claro que se viene repitiendo todos los años. De noviembre a marzo, en los que se origina el mayor número de víctimas mortales, se producen 7 de cada 10 víctimas mortales, ya que a más frío, más necesidad de generar calor, lo que conlleva más incendios y más fallecidos, especialmente en pisos y apartamentos, donde el porcentaje de víctimas es casi el doble que en viviendas unifamiliares.

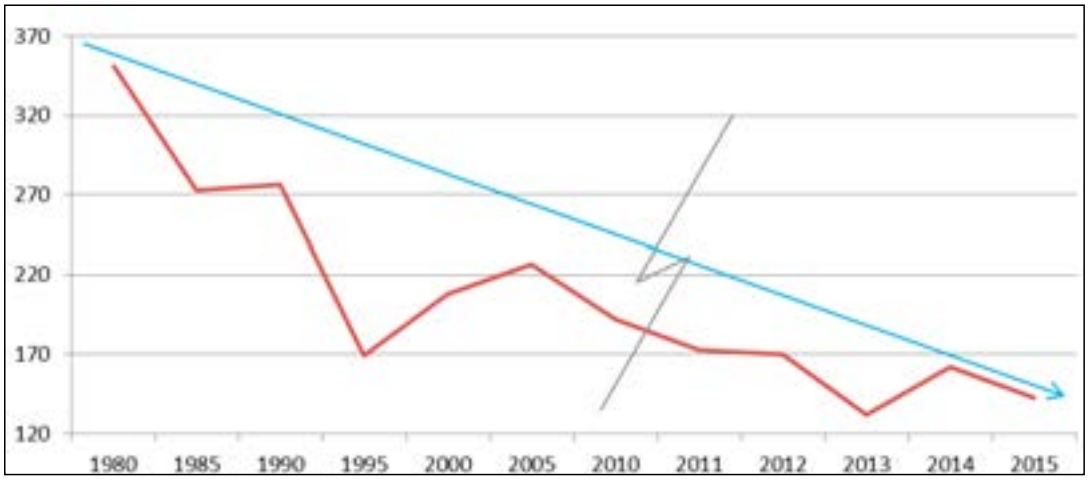
En 2015, además, la fatalidad ha

golpeado con especial crudeza a las residencias de mayores, que computan el 7% del total de fallecidos con 10 víctimas mortales.

Entre las causas más probables de incendio en el hogar con víctimas mortales siguen destacando los descuidos con aparatos productores de calor, como radiadores, chimeneas y braseros; los incidentes de tipo eléctrico; y el cigarrillo, el tercer motivo más frecuente, hábito que vuelve a situarse entre las principales causas.

El salón es la dependencia de la vivienda en la que se origina el mayor número de incendios, seguido por el dormitorio y la cocina, dato esencial para saber dónde se deben colocar los detectores de incendios.

Las personas que viven solas multiplican casi por 9 las posibilidades de morir en un incendio, en comparación con las que viven acompañadas. Las cifras empeoran si además son de edad avanzada: los mayores índices de víctimas mortales en viviendas son aquellos en los que habita un ocupante habitual en solitario y mayor de 75 años.



Evolución del número de víctimas mortales. Fuente: elaboración propia a partir de los datos de Servicios de Bomberos e IML

Víctimas mortales en viviendas por Comunidades Autónomas

Por Comunidades Autónomas, en 2015, las dos con mayor número de habitantes les corresponde también el mayor número de víctimas fallecidas. Cataluña es la primera con 29, seguida de Andalucía, que ha protagonizado un importante descenso con respecto al año anterior, pasando de 32 fallecidos hace dos años a 21 en 2015, y Comunidad Valenciana, con 10 víctimas.

> «Cataluña, Extremadura y Castilla La Mancha, Comunidades con mayores índices de fallecidos por millón de habitantes en viviendas»

Si nos referimos al índice de muertes en viviendas por millón de habitantes, las Comunidades con mayor tasa de siniestralidad en 2015 han sido Cataluña, con un índice de 3,8 víctimas mortales por millón de habitantes, seguida de Extremadura (3,66), Castilla La Mancha (3,40) y País Vasco (3,20).

Por el contrario, las que tuvieron menor tasa de víctimas mortales en viviendas por millón de habitantes en 2015 fueron, Navarra y La Rioja (un año más sin víctimas mortales), Castilla y León (con 0,81), Canarias (con 0,95) y Comunidad de Madrid (con 1,40). Islas Baleares, Murcia y el Principado de Asturias, que en 2014 fueron las Comunidades Autónomas más afectadas de todo el Estado, en cambio este año, han reducido las víctimas a la mitad y se sitúan en los ratios medios.

Medidas de Prevención

Para prevenir un incendio, Fundación MAPFRE recomienda no fumar en la vivienda, ya que los cigarrillos mal apagados son unas de las principales causas de incendio cuando hay víctimas mortales. También aconseja no sobrecargar los enchufes con ladrones, desconectar los aparatos eléctricos después de usarlos, no realizar manipulaciones caseras en las instalaciones eléctricas, y no dejar cerillas y mecheros al alcance de los niños.

A ello se suma una indicación importante, dirigida a que los ciudadanos instalen detectores de humo, cuyo precio oscila entre los 6 y los 20 euros. Según esta entidad, que aboga por extender el uso de este aparato en todo tipo de viviendas, los detectores son el mejor sistema para sobrevivir a un incendio por la noche. ●

Fotos: Mapfre

ASOCIACIÓN DE DIRECTORES DE SEGURIDAD

ADISPO: III Edición de los **Premios al Sector de la Seguridad Privada**

La Asociación de Directores de Seguridad, ADISPO, celebró el pasado día 7 de febrero en Madrid la III Edición de los «Premios al Sector de la Seguridad Privada», un encuentro que congregó a profesionales y representantes del sector.

EL encuentro, presidido por Andrés Sanz Coronado, Coronel Jefe del Servicio de Protección y Seguridad de la Guardia Civil (SEPROSE), y Manuel Yanguas Menéndez, Comisario Jefe de la Brigada Central de Empresas y Personal de la Unidad Central de Seguridad Privada del Cuerpo Nacional de Policía, comenzó la intervención de Vicente Hernández Sánchez, presidente de ADISPO quien destacó que estos galardones «son un agradecimiento a la labor de apoyo y difusión de la cultura de la seguridad».

Acto seguido tuvo lugar la entrega de premios que en esta edición recayeron en:

– Ángel Navas Tiscar, socio de ADISPO y director general de Control System Seasa, por sus más de 35 años de «trayectoria» en el Sector de la Seguridad Privada.

– Germán Sánchez Roses, socio de ADISPO, por su gestión y colaboración con la Asociación en la realización de las Jornadas sobre Terrorismo Yihadista en Granada y a la «dedicación como socio».

– Premio a la Asociación de Diplomados Españoles en Seguridad y Defensa ADESyD, por su ejemplar difusión de la Seguridad y su potenciación de la «colaboración público-privada» en el sector de la Seguridad. María Angustias Caracuel, presidenta de la Asociación y también directora de Spanish Women in International Security (SWIIS, recogió el galardón.

– Premio a la Asociación Internacional de Seguridad y Protección Civil «San Cristóbal de Magallanes» AISPC, por su «apoyo institucional entre asociaciones» del sector de la Seguridad Privada». Recogió el premio su presidente, José Luis Aparisi Guardiola, y su secretario Nacional, Gregorio Saldaña Martín de Eugenio.

– Premio de «Comunicación en Seguridad» al equipo del programa de Protegidos Radio, ahora en Intereconomía. El galardón fue recogido por su director y productor, el socio de ADISPO Pedro Gómez de Quirós, en reconocimiento a su excelente labor de difusión de la cultura de la seguridad en los medios.

PUBLIRREPORTAJE: PSA GROUP

P.S.A

Protección y Seguridad de Activos S.L

El grupo establecido en este año 2017, cuenta con un aval importante, la experiencia en el sector de los cierres de Seguridad, al introducir este medio en España.

Nuestros cierres de una seguridad plena y eficaz, dan la tranquilidad detener los inmuebles protegidos, la calidad es un aval importante y esta es nuestra mejor carta de presentación, la satisfacción de nuestros clientes.

Nuestra mejor herramienta es nuestro producto, un I+D+I constante, mediante la evolución de nuestros cerramientos, nuestra gran estrella es la tecnología y para ello estamos estudiando la implantación de cerradura electrónicas de alta fiabilidad, dando una mayor calidad a nuestros servicios y eficacia.

Nuestro personal con más de 5 años de experiencia en este novísimo producto, es otro de nuestros beneficios nuestro personal formado en áreas de cerramientos y cerrajería

Damos cobertura Nacional para nuestros clientes donde lo necesites, una nutrida flota de vehículos a nivel Nacional dan rapidez e inmediatez en los servicios, para que nuestro cliente no tenga problemas de ocupaciones, además ponemos a disposición de quien lo necesite y tenga miedo a los robos con violencia nuestras puertas de acero, pintadas con colores parecidos a una puerta normal de cualquier casa, y este servicio lo proporcionamos por si Vd. se marcha de vacaciones estivales o navideñas por 15 días, un mes o el tiempo que Vd. lo solicite, mantenga su casa protegida de los amigos de lo ajeno

PSA Group somos fabricantes y es por ello que nos diferenciamos de la competencia, con maquinaria preparada para dar un volumen importante de fabricación máquinas de cortes de laser o de agua, máquinas de última generación de corte preciso.

La tecnología al lado de PSA Group pues seguimos investigando y mejorando nuestros productos que además de Puertas fabricamos paneles para cerrar balconeras y Ventanas, también utilizamos para ello, la fabricación de rejas a medida

Nuestros clientes Nacionales confían en PSA Group, damos un servicio de calidad, puntual y de seguridad, a precios muy reducidos, todo para su tranquilidad y bienestar, confíe Vd. también en nuestro grupo y podrá comparar.

PSA Group realiza trabajos de rehabilitaciones de viviendas, pequeñas obras y la limpieza de esto inmuebles

Cerramientos DASER, fabrica, instala y realiza el mantenimiento de nuestros cerramientos

Grupo empresarial Nacional tecnológico e industrial.

Seguridad pasiva

Puertas reforzadas antiokupa

Puerta con cerradura, hoja y marco reforzado con gato mecánico de alta presión y llave no reproducible por el público general.

Paneles Metálicos

Paneles para cerrar un hueco desde dentro, con un marco reforzado y dobles gatos de alta presión ieviolables, posibilidad de asociar varios paneles para las aperturas de gran tamaño y zapatas de goma para una colocación sin riesgo.

Pantallas de Acero

Pantallas para cerrar un hueco hacia el exterior, con un sistema de resistencia a la deformación gracias a ángulos reforzados por el plegado de las aristas, varias medidas posibles son para una mejor integración en el bastidor exterior.

SOLUCIONES DE SEGURIDAD
EDIFICIOS VACÍOS

Las empresas Grupo DASER, expertas en gestionar servicios integrales y seguridad electrónica a propiedades desocupadas, han unido su experiencia para ofrecer en España una solución conjunta de seguridad y protección para edificios vacios.

Hace 10 años se contabilizaron 3,1 millones de viviendas vacías, el 15% de las censadas. Ahora, la cifra será, sin duda, muy superior. Partiendo de esos 1,6 millones que siguen sin comprador y que, a efectos estadísticos, se considerarán vacías, al no estar ya en construcción, algunas fuentes consultadas se atreven incluso a señalar que en España podría haber ya entre cinco y seis millones de viviendas vacías, superando el 20% del parque inmobiliario residencial

CIERRES DASER

C/ Montsia, 79
08211 Castellar del Valles
T. +34 693 603 444
acedenilla@psagroup.es

daser
seguridad

La UE elige a Genaker entre 2.000 empresas para un proyecto sobre innovación

GENAKER, empresa española con sede en la ciudad condal y dedicada a la venta de servicios de comunicaciones móviles profesionales, acaba de recibir un fondo de la Unión Europea de un millón tres cientos mil euros del programa Horizon 2020. Genaker recibió la puntuación más alta en innovación entre las más de 2.000 empresas participantes.

El fondo le permitirá poder jugar en la «Liga de Campeones» de este sector. Con este apoyo, Genaker va a poder llevar al mercado más rápidamente su siguiente generación del servicio Push-To-Talk para comunicaciones críticas basada en que móviles especialmente equipados podrán funcionar en redes de 4G. Así, la compañía española podrá suministrar comunicaciones móviles integradas de voz, datos y vídeo que permitirán que equipos de seguridad y emergencias en Europa puedan funcionar de modo seguro en casi cualquier red y bajo situaciones de cobertura escasa. Fundada en 2004 por Miquel Teixidor (CEO), ex director general del centro de I+D de Nokia de Barcelona que se cerró en 2003, y otros siete antiguos directivos e ingenieros de la empresa finlandesa, Genaker, empresa privada e independiente, nació como una start-up dispuesta a seguir haciendo lo que hacían en Nokia: desarrollar soluciones móviles de vanguardia y venderlas a clientes del sector profesional y de seguridad en España y en el resto del mundo. En España cuenta con clientes de prestigio como Iberia, Sabic (petroquímica), varias policías locales y ayuntamientos como el de Madrid, así como Telefónica y Vodafone.

HiWatch y Globomatik: nuevo acuerdo de distribución

HiWatch, fabricante experto en soluciones y productos de videovigilancia, ha alcanzado un acuerdo de distribución con Globomatik, mayorista de nuevas tecnologías y distribuidor de sistemas de CCTV con sede en Almería y con cobertura nacional a través de sus delegaciones en Málaga, Madrid y Barcelona.

Red de Partners

Con este acuerdo Globomatik se une a la red de partners de HiWatch y comercializará una amplia gama de productos de CCTV, consiguiendo así completar su catálogo de videovigilancia e incrementar las oportunidades de negocio en su canal, ofreciendo productos que cumplirán con las expectativas de sus clientes, a nivel de prestación, calidad y precio.

En palabras de Pedro Repeto de Globomatik «Estamos orgullosos de añadir HiWatch a nuestra gama de productos. Este acuerdo reforzará nuestra presencia en el área de la seguridad con el objetivo de acercar a nuestros clientes una nueva línea de productos adaptados a las diferentes necesidades del mundo actual».

Alex You, responsable de HiWatch en España, afirma que «contar con Globomatik supone un gran impulso para nuestro crecimiento en el mercado nacional. Como fabricante líder en nuestro sector, es importante contar con los mejores aliados para ofrecer a los profesionales soluciones tecnológicas avanzadas económicamente asequibles».

Detnov, presente en Intersec 2017

FIEL a su proyección internacional, con el objetivo de mostrar sus últimos avances tecnológicos en el marco de la detección de incendios, Detnov estuvo presente en Intersec, feria referente en el sector de la seguridad y contra incendios en Oriente Medio que se celebró del 22 al 24 de enero en Dubai (Emiratos Árabes Unidos).

Detnov presentó en su stand todas las novedades y soluciones que la compañía ha lanzado al mercado durante el último año, así como los avances tecnológicos que presentarán en los próximos meses.

«Hemos aprovechado para mostrar nuevas funcionalidades de las gamas actuales de los sistemas analógico, convencional y detección de monóxido. Los productos que más han sorprendido a los visitantes han sido: la innovadora generación de repetidores gráficos RTD-150 para el sistema analógico; la nueva tarjeta de comunicación TED-151WS para la gestión y control bidireccional de las centrales convencionales y analógicas; el nuevo detector con certificación LPCB; y la central analógica CAD-250 con pantalla táctil con gestión gráfica integrada en la propia central», explica Eugeni Mulà, director comercial de Detnov.

El equipo de Detnov quiere agradecer «el interés mostrado a todos los visitantes, clientes, amigos y colaboradores en su visita a nuestro stand de Intersec. Es la cuarta edición en la que estamos presentes en dicha feria y nos enorgullece especialmente la acogida e interés que han tenido nuestros productos, en esta ocasión, nos han visitado clientes de más de 25 países diferentes», añade.

AES: Elecciones a la Junta Directiva

En la Junta Directiva de la Asociación Española de Empresas de Seguridad (AES) celebrada el pasado día 17 de enero, tuvieron lugar las elecciones a presidente y vicepresidente de la Asociación. Antonio Pérez Turró fue reelegido presidente, quien agradeció la confianza y trabajo del resto de los miembros de la Junta Directiva durante estos tres últimos años, y se comprometió a continuar con el trabajo de AES para los tres próximos. Asimismo, Antonio Escamilla Recio fue reelegido vicepresidente, y continuará apoyando al presidente en su labor.


Antonio Pérez, presidente de AES


Antonio Escamilla, vicepresidente de AES

Eulen Seguridad, en la Feria de Valencia

EULEN Seguridad, empresa decana en el sector de seguridad perteneciente al Grupo EULEN, empresa destacada en nuestro país en la prestación de servicios generales a empresas, ha resultado adjudicataria del Servicio de Vigilancia de las instalaciones de la Feria de Muestrario Internacional de Valencia.

El contrato, de gran importancia en la Comunidad Valenciana, tiene un importe total de 1.101.000 euros, con una duración de tres años, con posibilidad de prórroga de dos años más.

Para el desarrollo del servicio, Eulen Seguridad contará con 13 empleados fijos, una cifra que podrá aumentar según las necesidades de los eventos que se realicen.

Hanwha Techwin: Wisenet Live Tour 2017

HANWHA Techwin ha presentado Wisenet Live Tour 2017, la forma más sencilla y rápida de conocer las nuevas soluciones de seguridad de Hanwha Techwin.

En este sentido, Wisenet Live Tour 2017, que tendrá lugar en las principales ciudades de España y Portugal, es un formato innovador que permite conocer las principales prestaciones de las gamas Samsung Wisenet Q, Wisenet P y, la recién presentada, Wisenet X.

Presentaciones dinámicas

En presentaciones dinámicas de 30 minutos y en grupos reducidos de máximo 5 personas, instaladores, integradores e ingenieros podrán conocer de primera mano los secretos de cámaras, NVRs y el nuevo VMS (SSM – Smart Security Manager) de Hanwha Techwin. Cada día se organizarán hasta 8 grupos para que todos aquellos interesados puedan asistir.

«Hemos querido crear un formato nuevo, más personalizado, para mostrar cómo nuestros equipos pueden ayudar a mejorar las necesidades de seguridad que demandan los clientes», afirma José Luis Romero, General Manager de Hanwha Techwin Spain & Portugal.

El primer evento Wisenet Live Tour 2017 tuvo lugar en Madrid, en las oficinas de Hanwha Techwin en España, el pasado 2 de marzo.

Por otro lado, una de las ventajas del formato es que se puede elegir la franja de horaria que mejor se adapte a cada uno.Después de Madrid, Wisenet Live Tour recorrerá Lisboa, Valencia, Zaragoza y Sevilla, y después del verano, volverá a Madrid para continuar en Barcelona, Oporto, Valencia y Sevilla.

Estudio Hochiki: uno de cada 5 propietarios de edificios desconoce los requisitos legales de seguridad

Un nuevo estudio de Hochiki Europe indica mejoras en el conocimiento de los requisitos de mantenimiento de los sistemas de seguridad por parte de los propietarios y gerentes de edificios.

Un estudio de 2016 sobre los instaladores europeos, llevado a cabo por el fabricante destacado de soluciones de seguridad, ha revelado que el número de propietarios y gerentes de edificios que desconocen los requisitos legales relacionados con el mantenimiento de los sistemas de seguridad se ha reducido a la mitad. El estudio de 2015 de la empresa mostraba que dos de cada cinco (el 46%) no tenía conocimiento de estos requisitos, pero esa cifra ha descendido a uno de cada cinco (el 22%) en los últimos doce meses.

De la misma forma, el número de instaladores que se encuentra con edificios en los que los clientes han cambiado el uso de los espacios, pero no han ajustado los sistemas de seguridad de la forma correspondiente, ha bajado ligeramente, ya que se ha reducido de algo más de la mitad (55%) a exactamente la mitad (50%).

Los cuatro problemas principales relacionados con el mantenimiento de los sistemas de protección contra incendios que han detectado los instaladores en 2016 son los siguientes:

– Cambio del uso del edificio o sala sin modificar correctamente el sistema de protección contra incendios (50%).

– El instalador original no ha instalado el mejor sistema para el entorno (40%).

– Es necesario limpiar los detectores (33%).

– Es necesario sustituir los detectores (27%).

Los cuatro problemas principales relacionados con el mantenimiento de los sistemas de luces de emergencia son los siguientes:

– Lámparas rotas/defectuosas (44%).

– Señalización inadecuada de las luces de emergencia (39%).

– Baterías sin carga en las unidades de luces de emergencia (35%).

Niveles de lux inadecuados (25%).

Hyundai aumenta a tres años la garantía de sus sistemas de CCTV y alarma

HYUNDAI aumenta a tres años la garantía de sus sistemas de CCTV y alarma.

Hyundai Corporation, en acuerdo con su distribuidor exclusivo By Demes Group, amplía de dos a tres años el período de garantía de todos sus sistemas de seguridad como muestra de la confianza que tiene en la fiabilidad de sus equipos.

Aportar valor

Son muchos los instaladores que confían en la marca Hyundai por su prestigio y su más avanzada tecnología en cualquiera de los mercados en los que opera, los cuales aportan valor a las instalaciones y la satisfacción de las necesidades de seguridad más exigentes. Los profesionales también son conscientes de la longevidad y fiabilidad de sus equipos de seguridad, valores que se posibilitan gracias a los más rigurosos tests e inspecciones de calidad previos a su producción y comercialización.

Para seguir demostrando la confianza que tiene en sus productos y el alto compromiso con sus clientes, Hyundai ha decidido brindar a los instaladores el valor añadido de tres años de garantía para todo su catálogo de sistemas de CCTV y de alarma.

Así, los clientes finales podrán disfrutar del máximo confort con sus sistemas de seguridad. Este factor novedoso llega como estrategia de constituir a Hyundai como una marca aún más decisiva para instaladores y clientes finales.

Securitas se integra en la CEOE

Securitas Seguridad España ha pasado a formar parte de la Confederación Española de Organizaciones Empresariales, tras la firma de un acuerdo de vinculación que integra a la compañía de seguridad privada, multinacional de origen sueco, en la patronal española. De este modo, Securitas se integra en la CEOE, lo que permitirá a la compañía colaborar y participar de forma activa en sus órganos consultivos, tanto en consejos, comisiones y grupos de trabajo, así como en otras iniciativas. Además, el Consejero Delegado de Securitas formará parte del Consejo Asesor del Presidente de la CEOE.

«Nuestra integración en la CEOE es un paso lógico y natural para una compañía de la trayectoria y peso que tiene Securitas en el sector de la seguridad privada en España», asegura Zacarías Erimias.

El acuerdo de adhesión llega en un momento clave para Securitas, que en los últimos cuatro años ha llevado a cabo un profundo proceso de transformación de su modelo de negocio, apostando por impulsar sus soluciones de seguridad con un acentuado componente tecnológico, en lugar de únicamente ofrecer servicios de vigilancia presencial. Asimismo, la compañía ha llevado a cabo una ambiciosa política de selección de nuevo talento y contratación de nuevos perfiles, en particular ingenieros y técnicos, capaces de contribuir al desarrollo de esta nueva estrategia.

«Somos conscientes de que una seguridad privada honesta, sólida y responsable con la sociedad que le rodea va a redundar en beneficio de todos, empezando por las empresas, que son nuestros principales clientes. Vivimos en un mundo cambiante en el que la seguridad se está convirtiendo en algo muy necesario a todos los niveles de la sociedad», Zacarías Erimias.

ISMS Forum: Cybersecurity & Privacy trends 2017

Nadie pone hoy en duda que la ciberseguridad es uno de los pilares básicos de la sociedad del siglo XXI. La configuración actual de la sociedad se ha confeccionado gracias a la creación de servicios que están soportados ya sea directa o indirectamente en Tecnologías de la Información, a su vez en gran medida gestionadas por empresas privadas. Nos encontramos en un momento bastante disruptivo, pero a la vez bonito, en el que estamos tocando el punto de inflexión que realmente nos ayude a darnos cuenta de que el cambio de era ha tenido finalmente lugar.

La seguridad está disfrutando de un momento de singularidad al calor del auge de la eclosión de la TI. Esta situación modifica por completo el escenario actual, ya que afecta tanto a las amenazas como a los riesgos. La automatización y la digitalización de procesos supone para la Industria toda una nueva revolución de la que nadie puede quedar al margen, por lo que la ciberseguridad se constituye como eje principal y garantía de la transformación digital en empresas y en la sociedad en general. Un proceso de cambio sin precedentes en las últimas décadas, que conlleva una fuerte demanda de profesionales de la Ciberseguridad y, por ende, la elevación de la figura del Chief Information Security Officer en las estructuras organizativas.

La situación actual ha producido un aumento del riesgo, tanto por su dependencia con las TI como el mayor peso que las TI han tomado y van a tomar. La eclosión del Big Data corporativo y los servicios a medida y el denominado Internet de las Cosas, darán paso a una revolución tecnológica que, si no conocemos el alcance y las implicaciones que suponen en términos de seguridad y privacidad, nos puede llevar en poco tiempo a generar una auténtica jungla digital donde impere el caos.

La seguridad desde el diseño resultará imprescindible para garantizar el desarollo del machine learning o aprendizaje automático aplicado en coches, drones, robots..., que operarán de manera autónoma y tomarán decisiones prediciendo resultados a partir de ciertos patrones prestablecidos.

Por su parte, los problemas para la detección y gestión del crimen y el fraude cibernéticos, unidos al lento desarrollo normativo y a la falta de concienciación, propiciarán la aparición de nuevas ciberamenazas y el incremento de las ya existentes, como el Crime-as-a-Service, ransomware, ciberespionaje o ciberterrorismo, entre otras.

Con el objetivo de poner de manifiesto las principales inquietudes del Sector, ISMS Forum ha elaborado su primer Cybersecurity & Privacy trends 2017. A continuación, se muestran gráficamente las principales claves de 2017.

Tyco recibe la Certificación Cepreven de PCI

TYCO Integrated Fire & Security, empresa mundial en soluciones de seguridad y protección contra incendios, ha recibido la calificación Cepreven como instalador de Sistemas de Extinción automática por gas: Inertes y Químicos. Esta calificación es un sistema complementario de las exigencias oficiales que reconoce la calidad y eficacia de las instalaciones de seguridad contra incendio de las empresas.

Cepreven es una Asociación sin ánimo de lucro, creada en 1975, que tiene por finalidad fomentar, en materia de Prevención, el intercambio de informaciones y experiencias con organismos, entidades y profesionales, así como contribuir al perfeccionamiento, instrucción y capacitación de todos los actores involucrados en la Prevención y Protección de Riesgos mediante la promoción de actividades de Formación, Comisiones de Trabajo y edición de publicaciones especializadas.

Tyco dispone de diversas soluciones de extinción de fuego por gas que satisfacen las diferentes necesidades de protección en cualquier tipo de entorno: La serie INERGEN permite extinguir el fuego sin dañar el medioambiente, no es tóxico, y está hecho a base de gas natura, y la serie SAPPHIRE está basada en los agentes químicos líquidos limpios de extinción de fuego 3M™ Novec™ 1230 Fire Protection Fluid.

La venta de drones se dispara en todo el mundo

LA venta de aviones no tripulados para uso personal y comercial crecerá rápidamente este año al llegar a casi tres millones de unidades en todo el mundo, un 39 por ciento más que en 2016 según el pronóstico de la consultora Gartner. El estudio prevé que los ingresos del mercado mundial aumenten un 34 por ciento para llegar a más de 6.000 millones de dólares (5.600 millones de euros) en 2017 y a más de 11.200 millones (10.500 millones de euros) en 2020.

El análisis de Gartner recoge que el mercado de los drones en general experimentará un crecimiento sustancial, pero la dinámica de los submercados personales y comerciales será muy diferente. Los drones personales seguirán aumentando en popularidad como una extensión asequible de los smartphones de los consumidores para tomar fotografías y selfies y para otras opciones de entretenimiento, señala el estudio.

La consultora recuerda que estos dispositivos «pueden volar a corta distancia y tiempo, por lo general no más de 5.000 metros y durante una hora, con una altura de vuelo limitada a menos de 500 metros. Pesan menos de 2 kilos y cuestan menos de 5.000 dólares».

Nace el Centro de Seguridad en Internet para Menores

El secretario de Estado de Seguridad, José Antonio Nieto, asistió a la presentación del Centro de Seguridad en Internet para Menores que ha realizado el ministro de Energía, Turismo y Agenda Digital, Álvaro Nadal, con motivo del Día Internacional de Internet Seguro.

A continuación, Nieto participó en una mesa redonda en la que se evaluó la acción coordinada del Gobierno, en el marco de la Estrategia de Seguridad Nacional, para conseguir un ciberespacio más seguro. Una acción coordinada donde, según Nieto, «son fundamentales la prevención y la educación». Fruto de esta colaboración, se ha referido al Plan Director para la mejora de la seguridad en los centros educativos y sus entornos, a través del que, en 2016, las FCSE impartieron entre los más pequeños, 10.961 charlas sobre acoso escolar, 16.296 sobre nuevas tecnologías y 3.933 sobre violencia contra la mujer.

Durante su intervención, el secretario de Estado de Seguridad puso de relieve la colaboración institucional, del ámbito educativo y de la industria del sector que, a través de diferentes convenios y actuaciones han puesto en marcha diversas iniciativas divulgativas para mejorar la seguridad de los menores en internet. Entre ellas, ha destacado las jornadas, «Embajadores de un internet responsable», organizadas por la Policía Nacional con la colaboración de Google, o el proyecto «Ciberexpertos», desarrollado con la colaboración de Telefónica y la Fundación Cibervoluntarios.

Por otra parte, se ha referido a las campañas desarrolladas por la Guardia Civil como «Peque GDT Consejos Especial Verano», del Grupo de Delitos Telemáticos o el acuerdo con Walt Disney para hacer atractivos mensajes que mejoren la seguridad de los menores en internet. Asimismo, ha puesto de relieve el carácter preventivo tanto de Policía como de Guardia Civil debido «al enorme potencial de sus perfiles en las redes sociales que les permite investigar y perseguir delitos como el ciberbulling, el grooming o sexting o para desterrar crímenes tan aberrantes como la explotación sexual online».

Finalmente, el secretario de Estado de Seguridad se refirió a la futura puesta en marcha de una Mesa para un internet seguro, -anunciada por el ministro del Interior el pasado mes de diciembre- a semejanza del Foro Unión Europea-Internet, donde las instituciones y los principales actores de la industria de internet trabajarán conjuntamente en el desarrollo de políticas que redunden en beneficio de la seguridad ciudadana.

La Generalitat refuerza las medidas de protección ante ciberataques

EL Gobierno catalán cuenta con un nuevo colaborador de prestigio internacional, la multinacional estadounidense Oracle, para garantizar una sociedad digital catalana segura para todos (administraciones, ciudadanía y empresas). Así se desprende del convenio firmado entre el Centro de Seguridad de la Información de Cataluña (CESICAT), organismo encargado por el Gobierno catalán de la protección, prevención y gobernanza de la ciberseguridad de la Administración de la Generalidad de Cataluña, y esta multinacional tecnológica norteamericana, especializada en gestión de base de datos y proveedora referente de soluciones empresariales, de Big Data y servicios en la nube.

La firma del convenio se llevó a cabo en San Francisco, en el marco de la RSA Conference 2017, y por parte de la Generalitat firmaron el secretario de Telecomunicaciones, Ciberseguridad y Sociedad Digital y presidente del Centro de Seguridad de la información de Cataluña (CESICAT), Jordi Puigneró. A la firma también estuvo presente el director general del CESICAT, Xavier Gatius.

El convenio firmado fija las bases de una colaboración entre ambas entidades que refuerza las capacidades del CESICAT como CSIRT (equipo de respuesta a incidentes) gubernamental para la detección y respuesta ante los incidentes de ciberseguridad que se produzcan en Cataluña. El convenio permitirá a la vez contribuir a la consecución de los objetivos fundacionales de este organismo, que pasan por el establecimiento y seguimiento de los programas y planes de actuación necesarios para garantizar una sociedad digital segura para Cataluña.

Así, el convenio establece la compartición de información sobre vulnerabilidades y otros ámbitos de colaboración para prevenir y dar respuesta a ciberataques, además de sesiones y workshops periódicos para revisar y hacer seguimiento de proyectos en curso, compartir información sobre tendencias y novedades en el ámbito de las soluciones de seguridad TIC y analizar o demostrar las capacidades técnicas de las soluciones empleadas.Con este acuerdo, ambas partes se comprometen a colaborar activamente en el establecimiento y consecución de las líneas establecidas en el convenio, todos ellos en consonancia con las líneas de trabajo sobre seguridad tecnológica tanto por parte de la multinacional Oracle como del CESICAT.

Tecnifuego-Aespi y Asepal firman un acuerdo de colaboración

La Asociación Española de Sociedades de Protección contra Incendios, Tecnifuego-Aespi, y la Asociación de Empresas de Equipos de Protección Individual, Asepal, han firmado un acuerdo para reforzar la colaboración en el ámbito de la prevención y la seguridad.

Adrián Gómez, presidente de Tecnifuego-Aespi, y Luis del Corral, presidente de Asepal, rubricaron el acuerdo con el objetivo de generar sinergias entre ambas organizaciones, las cuales desempeñan un papel relevante en el ámbito técnico, científico y socioeconómico de sus respectivos sectores de actividad.

Durante la firma, se destacó el interés común por reforzar la colaboración y el intercambio de información relacionada con la normativa y reglamentación nacional aplicable a la seguridad contra incendios (SCI) y seguridad laboral; la organización de actividades conjuntas de formación y difusión tales como congresos, jornadas, conferencias, etc.

Adrián Gómez manifestó que «en un sector crítico como el de seguridad contra incendios (SCI), los riesgos laborales son una preocupación compartida, y por ello la adecuada información y formación en relación a equipos de protección individual (EPI) es fundamental. Igualmente para todos los trabajadores y usuarios el estar debidamente protegidos y saber utilizar los equipos básicos de SCI es un reto que debemos alcanzar».

Luis del Corral destacó «la importancia de la adecuada instalación de medidas de SCI y el momento actual del sector de los EPI con el nuevo Reglamento que entrará en vigor el próximo año. La colaboración con Tecnifuego-Aespi refuerza el compromiso de Asepal con la seguridad y en especial con un sector como el de la protección contra incendios, donde los EPI tiene un papel muy destacado».

Un pionero sistema de control de aforo evitará tragedias como la del Madrid Arena

LOS excesos de aforo que pueden derivar en tragedias como la del Madrid Arena tienen los días contados. La Asociación Empresarial Innovadora Control de Aforo ha presentado en Madrid un sistema revolucionario y pionero a nivel internacional plenamente desarrollado en España que permite conocer con precisión legal el número de personas que se encuentran en el interior de un recinto.

El VIABOX ML1 es el primer sistema en contar con la homologación oficial del Centro Español de Metrología, que ha sometido al nuevo dispositivo a los controles exigidos por la UE. De esta forma, ya será posible controlar que la asistencia a establecimientos de aforo limitado, como espectáculos, actividades recreativas, salas de fiesta e, incluso, las celebraciones de Fin de Año en la Puerta del Sol, cumple las disposiciones legales.

«Contar es vida», recalcó durante la presentación oficial Félix Navarro, presidente de Control de Aforo, quien señaló que este avance permitirá mejorar los protocolos de evacuación de las instalaciones y, en consecuencia, la seguridad de quienes se encuentran en ellas. «Es una tecnología que anteriormente no existía», añadió Navarro, quien subrayó que de este modo «vamos a pasar de contar a mano a contar a máquina», con la ventaja añadida de que el sistema puede almacenar la información durante dos años y cuenta con validez reconocida en procedimientos judiciales. El nuevo sistema será comercializado a través de distribuidores homologados y que están inscritos en el Registro de Control Metrológico: Age2, Comunicalia Grupo, Prosegur y Securitas.

Tecosa instalará 36 equipos para inspección de líquidos en aeropuertos de AENA

Tecosa, compañía del Grupo Siemens, especializada en la integración de sistemas de seguridad, ha sido la adjudicataria por parte de AENA del contrato para el suministro y puesta en servicio de 36 equipos para inspección de líquidos. Estos sistemas se instalarán en una veintena de aeropuertos de la red de AENA, distribuidos por todo el país. El plazo de ejecución será de 24 meses. El equipo EMA-3, de CEIA, es un analizador de líquidos que permite inspeccionar botellas, y envases comerciales, capaz de detectar la presencia de líquidos no permitidos a bordo. Al colocar la botella en el lugar destinado para la inspección, este sistema detecta automáticamente su presencia y comienza el proceso de análisis. Esta tecnología ofrece un diagnóstico claro e inmediato y muestra el resultado, bien con un «OK» si se trata de un contenido apto, o bien con un «Producto no permitido», en caso de que no lo sea. Además, es capaz de realizar un análisis automático de recipientes sellados. El CEIA EMA-3 es un equipo de última generación, que cuenta con un diseño compacto y una eficacia operativa probada en aplicaciones reales. Además, está certificado por CEAC de acuerdo a la normativa europea para inspección de tipo A y tipo B de LAGs (Líquidos, Aerosoles y Geles). AENA ha adjudicado a Siemens-Tecosa equipos de alta seguridad y alta calidad. La compañía tiene como objetivo prestar un buen servicio como en todos los proyectos acometidos con anterioridad.

La Cyber Threat Alliance se convierte en entidad no lucrativa

LA Cyber Threat Alliance (CTA) ha anunciado el nombramiento de Michael Daniel como presidente de la organización y su transformación en entidad no lucrativa. Asimismo, los miembros fundadores Fortinet®, Intel Security, Palo Alto Networks, y Symantec han confirmado la incorporación de Check Point® Software Technologies Ltd. y Cisco como nuevos miembros fundadores de la Alianza. Todos ellos han contribuido al desarrollo de una nueva plataforma para compartir la inteligencia de amenazas de forma automatizada, a través de la cual pueden intercambiar datos de amenazas, impulsando la misión de la CTA para una mejor coordinación de esfuerzos frente al cibercrimen. El Consejo de Dirección de la CTA está compuesto por los CEOs y responsables senior de los seis mayores proveedores de ciberseguridad: Check Point, Cisco, Fortinet, Intel Security, Palo Alto Networks y Symantec.

El propósito corporativo de la CTA como organización sin ánimo de lucro es compartir entre sus miembros información sobre amenazas con el objetivo de mejorar las defensas frente a los ciberciminales para proteger a sus clientes, avanzar en el desarrollo de soluciones de ciberseguridad para infraestructuras de TI críticas e incrementar la seguridad, disponibilidad, integridad y eficiencia de los sistemas de información.

Además la CTA ha incorporado nuevos miembros afiliados, incluyendo IntSights, Rapid7 y RSA, que se unen a organizaciones que ya conformaban este grupo, Eleven Paths y ReversingLabs.

Expodrónica 2017, 21 y 22 de septiembre

ZARAGOZA acogerá de nuevo, el 21 y 22 de septiembre Expodrónica, la feria profesional de drones civiles más importante de Europa. Esta edición pretende acercar al público de manera diferente a los drones, haciendo de esta feria una experiencia para disfrutar con todos los sentidos.

Expodrónica, clasificada ya como la feria profesional y comercial más importante y completa de Europa y una de la más importantes del mundo, es la única en Europa con la posibilidad de ver drones acuáticos y subacuáticos, gracias a las instalaciones de la Feria de Zaragoza. El año pasado, casi 7000 profesionales asistieron a la segunda edición, superando los casi 6000 asistentes de la primera edición.

El sector de los drones sigue creciendo en España cada vez más. En 2016, en España, el número de inscripciones de operadores aumentó en un 156%.

Lanzamiento del Sello Cepreven de producto

En el marco del Plan Estratégico y para continuar con uno de los principales objetivos de la asociación, que es garantizar la calidad y eficacia de las instalaciones, se produce el lanzamiento del «Sello CEPREVEN de Producto», consistente en una marca voluntaria que se confiere a aquellos productos que la solicitan y que hayan acreditado, mediante inspección periódica, el cumplimiento de las normas o protocolos de fabricación aplicados, así como la superación de los correspondientes controles y pruebas para evaluar la calidad y prestaciones de los mismos.

Hasta el momento, se puede solicitar el «Sello CEPREVEN de Producto» en las siguientes gamas: Tuberías, Hidrantes y Depósitos de PCI, y ya se está trabajando en Extintores y Grupos de Bombeos contra Incendios, que verán la luz próximamente.

CEPREVEN desarrollará nuevos procedimientos a petición de los fabricantes de los diferentes sistemas de protección contra incendios.

Este sistema aporta una herramienta más a aseguradores y usuarios finales para identificar, dentro de una misma gama de productos, aquellos cuyas prestaciones son contrastadas y evaluadas por una entidad externa, y supone para sus fabricantes la posibilidad de presentarlos al mercado con un sello de calidad y fiabilidad.

Al mismo tiempo, aparece la página web www.sellocepreven.com, en la que se pueden consultar, entre otros aspectos, todos los procedimientos que regulan su concesión, cómo se estructuran los mismos y su duración.

StrongPoint ASA adquiere PyD Seguridad

StrongPoint ASA, grupo noruego especialista en soluciones para el sector retail, da un paso adelante en su estrategia de implantarse en los mercados español y portugués, con un ambicioso plan de implantación, siendo el primer paso de dicho plan, la adquisición de PyD Seguridad.

StrongPoint y PyD Seguridad han mantenido una relación activa a lo largo de más de 10 años. PyD Seguridad ha sido el principal distribuidor de la solución de gestión de efectivo CashGuard en España. La empresa cambiará su denominación por la de StrongPoint S.L.U. y ofrecerá a sus clientes el porfolio completo de productos de StrongPoint.

PyD Seguridad ha distribuido e instalado cientos de sistemas CashGuard en España, Portugal y Andorra. La empresa ha jugado un papel crucial en la exitosa implantación de más de 700 sistemas CashGuard en la cadena asturiana de supermercados Alimerka.

El fundador y principal propietario de PyD Seguridad, Javier Aguilera, continuará como director general de la compañía, y pasará a formar parte del equipo EMEA de StrongPoint.

«StrongPoint ASA ya es líder en el mercado Noruego, Sueco y Países Bálticos. Esta operación fortalece nuestra presencia internacional y nos da acceso directo a uno de los mercados más interesantes de Europa», dice Jørgen Waaler, CEO de Strong Point ASA. «El objetivo general de esta adquisición es invertir y construir StrongPoint España basado en el mismo modelo de Noruega, Suecia y Países Bálticos.»

U-Tad lanza el programa «Experto en Pilotaje de Drones Profesionales»

U-tad, Centro Universitario de Tecnología y Arte Digital, ha lanzado el programa «Experto en Pilotaje de Drones Profesionales» más completo del mercado. Actualmente se emplean drones para multitud de aplicaciones comerciales como operaciones de rescate y vigilancia, control de incendios forestales, monitorización de tráfico, realizar fotografías aéreas, fumigación y fertilización de cultivos, vídeos deportivos, etc., que se traduce en nuevas oportunidades de empleo y por tanto de profesionales formados que den continuidad a esta nueva tecnología.

La Comisión Europea estima que en diez años los drones representarán alrededor de un 10% del mercado de la aviación en Europa, revolución que conlleva una explosión en el crecimiento económico y en las oportunidades de trabajo en España y en el mundo.

Como Centro Universitario pionero y especializado en la formación de profesionales en los sectores más vanguardistas de la sociedad, U-tad lanza el programa «Experto en Pilotaje de Drones Profesionales» impartido conjuntamente con AEROFAN (Centro de Formación Aeronáutico). Dada la cercanía de U-tad con la industria, el personal docente lo componen pilotos e ingenieros en activo de importantes empresas nacionales, así como del Centro de Formación Aeronáutica AEROFAN. Los alumnos recibirán una completa formación teórica presencial en las instalaciones de U-tad (cuatro meses) y operativa en AEROFAN (dos meses) para que una vez finalizada la formación, posean los conocimientos teóricos y prácticos necesarios para desenvolverse profesionalmente en el ecosistema de empresas que está surgiendo alrededor de los RPAS.

Una importante novedad de este programa es que se trata del único en España que forma a los alumnos en el pilotaje de todas las plataformas de aeronaves disponibles en el mercado; ala fija (aviones), ala rotativa (helicópteros) y multicópteros. Tras la finalización del curso, el alumno dispondrá de un título oficial y una licencia para pilotar todo tipo de drones en España. Los únicos requisitos de acceso es ser mayor de 18 años y tener conocimientos mínimos de inglés. También es necesario superar un certificado médico de «Clase dos», pero que puede realizarse durante el curso o a su finalización.

Contactos de empresas, p. 9.

Bunker: gran aceptación de las columnas pre-instaladas easyPack de Prodextec

Las columnas pre-instaladas de la marca easyPack representan gran cantidad de ventajas de cara al instalador de seguridad perimetral. Por un lado, todos los equipos se suministran completamente instalados, cableados y probados, con lo cual, se reducen significativamente los tiempos en la instalación, ya que únicamente necesitará fijar la columna en su posición definitiva, alimentar y configurar las barreras IR en función de las condiciones de la zona a proteger. También aportan ventajas desde el punto de vista logístico, puesto que se reduce el número de bultos que hay que transportar y almacenar antes y en la propia instalación, reduciendo costes y evitando pérdidas de accesorios, pequeños elementos, etc.

Dentro del catálogo de Prodextec hay una amplia gama de opciones en cuanto a la altura de la columna, ubicación a suelo o en la pared, de una o dos caras y, por supuesto, nuestros clientes pueden elegir el modelo de barrera que requieren para cada instalación. Además, existe la posibilidad de personalizar la columna, tanto en cuanto a los accesorios utilizados (calefactores, ventiladores, fuente de alimentación) como en la altura de colocación de las barreras y dichos accesorios dentro de la propia columna, o incluso en las dimensiones de la columna, pudiendo adaptar su altura a las necesidades específicas del proyecto: que no aparezca en el catálogo no quiere decir que no lo podamos hacer; si tiene una necesidad específica, consúltenos.

La gran acogida y demanda de este tipo de columnas que estamos experimentando desde que lanzamos Prodextec «nos indica que vamos en la línea correcta y nos anima a seguir buscando soluciones que se adapten a las necesidades reales del mercado en general y de nuestros clientes en particular».

Hanwha Techwin: Wisenet X define un nuevo estándar

Hanwha Techwin, especialista global en Soluciones de Seguridad, lanza al mercado la serie Wisenet X con chipset propio integrado. La serie Wisenet X ofrece un Amplio Rango Dinámico (WDR) de 150dB, estabilización de imágenes mediante sensores giroscópicos e imágenes muy nítidas las 24 horas del día, con un rendimiento muy alto en condiciones de poca iluminación. Al emplear la tecnología de compresión WiseStream II exclusiva de Hanwha Techwin, la serie Wisenet X ofrece la gama de cámaras de menor consumo de ancho de banda. También aporta muchos otros beneficios importantes, entre ellos, una gran variedad de analíticas integradas.

Con el lanzamiento de la serie Wisenet X, Hanwha Techwin cubre la demanda del mercado en todas las áreas de la videovigilancia. Al incorporar la serie Wisenet X a las recientemente lanzadas Wisenet Q y Wisenet P, Hanwha Techwin ha creado un portfolio completo, desde productos económicos de nivel básico hasta productos competitivos de gama alta que cubrirán las necesidades, bien de proyectos bien de usuarios finales, en todos los mercados verticales.

Hanwha Techwin ha captado extraordinariamente la atención con la nueva serie Wisenet X y tiene planes de ampliar sus inversiones de manera relevante en las áreas de desarrollo y marketing de productos.

Pelco: cámaras Optera, vistas panorámicas de calidad incomparable

Optera es la experiencia más cercana a estar en medio de la escena observada proporcionando la posibilidad de encontrar y captar la evidencia necesaria para tomar decisiones críticas relacionadas con su negocio.

La cámaras Optera proporcionan vistas panorámicas de una calidad incomparable, con un cosido perfecto de las imagenes capturadas por cada uno de los sensores sin la distorsión y los defectos habituales en otros productos similares –una experiencia visual que el resto de competidores simplemente no pueden alcanzar. Con sus 12 MP de resolucion y su PTZ electrónico a través de toda la vista panorámica, Optera nos da la máxima calidad de imagen y nivel de detalle posible, elevando el analísis forense del vídeo en vivo y grabado a un nivel nunca visto hasta ahora en el mercado de la vídeo seguridad.

La tecnología SureVision 2.0 permite evitar los deslumbramientos y obtener una imagen perfecta en condiciones de baja luminosidad. Encuentre más información sobre SureVision 2.0 y la experiencia panomersiva Optera, dos tecnologías desarrolladas por Pelco únicas en el mercado de la vídeo seguridad, visitando pelco.com/optera.

Características:

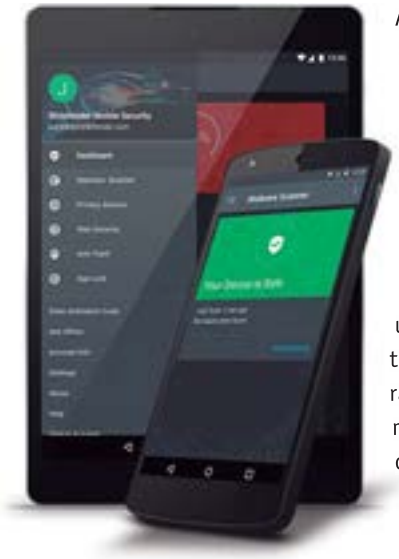
- Zoom para el detalle en vivo o retrospectivo con dewarping en el cliente.
- Resolución de 12 Megapixels para un mejor detalle a larga distancia.
- Hasta 12.5 Frames por Segundo (fps) a resolución máxima.
- Inmejorable rendimiento en condiciones de baja luminosidad y WDR simultáneamente.
- 8 analíticas de vídeo de Pelco incluidas.
- Almacenamiento local (Micro SD).
- ONVIF Perfil S y G.
- Compatible con Pelco VideoXpert™, Digital Sentry y VMS de terceros
- Alimentación a través de Ethernet (PoE+)
- 3 años de garantía.

Bitdefender, elegido mejor software antivirus para android en los test independientes

Bitdefender, el innovador fabricante de soluciones de software antivirus, se ha confirmado como especialista técnico en seguridad para dispositivos móviles, al obtener la mejor puntuación en los test independientes AV-TEST y ser galardonado como mejor antivirus para Android del año.

Así Alcatraz Solutions como country partner en España para las soluciones de consumo, corrobora su decisión de incorporar Bitdefender para completar su porftolio de Ciberseguridad para PYMES.

La aplicación de seguridad Bitdefender Mobile Security se impuso a muchos competidores con los mejores resultados, entre otras cosas, en la detección en tiempo real de malware para Android, así como excelentes resultados en la detección de los programas maliciosos más novedosos. Además, Mobile Security ofrece multitud de medidas de seguridad.



Guido Habicht, CEO de AV-TEST GmbH ratifica que «Mobile Security de Bitdefender ofrece numerosas funciones para proteger dispositivos Android contra malware con excelentes resultados.»

Para Leopoldo Mallo, director general de Alcatraz Solutions, «Bitdefender no es un antivirus cualquiera. Detrás de su protección contra el malware avanzado y el ransomware se esconden las tecnologías más avanzadas en detección y protección que queremos dar a conocer al canal y, sobre todo, a las pequeñas y medianas empresas».

Solución Dahua de Aparcamiento Inteligente

En las dos últimas décadas, el crecimiento económico mundial ha dado lugar a un significativo aumento de vehículos en casi todos los rincones del mundo. Los informes demostraron que en las ciudades, la mayoría de los edificios de viviendas de gran altura tenían dificultades para gestionar sus plazas de aparcamiento. La emisión de tarjetas de identificación, la facturación, el control de entrada y el pago hicieron que el procedimiento de entrada fuera muy ineficiente. El sistema tradicional de gestión de tarjetas inteligentes limita el acceso a aquellos que tienen una tarjeta inteligente asignada. Sin embargo, las tarjetas pueden ser robadas y la pérdida de una tarjeta supone un proceso muy desagradable.

Con una amplia experiencia en videovigilancia, Dahua lanza esta novedosa solución avanzada e integral para aparcamiento. La solución Dahua de Aparcamiento Inteligente se basa en vídeo vigilancia y tecnologías de análisis de vídeo. Además, se integra con el sistema de análisis inteligente DH-DSS4004-EMS. La función de control de entrada de la solución de aparcamiento inteligente Dahua ahorra costes de personal y ofrece un acceso mucho más fácil y más seguro.

Estacionamiento Inteligente Dahua

– La función de Control de Entrada está diseñada con 4 aspectos esenciales.

Control de Entrada

– Control Digital de Entrada a través de la cámara ANPR

La eficacia se mejora en gran medida con la tecnología ANPR. Los vehículos autorizados serán identificados por la cámara ANPR, que lee las matrículas de los coches y controla la entrada.

Para los visitantes, al presionar el botón de vídeo intercomunicador VTT201 se puede hablar con el operador.

– Vigilancia de entrada en tiempo real mediante reconocimiento rápido y preciso de matrículas

1

Las cámaras ANPR ITC237-PU1A-IRHL tienen una tasa de reconocimiento superior al 95% con cobertura de todas las matrículas de países europeos. Sin necesidad de instalar bucle.

– Búsqueda difusa de todas las matrículas europeas a través de cámara 4K NVR

El modelo NVR5208-8P-4KS2 admite grabación de 4K ultra HD (3840 x 2160), visualización en vivo y reproducción. Utilizando la función de búsqueda más perfecta, la información incluye la imagen del vehículo, el número de matrícula, el registro de historial de entrada y salida y se muestra el vídeo grabado. El grabador también ofrece la opción de exportación de series de datos de matrículas con fecha exacta, hora, canal, etc. a una memoria USB.

– Gestión inteligente a través del sistema DH-DSS4004-EMS

Con sistema de gestión sobre Windows, el análisis inteligente DH-DSS4004-EMS está especialmente diseñado para el Centro de Gestión. Es multifuncional, fácil de usar y rentable. El Centro de Gestión puede responder a la llamada de emergencia del VTT201 y buscar vídeos e imágenes por fecha / hora / número de matrícula.

Utilizando tecnología avanzada (ITC237 cámaras ANPR, NVR5208-8P-4KS2 4K NVR, sistema de análisis inteligente DH-DSS4004-EMS y etc.), la función de control de entrada de la Solución Dahua de Aparcamiento Inteligente ofrece alta eficiencia y entrada segura para zonas residenciales. Además, esta solución es escalable para expandirse con el crecimiento de la infraestructura compuesta y flexible para actualizar con el cambio tecnológico. Más funciones de este sistema avanzado de aparcamiento Dahua serán publicadas en breve. Esperamos que las siga con interés.

2

1.- Estructura general del sistema.

2.- Simulación del Control de Entrada de la solución Dahua de Aparcamiento Inteligente.

Cisco presenta el primer Secure Internet Gateway en el Cloud del mercado

Cisco ha presentado el primer Secure Internet Gateway (SIG) en el Cloud del mercado -Cisco Umbrella-, diseñado para responder a los nuevos retos de seguridad de las empresas que resultan de la movilidad y la evolución a la nube.

Muchas sucursales y oficinas remotas se conectan directamente a Internet, sin utilizar los mecanismos de seguridad web de la red corporativa, y por tanto un gran número de usuarios no están protegidos. Esta situación deja también a las organizaciones sin una gran parte de visibilidad frente a las amenazas.

Para responder a esta situación, la mayoría de organizaciones utilizan conexiones VPN (Virtual Private Network), pero muchos trabajadores móviles -hasta el 82 por ciento según una encuesta de IDG- admiten que no siempre las utilizan. Otras se apoyan en soluciones secure web gateway instaladas localmente (on-premise) y en distintos agentes asociados, creando complejidad y problemas de latencia.

Se requiere así una nueva aproximación basada en la protección Cloud que se convierta en la primera línea de defensa para las organizaciones, capaz de proporcionarles visibilidad y control justo en el extremo de Internet.

Cisco responde a esta necesidad creando una nueva categoría de producto -Secure Internet Gateway (SIG)- que proporciona un acceso seguro a Internet en cualquier lugar donde se conecten los usuarios, incluso cuando están desconectados de la VPN. Un SIG actúa como un puerto seguro a Internet y proporciona la primera línea de visibilidad y defensa con independencia de la ubicación de los usuarios o de a qué se quieren conectar.

Como plataforma de seguridad gestionada desde el Cloud, que protege a los trabajadores conectados o no a la red corporativa, Cisco Umbrella detiene las amenazas conocidas y desconocidas actuando sobre todos los puertos y protocolos para lograr la protección más completa. La solución bloquea el acceso a dominios, URLs, IPs y archivos maliciosos antes de establecer la conexión o de descargar un archivo. Debido a que la mayoría de amenazas afectan a los terminales, resulta esencial cubrir todos los puertos y protocolos para proporcionar una navegación segura que proteja del 100 por cien del tráfico.

Además, Cisco Umbrella evita los típicos problemas de complejidad operativa. Al gestionar todo desde el Cloud, no hay que instalar hardware ni actualizar el software de forma manual.

SoftGuard: SmartPanics, nueva APP para seguridad y otras emergencias personales y familiares

SoftGuard Tech Corp presentó en el Mobile World Congress su nueva APP SmartPanics que revoluciona la prevención de la seguridad personal, familiar y otros tipos de emergencia. Además de las funciones de SOS, Incendio y Asistencia, SmartPanics dispone en su pantalla principal de la opción «En Camino» para prevenir una posible urgencia en ruta y que realiza el acompañamiento pasivo del usuario, desde donde se encuentre hasta el punto del mapa que haya definido como destino o por el tiempo determinado que configure.

Si el usuario es interceptado, desviado de su ruta o no llega a destino en el tiempo estipulado, la aplicación envía una alerta a la central receptora para actuar en consecuencia. Mientras tanto, el smartphone estará reportando su ubicación cada 20 segundos, de manera que se pueda conocer su localización exacta en todo momento.

La aplicación puede generar grupos de seguimiento de los miembros de la familia o personas agregadas y crear «geocercas» de exclusión e inclusión de usuarios de un área geográfica determinada.

Por ejemplo, en caso de hijos en edad adolescente, SmartPanics puede programar alertas en el smartphone para enviar avisos en caso de que se desplacen a una velocidad excesiva, si tuviesen poca batería en su teléfono móvil o si desactivaran el seguimiento.

By Demes Group: UNIVIEW, tecnología de futuro para los retos presentes

By Demes Group ha presentado las novedades de UNIVIEW, fabricante que ha realizado una gran apuesta en cuanto a innovación y desarrollo con el lanzamiento de una serie de productos de muy alta gama.

UNIVIEW es una compañía que ha experimentado un gran crecimiento económico en los últimos años y que invierte gran parte de sus beneficios en desarrollo técnico e industrial, con la consecuente obtención de numerosos galardones internacionales (IF AWARDS) e infinidad de certificaciones (ISO, UL, GS, CE, etc.) a nivel mundial. UNIVIEW está posicionado como número 7 en el mercado global de cámaras IP y como número 8 en el de CCTV, según el último informe de investigación de mercado de IHS de 2015.

Las soluciones completas de la marca están basadas en productos IP. Disponen de una gran variedad de equipos concebidos para proyectos y sus soluciones se integran con plataformas de otros fabricantes, ya que además UNIVIEW es uno de los 40 miembros destacados dentro del ONVIF Full Members.

En continua mejora en cuanto a los códec de compresión, UNIVIEW dispone de una línea completa de productos tanto en cámaras como en NVRs con el nuevo U-code H.265.

Otra de las mejoras destacables reside en sus equipos de grabación (SMART SERIES), ya que estos incluyen detección facial para una mayor rapidez y eficacia en la búsqueda de imágenes, conteo de personas, videosensor avanzado y cruce de línea. También son subrayables los nuevos modelos con capacidad de hasta 128 canales, grabación en RAID, 512 Mbps de entrada y 384 Mbps de salida y fuente redundante. Además soluciones para proyectos, UNIVIEW dispone de un equipo de centralización capaz de gestionar hasta 1.000 dispositivos y 2.000 canales de vídeo.

Por lo que respecta a las cámaras, el equipo de ingeniería y grandes proyectos de By Demes Group destaca los modelos de domos motorizados con zoom 44X que incluyen la opción DEFOG, la cual permite mostrar una imagen nítida en condiciones de niebla espesa. Siguiendo con la gama de domos motorizados, destaca la serie FULL SPECTRUM, la cual dispone de modelos que combinan iluminación mediante luz blanca hasta 30 metros (modo color) para distancias cortas y mediante leds IR hasta 150 metros (modo B/N) para distancias largas.

En la gama de cámaras IP convencionales, son de destacar los modelos que incluyen los nuevos sensores STARVIS (modo STARLIGHT, también incluido en los domos motorizados), los cuales mejoran la visión de las cámaras en condiciones de baja luminosidad en modo color.

Vivotek: seis productos de vigilancia IP, galardonados con los Premios Taiwan Excellence 2017

Vivotek ha anunciado que seis de sus productos de vigilancia IP inteligentes fueron galardonados con los reconocidos premios Taiwan Excellence 2017. Los productos reconocidos son tres modelos H.264: MS8391 EV, MD8563-EH y la cámara APC (conteo automático de personas), así como los modelos H.265: IZ9361-EH, FE9381-EHV y SD9364-EH. Entre estos seis productos, la cámara tipo domo de alta velocidad SD9364-EH fue seleccionada para el premio Taiwan Excellence Gold Standard entre 528 productos competidores.

Owen Chen, presidente de Vivotek declaró que: «Nos sentimos honrados de recibir los premios Taiwan Excellence. Nos gustaría agradecer a MOEA y al Consejo de Desarrollo del Comercio Exterior de Taiwán (TAITRA), a los organizadores de los premios Taiwán Excellence y a los honorables jueces por sus veredictos. Vivotek, proveedor de soluciones de vigilancia en red en Taiwán, mantendrá su compromiso de ofrecer productos y soluciones de vigilancia con valor agregado, y de expandir nuestra presencia en el mercado mundial».

Bosch: actualización del software de Building Integration System

Bosch ha lanzado la actualización 4.3 de su software Building Integration System (BIS) que permite a los administradores de seguridad gestionar y configurar el control y la autorización de accesos de sitios distribuidos por todo el mundo, desde un solo servidor central.

Estos sistemas distribuidos suelen encontrarse en las grandes empresas multinacionales con muchos sitios diferentes en distintas regiones del mundo. Pueden incluir, por ejemplo, empresas internacionales con oficinas en todo el mundo o compañías con responsabilidad de seguridad corporativa pero con instalaciones distribuidas geográficamente, como el metro o las cadenas minoristas.

Con BIS 4.3 de Bosch, las empresas que administran sistemas distribuidos ahora pueden beneficiarse del control central. Todos los cambios y las actualizaciones que se realicen en el servidor corporativo central se replicarán de inmediato en todos los sitios y servidores.

Los administradores de seguridad pueden utilizar un solo servidor de autorización central para manejar una amplia gama de servidores en todo el mundo para la administración central de titulares de tarjetas, facilitando así la inscripción central de empleados nuevos o modificando las autorizaciones de acceso para los titulares de tarjetas de todo el mundo. El efecto es inmediato en todos los sitios, para que los empleados que se desplacen entre sitios ya no tengan que pedir permisos de acceso locales.

También es posible otorgar acceso regional desde el servidor de autorización central. Esto permite, por ejemplo, que un fabricante internacional en Berlín pueda otorgar o denegar al instante el acceso a titulares de tarjeta empleados en una planta industrial remota de Brasil desde su sede central en Berlín.

Aldir amplía su oferta con soluciones para operadores de TP-Link

Aldir, S.A., empresa dedicada a la distribución de soluciones informáticas, electrónicas y de telecomunicaciones, ha anunciado la disponibilidad de una gama completa de soluciones para operadores de telecomunicaciones de TP-Link.

Compuesta por routers de banda ancha, terminales PON, radioenlaces, puntos de acceso corporativos y otros muchos productos, esta familia de TP-Link ha sido desarrollada para ofrecer rendimiento profesional y facilidad de uso con un diseño elegante y, por lo tanto, satisfacer las necesidades de redes inalámbricas (domésticas y empresariales).

Router de banda ancha WR841N

Este router con nuevo firmware para operadores y velocidad inalámbrica de 300 Mbps se convierte en el equipo ideal para aplicaciones sensibles a las interrupciones, como reproducción de streaming de vídeo HD, llamadas VoIP y juegos online.

Terminal ONT TX6610

Este terminal con puertos GPON y Gigabit Ethernet y gestión remota mediante OMCI resulta idóneo en aplicaciones Fiber To The Home (FTTH).

Radioenlaces CPE510 y WBS510

Esta pareja de radioenlaces de 300 Mbps con tecnología TP-Link Pharos MAXtream TDMA aporta mejoras en rendimiento, capacidad y latencia, algo esencial en aplicaciones PTMP.

Puntos de acceso corporativos EAP225 y EAP330

Finalmente, estos puntos de acceso incluyen el software EAP Controller de Auranet para poder administrar fácilmente cientos de unidades EAP y soportan alimentación a través de Ethernet (PoE - 802.3af y 802.3at) para agilizar la instalación.

Contactos de empresas, p. 9.

ÍNDICE

MATERIALES, EQUIPOS Y SISTEMAS DE SEGURIDAD

SERVICIOS DE SEGURIDAD

ALARMA Y CONTROL

PYRONIX

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

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

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

Tyco Integrated Fire & Security

Edificio Ecu-I
Ctra. de La Coruña, km 23,500
28290 Las Rozas (Madrid)
Tel.: 902 444 440 - Fax: 91 631 39 78
www.tyco.es

San Fructuoso, 50-56 - 08004 **Barcelona**
Tel.: 934 254 960* - Fax: 934 261 904
Madrid: Matamorosa, 1 - 28017 Madrid
Tel.: 917 544 804* - Fax: 917 544 853
Sevilla: Tel.: 954 689 190* - Fax: 954 692 625
Canarias: Tel.: 928 426 323* - Fax: 928 417 077
Portugal
Rua Ilha da Madeira, 13 A
Olival Basto 2620-045 Odivelas (Lisboa)
Tel.: 219 388 186* - Fax: 219 388 188
www.bydemes.com

FUNDADA EN 1966

INSTALACIONES A SU MEDIDA

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

Central Receptora de Alarmas/Videovigilancia
Autorizada por la D.G.P. con el nº. 729
Avda de Olivares 17 – Plg. Industrial PIBO
41110 Bollullos de la Mitación (Sevilla)
Tlfno. 902194814 – 954108887
Fax. 954002319
gerencia@gruporomade.com
SERVICIOS EN TODA ESPAÑA

Accesos | CCTV | Incendio | Intrusión
Oficina Central:
Maresme, 71-79 · 08019 Barcelona
Fax 933 518 554
902 202 206 www.casmar.es

Calle López de Neira, nº3, oficina nº 301
36202 Vigo España
Tel.: +34 986 220 857 / 693 422 688
FAX: +34 986 447 337
www.aforsec.com
aforsec@aforsec.com

CONTROL DE ACCESOS ACTIVO

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

CONTROL DE ACCESO, HORARIO, TIEMPO Y PRESENCIA

C/Samonta 21
08970 Sant Joan Despi
Tel.: +34 934774770
info@primion-digitek.es
www.digitek.es

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

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

BIOSYS
(Sistemas de Tecnología Aplicada)

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

bydemes
avanzando juntos hacia el futuro

San Fructuoso, 50-56 - 08004 **Barcelona**
Tel.: 934 254 960* - Fax: 934 261 904
Madrid: Matamorosa, 1 - 28017 Madrid
Tel.: 917 544 804* - Fax: 917 544 853
Sevilla: Tel.: 954 689 190* - Fax: 954 692 625
Canarias: Tel.: 928 426 323* - Fax: 928 417 077
Portugal
Rua Ilha da Madeira, 13 A
Olival Basto 2620-045 Odivelas (Lisboa)
Tel.: 219 388 186* - Fax: 219 388 188
www.bydemes.com

RISTER
PRESENTCO®

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

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

accesor

Soluciones integrales en control de Accesos y seguridad

DDS

Carrer Esperança, 5
08500 Vic (Barcelona)
Tel.: 902 447 442
Fax.: 938 864 500

info@accesor.com
www.accesor.com

DORLET

DORLET S. A. U.

Parque Tecnológico de Álava
C/Albert Einstein, 34
01510 Miñano Mayor - ALAVA - Spain
Tel. 945 29 87 90 • Fax. 945 29 81 33

e-mail: comercial@dorlet.com
web: http://www.dorlet.com

setelsa link
Sistemas Electrónicos y Telecomunicación S.A.

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

DETECCIÓN DE EXPLOSIVOS

COTELSA

COTELSA
Basauri, 10-12, Urb. La Florida
Ctra. de La Coruña, Aravaca
28023 Madrid
Tel.: 915 662 200 - Fax: 915 662 205
cotelsa@cotelsa.es
www.cotelsa.es

TECOSA

Telecomunicación, Electrónica y Conmutación

Grupo Siemens
Infraestructure & Cities Sector
División Building Technologies
Ronda de Europa, 5
28760 Tres Cantos - Madrid
Tel.: +34 91 514 75 00
Asistencia Técnica: 902 199 029
www.tecosa.es

TARGET TECNOLOGIA

TARGET TECNOLOGIA, S.A.
Ctra. Fuencarral, 24
Edif. Europa I - Portal 1 Planta 3ª
28108 Alcobendas (Madrid)
Tel.: 91 554 14 36 • Fax: 91 554 45 89
info@target-tecnologia.es
www.target-tecnologia.es

SISTEMAS DE EVACUACIÓN

OPTIMUS
SOUND & COMMUNICATION

OPTIMUS S.A.

C/ Barcelona 101
17003 Girona
T (+34) 972 203 300

info@optimus.es
www.optimusaudio.com

PROTECCIÓN CONTRA INCENDIOS. ACTIVA

detnov

C/ Alguer nº8 08830 Sant Boi de Llobregat (Barcelona)

Tel: +34 93 371 60 25
Fax:+34 93 640 10 84

www.detnov.com
info@detnov.com

bydemes
avanzando juntos hacia el futuro

San Fructuoso, 50-56 - 08004 **Barcelona**
Tel.: 934 254 960* - Fax: 934 261 904
Madrid: Matamorosa, 1 - 28017 Madrid
Tel.: 917 544 804* - Fax: 917 544 853
Sevilla: Tel.: 954 689 190* - Fax: 954 692 625
Canarias: Tel.: 928 426 323* - Fax: 928 417 077
Portugal
Rua Ilha da Madeira, 13 A
Olival Basto 2620-045 Odivelas (Lisboa)
Tel.: 219 388 186* - Fax: 219 388 188
www.bydemes.com

aguilera

GRUPO AGUILERA

FABRICANTES DE SOLUCIONES PCI DETECCIÓN Y EXTINCIÓN DE INCENDIOS

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

Delegaciones en:
Galicia: Tel. 98 114 02 42 • Fax: 98 114 24 62
Cataluña: Tel. 93 381 08 04 • Fax: 93 381 07 58
Levante: Tel. 96 119 96 06 • Fax: 96 119 96 01
Andalucía:Tel. 95 465 65 88 • Fax: 95 465 71 71
Canarias: Tel. 928 24 45 80 • Fax: 928 24 65 72
Portugal: Tel.+351 213 563 295 • Fax:+351 213 563 295

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

Soluciones y sistemas:
** DETECCIÓN **
Algorítmica • Analógica • Aspiración • Convencional • Monóxido • Oxyreduct® • Autónomos • Detección Lineal
** EXTINCIÓN **
Agua nebulizada • Fe-13™ • Hfc-227ea • Co_2

pefipresa
FIRE, SAFETY & SECURITY

PEFIPRESA, S. A. U

INSTALACIÓN Y MANTENIMIENTO DE SISTEMAS DE SEGURIDAD Y CONTRA INCENDIOS

www.pefipresa.com

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

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

¿No cree...
... que debería estar aquí?

El directorio es la zona más consultada de nuestra revista.

Módulo: 660€/año*

Más información:
Tel.: 91 476 80 00
e-mail: publi-seguridad@epeldano.com
* Tarifa vigente 2017

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

PROTECCIÓN CONTRA INCENDIOS. PASIVA

solexin

Calle Alberto Alcocer, 28, 1º A
28036 Madrid
Tel. 913 685 120

info@solexin.es
www.solexin.es

DICTATOR Española

DICTATOR ESPAÑOLA
Mogoda, 20-24 • P. I. Can Salvatella
08210 Barberá del Vallés (Barcelona)
Tel.: 937 191 314 • Fax: 937 182 509
www.dictator.es
dictator@dictator.es

PROTECCIÓN CONTRA INTRUSIÓN. ACTIVA

bydemes

avanzando juntos hacia el futuro

San Fructuoso, 50-56 - 08004 **Barcelona**
Tel.: 934 254 960* - Fax: 934 261 904
Madrid: Matamorosa, 1 - 28017 Madrid
Tel.: 917 544 804* - Fax: 917 544 853
Sevilla: Tel.: 954 689 190* - Fax: 954 692 625
Canarias: Tel.: 928 426 323* - Fax: 928 417 077
Portugal
Rua Ilha da Madeira, 13 A
Olival Basto 2620-045 Odivelas (Lisboa)
Tel.: 219 388 186* - Fax: 219 388 188
www.bydemes.com

RISCO GROUP

Creating Security Solutions

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

Tecnoalarm

Hi-Tech Security Systems

TECNOALARM ESPAÑA

C/ Vapor, 18 • 08850 Gavà (Barcelona)
Tel.: +34 936 62 24 17
Fax: +34 936 62 24 38
www.tecnoalarm.com
tecnoalarm@tecnoalarm.es

PROTECCIÓN CONTRA ROBO Y ATRACO. PASIVA

AGA

LA INDUSTRIA DE LA CERRAJERÍA

Talleres AGA, S.A.
C/ Notario Etxagibel, 6
20500 Arrasate-Mondragón (Guipuzkoa)
Tel.: +34 943 79 09 22
info@aga.es / www.aga.es

TELECOMUNICACIONES

Alai Secure

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

Condesa de Venadito 1, planta 11
28027 Madrid
T. 902.095.196 • F. 902.095.196
comercial@alai.es • www.alaisecure.com

VIGILANCIA POR TELEVISIÓN

HIKVISION

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

WISENET SAMSUNG

Hanwha Techwin Europe Ltd

Avda. De Barajas, 24, Planta Baja, Oficina 1
28108 Alcobendas (Madrid)España(Spain)
Tel.: +34 916 517 507

www.hanwha-security.eu
hte.spain@hanwha.com

GRUPO IPTECNO

Tel. 902 502 035 - Fax 902 502 036
iptecno@iptecno.com - www.iptecno.com

SEDE BARCELONA
IPTECNO Videovigilancia S.L.
C. Pla del Ramassar, 52, Nave 19
08402 Granollers

SEDE MADRID
IPTECNO Seguridad S.L.
Avda. Tenerife, 2 - Blq. 2, Pta. 3
28703 S. S. de los Reyes

dahua TECHNOLOGY

DAHUA IBERIA
C/ Juan Esplandiú 15 1-B. 28007 Madrid

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

VISIOTECH

Visiotech
Avenida del Sol, 22
28850, Torrejón de Ardoz (Madrid)
Tel.: 911 836 285 • Fax: 917 273 341
info@visiotech.es
www.visiotech.es

LSB

www.lsb.es

Expertos en VIDEOVIGILANCIA

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

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

RISTER
PRESENTCO

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

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

INGRAM MICRO

Viladecans Business Park
Edificio Australia. C/ Antonio Machado 78-80, 1ª y 2ª planta
08840 Viladecans (Barcelona)
Web: www.ingrammicro.es
Teléfono: 902 50 62 10
Fax: 93 474 90 00
Marcas destacadas: Axis y D-Link.

ASOCIACIONES

bydemes
avanzando juntos hacia el futuro

San Fructuoso, 50-56 - 08004 **Barcelona**
Tel.: 934 254 960* - Fax: 934 261 904
Madrid: Matamorosa, 1 - 28017 Madrid
Tel.: 917 544 804* - Fax: 917 544 853
Sevilla: Tel.: 954 689 190* - Fax: 954 692 625
Canarias: Tel.: 928 426 323* - Fax: 928 417 077
Portugal:
Rua Ilha da Madeira, 13 A
Olival Basto 2620-045 Odivelas (Lisboa)
Tel.: 219 388 186* - Fax: 219 388 188
www.bydemes.com

AXIS COMMUNICATIONS

AXIS COMMUNICATIONS
C/ Yunque, 9 - 1ºA
28760 Tres Cantos (Madrid)
Tel.: +34 918 034 643
Fax: +34 918 035 452
www.axis.com

PELCO
by Schneider Electric

PELCO by Schneider Electric
C/ Valgrande 6
28108, Alcobendas, Madrid
Tel.: +34 911 234 206
pelco.iberia@schneider-electric.com
www.pelco.com

UAS

C/ Alcalá 99
28009 Madrid
Tel. 915765255
Fax. 915766094

info@uaseguridad.es
www.uaseguridad.es

Dallmeier

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

FF Videosistemas
GEUTEBRÜCK

GEUTEBRÜCK ESPAÑA
Edificio Ceudas
Camino de las Ceudas, 2 Bis
28230 Las Rozas (Madrid)
Tel.: 902 998 440
Fax: 917 104 920
ffvideo@ffvideosistemas.com
www.geutebruckspain.com

EVENTOS DE SEGURIDAD

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

C/ Emiliano Barral, 43
28043 Madrid
Tel 91 564 7884 • Fax 91 564 7829
www.aecra.org

WD
A Western Digital® Company

WD ESPAÑA
4 boulevard des Iles
92130 Issy les Moulineaux · Francia
florence.perrin@wdc.com
Tel.: 615 235 013
www.wdc.com

GRUPO ALAVA INGENIEROS
Área Seguridad

Grupo Alava Ingenieros
Área Seguridad

C/Albasanz, 16 – Edificio Antalia
28037 Madrid
Telf. 91 567 97 00 • Fax: 91 567 97 11
Email: alava@alava-ing.es
Web: www.alavaseguridad.com

Security FORUM

SECURITY FORUM
Tel.: +34 91 476 80 00
Fax: +34 91 476 60 57
www.securityforum.es
info@securityforum.es

AEINSE
Asociación Española de Ingenieros de Seguridad

ASOCIACIÓN ESPAÑOLA
DE INGENIEROS DE SEGURIDAD

C/ San Delfín 4 (local 4 calle)
28019 MADRID
aeinse@aeinse.org
www.aeinse.org

BOSCH

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

ata98
Security Company
C.C.TV.

Josep Estivill, 67-69
08027 Barcelona, Spain.
www.ata98.com
info@ata98.com
Tel. +34 931 721 763

¿No cree...
... que debería estar aquí?

El directorio es la zona más consultada de nuestra revista.

Módulo: 660€/año*

Más información:
Tel.: 91 476 80 00
e-mail: publi-seguridad@epeldano.com

* Tarifa vigente 2017

ACAES

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

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

ASOCIACION ESPAÑOLA DE SOCIEDADES DE PROTECCION CONTRA INCENDIOS
C/ Doctor Esquerdo, 55. 1º F.
28007 Madrid
Tel.: 914 361 419 - Fax: 915 759 635
www.tecnifuego-aespi.org

ASOCIACIÓN PROFESIONAL DE COMPAÑÍAS PRIVADAS DE SERVICIOS DE SEGURIDAD
Marqués de Urquijo, 5 - 2ºA
28008 Madrid
Tel.: 914 540 000 - Fax: 915 411 090
www.aproser.org

ASOCIACIÓN NACIONAL DE TASADORES Y PERITOS JUDICIALES INFORMÁTICOS (ANTPJI)
C/ Juan de Mariana, 5
28045 Madrid
Tlf 91 / 469.76.44
www.antpji.com
contacto@antpji.com

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

ASOCIACION ESPAÑOLA DE LUCHA CONTRA EL FUEGO
Calle Escalona nº 61 - Planta 1
Puerta 13-14 28024 Madrid
Tel.: 915 216 964
Fax: 911 791 859

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

FORMACIÓN DE SEGURIDAD

ANPASP
Asociación Nacional de Profesores Acreditados de Seguridad Privada
C/ Anabel Segura, 11 - Edificio A - Planta 1ª
28108 Alcobendas (MADRID)
info@anpasp.com • www.anpasp.com

APDPE
Asociación Profesional de Detectives de España
Marqués de Urquijo, 6, 1ºB
28008 - Madrid
Tel.: +34 917 581 399
Fax: +34 917 581 426
info@apdpe.es • www.apdpe.es

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

Homologado por el Ministerio del Interior y la Junta de Andalucía.
Avda de Olivares 17 • Plg. Industrial PIBO.
41110 Bollullos de la Mitación (Sevilla).
Tlfno. 902194814 – 954108887
Fax. 954002319
gerencia@gruporomade.com

ADSI - Asociación de Directivos de Seguridad Integral
Gran Via de Les Corts Catalanes, 373 - 385
4ª planta (local B2)
Centro Comercial **Arenas de Barcelona**
08015 Barcelona
info@adsi.pro • www.adsi.pro

ASOCIACIÓN DE EMPRESAS DE EQUIPOS DE PROTECCION PERSONAL
Alcalá, 119 - 4º izda.
28009 Madrid
Tel.: 914 316 298 - Fax: 914 351 640
www.asepal.es

ASOCIACIÓN DE JEFES DE SEGURIDAD DE ESPAÑA
Avd. Meridiana 358. 4ºA.
08027 Barcelona
Tel. 93-3459682 Fax. 93-3453395
www.ajse.es presidente@ajse.es

CENTRALES DE RECEPCIÓN Y CONTROL

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

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

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

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

INTEGRACIÓN DE SISTEMAS

ARQUERO SISTEMA CORPORATIVO

Avda. de la Feria 1
Edificio Incube - sala 8
35012 Las Palmas de Gran Canaria
Tel.: **928 09 21 81**
www.sci-spain.com

INSTALACIÓN Y MANTENIMIENTO

TECOSA

Telecomunicación, Electrónica y Conmutación

Grupo Siemens
Industry Sector
División Building Technologies
Ronda de Europa, 5
28760 Tres Cantos - Madrid
Tel.: +34 91 514 75 00 - Fax: +34 91 514 70 30

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

SEGURIDAD LEVANTE
Homologación de registro D.G.S.E. nº 432

INSTALACIÓN Y MANTENIMIENTO
INTRUSIÓN – CCTV – INCENDIO – ACCESOS
SUBCONTRATACIÓN
ALICANTE, VALENCIA, MURCIA, ALBACETE

www.seguridadlevante.com
902 400 022
info@seguridadlevante.com

AGÜERO
Proyectos e Instalaciones, S.L.

FUNDADA EN 1966

INSTALACIONES A SU MEDIDA

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

PUBLICACIONES WEB

PUNTO SEGURIDAD.com

PUNTOSEGURIDAD.COM
TF: 91 476 80 00

info@puntoseguridad.com
www.puntoseguridad.com

INSTALSEC

Avda. Manzanares, 196
28026 Madrid
Tel.: 914 768 000 - Fax: 914 766 057
publi-seguridad@epeldano.com
www.instalsec.com

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

MATERIAL POLICIAL

SABORIT INTERNATIONAL

Avda. Somosierra, 22 Nave 4D
28709 S. Sebastián de los Reyes (Madrid)
Tel.: 913 831 920
Fax: 916 638 205

www.saborit.com

VIGILANCIA Y CONTROL

SECURITAS SEGURIDAD ESPAÑA

C/ Entrepeñas, 27
28051 Madrid
Tel.: 912 776 000
email: info@securitas.es

www.securitas.es

Grupo RMD

Autorizada por la D.G.P. con el nº. 729
Avda de Olivares 17 – Plg. Industrial PIBO
41110 Bollullos de la Mitación (Sevilla)
Tlfno. 902194814 – 954108887
Fax. 954002319
gerencia@gruporomade.com
SERVICIOS EN TODA ESPAÑA

TRANSPORTE Y GESTIÓN DE EFECTIVO

LOOMIS SPAIN S. A.

C/ Ahumaos, 35-37
Poligono Industrial La Dehesa de Vicálvaro
28052 Madrid
Tlf: 917438900
Fax: 914 685 241

www.loomis.com

CUADERNOS DE SEGURIDAD

Suscríbase

RELLENE SUS DATOS CON LETRAS MAYÚSCULAS (fotocopie este boletín y remítanoslo)

Entidad: _____ N.I.F.: _____
D. _____ Cargo: _____
Domicilio: _____
Código Postal: _____ Población: _____
Provincia: _____ País: _____
Teléfono: _____ Fax: _____
Actividad: _____
E-mail: _____ Web: _____

Forma de pago:

❑ Domiciliación bancaria c.c.c. nº _____
❑ Cheque nominativo a favor de EDICIONES PELDAÑO, S. A.
❑ Ingreso en CaixaBank ES80 2100 3976 21 0200107897
❑ Cargo contra tarjeta VISA nº _____ Caducidad _____

Firma

TARIFAS (válidas durante 2017)

ESPAÑA
❑ 1 año: 93€ ❑ 2 años: 165€ (IVA y Gastos de envío incluido)

EUROPA
❑ 1 año: 124€ ❑ 2 años: 222€ (Gastos de envío incluido)

RESTO
❑ 1 año: 133€ ❑ 2 años: 239€ (Gastos de envío incluido)

Peldaño

DEPARTAMENTO DE SUSCRIPCIONES: 902 35 40 45
Avda. del Manzanares, 196 • 28026 Madrid • Tel.: +34 91 476 80 00 • Fax: +34 91 476 60 57
suscripciones@epeldano.com • www.puntoseguridad.com

Joan Josep Pintado

Director de Seguridad del Museu Nacional d`Art de Catalunya

Gemma G. Juanes

«La vida no te regala nada si no trabajas duro»

Si pudiéramos verlo sin ser vistos descubriríamos a un hombre sencillo, sensible, espontáneo, cariñoso, generoso y cordial. A veces muy ingenioso y por momentos incluso osado. Pero de puertas para afuera él es una incógnita. Serio, reservado, disciplinado, metódico en el trabajo y con una inteligencia teñida de sentido del humor. Hoy conocemos su mejor parte, aquella que asoma tras esta conversación.

Detrás del compromiso y responsabilidad que implica un cargo como el de director de Seguridad del Museu Nacional d´Art de Catalunya (MNAC), Joan Josep Pintado se muestra próximo, dispuesto y con una libertad absoluta para hablar. Todo en él resulta tan extremadamente natural y cercano –incluso ese tono de voz sutilmente radiofónico- que uno al final acaba olvidando el ritual que conlleva hacer una entrevista en un despacho. Ni un par de preguntas han hecho falta para saber que nuestro interlocutor es de aquellos hombres que elevan su profesión con solo una frase –«¡El mundo de la seguridad es apasionante!»–, y que disfrutan de la vida casi sin darse cuenta.

Su ruta por el mundo de la seguridad arranca como miembro de la primera promoción de Mossos d´Escuadra, donde llegó a desempeñar puestos de gran responsabilidad; pero un espíritu inquieto y tenaz –y ya con el postgrado en Dirección de Seguridad bajo el brazo- le empujó a adentrarse en el sector de la seguridad privada. El cambio de siglo coincidió con su andadura profesional en el MNAC, justo cuando la instalación pasaba por un ambicioso proyecto de reforma, donde aportó su experiencia y conocimiento en aspectos de seguridad. Desde entonces, al frente del área de Seguridad del centro y «junto a un equipo –matiza- de excelentes profesionales», cuida de que nada pueda alterar el día a día de los trabajadores y visitantes, así como del fondo artístico que alberga.

Piensa cada palabra concienzudamente y usa los silencios para ganar tiempo al entrevistador, pero replica al instante para asegurar que el ciudadano cada vez es «más consciente de que las obras de arte se conservan mejor si entre todos las respetamos. Los museos son instalaciones para disfrutar y respetar».

Cuando aflora el tema de su vida más personal no le incomoda meterse en terrenos quizás para otros pantanosos. Cuenta que hoy reside en la misma calle de Hospitalet de Llobregat (Barcelona) donde sus padres, emigrantes andaluces, lucharon por sacar adelante a 6 hijos. «Una familia humilde -apunta- donde aprendimos que la vida no te regala nada si no trabajas duro». Seguidor del Barça -«¡pero no soy de los que discuten por el fútbol!», insiste que apuntemos-, practicó el salto de altura y atletismo de adolescente. Ahora disfruta de tranquilos paseos por la playa de Sitges junto a su mujer, escuchando a Serrat, degustando un arroz caldoso o, simplemente, pudiendo contemplar cada día el Ábside de Sant Climent de Taüll –obra maestra del románico europeo– o «La Vicaría» de Fortuny. Hoy sí conocimos a ese hombre sensible, sencillo, espontáneo… ●

Security FORUM

International Security Conference & Exhibition

CCIB
Centro de Convenciones
Internacional de Barcelona

17 y 18 de mayo
BCN2017

VER PARA CREAR

#SecurityForumBCN2017

www.securityforum.es
info@securityforum.es
+34 914 768 000
@SecurityForumES

IBERIA renfe

Peldaño

HIKVISION

UN PARTNER SÓLIDO, COMPROMETIDO, INNOVADOR, FIABLE, PRESENTE.

El valor de un partner tecnológico se mide por su capacidad de generar ventaja competitiva, así como por su actitud y el poder de transmitir determinación, entusiasmo, y motivaciones siempre nuevas. Hikvision garantiza profesionalidad, solidez empresarial, compromiso, fiabilidad tecnológica, innovación continua y un alcance global con presencia local.

Hikvision Spain
C/ Almazara, 9
28760 Tres Cantos (Madrid)
T +34 91 7371655
F +34 91 8058717
info.es@hikvision.com

www.hikvision.com