30 AÑOS

CUADERNOS DE SEGURIDAD

Núm. 336 • SEPTIEMBRE 2018 • 10,50 euros // cuadernosdeseguridad.com

Seguridad, clave en las instalaciones sanitarias

Intrusión/Centrales Receptoras de Alarmas

Edita Peldaño

Actualidad: innovación en equipos y sistemas, jornadas...

II Jornada Técnica
RPAS y Seguridad Privada

MADRID
30.10.2018

Más información e inscripciones:

dronesyseguridad.com info@dronesyseguridad.com +34 914 768 000

Con la colaboración de: CUADERNOS DE SEGURIDAD

Organiza: Peldaño

COMUNICAMOS, CONECTAMOS, IMPULSAMOS

El mundo cambia, nosotros también

Con este número postvacacional empezamos un nuevo curso y lo hacemos con la misma ilusión de siempre. Emprendemos esta trayectoria de continuidad con renovados bríos, planteándonos ambiciosos retos y confiados en que los próximos meses nos permitirán seguir progresando. Y uno de los cambios mas significativos es que Peldaño, empresa editora de Cuadernos de Seguridad, renueva su identidad corporativa y su estrategia para hacer más grande su esencia.

Pieza clave de esta nueva etapa es la nueva imagen, más amable y moderna que, proyecta ese espíritu de cambio y de avance constante. A ello se une una auténtica declaración de intenciones que pone en valor el papel de Peldaño en el ámbito empresarial, y de manera concreta en el sector de la Seguridad. Bajo el claim «Comunicamos. Conectamos. Impulsamos», Peldaño tiene como prioridad dar respuesta a las necesidades e intereses de sus clientes, por lo que el punto estratégico de este cambio es la reorganización de sus servicios para poder dar una «mayor y mejor respuesta a un mercado demandante y exigente». Un cambio que muestra nuestra capacidad para adaptarnos a la evolución de nuestro entorno y a la voluntad de acompañar a todos los agentes que forman parte de este sector en este viaje compartido hacia el futuro; contribuyendo, desde nuestra especial esfera comunicativa, a convertir en más competitivos cada uno de los negocios que configuran este mercado y ayudando al crecimiento conjunto del mismo.

En este contexto, y como respuesta a las necesidades del sector, Cuadernos de Seguridad organiza el próximo 30 de octubre, en Madrid, la II Jornada RPAS y Seguridad Privada, con el objetivo de establecer un foro en el que se analizarán las últimas novedades en materia legislativa y los retos y oportunidades que ofrece esta tecnología al sector de la Seguridad Privada.

En una era con la revolución tecnológica como protagonista, las empresas se adaptan y ofrecen a sus clientes nuevas soluciones y servicios, como sistemas de última generación capaces de aumentar nuestro control y seguridad sobre el entorno. Es el caso de los RPAS, conocidos popularmente como drones, que han cambiado la metodología y servicios de muchas empresas de Seguridad, emergiendo como uno de los sectores de mayor crecimiento y proyección futura.

Es el propio sector de la Seguridad, atento a la revolución tecnológica, quien demanda de manera constante una adaptación en sistemas, servicios y legislación para poder ofrecer las mejores soluciones y medidas de protección y seguridad.

Durante el encuentro, dirigido a directores y gestores de seguridad en entidades pública y privadas, centros de formación y a todos los profesionales de empresas de RPAS y de seguridad en general, se abordarán, entre otros temas: «Normativa actual sobre el uso de RPAS en España»; «Normativa de Seguridad Privada y su aplicación a RPAS»; «RPAS en la lucha contra incendios y emergencias»: «Contramedidas frente al uso de RPAS como amenaza»; «Aplicación del RGPD en el uso de los RPAS con fines de seguridad»; y «Retos y oportunidades del RPAS en la industria de la Seguridad».

CUADERNOS DE SEGURIDAD

www.cuadernosdeseguridad.com

Nº 336 • SEPTIEMBRE 2018

Peldaño

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

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

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

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

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

Printed in Spain

Depósito Legal: M-7303-1988

ISNN: 1698-4269

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

FIPP · EUROPEAN PRESS NETWORK Fire prevention division · EUROPEAN PRESS NETWORK Security division · AEEPP

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

OCTUBRE 2018 - Nº 337

EN PORTADA

CIBERSEGURIDAD CORPORATIVA

En un mundo totalmente globalizado, donde la información traspasa fronteras, la ciberseguridad se ha convertido en un elemento fundamental para las empresas. Y es que el amplio volumen de pérdidas, tanto económicas como de imagen, que puede suponer para las compañía un ciberataque, hace necesario implantar políticas de prevención y protección.

La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno.

SEGURIDAD RESIDENCIAL

Nuestra vivienda es el lugar donde más tiempo pasamos y donde convivimos con nuestra familia, así como donde tenemos nuestras pertenencias y objetos de valor. Es probablemente el lugar donde nosotros y los nuestros nos sentimos más cómodos. Sin embargo, los robos y los asaltos a los domicilios y comunidades están a la orden del día, por eso cada vez más las comunidades de vecinos consideran la instalación de medidas de seguridad como una necesidad de mejorar su calidad de vida y seguridad. Hoy en día estas comunidades de vecinos tienen a su disposición una amplia oferta de soluciones de seguridad para garantizar la seguridad de sus propietarios, inquilinos, visitantes y administradores. Los ciudadanos cuentan con soluciones integradas que aportan una protección total de la comunidad y de las personas.

SEGURIDAD EN MUSEOS

Los museos, centros de arte, galerías...deben contar con un adecuado y aceptable nivel de seguridad. Se trata de instalaciones que, junto a las valiosas e insustituibles piezas y obras que albergan, se encuentran expuestas a un amplio catálogo de riesgos. Y es que la conservación y, por supuesto, la seguridad de nuestro patrimonio artístico, es uno de los objetivos de los directores de los museos, y no solo de ellos, de nuevo viene a jugar un papel fundamental la figura del responsable de Seguridad del centro museístico. Para garantizar esta prevención y seguridad, la tecnología ha jugado y juega actualmente un papel imprescindible de ayuda. Medios y sistemas de seguridad que sirven de complemento al trabajo que realizan los responsables de Seguridad.

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

Protección exterior de confianza

XDL12TT-AM

Detección eficaz, instalación sencilla

Características principales

- Nuevo diseño, más fácil de instalar
- Protección anti enmascaramiento y anti bloqueo
- Protección de intemperie IP55
- Lógica de Detección de Triple Señal (Doble PIR + MW)
- Soportes opcionales
- Supresión del movimiento de la vegetación
- Compensación digital de la temperatura
- Zumbador de prueba de paso integrado
- Filtro ultra violeta de última generación
- Protección perimetral de 12 m
- Inmunidad a mascotas de hasta 55 kg
- Protección del perímetro exterior

Hikvision Spain, C/ Almazara, 9 Tres Cantos 28760, Madrid
T: +34 91 737 16 55 E: info@hikvision.com

ÍNDICE DE EMPRESAS CITADAS EN ESTA EDICIÓN

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

EMPRESA	PAG.	TELÉFONO	WEB
ADVANCED SECURITY BUSINESS GROUP	78	917873170	www.advancedsecuritytools.com
BY DEMES	17,72	934254960	www.bydemes.com
CUEVA VALIENTE-INERCO	74,77	918047364	www.inerco.com www.cuevavaliente.com
CYRASA SEGURIDAD	21	902194749	www.cyrasa.com
DAHUA	91	917649862	www.dahuasecurity.com
DALLMEIER	90	915902287	www.dallmeier.com/es
DEISTER ELECTRONIC	29,52	495105516111	www.deister.com
DETNOV	86	933716025	www.detnov.com
DORMAKABA	54	917362480	www.dormakaba.com
ESET	71	902334833	www.eset.es
FUJITSU	88	917849509	es.fujitsu.com
GRUPO RMD	83	902194814	www.grupormd.com
HANWHA TECHWIN EUROPE	60,91	916517507	www.hanwha-security.eu
HIKVISION	4ª Cubierta, 7,62,63,88,92	917371655	www.hikvision.com/es
HOCHIKI	53	441634260133	www.hochikieurope.com
HOMMAX SISTEMAS	85	961594646	www.hommaxsistemas.com
II JORNADA RPAS Y SEG. PRIVADA	2ª Cubierta	914768000	www.dronesyseguridad.com
JABLOTRON	89		www.jablotron.com/es
JOHNSON CONTROLS	68,9	916313999	www.johnsoncontrols.com
MORSE WATCHMANS	27		www.morsewatchmans.com
PECKET	3ª Cubierta	914768000	www.pecket.es
PYCSECA	37	932313105	www.pycsecaseguridad.com
RISCO GROUP	59,66,85,93	914902133	www.riscogroup.com
SECURE IT	85	911196995	www.secureit.es
SECURITAS DIRECT	49	917097500	www.securitasdirect.es
SUPPORT SECURITY	5	942544354	www.support-seguridad.es
SYNOLOGY	93	33147176288	www.synology.com
TECHCO SECURITY	64	900777780	www.techcosecurity.com
TESA	69	943669100	www.tesa.es
WD	33	615235013	www.wdc.com

ÍNDICE DE ANUNCIANTES

El futuro es para...
marcas que se adaptan,
marcas que dan credibilidad,
marcas que aportan valor,
marcas que conectan.

El mundo cambia, nosotros también.

peldano.com

Peldaño

Comunicamos. Conectamos. Impulsamos.

El mundo cambia, Peldaño también.

La imagen y la identidad corporativa configuran el ADN de una empresa, tanto en su estrategia general como en la imagen que traslada a la sociedad. El futuro es para las marcas que se adaptan, que dan credibilidad, que aportan valor y que conectan. Por eso, en Peldaño nos adaptamos; cambiamos por fuera y por dentro para hacer más grande nuestra esencia: comunicar, conectar e impulsar.

Así cambia Peldaño por fuera

LOGOTIPO
Nuestro nuevo logo es un símbolo memorable y potente, con un gran significado. La «P» de Peldaño como una pieza sólida clave que sirve como conector y como el soporte perfecto donde poder apoyarse y coger impulso. Un símbolo dinámico, con espíritu de cambio y la intención constante de avanzar.

AZUL PELDAÑO
Nuestro color corporativo ahora es un azul mucho más luminoso y actual.

TIPOGRAFÍA
Una tipografía más amable y moderna que nos acompañará ahora en todas nuestras comunicaciones.

ANTES

DESPUÉS

Comunicamos. Conectamos. Impulsamos.

Así cambia Peldaño por dentro

NUESTROS VALORES

Siempre nos exigimos más
Siempre en movimiento, siempre inquietos, buscando nuevos conocimientos, canales, formas de acercarnos a nuestras audiencias.

Hacemos que las cosas pasen
Somos impulsores y potenciadores de nuestros lectores y clientes.

Primero entendemos, luego creamos
Tratamos de dar respuesta a las necesidades e intereses de nuestros clientes, por lo que escucharles y adaptarnos a lo que buscan, es nuestra prioridad.

Unimos los puntos para crear caminos
Usamos esta capacidad para convertir el conocimiento en información útil, el desconocimiento en visibilidad y las inversiones en éxitos.

NUEVO RUMBO, NUEVOS SERVICIOS

En Peldaño reorganizamos nuestros servicios para poder dar una mayor y mejor respuesta a un mercado demandante y exigente, ofreciendo cuatro servicios diferenciados:

Editorial · **Estrategia** · **Experiencias** · **Innovación**

EL CLAIM

Un nuevo claim surge de nuestra esencia. Una auténtica declaración de intenciones, contundente y concisa, que pone en valor el papel de Peldaño en el mundo.

Comunicamos. Conectamos. Impulsamos.

Peldaño

Monkey Business/Shutterstock

El sector sanitario: en lucha para trabajar con seguridad y sin agresiones

El porcentaje de profesionales de la medicina y la enfermería que afirma haber sido agredido en el ejercicio de su labor supera el 60%. Los responsables de seguridad pública y privada actúan para prevenir y combatir esta problemática

CUANDO generalmente se piensa en las profesiones más peligrosas nos vienen a la mente las de policía, militares, bomberos o incluso toreros. Esta percepción social está virando hacia otros ámbitos cuyo desempeño laboral está asumiendo cada vez mayores riesgos. Uno de ellos es el de personal sanitario.

Los datos que facilitan las organizaciones del sector corroboran esta tendencia: el 65% de los médicos españoles afirma haber sufrido agresiones en el ejercicio de su profesión. Así lo recoge la V Oleada de la «Encuesta sobre la situación de la profesión médica en España», promovida por la Organización Médica Colegial (OMC) en colaboración con la Confederación Estatal de Sindicatos Médicos (CESM).

De los 8.700 profesionales que afirmaron en esta encuesta haber sido agredidos, el 60% no presentó denuncia, siendo el perfil de víctima más común el de las mujeres de entre 41 y 60 años.

La situación no mejora mucho si fijamos la vista en otros colectivos sanitarios como el de enfermería. Según el último informe elaborado por el Observatorio Nacional de Agresiones a Enfermeras y Enfermeros, uno de cada tres profesionales (33%) ha sido víctima o ha presenciado una agresión física a otro compañero. Un porcentaje que se eleva al 69% si hablamos de agresiones verbales. La mayor parte de las agresiones (un 52%) las realiza un familiar del paciente, siendo la causa principal, según este estudio, «no satisfacer sus expectativas en cuanto a tiempos de espera de pruebas realizadas», lo que concita un 41% de los casos.

Aunque no hay estadísticas disponibles, estas situaciones de violencia se viven también en otros colectivos, como el de los farmacéuticos.

Ante esta situación, el anterior Gobierno elaboró la Instrucción 3/2017 de la Secretaría de Estado de Seguridad sobre medidas policiales a adoptar frente a agresiones a profesionales de la salud, entre las que destaca la creación del Interlocutor Policial Territorial Sanitario.

En el ámbito de la Policía Nacional ocupa ese puesto el comisario Javier Galván, Jefe de la Brigada Central de Inspección e Investigación de la Unidad Central de Seguridad Privada. Según indica, el objetivo de su labor es «reducir al máximo tanto los delitos como los comportamientos incívicos producidos contra los profesionales del sector sanitario».

En cuanto a su actuación sobre el terreno, la Policía Nacional «intervendrá de dos formas: de manera preventiva, desplegando sus recursos al objeto de evitar la victimización de los profesionales sanitarios por el ejercicio de sus funciones, y de manera reactiva, ante cualquier situación delictiva o incívica que sufra este colectivo, denunciando conforme al Código Penal en el primer caso y mediante la denuncia administrativa conforme a la Ley de Seguridad Ciudadana, en el segundo», señala el comisario Galván.

Esta tarea de velar por que los profesionales sanitarios puedan realizar su trabajo sin ser víctimas de agresiones físicas o verbales es parte de la labor que llevan a cabo los encargados de la seguridad de centros hospitalarios, a la que se une la de proteger a los pacientes y a las instalaciones y equipos.

Así lo corrobora Gracia Quevedo, responsable de la Gestión del Servicio de Seguridad del Hospital Universitario de Fuenlabrada, para quien la prioridad es «mantener el orden para que los profesionales puedan realizar su trabajo con el menor riesgo posible».

Una de las claves para conseguir ese objetivo es la prevención. En opinión de Manuel Manglano, jefe de Equipo de Seguridad del Hospital Severo Ochoa de Madrid, para avanzar en este camino es fundamental «dotar al profesional de la seguridad de los equipos adecuados, formación continúa e invertir en materia de seguridad y tecnología».


Monkey Business/Shutterstock

En su opinión, también es necesario «concienciar al ciudadano y al trabajador de que tanto las medidas de seguridad como el profesional que las implanta y realiza están para hacer más cómoda su estancia en las instalaciones y velar por las posibles amenazas». ●

Texto: *E.S. Cófreces y Gemma G. Juanes*
Fotos: *Shutterstock*

Los ciberataques a equipos médicos se incrementarán durante este año

Las ciberamenazas y presiones en el sector salud van a seguir aumentando a medida que los centros médicos cuenten con más dispositivos conectados y aplicaciones web. Las tendencias en este año, según un estudio de Kaspersky, pasan por:

– Aumento de los ataques dirigidos contra equipos médicos con intención de extorsionar o afectar al servicio.

– Crecimiento en el número de ataques dirigidos al robo de información. La cantidad de datos de pacientes y de información médica que procesan y mantienen los sistemas conectados de atención médica, no para de crecer.

– Mayor número de incidentes de ransomware contra instituciones sanitarias. Esto implicará cifrado de datos y bloqueo de dispositivos.

– El perímetro corporativo es cada vez más difícil de perfilar en las instituciones médicas, donde hay un número cada vez mayor de estaciones de trabajo, servidores, dispositivos móviles y equipos conectados.

– La información sensible y confidencial transmitida entre los wearables, incluidos implantes, y los profesionales del sector sanitario, continuará creciendo como objetivo de los ciberdelincuentes a medida que su uso en diagnóstico médico, tratamiento y cuidado preventivos se incremente.

– Los sistemas estatales y locales de salud, que comparten datos e información sin cifrar de terceros, como hospitales, centros de salud, laboratorios, etc, seguirán atrayendo a los ciberdelincuentes interesados por interceptar los datos que circulan sin la protección de los firewalls corporativos.

– El creciente uso que hacen los consumidores de monitores de actividad física y salud pone a disposición de los ciberdelincuentes un importante volumen de datos personales prácticamente desprotegidos.

– Ataques disruptivos, ya sea bajo la forma de denegación de servicio o «ransomware» que simplemente destruye datos, como es el caso de Wannacry, representan una amenaza creciente para unas instalaciones médicas cada vez más digitalizadas. -

– El número cada vez mayor de estaciones de trabajo, gestión de registros electrónicos y procesos comerciales digitales presentes en cualquier organización moderna, amplía el número de objetivos potenciales.

– Por último, y no por ello menos importante, tecnologías emergentes como prótesis artificiales conectadas, implantes inteligentes para mejoras fisiológicas, realidad aumentada incorporada, etc

JAVIER GALVÁN. COMISARIO, JEFE DE LA UNIDAD CENTRAL DE INSPECCIÓN E INVESTIGACIÓN DE LA UNIDAD CENTRAL DE SEGURIDAD PRIVADA DEL CNP. INTERLOCUTOR POLICIAL NACIONAL SANITARIO.

«Con que se produzca una sola agresión a los profesionales sanitarios ya es una situación no deseada para nosotros»

REDUCIR al máximo tanto los delitos como los comportamientos incívicos que sufren los profesionales del sector de la salud es el objetivo del Interlocutor Policial Sanitario, cargo creado en 2017. Su actual responsable a nivel nacional, el comisario Javier Galván, explica en esta entrevista los retos y claves de su labor.

—¿Cuáles son las razones que han impulsado la creación de la figura del Interlocutor Policial Sanitario?

—Desde hace años los profesionales sanitarios vienen sufriendo agresiones en el ejercicio de su actividad, por lo que la Organización Médica Colegial, a través del Observatorio Nacional de Agresiones a Médicos, viene elaborando informes al respecto que les han permitido constatar esta evolución y tomar medidas para intentar erradicar dicha problemática.

Fruto de esta actividad, los profesionales de la salud consiguieron que la reforma del código penal, llevada a cabo en 2015, modifica el artículo 550 al objeto de ser considerados como autoridad los sanitarios, del ámbito público, agredidos en el ejercicio de sus funciones o con ocasión de ellas.

A su vez, la Organización Médica Colegial inició los contactos con el Ministerio del Interior al objeto de dar una respuesta a esta demanda de seguridad por parte de las Fuerzas y Cuerpos de Seguridad del Estado. Consecuencia de estos contactos fue la publicación de la Instrucción 3/2017, de la Secretaría de Estado de Seguridad, sobre medidas policiales a adoptar frente a agresiones a profesionales de la salud, por la que los operadores públicos estatales de seguridad deben llevar a cabo una serie de actividades al objeto de prevenir y reaccionar ante las agresiones a estos profesionales.

Policía Nacional ya daba una respuesta en seguridad a los profesionales de la salud desde un punto de vista preventivo y reactivo pero es, a raíz de esta Instrucción, cuando se crea la figura del Interlocutor Policial Sanitario, a nivel nacional y territorial, y se lleva a cabo una planificación estratégica de la actividad con el objetivo de reducir al máximo tanto los delitos como los comportamientos incívicos producidos contra los profesionales del sector sanitario.

Entre las acciones desarrolladas se ha podido tener un conocimiento exhaustivo de los hechos denunciados en cada ámbito competencial y su evolución, así como el estudio de las medidas a adoptar por cada plantilla policial, que está resultando efectiva.

—¿Cuáles serán sus funciones concretas?

—Lo primero que hay que decir es que la Comisaría General de Seguridad Ciudadana y, en concreto, la Unidad Central de Seguridad Privada asumen, en el ámbito de Policía Nacional la figura del Interlocutor Policial Sanitario, el cual establece, con su equipo de trabajo creado al efecto, la unidad de acción de la Policía Nacional para esta demanda de seguridad, formando, coordinando y supervisando, la actividad de los 55 Interlocutores Policiales Territoriales Sanitarios en todas las provincias y en las ciudades de Vigo, Algeciras y Gijón.

Entre sus actividades destacan:

- Mantener actualizado el catálogo de Centros Sanitarios, especificando los cambios habidos en relación a los niveles de riesgo o la variación en el número de centros.
- Mantener las relaciones institucionales oportunas con los diferentes actores del sector sanitario en aras de proporcionar una respuesta coordinada y transversal a dicho problema.
- Asesorar sobre la implantación de la figura del director de Seguridad y del departamento de Seguridad en la estructura organizativa de la Sanidad en función del riesgo donde se estime necesario.
- Informes estadísticos sobre la evolución de la criminalidad en el sector, lo que permite tener una visión real de la situación en el territorio y desarrollar los operativos preventivos por parte de las diferentes Unidades Policiales.
- Jornadas formativas para la mejora de la capacitación del personal sanitario para que sea capaz de gestionar de forma efectiva situaciones conflictivas con los ciudadanos.
- Asesorar a los gerentes o cualquier otra persona que lo solicite sobre materia de seguridad.

—¿Cómo se coordinará con los profesionales sanitarios? ¿Y con el resto de fuerzas de seguridad tanto públicas como privadas?

—Desde la puesta en marcha de la citada Instrucción 3/2017, la incesante labor institucional llevada a cabo por parte de todos los Interlocutores Policiales ha ido encaminada a establecer una vía eficaz de comunicación con los profesionales de la salud. Son numerosas las reuniones llevadas a cabo a nivel en todo el territorio nacional con los Colegios Oficiales de estos profesionales, autoridades sanitarias de la administración central y periférica, centros sanitarios, etc.

Por otro lado, se ha establecido un grupo de trabajo, en el seno de la Secretaría de Estado de Seguridad, en el que participan las Fuerzas y Cuerpos de Seguridad del Estado y donde se establece la estrategia a seguir, pautas de trabajo y, cómo no, donde se informa de los resultados obtenidos.

> «Intervenimos para evitar que se victimice a los profesionales sanitarios y para reaccionar ante cualquier delito»

—¿En qué tipo de casos intervendrá y cómo?

—La Policía Nacional interviene e intervendrá de dos formas: de manera preventiva, desplegando sus recursos al objeto de evitar la victimización de los profesionales sanitarios por el ejercicio de sus funciones, y de manera reactiva ante cualquier situación delictiva o incívica que sufra este colectivo, denunciando conforme al código penal en el primer caso y mediante la denuncia administrativa conforme a la Ley de Seguridad Ciudadana, en el segundo.

—¿De qué manera contribuirá a reducir las agresiones?

—Lo primero que tenemos que tener en cuenta es cuantificar las agresiones, dónde se producen, en qué horarios y quiénes son las víctimas. Por ello, desde julio del año pasado, se ha adaptado el sistema estadístico de criminalidad al ámbito sanitario, creando un ámbito específico de recogida de todos aquellos delitos denunciados por los profesionales sanitarios con el objetivo de tener una información exacta de la situación de las agresiones que sufren, hacer inteligencia y poder llevar a cabo una respuesta planificada y eficaz.

A su vez, se están llevando a cabo las siguientes acciones preventivas y transparentes no sólo al sector sanitario sino

a toda la sociedad con el objetivo de que esta pueda visualizar la sinergia en seguridad entre la Policía Nacional y el sector sanitario, y en concreto con nuestros médicos, enfermas, odontólogos, y demás profesionales:

• Incidiendo en la importancia de la prevención desde los propios centros sanitarios a través de la concienciación de la importancia de la comunicación no verbal, la empatía y la escucha activa. Para ello, la Unidad Central de Seguridad Privada, y en concreto el equipo del Interlocutor Policial Nacional Sanitario se ha formado con Policías Nacionales con un perfil académico en Psicología y en Trabajo Social, equipo de trabajo donde se ha planificado y organizado actividades formativas para todos los Interlocutores Policiales Territoriales encaminadas a lo anterior, contando con la participación en esta formación de unidades policiales especializadas como la Sección Operativa de Secuestros y Extorsiones, el Equipo Nacional de Negociadores y el Centro de Actualización y Especialización de la División de Formación.

• Incidiendo en la importancia de la denuncia por parte de los profesionales sanitarios agredidos, recalcando la necesidad de la denuncia para evitar la impunidad de los agresores y que vuelvan a repetir su conducta.

• Asesorando a los principales actores del sector sanitario sobre la importancia de la implantación en los centros que lo requieran de medidas de seguridad (director de Seguridad, departamento de Seguridad, etc.).

• Puesta en marcha de otras iniciativas como la aplicación ALERTCOPS, que cuenta con una opción diseñada para dar respuesta anticipada y al momento de posibles agresiones «in situ». Esta aplicación permite que en caso de necesidad, sólo se tiene que pulsar de forma repetida el botón SOS y en menos de dos segundos junto con una grabación de audio de quince segundos aproximadamente, el sistema remite la alerta al centro policial más cercano donde se recepcionará la señal y se seguirán los protocolos de respuesta establecidos.

—¿Cómo se definirá el nivel de riesgo de los centros hospitalarios?

—El nivel de riesgo de los centros sanitarios está ya definido una vez elaborado el Catálogo Nacional de Centros Sanitarios, todo ello atendiendo a factores como: medidas de seguridad previamente existentes, reiteración de agresiones sufridas en dicho Centro Sanitario, ubicación de la instalación sanitaria, número de profesionales que ejercen la actividad en esos centros, y otras circunstancias que pueden ser relevantes de acuerdo a la apreciación que hace el Interlocutor Policial Sanitario.

—¿Hay algún ámbito sanitario o geográfico donde la situación sea más grave?

—Partiendo de que con que haya una sola agresión a un profesional sanitario es ya una situación no deseada para nosotros, hay que decir que las estadísticas de la Organización Médica Colegial y las del Ministerio del Interior son coincidentes en varios parámetros como: los lugares donde se producen más agresiones y la victimización del personal, si bien hay que destacar que es evidente que los índices aumenten en aquellas provincias donde hay un mayor núcleo poblacional y en algunos territorios donde los índices de criminalidad están por encima de la media. El Grupo de Inteligencia (ISECI) de la Comisaría General de Seguridad Ciudadana una vez analizada toda la información recibida (delitos producidos en este ámbito, informaciones aportadas por los Interlocutores Territoriales y de la estructura organizativa sanitaria, elabora unos informes de inteligencia que sirven al Interlocutor Policial Nacional Sanitario para planificar actividades y marcar pautas de actuación en aquellas provincias donde se produce un mayor número de agresiones o comportamientos incívicos. ●

Texto y fotos: Gemma G. Juanes/ Emilio S. Cófreces

AlarmSpace® CCTV

by demes GROUP

¡NUEVA VERSIÓN MEJORADA DE **ALARMSPACE 2.5**!

La plataforma **más completa del mercado** diseñada para **aumentar la efectividad** del operador **de CRA y reducir el tiempo de actuación** en caso de emergencia y realizar una **vídeo-verificación inmediata** de todos sus grabadores.

HIKVISION · alhua · AirSpace CCTV · HYUNDAI · COLOSO

¡Nuevas funcionalidades!

- **Integración de las principales marcas del mercado y las plataformas CRAs más importantes**
- **Control Active X optimizado compatible con TODAS las centrarles de alarma del mercado**
- **Estabilidad total y mayor velocidad de carga/gestión con aviso de desconexiones 24/7**
- **Simplificación de la gestión y sincronización de horas**
- **El único sistema P2P Multi-marca con Watchdog**
- **Exportación de bases de datos simplificada**
- **Mejoras en el control PTZ y nueva función de control de relés**

by demes GROUP

www.bydemes.com

San Fructuoso, 50-56
08004 Barcelona
Teléfono: 934 254 960
Fax: 934 261 904
bydemes@bydemes.com

ESPAÑA
BARCELONA | MADRID | CANARIAS

INTERNACIONAL
PORTUGAL | FRANCIA | ITALIA | BENELUX
POLONIA | IRLANDA | AUSTRIA | CHINA

FERNANDO BOCANEGRA. DIRECTOR DE SEGURIDAD CORPORATIVA. SERVICIO MADRILEÑO DE SALUD. SERMAS

*«Debemos diseñar una **política uniforme** y **coordinada** para mejorar la **seguridad** en los centros sanitarios»*

Al frente de la Dirección de Seguridad Corporativa del Servicio Madrileño de Salud, Fernando Bocanegra se ha marcado el reto de mejorar la seguridad de los profesionales, pacientes y visitantes de los centros sanitarios bajo su competencia.

—Para comenzar, ¿qué objetivos se ha marcado tras su nombramiento como Director de Seguridad Corporativa del Servicio Madrileño de Salud?

—Me gustaría resaltar la importancia de la apuesta pionera de la Consejería de Sanidad de la Comunidad de Madrid, con la creación de esta Dirección de Seguridad Corporativa en el Servicio Madrileño de Salud, SERMAS. No solo recoge las propuestas de los profesionales de seguridad hospitalaria, sino que además nos adaptamos al modelo de seguridad en centros sanitarios, que parece incluirá el Real Decreto del Reglamento de desarrollo de la Ley de Seguridad Privada.

Los objetivos que nos marcamos son, lógicamente, mejorar la seguridad de los trabajadores, pacientes y visitantes de los centros sanitarios. Entiendo que para desarrollar estas mejoras, es fundamental unificar los criterios de actuación y las medidas de seguridad, tanto activas como pasivas, debemos diseñar una política de seguridad uniforme y coordinada, teniendo en cuenta, las especiales características y problemáticas de cada centro sanitario, según los diferentes factores que inciden, afluencia, grado de inseguridad, características de los edificios, servicios que se prestan, existencia de materias o productos peligrosos, etc.

—¿Cómo está estructurado el Área de Seguridad Corporativa del Servicio Madrileño de Salud? ¿Cuáles son sus funciones concretas?

—Esta Dirección de Seguridad Corporativa del SERMAS cuenta con unos meses, y estamos en el proceso organizativo. Una de las primeras decisiones, fue la de crear el Comité de Seguridad Corporativa del Servicio Madrileño de Salud, órgano fundamental compuesto por los responsables de la asistencia especializada y la asistencia primaria, facilitando que la coordinación de la seguridad sea efectiva en estos dos ámbitos, así como poder diseñar una política de seguridad uniforme, más eficaz y con los mismos criterios de actuación.

La organización con la que nos queremos dotar tendrá una estructura territorial, sin ninguna diferencia entre los dos tipos de asistencia, dividiremos la Comunidad de Madrid en siete zonas, que incluirán otras tantas Direcciones de Seguridad, situadas en centros sanitarios, que tendrán la responsabilidad de coordinar, y el día a día de la seguridad, todos los centros sanitarios, ya sean hospitales o centros de asistencia primaria, salud mental; con esto pretendemos unificar todas las medidas de seguridad, con las que contamos actualmente, pero que no den solo cobertura, por ejemplo a un hospital, sino también a los centros de su influencia, y consolidar una unidad de acción que redunde en la eficacia y mejora de la seguridad.

Por ejemplo, si en la mayoría de los hospitales contamos con un Centro de Seguridad 24 horas, los centros de asistencia primaria, deben estar conectados con este centro, tanto en visionado

de imágenes como respuesta a circunstancias que se puedan producir. Estos siete directores de Seguridad, dependerán del Departamento de Seguridad Corporativa del Servicio Madrileño de Salud, adecuándonos, como decía anteriormente, al Reglamento de la Ley de Seguridad, y a la Ley de Infraestructuras Criticas, en el que la Salud, es uno de sus sectores estratégicos.

Entre las funciones que tiene la Dirección de Seguridad Corporativa, destacar la coordinación de la implantación y actualización de los Planes de Autoprotección, de la elaboración de los pre planes de actuación de Bomberos, el impulso del cumplimiento de toda normativa exigible en materia de seguridad, la coordinación, interlocución y colaboración con las Fuerzas y Cuerpos de Seguridad del Estado y con las Policías Municipales y Locales, permanente colaboración con la Agencia de Seguridad y Emergencias de la Comunidad de Madrid, colaborar con la Dirección General de Sistemas Informáticos de la Consejería de Sanidad, en cooperación con los Servicios de Riesgos Laborales, realización de jornadas de formación permanente, en materia de seguridad.

—¿Cuáles son sus ámbitos de competencia?

—Las competencias del departamento de Seguridad Corporativa del SERMAS, son las que dota la Ley de Seguridad, para los 34 hospitales y 470 centros de asistencia primaria, con los que cuenta la Sanidad Madrileña.

—¿Qué tipo de colaboración y coordinación existe entre el área de Seguridad Corporativa y los responsables de Seguridad de los centros hospitalarios de la Comunidad de Madrid?

—Decía al principio de la entrevista, que la creación de la Dirección de Seguridad Corporativa era algo deseado

por todos los que nos venimos dedicando a la compleja seguridad en centros sanitarios, y todos estos profesionales, son los que han hecho progresar y mejorar la seguridad en este sector. Sin la aportación de estos, de organizaciones como el Observatorio de Seguridad Integral de Centros Hospitalarios, Unidad Central de Seguridad Privada de la Policía Nacional, revistas especializadas en seguridad, no estaríamos en un momento de reconocimiento de la importancia de la seguridad. No era lógico que dependiéramos de si en un centro o no, exista un director y un departamento de Seguridad, según hubiera una mayor sensibilización o que se contara con recursos o que las prioridades fueran por otro lado.

Estoy convencido, que con la creación de las siete zonas territoriales, que estarán cada una físicamente en un hospital, y que por supuesto en la mayoría de los casos serán asumidas por los actuales responsables de Seguridad, que aumentarán su responsabilidad, ya que tendrán hospitales, y centros de asistencia primaria.

No podemos contar con un director de Seguridad en cada centro, entendiendo que no sería necesario, pero creo firmemente que con esta organización territorial, y en colaboración con los servicios de mantenimiento, servicios de riesgos laborales, mejoraremos sensiblemente la eficacia en materia de seguridad.

—Teniendo en cuenta que cada instalación -hospitales, centros de asistencia primaria, etc- tiene una singularidad propia, ¿podría explicarnos cómo se articula la seguridad de estas instalaciones, y cuáles son los medios y medidas de seguridad generales que se deberían implantar?

— Lo que estamos diseñando es una seguridad «para todos», no podemos contar con una seguridad para la asistencia especializada y otra para la asistencia primaria, debemos poner en común los medios con los que contamos y darle una utilidad global, los problemas en un 70% son comunes, y los medios con los que contamos, no son siempre iguales.

Tenemos que contar con datos globales en tiempo real de las incidencias que se producen diariamente, que nos permitan la toma de decisiones de mejora en la seguridad.

Creo que debemos continuar apostando por el aumento de la videovigilancia,

asimismo debemos instalar en los ordenadores de cada trabajador, una tecla de alerta, que suponga una activación y una respuesta rápida y eficaz, debemos elaborar pre planes de actuación de bomberos, que faciliten el trabajo a los Departamento de Extinción de Incendios, hay que intensificar la instalación de puertas que limiten la intrusión, de personas ajenas a los profesionales sanitarios, en zonas señaladas.

—¿Qué riesgos y problemas se encuentra habitualmente el área de Seguridad Corporativa del Servicio Madrileño de Salud, en los centros de su competencia en materia de seguridad?

— Principalmente los riesgos y problemas que nos encontramos son los habituales que tienen los departamentos de Seguridad Corporativa de otros sectores, pero solo que en sanidad, se aumentan considerablemente, agresiones a profesionales sanitarios y trabajadores del centro, robos, tanto patrimoniales como a personas, robos en aparcamientos…, tenemos que tener en cuenta, que un centro sanitario, es un edificio abierto las 24 horas del día los 365 días del año, que recibe a decenas de miles de personas diariamente, que contamos con pacientes ingresados con movilidad reducida o nula en caso de un siniestro, con problemas de movilidad y tráfico en los accesos, donde debemos y somos extremadamente rigurosos en el cumplimiento de la Ley Orgánica de Protección de Datos y del Reglamento de la Comunidad Europea, que ha entrado en vigor recientemente.

—¿Han variado en los últimos años los riesgos y amenazas, en términos de ciberseguridad?

— Los riesgos y amenazas en ciberseguridad aumentan continuamente, pero si es verdad que la Dirección General de Sistemas Informáticos de la Consejería, con la que colaboramos asiduamente, así como las comisiones de seguridad de la información, elaboran protocolos y auditorías permanentes que están reforzando la seguridad en el SERMAS.

—¿Cuáles considera que son las claves para una seguridad satisfactoria en las instalaciones hospitalarias?

— Considero fundamental, y siempre partiendo de la base que la seguridad total no existe, la coordinación de todas las medidas, compatibilizar las inversiones que se han ido realizando estos últimos años en todos los centros y no solo en uno, y algo que parece una obviedad, pero que algunas veces se olvida, la seguridad debe estar dirigida por profesionales. Recuerdo la frase del Dr Abraho, entonces Presidente de la Federación Mundial de Hospitales, que decía: «La Seguridad mejora la calidad asistencial».

—Hace casi un año el Ministerio del Interior presentó la Instrucción 3/2017 sobre medidas policiales a adoptar frente a agresiones a profesionales de la Salud, así como la creación de la figura del Interlocutor Policial Territorial Sanitario, ¿qué cree que ha aportado esta iniciativa a los profesionales de la Salud? ¿Qué valoración haría de su primer año de implantación?

— Desde un primer momento en que la Secretaría de Estado de Seguridad, presentó la instrucción sobre medidas policiales a adoptar frente a agresiones a profesionales de la salud, entendiendo el paso adelante que suponía y lo necesaria que era la figura del Interlocutor policial, estaba seguro que no se quedaría solo en el grave problema de las agresiones, sino que se convertiría en una herramienta imprescindible de colaboración entre las Fuerzas y Cuerpos de Seguridad del Estado y las Instituciones Sanitarias. En la Dirección de Seguridad Corporativa mantenemos reuniones muy frecuentes y estamos trabajando en la realización de cursos de formación, un catálogo de recurso de seguridad, identificación de los centros más conflictivos, tanto con el Interlocutor Policial Sanitario de la Policía Nacional, como del Interlocutor de la Guardia Civil. ●

Texto y Fotos: Gemma G. Juanes.

SEGURIDAD

OPERADOR DE RPAS

DRONES

VIDEOVIGILANCIA

CONTROL DE ACCESOS

CENTRAL RECEPTORA DE ALARMAS

PROTECCIÓN CONTRA INCENDIOS

INSTALACIÓN Y MANTENIMIENTO DE SISTEMAS DE SEGURIDAD

CENTRO DE FORMACION DE SEGURIDAD

SISTEMAS INTEGRALES DE SEGURIDAD

SERVICIO DE ACUDAS Y CUSTODIA DE LLAVES

VIGILANTES DE SEGURIDAD

BUREAU VERITAS Certification

CYRASA

D.G.P. 3625

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

JOSÉ MARÍA RAMÓN DE FATA. DIRECTOR CORPORATIVO DE OPERACIONES DE VITHAS;
JOSÉ MANUEL GUILLOT. RESPONSABLE DE INGENIERÍA DE VITHAS.

«*La concienciación en **seguridad de la información** es imprescindible para minimizar los **ciber-riesgos***»

EL mantenimiento preventivo y correctivo de las instalaciones hospitalarias, así como el estricto cumplimiento normativo son para José Manuel Guillot, responsable de Ingeniería de Vithas, las claves para alcanzar una seguridad satisfactoria en los centros hospitalarios. Mientras, en esta misma entrevista, José María Ramón de Fata, director Corporativo de Operaciones de Vithas, asegura que los ciberriesgos para los centros hospitalarios no han variado en los últimos tiempos en el ámbito nacional, en lo relativo a sofisticación, pero sí de forma muy relevante en cuanto a intensidad, sobre todo en la vertiente dirigida a secuestrar información almacenada en ficheros con el objeto de solicitar un rescate.

—¿Cuál es la estructura e infraestructura actual del Área de Seguridad del Grupo Hospitalario Vithas?

— **José Manuel Guillot**: El área de Seguridad depende concretamente del área de Ingeniería donde se engloba la parte de infraestructuras e inversiones. Por tanto, todo el equipo que compone el área indicada es el referente en esta materia con el jefe de Mantenimiento e Ingeniería en cada hospital como responsable.

—¿Cuáles son las funciones concretas que lleva a cabo el Área de Seguridad?

— **JMG**: Velar por la seguridad de los usuarios y de las instalaciones de los centros, entendiendo como usuarios a pacientes/acompañantes, trabajadores y visitantes.

Hacer compatibles las medidas de seguridad con las necesidades propias del funcionamiento de las distintas áreas y secciones de los centros.

—¿Con qué medios y medidas de seguridad cuentan las instalaciones con que cuenta el Grupo Hospitalario Vithas?

— **JMG**: El Grupo Vithas está en estos momentos modelizando en función de varios parámetros sus estrategias de seguridad de cara a dar un salto de calidad en sus instalaciones. Dicho esto, evidentemente dispone de circuitos de vigilancia con conexión a central de alarmas, vigilancia presencial, controles de accesos, detección de incendios y detección de intrusión.

Por otra parte, el documento principal que aglutina los procedimientos de seguridad es el plan de autoprotección y emergencia. Con carácter diferencial del Grupo y como parte de su estrategia para la acreditación de sus centros en la JCI, se disponen además de otros procedimientos y protocolos de actuación, como por ejemplo, la seguridad ante obras, seguridad de suministros, ante emergencias/desastres, etc.

—¿Cuáles son las prioridades de seguridad y prevención de una instalación hospitalaria?

— **JMG**: La seguridad del paciente y sus familiares junto con los trabajadores, por encima de todo. En segundo lugar la de las instalaciones e infraestructuras.

—¿Cree que los usuarios de los centros hospitalarios valoran las medidas de seguridad implantadas o, sin embargo, se trata de un hecho que pasa desapercibido?

— **JMG**: Pasan desapercibidas para la mayoría de los usuarios.

—¿Cuáles considera que son las claves para una seguridad satisfactoria en las instalaciones hospitalarias?

—JMG: El mantenimiento preventivo y correctivo de las mismas y el estricto cumplimiento de la normativa.

—¿Han variado los riesgos y amenazas en los centros hospitalarios en términos de ciberseguridad?

— **José María Ramón de Fata**: Los ciber-riesgos y amenazas para los centros hospitalarios no han variado en los últimos tiempos en el ámbito nacional, en lo relativo a sofisticación, pero sí de forma muy relevante en cuanto a intensidad, sobre todo en la vertiente dirigida a secuestrar información almacenada en ficheros con el objeto de solicitar un rescate (la variante de ataque denominada ransomware). No obstante el daño causado no es significativo si se cuenta con una política adecuada de backup y recuperación de datos, todo lo cual minimiza enormemente el daño que se pretende causar, provocando eso sí molestias y retrasos puntuales.

En otros países sí que se ha incrementado la sofisticación de este tipo de ataques al orientarlos más hacia los servidores que a estaciones cliente, provocando una pérdida de servicio mucho más seria y con unos tiempos de recuperación e impacto en la organización más relevantes. Este tipo de ataque es personalizado, no de distribución masiva y por consiguiente espera un retorno económico importante. En España aún no es obligatorio reportar este tipo de incidentes (como sí lo es en otros países) por lo que no se dispone de una estadística contrastada. La introducción de la nueva reglamentación de protección de datos (GDPR) obligará a reportarlos, su impacto y las medidas que se han tomado para minimizarlo.

Finalmente, el mercado también reacciona a este tipo de amenazas con propuestas de valor que minimizan el riesgo de ataque o la cobertura posterior, como puede ser el caso de seguros específicos de cobertura de ciber-riesgos. Normalmente es el correo electrónico con diferencia el mayor vector de entrada de software malintencionado. En base a todo ello, un mejor control y especialización en el filtrado del correo entrante, junto con una estrategia de concienciación en seguridad de la información de los usuarios, son medidas imprescindibles a implementar en el corto plazo para minimizar estos riesgos. ●

Texto: Gemma G. Juanes.

Fotos: Vithas

ANTONIO PONCE ROSETE. DIRECTOR DE SEGURIDAD. HOSPITAL SON ESPASES. PALMA. (MALLORCA)

«Es prioritario establecer una **cultura de seguridad** que llegue a todos y cada uno de los **trabajadores**»

De Izquierda a derecha Toni Sánchez (Coordinador de servicios vigilancia), Cayetano Pantoja (Responsable Instalaciones CCTV, Control Accesos y Comunicaciones), y Toni Ponce, (Director de Seguridad).

LA seguridad debe entenderse en un sentido amplio como una seguridad integral, cubriendo todo el abanico de actividades diferentes involucradas en un centro hospitalario», asegura Antonio Ponce, director de Seguridad del Hospital Son Espases de Palma (Mallorca), para quien además el futuro de la seguridad en los hospitales deberá apoyarse en un elemento fundamental: la tecnología.

—¿Qué metodología de trabajo lleva a cabo el departamento de Seguridad del Hospital Universitario Son Espases de Palma (Mallorca)?

—Desde la creación del departamento de Seguridad, nuestro objetivo ha sido siempre el establecer un contacto directo con el resto de departamentos y servicios hospitalarios para planificar un marco de seguridad integral con vigencia en todo el centro. En ese sentido, tanto el Manual de Autoprotección como el Plan de Respuesta ante Catástrofes Externas (PRAHCE), nos dieron, de inicio, esa oportunidad.

El contacto con los servicios médicos, enfermería, celadores, mantenimiento…, ha sido siempre muy enriquecedor. Nuestro afán ha sido difundir una cultura de la seguridad común, en la que cada uno tiene un papel que desempeñar, como es el caso de la «Formación In Situ», en la que el departamento de Seguridad hace ver al personal, aquellas situaciones de riesgo que podrían originar una emergencia en su mismo puesto de trabajo («Como si estuviera pasando, en el lugar donde puede pasar»).

La implantación del sistema de gestión de seguridad supone un tratamiento estructurado y sistemático, en el que debe involucrarse muy directamente la dirección del centro, para que motive la participación del resto de servicios. En este sentido, podríamos definir al departamento de Seguridad del HUSE como una célula interdepartamental dirigida por un director de Seguridad que, dependiente de la Gerencia del centro, ayuda a planificar la política de seguridad a seguir, y lo hace sirviéndose del intercambio de información, el debate y la coordinación de iniciativas como principales herramientas de trabajo entre sus miembros.

—¿Qué aspectos debería contemplar un sistema de gestión de seguridad implantado en un gran centro hospitalario?

—Para conseguir una eficaz y eficiente gestión de la seguridad debe partirse de tres premisas:

-La seguridad es un elemento fundamental para la gestión del centro hospitalario.

-La seguridad forma parte inherente de la autoridad y es responsabilidad de la línea jerárquica.

-Todos somos partícipes de «la Seguridad».

La seguridad debe entenderse en un sentido amplio como seguridad integral, cubriendo todo el abanico de actividades diferentes involucradas en el centro hospitalario, entre otras: seguridad del paciente, riesgos biológicos, prevención de riesgos laborales, protección contra incendios, seguridad en las instalaciones de gases medicinales, seguridad en las instalaciones radiológicas, protección contra robo e intrusión, actos vandálicos,... de aquí se derivan el desarrollo de todos los planes específicos, como por ejemplo plan de emergencia, plan de catástrofes externas, etc.

En definitiva desarrollar un Plan de Seguridad Integral que defina la política de seguridad del centro.

Vista exterior del Hospital Universitari Son Espases.

—Hoy en día, ¿ha variado la seguridad, en cuanto a estrategia y logística, de los centros hospitalarios en los últimos años?

—La seguridad en los hospitales, sea cual sea su tamaño, ha venido evolucionando hacia criterios más amplios que los tradicionales de seguridad en el trabajo, seguridad contra incendios, contra intrusión, etc.

Esta evolución está siendo debida al alto coste y complejidad de las instalaciones, mayor número de demanda de los usuarios, desarrollo de normativa en todos los campos de la seguridad, y en general al incremento en la calidad de vida.

Si hace años no se concebía un hospital sin, por ejemplo, un eficiente Servicio de Mantenimiento, hoy día no es posible entender una eficaz Gerencia Hospitalaria sin una adecuada «gestión de la seguridad», que inevitablemente redunda en una mejor calidad de la asistencia sanitaria y genera al mismo tiempo mejores condiciones de trabajo al garantizar la seguridad de las personas (empleados, pacientes y visitantes) y la conservación del patrimonio y la imagen del centro hospitalario.

Planos Emergencia y Evacuación (505).

—¿Cuáles son las prioridades de seguridad y prevención de una gran instalación hospitalaria como es el Hospital Universitario Son Espases?

—La cultura de seguridad se define como el conjunto de valores y normas comunes a los individuos dentro de una misma organización, e implica un modelo mental compartido que posiciona la seguridad como un objetivo común a perseguir.

Lo más prioritario es darle el valor a la seguridad, establecer una cultura de seguridad que llegue a todos y cada uno de los trabajadores. Esta cultura se centra en informar, formar y prevenir, solo de esta forma se puede alcanzar una seguridad satisfactoria.

Acceso a área restringida.

—¿Cree que han cambiado los riesgos y amenazas de los hospitales sobre todo en cuanto a aspectos de ciberseguridad?

—No hay cambio en cuanto a riesgos y amenazas, lo que sí ha cambiado son los escenarios, como ya se hace referencia en la misma pregunta mencionando la ciberseguridad.

Con la ciberseguridad, estamos en la casilla de salida, y eso que los ciberataques han aumentado de forma exponencial. La facilidad de acceso a nuestras redes desde cualquier parte del mundo a través del correo electrónico, y la facilidad con la que el usuario abre cualquier correo, supone uno de los mayores riesgos en este momento. Este tipo de ataque en hospitales son mucho más problemáticos que en otro tipo de organizaciones, al poderse acceder a información muy delicada, como por ejemplo las historias clínicas.

Todavía no somos conscientes de esta problemática y lo vulnerables que somos.

Por eso, y como he comentado anteriormente, es prioritario el establecer una cultura de seguridad en la que participemos todos los trabajadores.

—¿Ha llevado a cabo el centro hospitalario mejoras en cuanto a infraestructura de seguridad en los últimos años?

—Podría decirse que desde el primer día de vida del Hospital.

Desde la puesta en servicio del Hospital en noviembre de 2010, ya se detectaron «carencias» en cuanto al dimensionamiento de los medios técnicos, además de una «inadecuada» distribución de algunos de ellos (aspectos que tenían su origen al recibir un Hospital «llave en mano» en el que no habíamos podido participar en su diseño), por lo que tuvimos que adaptarnos a las circunstancias, más teniendo en cuenta la crisis económica de esos momentos.

Nos centramos en la revisión del funcionamiento de los diferentes sistemas de seguridad, con el hospital en funcionamiento, adaptando los procedimientos de actuación ante el nuevo escenario (situaciones parecidas al hospital de origen, pero en diferente entorno), intentando que para el resto de servicios del hospital, no supusiera un cambio muy significativo (mantuvimos los números de emergencias de incendios 505, paro cardiaco 989, como ejemplo).

Para cubrir las carencias, llegamos a reutilizar instalaciones del antiguo hospital, como por ejemplo los sistemas de alarma ante una agitación/contención en las unidades de Psiquiatría de adultos e infantil, que el nuevo no disponía.

Durante los últimos años, nos hemos dedicado a la puesta en marcha y ampliación del sistema de control de accesos y cctv en áreas críticas, como por ejemplo laboratorios y edificio de investigación, Microbiología, Servicio de Radio Protección, y en un futuro próximo en aquellas zonas de mantenimiento «esenciales» para el funcionamiento del hospital.

> «Nuestro afán ha sido difundir una cultura de la seguridad común, en la que cada uno tiene un papel que desempeñar»

Centro de Control Seguridad.

SEGURO

Obtenga el mejor rendimiento y valor para la gestión de llaves y activos.

Nuestros sistemas KeyWatcher y AssetWatcher con tecnología RFID están repletos de funcionalidades y capacidades, diseñadas por expertos para proteger, controlar y rastrear sus llaves y activos.

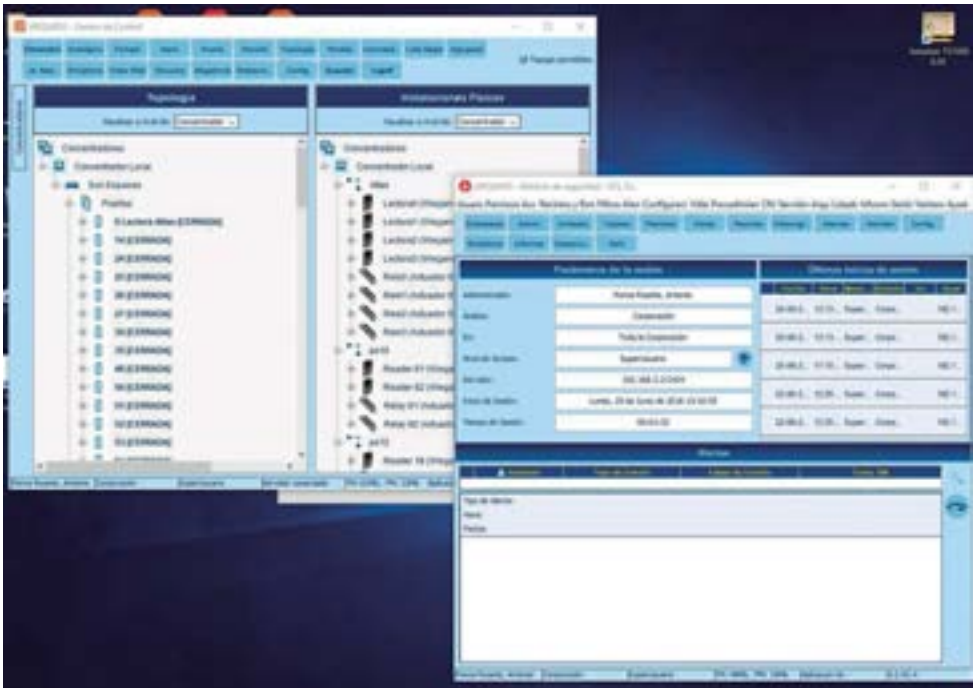
Es un ejemplo más de nuestro pensamiento abierto, que encontrará en la caja.

La puerta del producto no aparece en la imagen. Lector de huellas opcional.

Para obtener más información, visite morsewatchmans.com

MORSE WATCHMANS

piense en la caja.



Software gestión Control Accesos.

—Con una visión profesional, ¿cómo imagina el futuro de la seguridad en los centros hospitalarios?

—El futuro de la seguridad en los centros hospitalarios debe apoyarse en un elemento fundamental: la tecnología.

Las necesidades de las instalaciones hospitalarias han variado y han sido, de manera concreta, las innovaciones tecnológicas las que han hecho posible contar con equipos y sistemas que ayudan a conseguir una adecuada seguridad en los centros hospitalarios.

Además de medios técnicos, creo necesario que los hospitales cuenten con la labor de una figura que está adquiriendo un papel imprescindible en la gestión de la seguridad: el director de Seguridad al frente de un departamento de Seguridad. Esta figura debe pertenecer a la plantilla del centro, reconociéndose dicha categoría.

Además ha surgido en el escenario de la protección de estas singulares instalaciones un destacado profesional: el responsable de la oficina de Seguridad de la Información.

Creo que ambas figuras serán las encargadas de alcanzar ese nivel óptimo de seguridad imprescindible en todo centro hospitalario.

—¿Cree que todos los centros hospitalarios deberían contar con un departamento de Seguridad y un responsable a su cargo?

—Me he mostrado siempre firme defensor de la creación de departamentos de Seguridad en los hospitales españoles con un director de Seguridad de la plantilla a su cargo, en la línea de lo que defendemos como uno de los objetivos principales desde el Observatorio de Seguridad Integral en Centros Sanitarios (OSICH).

Un hospital es una pequeña ciudad donde se llevan a cabo multitud de tareas y todas ellas resultan fundamentales para conseguir el objetivo último, que es defender la salud pública. Tradicionalmente, la seguridad ha viajado a remolque, como si se tratara de una faceta subordinada, pero eso está cambiando poco a poco con el nacimiento de los departamentos de Seguridad. Los nuevos directores de Seguridad defendemos que debe ser una condición previa para que los aspectos sanitarios se desarrollen en toda su plenitud y con todas las garantías que se merecen.

El mensaje va calando, pero choca con la falta de recursos endémica que afecta a las administraciones de salud.

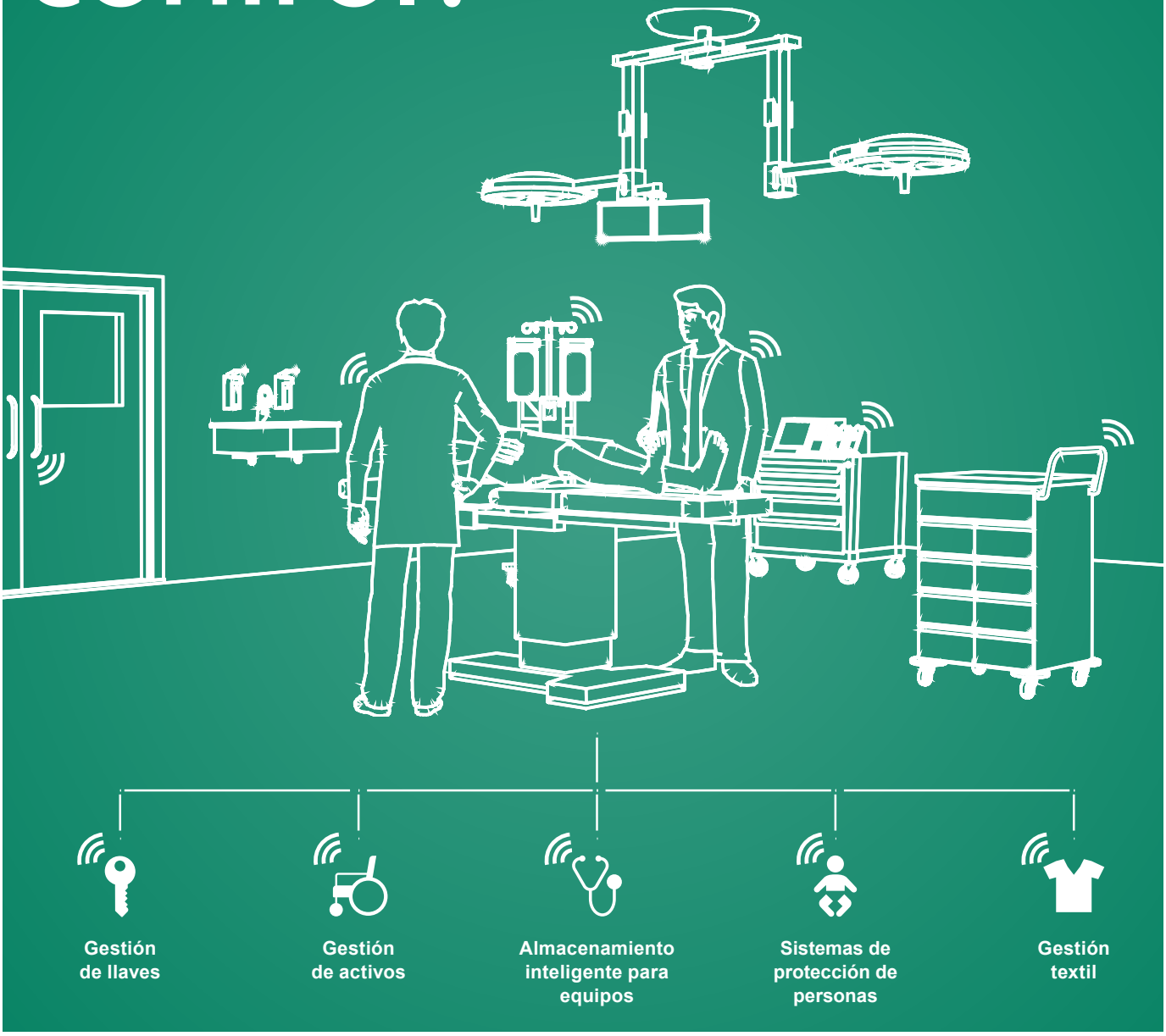
Según los datos del Observatorio Integral de Seguridad en Centros Hospitalarios (OSICH), de los aproximadamente 180 hospitales públicos españoles, no llegan a 20 los que cuentan con tal departamento de Seguridad.

El director de Seguridad es la figura responsable de la seguridad del centro sanitario, en la que esté constituido ese departamento de Seguridad, cuya dirección coordinación, supervisión y administración le compete. Nuestra figura debe ser más visible, y como he dicho en la anterior pregunta, reconocidos como categoría en plantilla. Los centros hospitalarios son instituciones de características especiales que precisan de medidas de seguridad concretas. Y nuestro departamento ha de ser una división más, integrada en la organización para dar respuesta y contrarrestar vulnerabilidades.

Creo que el departamento de Seguridad ha de tener una comunicación fluida con toda la organización y una comunicación directa con la Dirección. Como valor añadido a la organización debe estar presente y participar en los diversos comités y comisiones: comisión de obras, comité de seguridad y salud, de catástrofes externas, ...

Texto: Gemma G. Juanes.
Fotos: Hospital Son Espases

¿Tienes tus activos bajo control?



Administre sus activos y derechos de acceso de manera integral, todo perfectamente integrado en nuestro software.

Todos los activos de una empresa bajo control.

deister electronic

www.deister.com/es

DR. MARTÍN GONZÁLEZ Y SANTIAGO. DIRECTOR CORPORATIVO DE SEGURIDAD, PROTECCIÓN DE DATOS Y PRL. HOSPITALES SAN ROQUE. GRAN CANARIA.

«La **cultura de seguridad** debe hacerse extensiva a profesionales y usuarios para que los **hospitales sean entornos seguros**»

PARA comenzar, ¿podría explicar qué es Hospitales San Roque: número de hospitales, servicios que agrupa, número de empleados, etc.?

—Hospitales San Roque (HSR) está conformado por un conjunto de diversas sociedades mercantiles, cuyo Presidente es el Dr. D. Mario Rodríguez Rodríguez, empresario canario que ha logrado posicionar a la organización como la empresa líder en la prestación de servicios asistenciales de salud de la provincia de Las Palmas.

En la actualidad HSR tiene como pilares principales, un conjunto de tres centros: Hospitales San Roque en Las Palmas de Gran Canaria, fue el primero y es un centro de agudos ubicado en la ciudad de Las Palmas de Gran Canaria; Hospitales San Roque en Maspalomas, centro también de agudos, ubicado en la zona turística del sur de la isla de Gran Canaria; y el Hospital Queen Victoria, que es un centro sociosanitario de alto nivel, ubicado en una zona privilegiada de Las Palmas de Gran Canaria.

Además, HSR cuenta con varios centros médicos para consultas y diagnósticos por la imagen. En Gran Canaria el centro de García Tello para diagnóstico a través de la imagen. Otro centro en la isla de Lanzarote «Centro Médico Lanzarote», un centro médico en la zona centro de la ciudad de Las Palmas de Gran Canaria (calle Néstor de la Torre) para consultas externas, otro en Vecindario (sur de la isla de Gran Canaria, junto al aeropuerto), y otro en el archipiélago de Cabo Verde (Clínica Monte Cara).

HSR cuenta con más de 900 empleados, más de 400 camas, 13 quirófanos, 25 boxes de urgencias y 16 camas de UCI. Con nuestros centros cubrimos prácticamente todas las zonas de la isla de Gran Canaria, con una actividad de más de 12.000 ingresos, 90.000 urgencias, 11.800 intervenciones quirúrgicas, 76.000 estancias anuales, 178.000 consultas médicas y más de 300.000 pruebas diagnósticas.

Hospitales San Roque está en posesión de las ISO 9001, 14001, 27001, SICTED (Calidad Turística en Destino) y, en relación a la Seguridad y Salud de los Trabajadores[1] en un año nos certificaremos con la ISO 45000 creada en febrero del presente año y que viene a culminar el camino andado por su predecesora la OSHAS 18000 y, por último, en la cúspide de la pirámide, todo lo que tenga que ver con la Seguridad del Paciente para lo que Hospitales San Roque se está preparando para la implantación del estándar internacional de Seguridad Hospitalaria que es la Joint Comission.

—¿Cómo está estructurado el área de Seguridad?

—La seguridad en Hospitales San Roque se entiende y se estructura como realmente tiene que ser, es decir, un concepto global e integrador por la transversalidad del concepto y sin sesgos.

Por primera vez, puedo decir que las distintas Direcciones/Gerencias, así como la Dirección General de una organización hospitalaria son conscientes de la importancia del concepto de seguridad y sus responsabilidades, además de que el Director General Corporativo es un referente y experto conocedor

de esta materia. Flaquear en cualquiera de los aspectos referenciados puede llevar a cualquier organización a responsabilidades varias, como son la responsabilidad administrativa, la civil e, incluso, la penal con el consiguiente daño para la imagen corporativa de cualquier organización hospitalaria, ese intangible difícil de cuantificar, pero de consecuencias fatales para cualquier organización.

Para ello, Hospitales San Roque ha creado y dado de alta recientemente el departamento de Seguridad Corporativo ante la Dirección General de Policía con su número de registro correspondiente. Actualmente es el único hospital en Canarias que posee un departamento de Seguridad como principal medida organizativa y vertebradora sobre la que cuelgan las demás, ya sean medidas organizativas de más bajo nivel, medidas físicas, técnicas, humanas, etc.

La Dirección del Área Corporativa de Seguridad está estructurada en tres grandes subáreas que son:

- Seguridad Hospitalaria.
- Protección de Datos.
-Prevención de Riesgos Laborales con un Servicio de Prevención Mancomunado que da soporte a Hospitales San Roque.

—¿Cuáles son las funciones específicas que lleva a cabo el departamento?

—Todas las que tienen cabida en el departamento Corporativo para garantizar una adecuada Seguridad y Protección Integral, tanto de las personas, así como del patrimonio de la organización y sus distintos hospitales y centros de trabajo, entre ellas destacamos:

- Coordinación y canal de comunicación de las relaciones[2] de Hospitales San Roque con las Fuerzas y Cuerpos de Seguridad en lo que respecta a informaciones bidireccionales y consultas y, en su caso, con Protección Civil.

-Garantizar el buen funcionamiento de los servicios, tanto asistenciales como de apoyo o Servicios Auxiliares en lo que respecta a la transversalidad y globalidad del concepto de Seguridad Hospitalaria.
-Todo el ámbito competencial legal que las distintas leyes y normativas atribuyen al director de Seguridad[3] que ha de estar al frente de un departamento de Seguridad.

—Teniendo en cuenta que cada hospital tiene una singularidad concreta, ¿podría indicarnos a grandes rasgos los medios y medidas de seguridad con que cuentan estas instalaciones hospitalarias?

—Grosso modo y sin entrar en detalle con el objeto de no comprometer la seguridad de nuestra organización, tenemos implantadas todas las medidas organizativas, desde el departamento de Seguridad hasta los distintos protocolos o procedimientos para cada caso, muchos de esos protocolos, así como el Plan Integral de Seguridad (PIS) se están actualizando y revisando para una ulterior y adecuada implantación en la que se buscan las distintas sinergias para ello.

Destacamos, en líneas generales, los Medios Técnicos Activos; Detectores anti intrusión en los que se combinan varios sistemas de detección; Circuito Cerrado de Televisión con grabación permanente de imágenes en las distintas zonas hospitalarias, zonas restringidas y zonas críticas, así como en otras zonas «sensibles»; Conexión y Sistemas de Alarma al Puesto Permanente de Seguridad (PPS) con su armado y desarmado tras rondas de verificación y comprobación de seguridad. Servicio de Vigilancia humana llevado a cabo por Vigilantes de Seguridad habilitados y con la formación específica en Seguridad Hospitalaria, que efectúan controles de accesos, control perimetral, control de estacionamientos exteriores, control de paquetería y mercancías, control de los sistemas de seguridad, rondas internas de seguridad, control de llaves, actuación ante riesgos excepcionales, etc.

—¿Qué riesgos y problemas se encuentra el director de Seguridad de un centro hospitalario como los que tiene Hospitales San Roque?

—Todos los riesgos inherentes a un centro complejo que a la par Infraestructu-

ra Crítica, además de la necesidad de conocer lo que supone el concepto de Seguridad Hospitalaria, concepto que yo entiendo y defino, (y así lo recojo en la segunda Tesis Doctoral que estoy realizando), como la condición y la garantía de que los trabajadores, enfermos, visitas, acompañantes, proveedores de servicios, así como infraestructura, instalaciones, información y datos, tecnología, dotación y equipamiento estén libre de todo tipo de riesgos que les son inherentes per se. La Seguridad Hospitalaria integra la suma de otras «subseguridades» que son: Seguridad Estructural, Seguridad Física, Seguridad Lógica[4], Seguridad Contraincendios, Seguridad Industrial (instalaciones), Seguridad Biológica o Bioseguridad, Seguridad Alimentaria (aunque para ser más exactos hemos de referirnos también a la Tecnología de los Alimentos), Seguridad Medioambiental, Seguridad y Salud Laboral para que revierta todo en un último punto que es la Seguridad del Paciente[5].

Uno de los principales problemas es el poder dar una protección y seguridad adecuada sin que esto suponga una merma o un impedimento para el normal desarrollo de la actividad asistencial hospitalaria. Siempre hay que buscar un punto de encuentro, una entente o equilibrio entre la seguridad y la operativa en cuanto a la gestión diaria, tanto de los Servicios Asistenciales, de los Servicios Centrales, como el resto de servicios de apoyo o Servicios Generales. Si una medida de seguridad supone un lastre en la dinámica diaria, porque la ralentiza, no es ni conveniente ni efectivo por lo que habrá estudiar, buscar e implementar otras medidas alternativas que garanticen un alto nivel de seguridad.

Otro de los aspectos es la búsqueda de las adecuadas sinergias entre otros departamentos que han de ir siempre de la mano, es decir, las Tecnologías de la Información y Comunicación (TIC), crear puentes desde la integración y evitar la confrontación, desde el punto de vista de la Seguridad como concepto en el más amplio sentido del término. Para ello el director de Sistemas o de Informática ha de ir de la mano del director de Seguridad como de la dirección de Comunicación, e incluso, con el director de Ingeniería (en lo que respecta a la Seguridad de las instalaciones) en lo que configuraría una base perfecta sobre el que ha de descansar cualquier aspecto relacionado con la Seguridad y la Protección Integral de la organización.

Retos y estrategia de seguridad

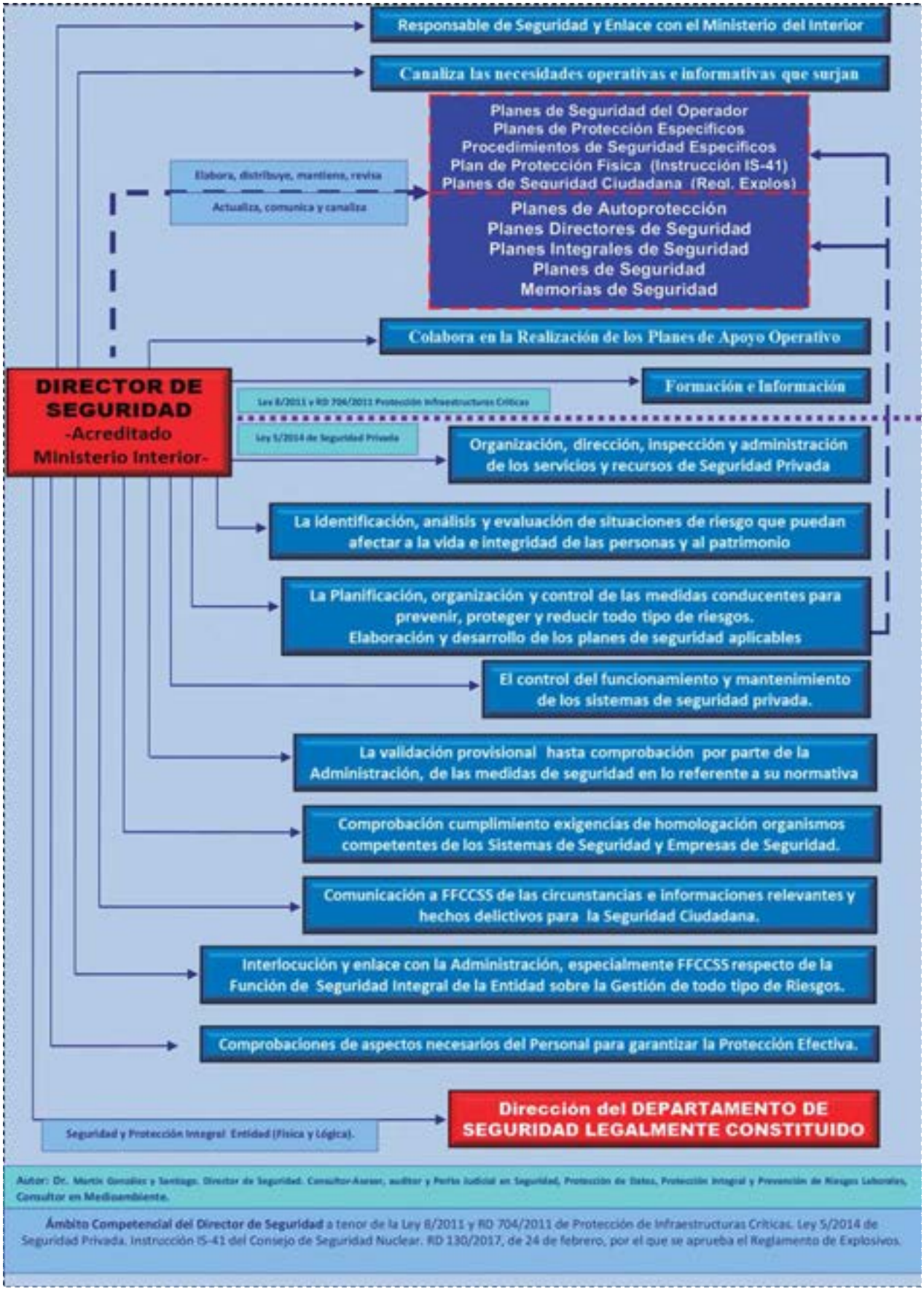
¿Qué retos debe asumir un director de Seguridad actualmente a la hora de implantar una estrategia de seguridad, en este caso, en el ámbito sanitario?

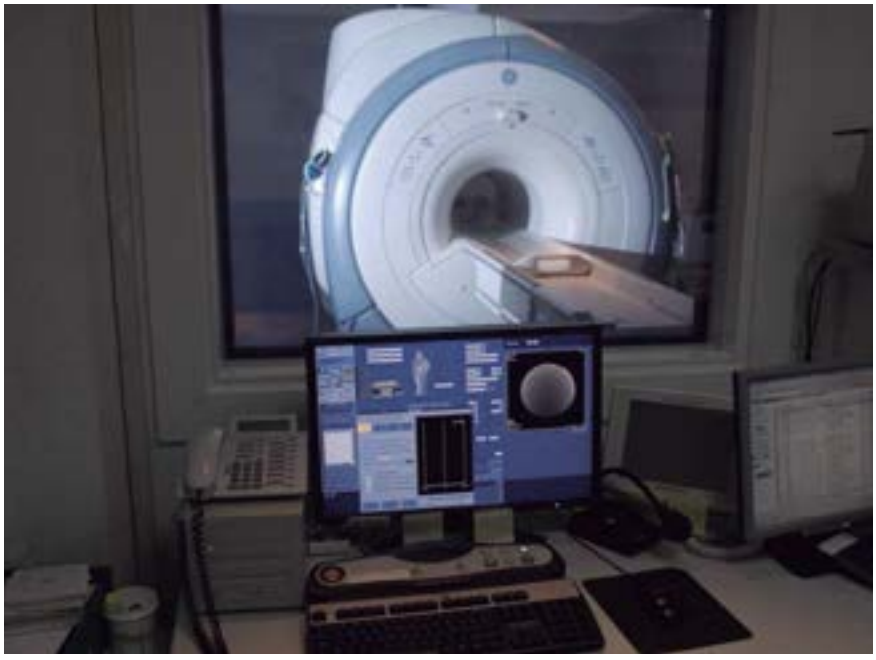
—Precisamente, liderar esa estrategia, contagiar esa necesidad de Seguridad con mayúsculas, motivar, transmitir, compartir y buscar sinergias, aliados, colaboradores que sepan y empaticen con la importancia del concepto, que como bien decía Maslow[6] es la necesidad más importante tras cubrir todas las necesidades fisiológicas sobre la que construir otras más elevadas. En una organización como Hospitales San Roque en la que la Alta Dirección y el personal está muy implicado hace que todo sea más «fácil» dentro de lo que supone el término cuando hablamos de no sólo quedarnos en el estricto cumplimiento legal, huimos de la mediocridad, sino, muy al contrario, al igual que el resto de las actividades asistenciales sanitarias, nuestra meta, nuestro objetivo primordial es la búsqueda de la excelencia. La organización quiere, todos queremos (y así será sin ningún género de dudas), ser un referente en Canarias no solo en cuestiones asistenciales, en las que ya somos líderes según el monitor de reputación sanitaria, sino también en Seguridad Hospitalaria. Estamos trazando el rumbo hasta llegar a ese destino. Siempre he pensado que hay un orden gradatorio y escalable y es que, sin seguridad no puede haber calidad e, incluso, calidad asistencial, y sin calidad asistencial no se puede ser excelente, pero, para eso, toda la organización tiene que estar implicada, todas las piezas de la maquinaria y el engranaje tienen que ir al unísono. Yo sólo entiendo dos formas de ser, mediocres y excelentes y, reitero, Hospitales San Roque busca con cada paso, la excelencia.

Western Digital®

MUCHO MÁS QUE VIDEOVIGILANCIA

LA PERFECTA TARJETA microSD™ OPTIMIZADA PARA VIDEOVIGILANCIA


Responsable de Seguridad y Enlace con el Ministerio del Interior
Canaliza las necesidades operativas e informativas que surjan
Planes de Seguridad del Operador
Planes de Protección Específicos
Procedimientos de Seguridad Específicos
Plan de Protección Física (Instrucción IS-41)
Planes de Seguridad Ciudadana (Regl. Explos)
Planes de Autoprotección
Planes Directores de Seguridad
Planes Integrales de Seguridad
Planes de Seguridad
Memorias de Seguridad
Elabora, distribuye, mantiene, revisa
Actualiza, comunica y canaliza
Colabora en la Realización de los Planes de Apoyo Operativo
DIRECTOR DE SEGURIDAD
-Acreditado Ministerio Interior-
Formación e Información
Ley 8/2011 y RD 704/2011 Protección Infraestructuras Críticas
Ley 5/2014 de Seguridad Privada
Organización, dirección, inspección y administración de los servicios y recursos de Seguridad Privada
La identificación, análisis y evaluación de situaciones de riesgo que puedan afectar a la vida e integridad de las personas y al patrimonio
La Planificación, organización y control de las medidas conducentes para prevenir, proteger y reducir todo tipo de riesgos.
Elaboración y desarrollo de los planes de seguridad aplicables
El control del funcionamiento y mantenimiento de los sistemas de seguridad privada.
La validación provisional hasta comprobación por parte de la Administración, de las medidas de seguridad en lo referente a su normativa
Comprobación cumplimiento exigencias de homologación organismos competentes de los Sistemas de Seguridad y Empresas de Seguridad.
Comunicación a FFCCSS de las circunstancias e informaciones relevantes y hechos delictivos para la Seguridad Ciudadana.
Interlocución y enlace con la Administración, especialmente FFCCSS respecto de la Función de Seguridad Integral de la Entidad sobre la Gestión de todo tipo de Riesgos.
Comprobaciones de aspectos necesarios del Personal para garantizar la Protección Efectiva.
Dirección del DEPARTAMENTO DE SEGURIDAD LEGALMENTE CONSTITUIDO
Seguridad y Protección Integral Entidad (Física y Lógica).
Autor: Dr. Martín González y Santiago. Director de Seguridad. Consultor-Asesor, auditor y Perito Judicial en Seguridad, Protección de Datos, Protección Integral y Prevención de Riesgos Laborales, Consultor en Medioambiente.
Ámbito Competencial del Director de Seguridad a tenor de la Ley 8/2011 y RD 704/2011 de Protección de Infraestructuras Críticas. Ley 5/2014 de Seguridad Privada. Instrucción IS-41 del Consejo de Seguridad Nuclear. RD 130/2017, de 24 de febrero, por el que se aprueba el Reglamento de Explosivos.



—¿Cree que los usuarios de los centros hospitalarios valoran las medidas de seguridad implantadas o, por el contrario, se trata de un hecho que pasa desapercibido?

—Creo que los usuarios cada vez perciben más positivamente la labor de los profesionales y las medidas de seguridad que se implantan en los hospitales. No obstante, precisamente esas medidas de seguridad en circunstancias normales pasan totalmente desapercibidas. Es sólo en el momento en el que ocurre una incidencia o una emergencia, cuando realmente se valora la implementación de dichos sistemas, se valora la capacidad de resolución, efectividad y procedimientos implantados por los departamentos de Seguridad.

Al hablar de Seguridad Hospitalaria nos encontramos ante una serie de riesgos heterogéneos que van desde los Riesgos de Carácter Natural hasta los Riesgos Antrópicos[7] entre los que destacan Los Riesgos Antrópicos de Carácter Antisocial, Riesgos Antrópicos de Carácter Estructural, Riesgos Antrópicos de Carácter Laboral, Riesgos Antrópicos Mixtos de Carácter Tecnológico y Laboral, Riesgos Antrópicos de Carácter Tecnológico, Riesgos Antrópicos Asociados a la Actividad o al Uso, Riesgos Antrópicos de Carácter Organizacional, Riesgos Antrópicos Mixtos de Carácter Antisocial y Tecnológicos, etc.

La cultura y la política de seguridad debe de hacerse extensiva no sólo a los Directores de Área, Jefes de Servicio o Gestores Hospitalarios, sino a todos los profesionales (indistintamente de su categoría profesional) y a usuarios con el objeto de que los hospitales sean «entornos seguros» o al menos más seguros sabiendo todos que la seguridad absoluta no existe.

—¿Cuáles son las prioridades de seguridad y prevención de una gran instalación hospitalaria como Hospitales San Roque?

—Mire usted, como hemos comentado con anterioridad, en Hospitales San Roque entendemos la seguridad como concepto global e integrador. La Seguridad Hospitalaria integra otras «subseguridades» que son:

-Seguridad Estructural.
-Seguridad Física.
-Seguridad Lógica.
-Seguridad Contraincendios.
-Seguridad Industrial (instalaciones).
-Seguridad Alimentaria y Tecnología de los Alimentos.
-Seguridad Biológica o Bioseguridad.
-Seguridad Medioambiental.
-Seguridad y Salud Laboral.
-Seguridad del Paciente.

La Seguridad Hospitalaria debe de integrar cada una de las seguridades anteriormente reflejadas porque todas ellas son importantes per se, y porque una de las premisas que yo sigo en materia de seguridad es que «Todo sistema es tan fuerte como su eslabón más débil».

—¿Cree que todos los centros hospitalarios deberían contar con un departamento de Seguridad y un responsable a su cargo?

—Mire, no sólo lo creo, lo afirmo. Si lo obviara sería hacer un ejercicio de cinismo y viviría en un universo paralelo e irreal ante la complejidad que exige dar seguridad y una protección integral en un hospital.

Existe una Ley de Infraestructuras Críticas, la Ley 8/2011 de Protección de Infraestructuras Críticas, así como un real decreto, el RD 704/2011 que la desarrolla. Ya se articula en esos mencionados preceptos legales la obligatoriedad de crear un departamento de Seguridad con un Director Habilitado por el Ministerio del Interior al frente en cualquiera de los doce sectores de actividad que dicha Ley recoge y, el sector hospitalario es uno de esos sectores. La Ley es de 2011 y estamos en la recta final de 2018. No seríamos ni responsables ni proactivos en materia de Seguridad si no nos anticipáramos y esperáramos sentados a que se realice la reunión sectorial que hace años tenía que haberse desarrollado y que la administración o los distintos agentes[8]que intervienen para la protección de Infraestructuras Críticas van retrasando una y otra vez. Ya es necesario el Plan Estratégico Sectorial en Hospitales para que, pos-

teriormente los Operadores Críticos a través de los Directores de Seguridad que estén al frente de una Infraestructura Crítica y una vez designados por el CNPIC como tales, puedan desarrollar el Plan de Seguridad del Operador y el Plan de Protección Específico que ha de ser validado por la Secretaría de Estado de Seguridad y que vendrá a complementarse con el Plan de Apoyo Operativo que las distintas Fuerzas y Cuerpos de Seguridad han de elaborar, pero con la colaboración del Director de Seguridad de la Infraestructura como experto conocedor de los riesgos inherentes a su instalación.

También hay más normativa que recoge esa obligatoriedad de constituir un departamento de Seguridad tal y como consta en una Instrucción que emana de la máxima autoridad nuclear en España, el Consejo de Seguridad Nuclear, esa Instrucción, la IS-41, también exige la constitución y la creación del departamento de Seguridad para dar una adecuada protección en aquellos hospitales que puedan utilizar fuentes radioactivas. Para ello, el director de Seguridad ha de elaborar un Plan de Protección Física frente a fuentes radioactivas e implementar una serie de medidas de seguridad.

En ese mismo sentido, ya se expuso el borrador del nuevo Real Decreto que desarrollará la Ley 5/2014 de Seguridad Privada y que establece que, en el Sector Sanitario, los Hospitales han de constituir un departamento de Seguridad con un director de Seguridad habilitado por el Ministerio del Interior al frente.

En cualquier caso, el director de Seguridad ha de actuar no sólo como un «Gerente de Riesgos» en relación a todas las funciones competenciales que legalmente tiene atribuidas, también ha de hacerlo como un compliance en la materia objeto de su responsabilidad. Debe orquestar toda la legislación y normativa que le es de referencia

vertebrando, estructurando cada área, dirigiéndola y gestionándola.

Además de lo anteriormente expuesto y en atención a la necesidad de crear y configurar los departamentos de Seguridad en hospitales quiero recordar que el Plan de Prevención y Protección Antiterrorista (PPPA) del Sistema Nacional de Alerta Antiterrorista en España, integra cinco niveles de amenaza terrorista y que actualmente estamos en el nivel de alerta 4 (NAA[9]). Tampoco hemos de olvidar los ciberataques sufridos hace escasamente poco tiempo (ransomware). Concluyo, pues, que negar esa obligatoriedad y esa necesidad en cuanto a la creación de los departamentos de Seguridad es hacer demagogia y desconocer no sólo la realidad sino la complejidad del Sector Hospitalario como Centros Complejos e Infraestructuras Críticas.

1.- Si se garantiza una adecuada política sobre la Seguridad y Salud de los Trabajadores, el Hospital es, sin ningún género de dudas más eficaz y eficiente, alcanzando todos los objetivos propuestos además de conseguir las adecuadas sinergias para garantizar el fin último de cualquier hospital como organización asistencial (independientemente de si es de titularidad pública o privada), limitando los «efectos adversos», es decir, garantizando siempre la Seguridad del Paciente.

2.- Todo ello a tenor de la Ley 8/2011 y RD 704/2011 de Protección de Infraestructuras Críticas, así como el artículo 36 de la Ley 5/2014 de Seguridad Privada.

3.- Ver Diagrama de Flujo de Datos Anexo al presente artículo en relación al ámbito competencial legal del Director de Seguridad.

4.- Se incluyen aquí se refiere a la seguridad en el uso de software y de los sistemas, la protección de los datos, procesos y programas, así como la del acceso ordenadores y privilegios de los usuarios en el acceso a la información. Hospitales San Roque posee la Certificación ISO 27000 de Seguridad de la Información.

5.- En relación a la Seguridad del paciente todo ello independientemente del modelo de certificación normalizado que se quiera implantar en la organización.

6.- La pirámide de Maslow o Jerarquía de las Necesidades es una teoría psicológica propuesta por Abraham Maslow que formula una jerarquía de necesidades humanas y defiende que conforme se satisfacen las necesidades básicas se pueden ir alcanzando otras más elevadas.

7.- Antrópico, del griego ἀνθρωπικός -anthropikós- humano; Son todos aquellos riesgos originados o modificados por la actividad humana.

8.- Secretaría de Estado de Seguridad, Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC), Ministerios y organismos integrados, Delegaciones del Gobierno, Comunidades Autónomas, Comisión Nacional para la Protección de las IC, Grupo de Trabajo Interdepartamental para la protección de las IC y por último los Operadores Críticos.

9.- Acrónimo de Nivel de Alerta Antiterrorista.

Texto: Gemma G. Juanes.

Fotos: Hospitales San Roque

PYCSECA
seguridad

PYCSECA SEGURIDAD, dispone de los más modernos medios técnicos necesarios para recibir correctamente las señales emitidas desde los sistemas de seguridad del usuario, verificándolas y gestionándolas, en caso necesario por los servicios de acuda al salto o bien por las fuerzas y cuerpos de seguridad del estado, según sea el tipo de la señal.

Instalación y Mantenimiento de sistemas de Seguridad

- Alarmas de intrusión.
- Sistemas de detección y extinción de incendios.
- Control de Accesos.
- C.C.T.V.
- Custodia de llaves.
- Servicio rondas y verificación de alarmas.

Dos centrales Receptoras Barcelona / Alicante

Disponemos de dos centrales receptoras totalmente independientes y funcionando en "Backup"

www.pycseca.com / www.pycsecaproyectos.com

Atención 24h. 902 402 700

Centro de Control 24h.

Destinado a la operatividad de nuestros servicios ofrece una atención rápida a nuestros clientes, dando solución rápida a cualquier incidencia.

Infórmese...

Custodia de llaves.

De acuerdo a la norma BS7499, nos aseguramos de que las llaves no se puedan extraer individualmente o en conjunto a menos sin su autorización.

Infórmese...

Atención personalizada.

PYCSECA Seguridad desea proyectar la Calidad y la Seguridad laboral en los servicios que ofrece basándose en las expectativas y necesidades de cada cliente.

Infórmese...

Delegaciones

Barcelona (Padilla nº 228) Madrid (Isable Colbrand nº 10/12 Alicante (Capitán Hernández Mira nº 1)
Palma de Mallorca (Almirante Oquendo nº 8) Valencia (Nicolás Estévanez nº 5) Murcia (Pio XII nº 47 bajos)
Málaga (Pico de las palomas nº 11 local45) Sevilla (Parsi 13 nº 28)

Centros de Trabajo

Girona - Tarragona - Lérida - Huesca - Zaragoza - Teruel - Castellón - Ibiza - Valladolid - Segovia - Zamora - Elche

MANUEL MANGLANO ANTÓN. JEFE DE EQUIPO DE SEGURIDAD. HOSPITAL SEVERO OCHOA. MADRID.

«La clave de la **prevención** es dotar al **profesional de** equipos adecuados, **formación e invertir en tecnología**»

CREO que falta mucho para concienciar al ciudadano y al trabajador que tanto las medidas de seguridad, y el profesional que las implanta y realiza, están para hacer más cómoda su estancia en las instalaciones y velar por las posibles amenazas», así lo asegura Manuel Manglano Antón, jefe de Equipo de Seguridad del Hospital Severo Ochoa de Madrid, quien en esta entrevista explica a nuestra publicación, entre otros aspectos, cuáles son los elementos clave para gestionar la seguridad de un centro hospitalario.

—¿Cuál es la estructura e infraestructura actual del Área de Seguridad del Hospital Severo Ochoa?

—El departamento de Seguridad depende y se compone de la Dirección de Gestión, una Jefa de Personal Subalterno y un Jefe de Equipo. Con una plantilla de vigilantes de seguridad que conoce ampliamente el hospital en los diferentes aspectos, para el desarrollo de sus funciones específicas y solución de los problemas planteados.

Una estructura que cuenta con los medios necesarios para desempeñar su específica función, así como también de medios y medidas de seguridad concretos.

—¿Cuáles son las funciones concretas que lleva a cabo el Área de Seguridad?

—Desde el departamento de Seguridad trabajamos constantemente para prevenir cualquier daño o amenaza que vivimos día a día y dar tranquilidad tanto a usuarios como a personal sanitario para que puedan desarrollar su trabajo con toda tranquilidad, dando cumplimiento a la legislación vigente y a nuestra Ley de Seguridad Privada.

—¿Cuál es la operativa diaria que desempeña el área de Seguridad, junto a su equipo?

—Teniendo en cuenta que cada día es distinto nos encontramos con varias situaciones a resolver.

Principalmente nos centramos en las zonas más débiles del hospital, haciendo hincapié en la realización de rondas, verificando las puertas de emergencias, sistemas contraincendios, bies, extintores, salidas y recorridos de evacuación en caso de alarma para obtener y dar una respuesta inmediata.

Sin olvidar los accesos de urgencias generales y materno infantil por la cantidad de usuarios que lo utilizan.

Además, estamos en constante comunicación con el CCTV, por si existiese cualquier tipo de amenazas, posibles hurtos en la zona de parking y vandalismo.

—¿Con que medios y medidas de seguridad cuentan las instalaciones el Hospital Severo Ochoa?

—Actualmente contamos con una serie de medios técnicos y físicos, así como un adecuado mantenimiento.

Contando con un centro de control CCTV con recursos humanos profesionales y cualificados 365 días del año 24 horas, que cuenta con 62 cámaras tanto fijas como domos, sistema de accesos de control mediante tarjeta (Farmacia, Admisión, etc.). Varios sistemas de alarma anti-pánico, puestos en zonas más expuestas y sensibles al personal sanitario.

Control de acceso a vehículos mediante barrera e identificación.

Una central de las alarmas de protección contra incendios.

Identificación de alarmas de gases medicinales.

Recepción de llamadas de los distintos ascensores para atender a personas encerradas o avería.

Alarma directa de una de las plantas más delicadas, Psiquiatría.
Contando con planes de emergencia y protocolos concretos de actuación.

—¿Qué riesgos y problemas se encuentra el jefe de Seguridad en el desempeño de sus funciones en un gran centro hospitalario como el de las características del Hospital Severo Ochoa?

—El riesgo en este tipo de centros hospitalarios no descansa ya que en el transcurso del día se mueven muchos usuarios con distintas intenciones.
Pero gracias al trabajo diario que desarrolla el departamento de Seguridad, en cuanto a delincuencia, hurtos en todas las instalaciones y usuarios queriéndose saltar las normas del centro, tenemos un índice muy bajo. Ya que se resuelven con profesionalidad y protocolos establecidos. Siendo los últimos los que nos encontramos más frecuentes.

—¿Cuáles son las prioridades de seguridad y prevención de una instalación hospitalaria?

—La prioridad del departamento de Seguridad es terminar nuestros turnos con las menores incidencias, minimizando todo tipo de daños.
Sin duda la clave para avanzar en la prevención en materia de seguridad es dotar al profesional de la seguridad, de los equipos adecuados, formación continúa e invertir en materia de seguridad y tecnología.

—¿Cree que los usuarios de los centros hospitalarios valoran las medidas de seguridad implantadas o, sin embargo, se trata de un hecho que pasa desapercibido?

—Teniendo en cuenta que entre los usuarios de un centro hospitalario, hay un gran abanico de edades, no todos ven al profesional y las medidas de seguridad implantadas como un pilar fundamental.
Creo que falta mucho para concienciar al ciudadano y al trabajador que tanto las medidas de seguridad y el profesional que las implanta y realiza, están para hacer más cómodo su estancia en las instalaciones y velar por las posibles amenazas.

—¿Cuáles considera que son las claves para una seguridad satisfactoria en las instalaciones hospitalarias?

—Teniendo en cuenta que la seguridad total no existe ya que hoy en día hay nuevas tecnologías, terrorismo, vandalismo, etc., la prioridad es minimizar al máximo los daños, dar una respuesta en tiempo y forma, utilizando las herramientas que tenemos a nuestro alcance, y al mismo tiempo hacer partícipes y sensibilizar a los ciudadanos y trabajadores del centro hospitalario de los riesgos que nos amenazan constantemente, permitiéndo anticiparnos a cualquier emergencia.

Texto: Gemma G. Juanes.
Fotos: Hospital Severo Ochoa

GRACIA QUEVEDO. RESPONSABLE DE LA GESTIÓN DEL SERVICIO DE SEGURIDAD. HOSPITAL UNIVERSITARIO DE FUENLABRADA. MADRID

*«La prioridad es que los **profesionales** trabajen con el **menor riesgo posible**»*

VELAR porque los profesionales sanitarios puedan realizar su trabajo asumiendo el menor riesgo posible es el objetivo prioritario de la estrategia de seguridad en el Hospital Universitario de Fuenlabrada, en Madrid.

—¿Cuál es la estructura e infraestructura actual del Área de Seguridad del Hospital Universitario de Fuenlabrada?

—El Servicio de Seguridad del Hospital depende del Área de Servicios Generales y Hostelería. Gracia Quevedo administrativo del Área, es la persona que lleva directamente este Servicio.

El personal de seguridad pertenece a una empresa externa, la cual es elegida mediante concurso público.

Por otra parte el Servicio de Seguridad está compuesto por 4 vigilantes 24 horas más un responsable de equipo.

—¿Cuáles son las funciones concretas que lleva a cabo el Área de Seguridad del centro?

—En este hospital junto con responsabilidades de carácter general sobre las parcelas, locales y bienes situados en ellas, incluido los exteriores dentro del recinto hospitalario, se les ha encomendado la responsabilidad del control de llaves del hospital y del mortuorio, además de formar parte de la estructura de autoprotección.

—¿Con qué medios y medidas de seguridad cuentan las instalaciones del Hospital Universitario de Fuenlabrada?

—El hospital, además de los vigilantes físicos, cuenta con medios de seguridad como son el circuito cerrado de televisión con unas 100 cámaras, sistemas de control de acceso, detectores magnéticos, volumétricos, etc.

—¿Qué riesgos y problemas se encuentra el responsable de Seguridad en el desempeño de sus funciones en un gran centro hospitalario como es el Hospital Universitario de Fuenlabrada?

—Uno de los mayores problemas es el hacer respetar las normas dentro del hospital, facilitando la estancia de pacientes y familiares, y permitiendo que el trabajo de los profesionales se realice con más efectividad. Muchas veces los usuarios del centro no son conscientes de los riesgos que implican determinadas acciones y hay que estar recordando verbalmente y con cartelería distribuida por el todo el centro, las normas hospitalarias.

—¿Cuáles son las prioridades de seguridad y prevención de una instalación como el Hospital Universitario de Fuenlabrada?

—Las prioridades de Seguridad son mantener el orden para que los profe-

sionales puedan realizar su trabajo con el menor riesgo posible. Con respecto a las instalaciones se realizan rondas por parte del personal de Seguridad, para ver o detectar incidencias como: roturas o desperfectos, deterioros, alteración del orden público, etc. y tomar las medidas necesarias para que se solucione lo antes posible.

—¿Cree que los usuarios de los centros hospitalarios valoran las medidas de seguridad implantadas o, sin embargo, se trata de un hecho que pasa desapercibido?

—Es un hecho que pasa inadvertido, el que las cosas estén en su sitio, no haya alteración del orden, no sucedan problemas en el parking, es algo que nadie es consciente de que cuando todo funciona bien, es porque existe un grupo de personas detrás que hacen que sea así y no de otra manera.

—¿Cuáles considera que son las claves para una seguridad satisfactoria en las instalaciones hospitalarias?

—La información y comunicación de los distintos procedimientos del hospital a los vigilantes y que estos cumplan con sus funciones llevando a cabo el plan operativo de la dirección; puestos fijos asignados como son el hall principal y urgencias y que consideramos que son vitales para que las personas que entran al hospital perciban la seguridad, y que en un momento determinado en caso de ocurrir cualquier alteración del orden o incidencia, puedan recurrir de manera inmediata al vigilante más cercano, y estos puedan resolver el problema existente o acudir a quien pueda resolverlo. Muy importante y vital para el control de la mayoría de las zonas del hospital es el circuito cerrado de televisión, donde hay un vigilante físico 24 horas, en el que si percibe algo anómalo, lo comunique al resto de compañeros, para que puedan personarse o enviar a quien corresponda para solucionar dicha incidencia. ●

> «Muchas veces, los usuarios del hospital no son conscientes del riesgo que implican determinadas acciones»

Texto: Gemma G. Juanes.
Fotos: Hospital de Fuenlabrada

AGUSTÍN RODRÍGUEZ RODRÍGUEZ. RESPONSABLE DE SEGURIDAD. HOSPITAL VIRGEN DE LA POVEDA. VILLA DEL PRADO. MADRID

«La base de la **seguridad** es la **prevención**»

ES obligatorio cumplir con los reglamentos y todas las disposiciones legales dirigidas a crear un ambiente de trabajo seguro y garantizar el bienestar de todos los pacientes, trabajadores y visitas en materia de seguridad, y es importante contar con el compromiso y apoyo de la Gerencia, Comité de Salud Laboral y Agentes Sociales», explica Agustín Rodríguez Rodríguez, responsable de Seguridad del Hospital Virgen de la Poveda (Villa del Prado. Madrid), quien en esta entrevista explica, entre otros aspectos, los retos a los que se enfrentan los centros hospitalarios hoy en día.

—¿Podría explicar datos concretos del centro hospitalario, como número de trabajadores, número de asistencia,...?

—El Hospital Virgen de la Poveda (HVP) está de celebración por su 40 aniversario desde su creación.

Desde su nacimiento como Hospital de Villa del Prado y siendo dependiente del entonces Hospital Provincial (en la actualidad Hospital General Universitario Gregorio Marañón), hoy en día el HVP, es un hospital perteneciente al SERMAS, y se encuentra ubicado a 5 Km de la localidad de Villa del Prado y a 65 km. de Madrid. Disponemos de una parcela de 43.000 m^2 y cuenta con una superficie de 20.000 m^2 construidos. El número de trabajadores es de 373, aproximadamente, y el número de ingresos anuales de media y larga estancia es de 1.004 en 2017, con una estancia media de 60 días.

—¿Cómo está estructurado el área de Seguridad del Hospital Virgen de la Poveda del que es usted responsable de Seguridad? ¿Cuáles son las funciones específicas que lleva a cabo el departamento?

—El área de Seguridad depende de la Dirección de Gestión y Servicios Generales. Yo llevo como responsable de Seguridad en el HVP 3 años; contamos con cuatro Vigilantes de Seguridad para todos los turnos, y siempre hay un vigilante en el Hospital. El contrato de vigilancia y seguridad con el que cuenta el centro es de 2013 y fue licitado en conjunto con 11 centros más de Atención Especializada adscritos al Servicio Madrileño de Salud.

Además de la coordinación de los Vigilantes de Seguridad también es función mía la organización del departamento de Control e Información, que cuenta con siete trabajadores para todos los turnos que, si bien no son personal de seguridad, sí que colaboran activamente con el departamento ya que su labor se desarrolla en recepción, que es donde tenemos la Central Receptora de Alarmas tanto de incendios como de intrusión, megafonía, monitores CCTV, central telefónica y walki-talkies para estar en comunicación con el Vigilante de Seguridad si fuera necesario.

Desde el área de Seguridad se llevan a cabo tareas de supervisión a las empresas mantenedoras homologadas que realizan mantenimiento en nuestras instalaciones, ya que en ocasiones el hecho de que te pongan un sello o una pegatina tras realizar un mantenimiento o una revisión, no quiere decir que ese trabajo esté bien hecho.

—¿Podría indicarnos a grandes rasgos los medios y medidas de seguridad con los que cuentan estas instalaciones hospitalarias?

—Es obligatorio cumplir con los reglamentos y todas las disposiciones legales dirigidas a crear un ambiente de trabajo seguro y garantizar el bienestar de todos los pacientes, trabajadores y visitas en materia de seguridad y es importante contar con el compromiso y apoyo de la Gerencia, Comité de Salud Laboral y Agentes Sociales.

En cuanto a CCTV contamos con 26 cámaras, tres de ellas domos, en relación a prevención de incendios cumplimos con el Reglamento de Instalaciones de Protección Contra Incendios RD. 513/2017 de 22 de mayo, y todos los medios que disponemos para la prevención y lucha contra incendios viene detallado en nuestro Plan de Autoprotección. Disponemos de algún área restringida que para acceder es necesario marcar un código numérico.

Estamos trabajando para tener centralizadas todas las alarmas de los equipos, como pueden ser: bombas de agua, ascensores, climatización, etc., tanto por averías como por falta de suministro.

Desde hace unos meses contamos con una técnico de PRL; esta nueva incorporación permitirá al hospital ser más efectivo en la implantación de la política preventiva, por un lado, una revisión completa de la evaluación de riesgos laborales ya existente para su actualización, de igual modo se llevará a cabo un estricto seguimiento del Plan de Prevención de Riesgos Laborales.

Por otro lado se prevé la implantación de nuevos protocolos en materia de seguridad que recojan la sistemática de actuación de las diferentes actividades específicas relacionadas con los procedimientos en materia de Prevención de Riesgos Laborales.

Pero si en algo se quiere hacer hincapié, en estos momentos, es en la necesidad de formación en materia de prevención, ya que dicha formación es el pilar fundamental para implantar una cultura preventiva que permita un cambio de actitudes y una adquisición de destrezas en materia preventiva.

—¿Qué riesgos y problemas se encuentra el responsable de Seguridad de un centro hospitalario como el Hospital Virgen de la Poveda?

—Aparte de los riesgos que pueden ser comunes a otros hospitales como robos a pacientes ingresados, robo de información, de material, fugas de combustibles, lucha contra incendios, etc., el HVP, al encontrarse en zona forestal y rodeada de vegetación, en concreto en una Zona ZEPA (zona de especial protección de aves), se ha hecho especial hincapié en el Plan de Autoprotección, en que el municipio de Villa del Prado, donde se encuentra el HVP, está incluido en un listado de la Comunidad Autónoma de Madrid definido como Zona de Alto Riesgo (ZAR) de incendio, por lo que el hospital constituye un interfaz urbano-forestal y debemos cumplir con las exigencias del Decreto 59/2017, de 6 de junio, del Consejo de Gobierno de la CAM, por el que se aprueba el Plan Especial de Protección Civil de Emergencia por Incendios Forestales en la Comunidad de Madrid (INFOMA). Otro problema que tenemos este año, que ha tenido una primavera muy lluviosa, aparte de la proliferación de la vegetación, ha sido el número no habitual de enjambres de abejas que han elegido los exteriores de nuestro hospital para hacer sus colonias, por lo que está colaborando un apicultor de la zona para que se lleve los enjambres a un lugar alejado del hospital.

También estamos situados cerca del río Alberche y para la elaboración del Plan de Autoprotección se ha tenido en

«La convergencia de seguridad se refiere al uso combinado de métodos y técnicas de protección tanto físicas como lógicas para proteger un bien»

cuenta la Directriz Básica de Planificación de Protección Civil ante el Riesgo de Inundación y el Plan de Actuación en caso de inundación que nos indica que estamos en una zona de riesgo menor.

—¿Cuáles son las prioridades de seguridad y prevención para el responsable de Seguridad de un centro como el Hospital Virgen de la Poveda?

—Una de mis prioridades desde que asumí el cargo fue la elaboración de un nuevo Plan de Autoprotección según indica el Real Decreto 393/2007, de 23 de marzo en la que se aprobó la Norma Básica de Autoprotección.

A principio de 2016 con el apoyo de la Gerencia del HVP y la ayuda inestimable de la Secretaria de Dirección, comencé con la elaboración del nuevo Plan que se presentó ante la División de Protección Civil de la Dirección General de Protección Ciudadana en agosto del año pasado. En la resolución que nos enviaron, nos indicaban que debíamos de reflejar alguna normativa reciente, una vez subsanado el requerimiento procedimos a enviarlo de nuevo y consideró la Dirección General de Protección Ciudadana como favorable el nuevo Plan de Autoprotección el día 31 de octubre de 2017, y desde el día 22 de marzo de este año tenemos inscrito dicho Plan en el Registro de Datos de Planes de Autoprotección, tarea esta del registro muy complicada y laboriosa.

Otra de mis prioridades ha sido la creación de un registro de incidencias para la realización de estadísticas e informes con el fin de tomar medidas sobre hechos ocurridos y concretos.

—¿Cuáles considera que son las claves para una seguridad satisfactoria en las instalaciones hospitalarias?

—La base de la seguridad es la prevención; es importante trenzar información, formación y simulacros con todo el personal y sobre todo que los equipos de emergencia (EPI, ESI, Jefes de Intervención, Responsables de Evacuación, etc.) sepan quién tiene que actuar y cómo hay que actuar en caso de emergencia. En el HVP hemos optado por la realización de acciones formativas propias y específicas dirigidas a los diferentes equipos de emergencias, esto nos permite adaptar la formación con los horarios de los diferentes departamentos y turnos. También se realizan los simulacros consensuados con el Comité de Salud Laboral, Policía Local de Villa del Prado y el Parque de Bomberos de Aldea del Fresno, que colaboran en todo lo que les es posible.

Un apoyo fundamental que tenemos los responsables de Seguridad en hospitales es contar con una asociación como OSICH (Observatorio de Seguridad Integral en Centros Hospitalarios) que como indica en su página web, tiene entre sus objetivos: «Servir de nexo de unión para los profesionales de la seguridad hospitalaria en materia de Seguridad Civil y Patrimonial, Orden Interno, Medio Ambiente y Lucha Contra Incendios».

También contamos desde hace unos meses con un director del departamento de Seguridad Corporativo de la Consejería de Sanidad de la Comunidad de Madrid, Fernando Bocanegra Morales, que está trabajando por tener una política global en materia de seguridad para todos los hospitales y centros de asistencia primaria de la Comunidad Autónoma de Madrid.

—Hoy en día el sector apuesta por la convergencia de la seguridad como concepto integral, ¿cree que los grandes centros hospitalarios están preparados para asumir este reto?

—El medio en el que los responsables de Seguridad desarrollamos nuestra actividad profesional, está permanentemente sometido a una serie de amenazas sobre las personas, los bienes y los datos, pudiendo alterar el normal funcionamiento de los diferentes departamentos del hospital.

La convergencia de la seguridad se centra en la unión de la seguridad física y la lógica, esto es, áreas de protección donde coinciden los departamentos de Seguridad y de Sistemas en las organizaciones.

En su expresión más amplia la convergencia de seguridad se refiere al uso combinado de métodos y técnicas de protección tanto físicas como lógicas para proteger un bien. En pocas palabras, el fin último de la convergencia es utilizar todas las herramientas posibles para proteger un bien, sin importar que el bien o los medios utilizados sean del mundo físico o lógico.

—¿Han variado en los últimos años los riesgos y amenazas, en términos de ciberseguridad en los hospitales?

—Los hospitales cada día dependemos más de la información y de la tecnología que nos permite gestionarla: ordenadores, teléfonos móviles y tabletas, bases de datos, líneas de comunicaciones, telemedicina e interconsultas con otros hospitales.

El 17 de mayo de 2017 sufrimos el ataque del malware denominado WannaCrry, que coincidió con la celebración en nuestro Hospital de las IX Jornadas de Telemedicina que afectó a las comunicaciones con otros países que participaban en estas jornadas como Brasil y Estados Unidos.

El HVP al pertenecer al SERMAS, la ciberseguridad es competencia de la Oficina de seguridad y centro de soporte especializado en el Área de Seguridad de Sistemas y Tecnologías de la Información del Servicio Madrileño de Salud (OSSI-CER).

Las líneas de servicio que nos ofrece la Oficina de Seguridad son los siguientes:

- Cumplimiento Legal y Normativo.
- Asesoría y Auditoría de Controles Seguridad de TI.
- Monitorización y Correlación de Eventos de Seguridad.
- Análisis de Software y Hardware.
- Comunicación y Formación en Seguridad de la Información.
- Gestión Documental.
- Transporte y custodia de copias de seguridad.
- Nuevas líneas de servicio.
- Actuación de la OSSI en el PIC.

Texto: Gemma G. Juanes.

Fotos: Hospital Vírgen de la Poveda

SANTIAGO GARCÍA SAN MARTÍN. RESPONSABLE DE SEGURIDAD. INSTITUTO PSIQUIÁTRICO JOSÉ GERMAIN. MADRID

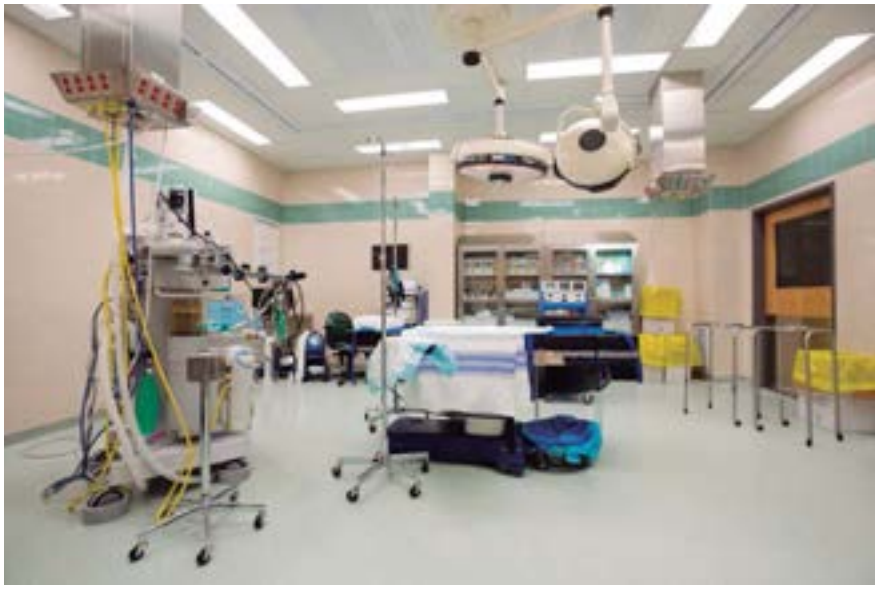
Los departamentos de Seguridad, clave en las instituciones sanitarias

Es el momento de apostar por este tipo de estructuras, que atiendan las necesidades integrales de seguridad del ámbito hospitalario y también de la atención primaria

NOS encontramos en un momento crucial de la seguridad en el ámbito sanitario, donde en este momento confluyen diversas fuentes normativas que intentan, de una vez por todas, estructurar y organizar la prestación y gestión de servicios en dicho ámbito, para procurar la seguridad de pacientes, trabajadores y organizaciones.

El borrador del Reglamento de la Ley de Seguridad Privada significa un salto cualitativo para la seguridad en el ámbito sanitario, evolucionando desde un modelo de seguridad que no había llegado a implantarse de forma efectiva, el de los departamentos de Seguridad por hospitales, hacia un modelo mucho más ambicioso y eficiente, el de los departamentos de Seguridad Corporativos para las organizaciones sanitarias.

En un mundo tan dispar y heterogéneo como el sanitario, donde la existencia de un director de Seguridad en la plantilla del hospital y la creación del departamento de Seguridad, dependía únicamente de la sensibilidad del Gerente del Hospital por la seguridad de su organización, el modelo de los departamentos de Seguridad hace tiempo que se ha demostrado ineficiente, como lo demuestra el bajo número de hospitales con departamento de Seguridad.



Este es el momento de apostar por departamentos de Seguridad Corporativos en las organizaciones sanitarias, que atiendan las necesidades integrales de seguridad de toda la organización, no solo del ámbito hospitalario, ya que bajo esta concepción, el ámbito de la atención primaria, sus trabajadores y pacientes quedaba desprotegido.

Para que este cambio no quede en papel mojado, los departamentos deben estructurarse y dimensionarse en base a criterios objetivos que actualmente el borrador no contempla.

Tal como figura en el borrador, todas las organizaciones e instituciones sanitarias deberán tener un departamento de Seguridad Corporativo, por lo que su aplicación queda desvirtualizada desde el momento que se equiparan organizaciones con dos pequeños centros sanitarios, con Consejerías de Sanidad dependientes de las Comunidades Autónomas, como la de Ma-

drid con 33 hospitales, 425 centros de salud y 100.000 trabajadores directos, y no se incluye ningún tipo de dimensionamiento al respecto. Este dimensionamiento debe garantizar unos medios adecuados a los riesgos presentes en las organizaciones, para que puedan ser gestionados de forma eficiente. Para ello debemos seguir criterios cuantitativos y cualitativos y nada mejor que aprovechar la tabla que aporta el propio reglamento, Cuadro 10 sector A, donde en base a los riesgos presentes en cada uno de los hospitales, los clasifica en Hospitales de Riesgo Bajo, Medio o Alto.

Medidas de seguridad

Esta tabla propone implantar diferentes medidas de seguridad en base a los riesgos y la criticidad del hospital, pero se olvida de la medida principal de gestión de la seguridad, el director de Seguridad. No podemos tener medios organizativos, físicos y personales (vigilantes de seguridad) sin un director de Seguridad que integre dichos elementos y le de consistencia a todo el conjunto.

Aceptando que no es eficiente tener un departamento de Seguridad por cada uno de los hospitales, sí que tenemos claro que hay hospitales que constituyen la cabecera de un área geográfica sanitaria (zona básica sanitaria como la define la Ley General de Sanidad 14/1986 o Áreas Sanitarias como se están definiendo en muchas comunidades autónomas) que tienen unas necesidades especiales en cuanto a gestión de la seguridad.

Por ello, nuestra propuesta es que el departamento de Seguridad Corporativo cuente con al menos el mismo número de directores de Seguridad delegados que hospitales valorados como riesgo alto dentro de la organización y que tendrían la responsabilidad de la gestión de la seguridad en la cabecera de dicha zona geográfica sanitaria, que incluiría el resto de hospitales de riesgo medio y bajo y los centros de salud de la zona y organización

> «Nuestra propuesta es que haya tantos directores de seguridad delegados como hospitales valorados de alto riesgo»

En el caso de que en determinadas áreas geográficas sanitarias no existan hospitales de riesgo alto, los hospitales de riesgo medio deberán agruparse formando una zona geográfica sanitaria con el resto de centros de salud de la zona y organización, formando una zona con un director de Seguridad delegado asignado a la misma, y que se sumara a los anteriores integrándose igualmente en el departamento de Seguridad Corporativo.

Esta estructura ya ha sido aplicada con éxito en los últimos años, al hacer que varios de los departamentos de Seguridad hospitalarios existentes se hiciesen cargo de su área sanitaria, como ha ocurrido por ejemplo con el departamento de Seguridad del Hospital Universitario Son Espases de Palma de Mallorca, que lleva otros tres hospitales de 200 camas cada uno y 40 centros de salud, o el departamento de Seguridad del Hospital General Universitario de Albacete, que se ha hecho cargo del resto de centros sanitarios de la provincia, incluido el Hospital Universitario Ntra. Sra. del Perpetuo Socorro de 200 camas.

Infraestructuras críticas

Además se define igualmente en la línea del resto de normativa concurrente sobre protección y seguridad de aplicación en los hospitales de dichos niveles de riesgo como la Ley de Protección de Infraestructuras Criticas, donde el Plan Estratégico Sectorial del Sector Salud, próximo a publicarse, designará a estos grandes hospitales con casi total seguridad, como Infraestructuras Criticas, y donde la figura del director de Seguridad tendrá que realizar las funciones de respon-

sable de Seguridad y enlace o de delegado de Seguridad.

de las agresiones a los trabajadores de dicho ámbito.

> «La Instrucción 3/2017 del Ministerio del Interior es un gran avance para mejorar la prevención de agresiones»

De igual manera la Instrucción IS-41 del Consejo de Seguridad Nuclear por la que se aprueban los requisitos sobre protección física de fuentes radiactivas obliga a la creación de departamentos de Seguridad Corporativos con un director de Seguridad a cargo de dichos hospitales y zonas sanitarias que a través de la implantación de medios organizativos físicos y personales procure la seguridad de dichas fuentes.

Por último y aunque quizá legalmente menos importante, la Instrucción 3/2017 de la Secretaría de Estado del Ministerio del Interior sobre coordinación para las Fuerzas y Cuerpos de Seguridad del Estado en la prevención de agresiones de los profesionales del ámbito sanitario, que a nivel práctico está suponiendo un gran avance y establece una serie de medidas para mejorar la prevención

Interlocutores territoriales

Entre ellas destacaríamos la designación de los Interlocutores territoriales del Cuerpo Nacional de Policía y la Guardia Civil (tanto nacionales como provinciales) y la clasificación de los centros en función del riesgo de agresión a los profesionales, lo que implica que los propios interlocutores estén ya proponiendo a los gestores sanitarios la implantación de la figura del director de Seguridad en determinadas áreas.

Todas las partes del puzzle encajan en la creación del departamento corporativo integrado por directores de Seguridad delegados responsables de áreas sanitarias y, coincidiendo con ese proyecto, tenemos el primer departamento de Seguridad Corporativo en el ámbito sanitario público, el del Servicio Madrileño de Salud, a cargo de Fernando Bocanegra Morales, a quien desde el OSICH estamos apoyando y creemos que está dando los pasos adecuados para dotar a la Sanidad Madrileña de una estructura de gestión de la seguridad eficiente, capaz de dar una respuesta estratégica y operativa y que pueda servir como ejemplo para que el resto de Servicios de Salud dependientes de las Consejerías de Sanidad de las Comunidades Autónomas tomen ejemplo y creen sus correspondientes departamentos. ●

Fotos: Shutterstock

La central de Alarmas más grande de Europa

Nº1 en Alarmas con verificación por imagen

Presencia en 14 países de Europa y Latinoamérica con más de 2,6 millones de clientes satisfechos.

Central de Alarmas Líder en España

Más de 1.000.000 clientes en España.
Más de 700 vigilantes de Acuda para garantizar una intervención inmediata.

5.000 profesionales pendientes de Usted

Le protegen 24 horas al día los 365 días del año.
Tiempo medio de respuesta 30 segundos.

Líderes en Seguridad.
Referencia en tecnología y usabilidad en Alarmas.

Verisure Smart Alarm de Securitas Direct cumple con las demandas más exigentes en materia de protección, tanto para su hogar como para su negocio.

902 33 44 50
www.securitasdirect.es

RNSP: 2737

Nº1 en Alarmas

SECURITAS Direct

PROF. DR. JOSÉ JULIÁN ISTURITZ. DIRECTOR GENERAL CORPORATIVO DE HOSPITALES SAN ROQUE

La Dirección de Seguridad desde la perspectiva de la Gerencia Hospitalaria

La seguridad es un ámbito crucial para la gestión hospitalaria porque aporta valor y en caso de no cumplir con la normativa, los directivos podrían afrontar consecuencias penales

AUNQUE durante décadas, la seguridad haya sido una asignatura pendiente y una materia muy residual en el ámbito de la gestión hospitalaria, es, sin embargo, un elemento crucial que aporta mucho valor a la gestión sanitaria, y por la que, además, los directivos de la salud, en caso de no cumplir con la normativa vigente, podrían tener que responder penalmente.

Cabe señalar, que bajo el término de «seguridad», se engloban una serie de componentes clave que la hacen ambigua, pero que resulta una inversión y no un gasto. Hablamos de una parte del análisis de riesgos, de «prever» (ver antes de), imaginar qué tipo de situaciones pueden afectar al discurrir ordinario de la vida del hospital y, por otro lado, de gestionar los riesgos previstos, tomando medidas preventivas para evitar que ocurran e interviniendo eficazmente, en el supuesto de que aparezcan.

Además, desde el punto de vista tanto de los usuarios, como de las personas que trabajan en los hospitales, la seguridad es la sensación de sentirse en un entorno seguro y controlado, un elemento objetivo capaz de ser medido. Y, en cualquier caso, la seguridad es algo que transmite, que los trabajadores manifiestan a los clientes en su actividad ordinaria y en su estilo de realizar las tareas que desempeñan, y que todas las personas que entran en cualquier centro sanitario perciben constantemente. Estamos por lo tanto ante una nueva cultura como es la seguridad organizacional.

Pese a lo antedicho, la gestión de la seguridad, en muchos centros, está distribuida en varios departamentos hospitalarios que casi no se hablan entre si (Ruiz Virumbrales, 2017).

Gestión de riesgos

También cabe decir, que la gestión de riesgos, tampoco debe ser una materia alejada de la realidad gerencial

habitual, no solo por su importancia transcendental ante un incidente, sino porque la alta dirección debe de estar transmitiendo y destacando constantemente la cultura de la seguridad, como uno de los pilares de la dirección fomentando el autocuidado (Cola Giacomo, 2013), y por lo tanto, de la implicación de los directivos y responsable en su actividad diaria, como un estilo y una manera de hacer constante. De todos modos, se puede decir que, en cuanto a la seguridad hospitalaria, en la actualidad ya empieza a crearse un clima favorable y como tema transcendental, sobre todo, en algunos países latinoamericanos, donde se ha creado hasta un índice de seguridad hospitalaria (Organización Panamericana de la Salud, 2018), que permite clasificar a los centros hospitalarios por niveles.

En España, tenemos indicadores de salud y de seguridad del paciente, pero todavía nos falta incorporar estos indicadores de seguridad, desde un punto de vista más global y organizacional.

De hecho, el estándar de calidad de mayor prestigio en el ámbito hospitalario como es la acreditación de la «Joint Commission International» dedica un amplio apartado a «la administración y seguridad de instalaciones», desde un punto de vista totalmente funcional teniendo en cuenta políticas e indicadores clave de la seguridad

Aportar valor

Un hospital, en definitiva, es un instrumento de servicio para la mejora de la salud de las personas, y desde este punto de vista, necesita aportar valor y satisfacer, o mejor superar, las expectativas de sus pacientes, de forma que la capacidad «científico técnica» se le supone, por lo que las personas que por diferentes motivos acuden a un hospital valoran sus servicios de manera subjetiva.

No solo por el hecho de que le hayan solventado su proceso patológico, sino también por otros valores subjetivos, tales como, el trato, el respeto a su tiempo, a su intimidad, la hostelería y cómo no, la seguridad entendida ésta, como valor por el cual se despreocupan por el resto de los riesgos que puedan existir al margen de su enfermedad. En este sentido, la seguridad bajo una perspectiva integral (Balbe, 2002) incluye un conglomerado de acciones preventivas y de protección relacionadas con múltiples riesgos tales como: riesgos de las estructuras, del entorno, informáticos, del conocimiento y la información, del patrimonio, de emergencias y autoprotección y de la seguridad individual.

Por lo tanto, la seguridad, al igual que otras disciplinas, como por ejemplo la prevención de riesgos laborales, en contra de lo que muchos técnicos piensan, para el gestor y para la alta dirección, no solo tiene como objetivo el cumplimiento de la normativa en vigor, que también, sino el de aportar valor como tal al negocio que gestiona.

Entender la seguridad exclusivamente como un cumplimiento normativo nos ha demostrado que es un gran fracaso que solo sirve para elaborar documentos que «decoran bibliotecas» o para entender su estricto cumplimiento, «cumplo» y «miento» (Morón 1986).

Así, cabe decir, que resulta muy adecuada la potenciación de organizaciones como el Observatorio de Seguridad Integral de Centros Hospitalarios que tienen como misión procurar información, formación y asesoramiento técnico a los responsables de seguridad en centros sanitarios, sea cual sea su ámbito de responsabilidad, y proporcionar un lugar de encuentro, análisis y reflexión para los implicados en la mejora de la seguridad (OSICH, 2018).

Gestores hospitalarios

Este tipo de organizaciones permiten a los gestores hospitalarios tomar conciencia de la importancia de contar con una adecuada gestión de riesgos en este ámbito y considerarla como una inversión.

En definitiva, para un alto directivo o gestor de un hospital, la seguridad tiene retorno de inversión para lo cual debe hacer crecer la misión del hospital, es una cultura, una manera de hacer y de trabajar, y por lo tanto, un estilo organizacional que aporta valor a la excelencia. ●

Fotos: *Shutterstock*

JESÚS GARZÓN. COUNTRY MANAGER IBERIA. DEISTER ELECTRONICS

Seguridad para el cuidado de la salud

Medidas y estrategias para incrementar la seguridad de los centros sanitarios desde la dirección de los hospitales

RECIENTEMENTE el OSICH se hacía eco de que hubo un total de 486 hechos delictivos en toda España en 2016 y más de 2.688 profesionales de la salud fueron víctimas de algún tipo de agresión en un lustro. Son cifras cuanto menos sorprendentes, que se convierten en alarmantes cuando se echa una mirada a la realidad diaria de muchos centros hospitalarios: palizas a sanitarios, sustracciones de materiales, robos a pacientes… Son hechos que no pueden entenderse como aislados, sino que forman parte de un contexto cambiante en el que los hasta ahora entornos de confianza se están convirtiendo en lugares donde la seguridad se ve comprometida. Pero, ¿qué se puede hacer desde la dirección de los hospitales?

La primera medida habrá de estar enfocada en la protección del personal y de los pacientes. Estos últimos han de estar en el eje de toda estrategia de seguridad dada su vulnerabilidad. La implantación de tecnología debe permitir situar y proteger a las personas gracias a dispositivos que sean detectados por localizadores. Estos a su vez también deberían poder controlar puertas y alarmas, por ejemplo, para cerrar o permitir el acceso a diferentes áreas del hospital.

Control de acceso correcto

Como se ha visto, es clave establecer un control de acceso correcto para cualquier área, por lo que es recomendable implantar soluciones que vigilen las entradas y salidas con lectores en línea, lectores de largo alcance para acceso de manos libres (tan demandados por el personal que traslada camillas), componentes de bloqueo digital en diferentes formatos y cajas de llaves electrónicas. Con estas alternativas, el control de acceso podrá expandirse de manera eficaz a todas las puertas de un edificio.

Gestión de los activos

Por supuesto, la gestión de activos es también significativa para el buen desempeño de un centro hospitalario. Para alcanzar la eficiencia en este aspecto se ha de hacer un segui-

miento de todos los materiales, desde las camas de los pacientes hasta los caros dispositivos de diagnóstico. Para esto es muy útil contar con transpondedores UHF pasivos que junto a potentes lectores de largo alcance instalados en ubicaciones estratégicas detectan los materiales en un rango de hasta 7 metros.

Además, el almacenamiento y la administración de artículos valiosos, tales como tablets, material quirúrgico o equipos importantes se puede llevar a cabo de manera segura con la implantación de cabinas inteligentes que escaneen automáticamente su inventario y realicen un seguimiento de lo que se toma, devuelve o ha de reponerse. Un requerimiento imprescindible que aconsejamos es que estos armarios solamente permitan a personas autorizadas abrirlos.

Administración centralizada

Por último, para que todas estas herramientas logren unos resultados óptimos es fundamental que se apueste por una administración centralizada de las mismas. Es aconsejable contar con un software ágil y accesible desde cualquier ubicación, por ejemplo, mediante un navegador web. Este tendrá que permitir, también, que la información entrante se recopile en un punto central y que se pueda recuperar en cualquier momento. Además, esta herramienta tendrá que facilitar que los informes sean adaptables y facilitar diversos perfiles de usuario en función del rol dentro de la organización.

> «La gestión de activos es también significativa para el buen desempeño de un centro hospitalario»

En definitiva, la tarea de proteger a las personas en una situación de fragilidad es una de las principales responsabilidades de las autoridades sanitarias. Este reto es cada día más fácilmente alcanzable gracias al desarrollo de tecnología inteligente, diseñada y desarrollada para minimizar los potenciales riesgos. Si se trabaja con este objetivo, entre todos, se contribuirá a la reducción de las estadísticas de criminalidad que nos sobresaltaban al inicio de este texto. ●

Fotos: deister electronics

Contactos de empresas, p. 8.

JOSEP FARO I MARÍN. SEGMENT MANAGER HEALTH CARE. DORMAKABA

Ley de **Protección de Datos** en el ámbito sanitario

Seguridad de acceso

CONFORME a la normativa de protección de datos personales, en el sector de la sanidad relacionado con la actividad empresarial es de suma importancia la custodia en todo el ámbito de la Seguridad Hospitalaria. Tanto para profesionales de la propia sanidad, como para las empresas del sector que precisan implantar sus sistemas. La protección de datos personales es un derecho fundamental recogido en el artículo 18.4 de la Constitución Española y regulado por el Reglamento Europeo de Protección de Datos (RGPD), la LOPD y su reglamento de desarrollo.

Esta normativa afecta a los profesionales que operan en el sector sanitario, a las clínicas, a los hospitales, a los centros médicos y a las instituciones sanitarias. En este caso en particular, la normativa en protección de datos se complementa con la Ley de Autonomía del Paciente 41/2002, la cual se encarga de regular los derechos y las obligaciones en materia de información y documentación clínica en la que se regula su historial.

Pero primero hay que dejar claro que histórica clínica es el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y evolución clínica de un paciente a lo largo de su proceso asistencial.

Datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

Por lo tanto cualquier información relativa a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo, un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro.

Por lo trascendental que puede tener este tipo de datos para la privacidad del interesado, el RGPD da a este tipo de datos el adjetivo de «Especialmente Protegidos», lo cual hace que se deban cumplir una serie de condiciones adicionales para su tratamiento conforme a la normativa.

Los principios fundamentales que deben formalizar los responsables de los datos para el cumplimiento de la normativa son:

La principal base legal para el tratamiento de este tipo de datos la encontramos en el artículo 9 del RGPD y es el consentimiento. Según la nueva normativa europea, este deberá ser explícito y recogido por escrito.

El secreto profesional es de obligatorio cumplimiento por el personal que tenga acceso a los datos del paciente.

Incluso cuando la relación que vincule a las partes haya finalizado. Se obliga a los centros médicos a adoptar las medidas necesarias para garantizar la confidencialidad y el procedimiento legal de acceso.

Medidas organizativas y de seguridad

La nueva normativa ya no establece las medidas de seguridad por niveles, sino que prevé que se apliquen medidas en función del riesgo que puedan ocurrir en el tratamiento de los datos.

Por lo tanto, atendiendo a esto, en el caso del tratamiento de datos de salud el nivel del riesgo es enorme, por lo que habrá que diseñar unas medidas organizativas y de seguridad conforme a dicho riesgo.

La evaluación de impacto es un análisis del riesgo cuyo objetivo es permitir a los responsables del tratamiento tomar medidas adecuadas para reducir dichos riesgos.

Asimismo, las medidas de seguridad y los protocolos que se deban llevar a cabo han de plasmarse en un Documento de Seguridad. Dicho documento deberá estar siempre a disposición de la Agencia Española de Protección de Datos para su consulta si así lo requiriera.

Se establece un plazo de conservación de al menos cinco años contados desde el alta de cada proceso asistencial. Por tanto, cuando un paciente reciba el alta o por cualquier motivo deje de asistir a la clínica, no se puede proceder a eliminar sus datos ya que existe una obligación de custodia de la historia clínica. Igualmente ocurriría en el caso de que el paciente solicitara la cancelación de sus datos. Estos no podrían ser cancelados, si no quedarían debidamente bloqueados.

El Código Civil establece un plazo de quince años para poder llevar a cabo una acción por responsabilidad civil, plazo que computa desde que el reclamante tiene conocimiento del daño. No obstante, a efectos prácticos, este plazo se incrementa en quince años más ya que si el daño se conoce justo antes de que venzan los primeros quince, automáticamente se prorrogará por otros quince años más.

Sólo puede tener acceso el personal directamente implicado en la atención del paciente, el incumplimiento de estos preceptos fundamentales implica sanciones económicas. Cabe destacar que con la aplicación de la nueva regulación las multas van en función de la vulneración de la norma, pudiendo llegar hasta los 10.000.000 € o el 4% de la facturación global anual.

En resumen, para el cumplimiento con los requisitos dictados por la normativa de protección de datos en materia sanitaria, los centros han de cumplir los siguientes puntos:

1. Los datos recogidos son siempre pertinentes y veraces.

2. El paciente siempre es informado y tiene acceso libre a sus datos.

3. Realizar una evaluación de impacto y mantener un registro de las actividades de tratamiento.

4. Nombrar un Delegado de Protección de Datos.

5. Cifrar los datos y guardarlos bajo estrictas medidas de seguridad.

6. Guardar secreto profesional en todo caso.

7. En caso de cesión de datos a terceras partes y se debe firmar un contrato que establezca el uso determinado y definido de los datos cedidos.

8. Facilitar los derechos ARCO respetando los plazos establecidos.

9. Inscripción y actualización de los ficheros en la AEPD. (Hasta el 25 de mayo de 2018).

Las empresas especializadas en la aplicación de sistemas de control de acceso pueden y deben asesorar adecuadamente, cómo regular el acceso a zonas cometidas en los controles, con la aplicación de soluciones digitales, que permitan monitorizar los accesos y las personas profesionales usuarias y responsables del cumplimento de la norma. Tanto subsidiariamente como bajo responsabilidad directa.

Los principales fabricantes de sistemas disponen de hardware on line, off line o diversas configuraciones de posibilidades de sistemas autónomos. Lo importante es una eficiente asesoría de ingeniería de sistemas, que determine dónde aplicar puntos de monitorización en estado continuado, otros u otras áreas de aplicación donde el grado de seguridad puede ser más bajo y monitorizado por alerta de evento. ●

Contactos de empresas, p. 8.

JOSÉ MIGUEL MARÍN RODRÍGUEZ. COMITÉ DE INSTALACIÓN, MATENIMIENTO E INGENIERÍA DE EQUIPOS Y SISTEMAS. TECNIFUEGO

El RIPCI en los centros hospitalarios

Reglamento de Instalaciones de Protección contra Incendios

LA protección contra incendios en hospitales, donde residen personas enfermas y que no se valen por sí mismas hay que extremarla. En España, las medidas mínimas que debe cumplir un hospital vienen detalladas en el Código Técnico de la Edificación (CTE), en su denominación de Uso Hospitalario. El término hospitalario es de aplicación a los edificios asistenciales sanitarios (hospitales, clínicas, sanatorios) que cuentan con hospitalización de 24 horas y que están ocupados por personas que en su mayoría son incapaces de cuidarse por sí mismos. En este artículo vamos a condensar las medidas que se deben cumplir para la instalación y mantenimiento de los equipos requeridos en el CTE, ya que desde el 12 de diciembre de 2017 está en vigor el Real Decreto 513/2017, de 22 de mayo, por el que se aprobó el Reglamento de Instalaciones de Protección contra Incendios (RIPCI) y sus tres anexos, que introducen cambios importantes para el usuario.

Objeto y ámbito de aplicación

El objeto de este RIPCI constituye las condiciones y los requisitos exigibles al diseño, instalación/aplicación, mantenimiento e inspección de los equipos, sistemas y componentes de las instalaciones contra incendios.

Empresas instaladoras y empresas mantenedoras de Protección contra Incendios (PCI).

Es obligatorio que las empresas instaladoras y mantenedoras cumplan los requisitos del RIPCI, es decir, estén debidamente habilitadas por el órgano competente de la Comunidad Autónoma, de un seguro RC de 800.000 €, como mínimo; dispongan de personal contratado adecuado a su nivel de actividad; tengan un certificado de calidad implantado (ISO 9001 (R.D.2200/1995 DE 28 DIC); y la empresa instaladora y mantenedora habilitada no podrá facilitar, ceder o enajenar certificados de instalación no realizados por ella misma.

Obligaciones de las empresas mantenedoras

Además, detallar la obligación de las empresas mantenedoras (una actividad básica, tratándose de equipos que están en reposo y solo se activan en caso de incendio) de realizar el mantenimiento de acuerdo con los plazos reglamentados utilizando recambios y piezas originales, siempre y cuando afecten a la certificación de producto.

Además:

- Corregir a petición del titular de la instalación, las deficiencias o averías que se produzcan en los equipos o sistemas cuyo mantenimiento tiene encomendado.

- Entregar un informe técnico al titular, de los equipos y/o sistemas que no ofrezcan garantía de correcto funcionamiento, presenten deficiencias, que no se puedan corregir durante el mantenimiento, que no cumplan con las disposiciones vigentes que le sean aplicables o no sean adecuadas al riesgo de incendio.

- Conservar al menos durante 5 años, la documentación justificativa de las operaciones de reparación y mantenimiento que se realice.

- Emitir un certificado del mantenimiento periódico efectuado, en el que conste o se haga referencia a los equipos y sistemas objeto del mantenimiento, anexando copia de la lista de comprobación utilizadas durante las operaciones y comprobaciones ejecutadas, con las anotaciones realizadas y los resultados obtenidos, firmados por la empresa mantenedora (responsable técnico).

- Por último, lo debe firmar el titular o representante de la propiedad de la instalación (en este caso gerente del hospital) para dar constancia de su conformidad y de que ha recibido los documentos.

Instalacion, puesta en servicio y mantenimiento de instalaciones contra incendios.

En los establecimientos hospitalarios la instalación de los equipos y sistemas contra incendios incluidos en el reglamento requieren de un proyecto o documentación técnica ante los servicios competentes en materia de industria de la Comunidad Autónoma.

El citado proyecto o documento será redactado y firmado por técnico titulado competente.

Deben de existir los dos documentos: el proyecto (para la instalación) y el certificado de la instalación (para la puesta en servicio).

Puesta en servicio

Para la puesta en servicio de las instalaciones de protección activa contra incendios de un hospital se requiere:

- La presentación del proyecto y certificados ante el órgano competente de la Comunidad Autónoma.
- Tener suscrito un contrato de mantenimiento con una empresa mantenedora debidamente habilitada.

Una vez realizada la puesta en servicio, se deberá conservar dicho contrato de mantenimiento, para poder presentarlo en el caso de que los soliciten las autoridades competentes o durante las inspecciones técnicas.

Inspecciones periódicas de las instalaciones contra incendios

En aquellos casos en los que la inspección de las instalaciones de PCI no esté regulada por reglamentación específica, los titulares deberán solicitar al menos cada 10 años, a un organismo de control acreditado. Se empezará a contar desde la puesta en servicio de la instalación.

El organismo de control solicitará al titular la documentación de dichas instalaciones y si detecta algún documento faltante, lo hará constar para que el titular lo subsane.

De dichas inspecciones se levantará un acta firmada por el técnico competente del organismo de control que ha procedido a la inspección y por el titular de la instalación.

Aplicación de este reglamento a equipos o sistemas ya instalados

A los equipos o sistemas ya instalados con fecha de solicitud de licencia de obra, con anterioridad a la entrada en vigor del nuevo RIPCI, únicamente les será de aplicación aquellas disposiciones relativas a su mantenimiento y a su inspección.

También se debe remarcar que la sustitución de uno o varios productos (componentes) de una instalación ya existente en un hospital (detectores, pulsadores,…) siempre que no se modifique su diseño general o funcional no implicará que dicha instalación tenga que adaptarse por completo al nuevo reglamento.

Sobre los productos para los que se pide considerar su vida útil

Hay algunos productos para los cuales el RIPCI pide que el fabricante establezca su vida útil. En caso de no decir nada se deberán cambiar los detectores a los 10 años, las mangueras de BIE a los 20 años, y las señales fotoluminiscentes a los 10 años.

> «Es obligatorio que las empresas instaladoras y mantenedoras cumplan los requisitos del RIPCI»

Según la Guía de aplicación del RIPCI, no vinculante, dichos requisitos solo se aplicarán a los productos instalados con posterioridad a la entrada en vigor del reglamento, de esta forma, conforme a lo dispuesto en la Disposición Transitoria Segunda, a los productos ya instalados con anterioridad no les será de aplicación el requisito de la vida útil.

Disposicion transitoria cuarta

Primera inspección de las instalaciones existentes en centros hospitalarios. Cuando la instalación tenga una antigüedad mayor o igual a:

- 20 años, en el plazo de un año.
- 15 años y menor de 20 años, en el plazo de 2 años.
- 10 años y menor a 15 años, en el plazo de 3 años.

Mantenimiento mínimo de las instalaciones de proteccion contra incendios

Los equipos y sistemas de protección activa contra incendios de un hospital se someterán al programa de mantenimiento establecido por el fabricante, y como mínimo se realizarán las operaciones que se establezcan en el propio RIPCI.

Las operaciones de mantenimiento que recogen señalización de equipos de PCI y evacuación serán efectuadas por personal del fabricante o de la empresa mantenedora o bien por el personal del usuario o titular de la instalación, con conocimiento para ello.

Las revisiones anuales serán efectuadas por personal del fabricante o de la empresa mantenedora.

Todas estas operaciones se recogerán en actas, que deberán ir firmadas por la empresa mantenedora y el representante de la propiedad.

Mala instalación de rociadores, sin conexión a la acometida.

Conclusiones

Los usuarios, en este caso, el gerente y/o director de Mantenimiento del Centro Hospitalario, deben de tener a disposición:

- Licencia de funcionamiento.
- Registros que procedan con PCI.
- Proyecto de instalaciones.
- Certificados que cumplan con el proyecto (solo por empresas autorizadas de PCI).
- Informes y certificados de mantenimiento anual y trimestral.

Destacar un tema con mucha consulta que es el de la vida útil, los detectores, mangueras y señales que sean necesarios cambiar, en fecha posterior a la entrada en vigor del nuevo RIPCI, estarán sujetos a las condiciones marcadas en dicho reglamento.

El objetivo del nuevo RIPCI es la existencia de instalaciones contra incendios que sirvan para lo que están proyectadas y se comporten como en el momento en que se pusieron en servicio así, para lograrlo, se necesita de un mantenimiento con un sentido de responsabilidad absoluta.

Malas prácticas, puerta cortafuegos y extintor.

> «La protección contra incendios en hospitales, donde residen personas enfermas y que no se valen por sí mismas, hay que extremarla»

Si tenemos algún elemento en mal estado (cerebro y corazón de las instalaciones de PCI), en caso de incendio, la respuesta será tardía y , por desgracia, puede acabar en un desastre.

Para completar la protección contra incendios nos faltarían tres cosas:

1. La protección pasiva (en cuanto a sectorización).
2. La prevencion (en educación diaria).
3. Los planes de emergencia (con su implantación continuada).

Lamentable cuando todo falla, tenemos que recurrir a nuestro eficiente y abnegado Cuerpo de Bomberos, aunque muchas veces está en nuestra mano evitar situaciones irreversibles, si siguiéramos todas las pautas y normativa referidas a las instalaciones. ●

Fotos: *Tecnifuego/Archivo*

riscogroup.es

RISCO GROUP

Familia de detectores inteligentes BWare™

Un Ganador en Todas las Categorías

BWare™ es la familia de detectores cableados, inalámbricos y en bus con las tecnologías de microondas banda-K para minimizar falsas alarmas y lente convexa para un mayor rendimiento.

- La serie BWare™ ofrece una amplia gama de detectores cableados, inalámbricos y en Bus, incorporando las principales tecnologías de detección de RISCO, como Anti-Cloak™ y microondas de banda-K para un mayor rendimiento de captura, incluido un exclusivo detector inalámbrico de DT con antienmascaramiento mediante IR activo.
- La familia de detectores inteligentes BWare™ ofrece flexibilidad para utilizar detectores profesionales en cualquier instalación, ideal para una amplia gama de aplicaciones comerciales y de alta seguridad, con versiones de Grado 2 y Grado 3.
- Con un diseño elegante y moderno, el detector inteligente BWare™ ofrece tecnología avanzada y fiabilidad, manteniendo una apariencia uniforme en todo el sitio.

RISCO Group Iberia
riscogroup.es | Tel.: 91 490 21 33 | Email: sales-es@riscogroup.com

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

Videovigilancia, seguridad y gestión en los hospitales

LOS hospitales y centros de salud llevan años aplicando una política de tolerancia cero frente a los delitos y las agresiones al personal sanitario que está dando frutos positivos gracias, entre otras medidas, a los avances en la tecnología de videovigilancia. Estos avances, además de mejorar aspectos meramente de seguridad, pueden ayudar al mismo tiempo a mejorar algunos aspectos de la gestión de los centros y organización de los espacios, pero también en la atención a los pacientes.

Los avances que han experimentado las últimas generaciones de cámaras de videovigilancia y el desarrollo en la analítica de vídeo de empresas especializadas, con las que llevamos colaborando en los últimos años, están aportando características, prestaciones y soluciones que hasta hace poco eran impensables. Algunas de ellas llevan apenas un par de años en el mercado y otras se están presentando en estos momentos. Hagamos un rápido repaso de los beneficios prácticos que están aportando en este momento.

Seguimiento automático digital

Las cámaras con resolución 4K (12 megapíxeles) permiten capturar imágenes de gran calidad. Algunos modelos, como los de la gama Wisenet P, disponen de seguimiento automático digital que puede utilizarse para detectar objetos o personas en movimiento durante los períodos de poca actividad como, por ejemplo, de noche. Esto facilita, al personal de seguridad del hospital y a los operadores del centro de control, mantener una mayor atención en zonas con mayor prioridad.

Analítica

Las cámaras con potentes chipsets DSP de plataforma abierta desarrolladas por fabricantes de referencia del mercado como nuestra compañía, ofrecen la posibilidad de ejecución de muchas aplicaciones de analítica integradas en la propia cámara. Una función de análisis de audio permite, por ejemplo, reconocer sonidos críticos (disparos de armas, explosiones, gritos y cristales rotos) e inmediatamente activar una alarma que permita al personal del hospital reaccionar de forma rápida y efectiva a cualquier incidente.

Una de las analíticas que ayuda a la gestión de los espacios y analizar el funcionamiento de los centros son el conteo de personas y mapas de calor, que con gran éxito se están implantando en otros sectores como el retail. Esta solución puede ayudar a gestionar de forma óptima las salas de espera de los centros y las visitas de familiares. Lo importante en todo momento es garantizar la seguridad e intimidad de los pacientes y personal sanitario.

WDR (amplio rango dinámico) 150db

La mayoría de cámaras dispone de la característica WDR, que combina 2 imágenes con exposiciones distintas para garantizar la captura de imágenes claras y nítidas en lugares donde hay condiciones de iluminación con fuertes contrastes. Un nuevo WDR, de 150dB, integrado en la Serie X de Wisenet, utiliza 4 imágenes para crear una imagen mucho más natural: imágenes nítidas y sin desenfoque, una debilidad crítica asociada al WDR estándar. Se trata de una innovación asombrosa para cámaras que han de instalarse en zonas de un hospital donde quedarán expuestas a condiciones de iluminación solar muy variables.

Las cámaras de 360 grados se especifican cada vez más en proyectos donde es necesario supervisar la actividad de forma ininterrumpida, como es el caso de las salas de urgencias de los hospitales. Una sola cámara de 360 grados suele ser suficiente para cubrir de forma eficaz y asequible toda un área que, de otro modo, requeriría un gran número de cámaras estándar. Una cámara de 360 grados complementará una solución de videovigilancia perfectamente dando al operador una vista completa de una zona, mientras que las cámaras de alta definición fijas o con giro e inclinación pueden instalarse en lugares donde se requiere hacer zoom para ver ampliados los detalles de cualquier evento y garantizar que no haya puntos ciegos.

Visualización de pasillo

La visualización de pasillo permite

supervisar con una alta eficiencia zonas verticales estrechas como pasillos de hospitales. Esta función permite que las cámaras generen imágenes con una relación de aspecto de 9:16 x 3:4 para funcionar eficazmente en espacios altos y estrechos, con el valor añadido de que minimiza los requisitos de ancho de banda y almacenamiento de vídeo.

Además de proporcionar una valiosa herramienta para detectar y disuadir actividades delictivas, un sistema de videovigilancia puede utilizarse en un hospital o centro de salud con muchos otros objetivos: localizar a un paciente desorientado o con alguna enfermedad mental que pudiera abandonar una sala del hospital, investigar problemas de seguridad y salud…

Tecnología de compresión complementaria

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

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

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

Gestión de vídeo

Es importante que los hospitales tengan la posibilidad, con una formación mínima, de gestionar sus sistemas de videovigilancia. Por esta razón fabricantes destacados como nuestra compañía ofrecen software de gestión para maximizar la eficiencia y facilidad de uso de sus cámaras de red IP, dispositivos de grabación y servidores. El nuevo VMS Wisenet Wave y el Smart Security Manager (SSM) Enterprise de Hanwha Techwin simplifican la integración con sistemas de terceros como, por ejemplo, alarmas de intrusión, detección de incendios, control de accesos y reconocimiento de matrículas de vehículos, para ofrecer una solución de seguridad totalmente integrada.

Supervisión de la salud sin contacto en centros especiales

Uno de los ejemplos más destacados de cómo la videovigilancia puede contribuir a mejorar, no sólo la seguridad de pacientes y personal sanitario, sino también la salud, es el control de las constantes vitales a través de una cámara que se ha desarrollado gracias a la asociación tecnológica establecida entre Oxehealth y nuestra compañía.

Esta solución de supervisión dará a las instituciones de salud psíquica, así como a la policía y centros penitenciarios, la oportunidad de medir de forma remota los movimientos y la frecuencia cardíaca y respiratoria de reclusos y pacientes.

A nivel global existe una creciente conciencia de la necesidad de tomar medidas de intervención tempranas para reducir los decesos en custodia. Las compañías desarrollan conjuntamente una solución que alerte de manera rápida al personal de seguridad sobre cualquier cambio repentino y drástico en la fisiología de una persona bajo custodia. Esta solución alertará al personal de salud mental o de custodia si un paciente deja de respirar o si su ritmo cardíaco cae por debajo de los umbrales programados. Funcionará con todas las condiciones de iluminación, incluida la oscuridad total y continuará supervisando la respiración incluso si un paciente o detenido se ocultase bajo una manta. ●

Fotos: Hanwha Techwin

Contactos de empresas, p. 8.

Hikvision ofrece un nuevo plug-in de comunicación con CRA

Hikvision ofrece un nuevo plug-in que permite la comunicación directa con las principales plataformas de software de gestión de alarmas: Manitou, IBS y MASterMind. Se trata del primer paso en un proceso de integración, que está previsto completar con una pasarela que permita ampliar las funciones disponibles para las Centrales Receptoras de Alarmas.

Gracias a este plug-in es posible realizar una verificación mediante vídeo cuando se haya producido una alarma, accediendo a un grabador - ya sea a través de IP estática o de un DNS, como el que ofrece Hik-Connect -el servicio de conexión DDNS para los equipos de Hikvision-.

De esta forma, es posible realizar las siguientes operaciones:

- Visualización de imágenes de vídeo grabado
- Visualización de vídeo en tiempo real
- Visualización dual de vídeo en tiempo real y vídeo grabado
- Control PTZ (función disponible según el programa)

Con este lanzamiento, los sistemas de vídeo del principal proveedor de soluciones de seguridad a nivel mundial son ahora compatibles con prácticamente la totalidad de plataformas software de gestión de alarmas que se emplea en nuestro país.

En total, en España se calcula que existen un total de 1.820.000 conexiones activas a CRA, según datos del el Observatorio Sectorial DBK de Informa. Esta cifra se ha venido incrementando en los últimos años. Concretamente, en 2017 creció un 8,5% con respecto a 2016, año en que ya había aumentado un 6,1%.

Además, las previsiones de este mismo estudio apuntan al mantenimiento de esta tendencia positiva de crecimiento. Así, se estima que el parque total cerrará el año 2018 con alrededor de 1.955.000 conexiones, lo que supondrá un incremento del 7,4% respecto a diciembre del año anterior.

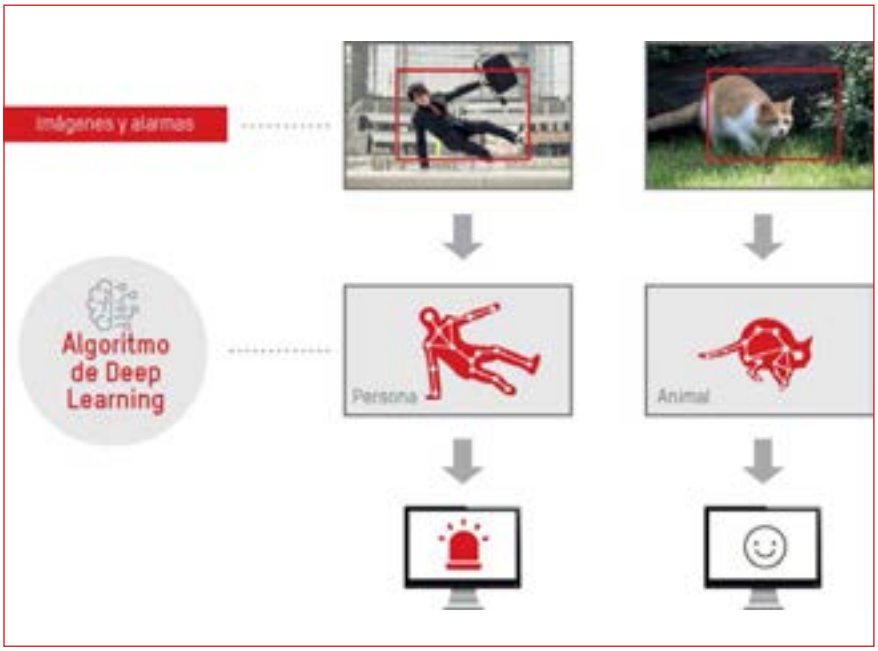
Reducción de falsas alarmas

De cara al futuro, Hikvision trabaja ya en el desarrollo de una pasarela que

permitirá, además de la verificación de la alarma, la incorporación de otras funciones adicionales como la recepción de eventos o el control del estado de un grabador desde la propia central.

La combinación de equipos de intrusión y sistemas de videovigilancia ofrece, a día de hoy, las mayores garantías en términos de seguridad pero además, los avances tecnológicos –especialmente en el ámbito del vídeo- han permitido incrementar la eficiencia y ampliar los servicios al usuario final (rondas virtuales, atención a los mayores, etc.)

La irrupción del Deep Learning ha permitido que los equipos de videovigilancia –tanto las cámaras como los grabadores- que integran estos nuevos algoritmos sean capaces de procesar la información con una eficacia desconocida hasta ahora. Desde el mismo momento en que se captura la imagen es posible determinar si se trata de un cuerpo humano o de un vehículo, por ejemplo. Además, los propios grabadores pueden distinguir movimientos convencionales de elementos habituales en un área (balanceo de las hojas en un jardín, movimiento de una mascota) para reducir las falsas alarmas hasta un 90%.



Internet Of Security Things

El futuro de la seguridad pasa por la interconexión de todos los elementos (equipos de vídeo, detectores de intrusión, sistemas de control de accesos…) en lo que llamamos Internet of Security Things. Hikvision ofrece garantías de interoperabilidad, tanto en el presente como de cara al futuro, ya que cuenta con un equipo de 10.000 ingenieros de I+D en todo el mundo. La innovación se implementa en todas las fases: desde la concepción del producto a hasta después de su puesta en el mercado. A través de la escucha activa a las necesidades del mercado, se realiza una continua actualización y adaptación de cada producto.

IGNACIO MORA DÍAZ. COORDINADOR CRA/SOC DE TECHCO SECURITY

La innovación y tecnología determinan el futuro de las CRAs

La aplicación de la tecnología más innovadora en los sistemas de seguridad ha supuesto toda una revolución en la gestión de las Centrales Receptoras de Alarmas (CRAs). De solo gestionar señales de robo, fuego y atraco, actualmente manejan un alto volumen de clientes e información muy compleja, convirtiéndose en Centros Operativos de Gestión.

LA adaptación a todos estos nuevos servicios que ha traído la tecnología más innovadora y puntera a las CRAs han motivado que el uso de drones, la teleasistencia a personas dependientes, la gestión reputacional en redes sociales, el vídeo embarcado en transportes de viajeros… hayan pasado a formar parte del catálogo de servicios remotos.

Entre estas soluciones destaca, por su potencial de crecimiento, los sistemas de vídeo, que cuentan ya con análisis de vídeo y vídeo inteligente o inteligencia artificial. El desarrollo de estas soluciones, apoyadas en sistemas de intrusión cada vez más funcionales, tendrá una gran proyección los próximos años, siendo gestionado por las Centrales Receptoras.

Igualmente, en Techco Security estimamos que se crearán servicios nuevos que, de una forma u otra, irán restando la necesidad o, cuando menos, disminuyendo la presencia de vigilantes. Hablamos de vídeo-rondas apoyadas en Drones o en Robots; unos servicios que no serán nada descabellados verlos a corto plazo. En este sentido, la capacidad de asumir funciones propias de Centros de Control de un cliente concreto será algo a lo que tendrán que adaptarse las Centrales Receptoras del futuro.

Asimismo, en poco tiempo veremos cómo el sistema de CCTV (Circuito Cerrado de Televisión) le quita mercado al clásico sistema de intrusión, asumiendo servicios nuevos y disminuyendo incluso el número de falsas alarmas gracias al análisis de vídeo e inteligencia artificial.

Comunicaciones ciberseguras

Otro de los pilares esenciales de las Centrales Receptoras en el futuro son las comunicaciones. Hemos pasado, en poco tiempo, de una conexión por RTB (Red Telefónica Básica), que desaparecerá en breve, a las comunicaciones IP (Internet Protocol) cuyos indicios nos hacen pensar que evolucionará a una infraestructura aún más segura, rápida y con mayor capacidad de tráfico de

datos, fundamental para el sector de la seguridad y el futuro desarrollo de sistemas sobre CCTV.

Mientras este nuevo contexto llega, en el que se necesitarán profesionales que sean capaces de administrar las comunicaciones IP para ofrecer una Central Receptora segura a sus clientes, coexistirá una receptora de backup de la principal, unos sistemas redundados y unas comunicaciones securizadas.

Todo ello sin olvidar protegerse de los ciberataques. En un mundo donde el bien a proteger ha pasado de ser físico a digital, los clásicos sistemas de seguridad no son efectivos y han de crearse nuevas soluciones para garantizar la protección de la información, entendida como un producto transformado en datos.

Por ello, las Centrales Receptoras también deberán adaptarse a los nuevos tiempos y tecnologías que vayan surgiendo, incorporando servicios de Ciberseguridad en la cartera de servicios.

Transición y convivencia

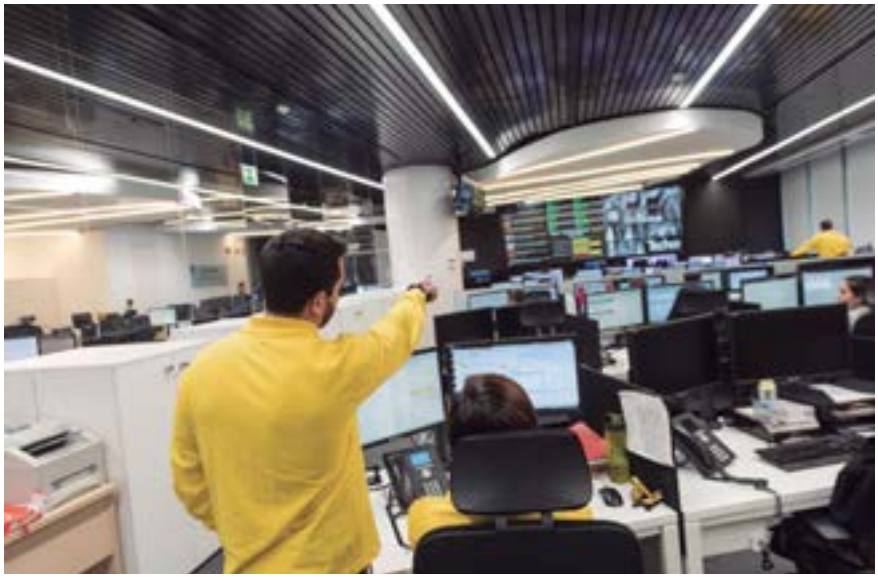
La convivencia de los sistemas denominados «tradicionales» —como la Intrusión y CCTV—, los nuevos ya descritos —como analizador de imagen, vídeo Inteligente, ciberseguridad…— y los futuros que puedan venir tendrá como consecuencia la revisión de operativas en las Centrales Receptoras y la definición de otras diferentes para adecuarse a este contexto tecnológico de seguridad «vivo» y en continua evolución. Así, estos centros dispondrán de plataformas para integrar los distintos sistemas y servicios que ofrezcan a sus clientes.

Por ello se hace imprescindible una continua inversión en las Centrales Receptoras por parte de las empresas del sector, contando, como ya se ha comentado anteriormente, con personal muy cualificado y mejor preparado. De la inversión que se realice, tanto en infraestructura como en el equipo de profesionales, dependerá, en gran medida, el alcance y capacidad de los servicios de cada una de las Centrales Receptoras.

> «La aplicación de la tecnología más innovadora en los sistemas de seguridad ha supuesto toda una revolución en la gestión de las CRAs»

En Techco Security creemos en la innovación y en la necesidad de adaptar el sector a las nuevas tecnologías, pero también en la formación y cualificación de las personas. Este tándem entre tecnología y consultoría, realizada por expertos profesionales, es clave para consolidar la eficacia y calidad de nuestra Central Receptora de Alarmas. ●

Fotos: Techco Security



Contactos de empresas, p. 8.

AVI KRAINER VP PRODUCT MARKETING. RISCO GROUP

Tecnologías de detección de vanguardia para máxima seguridad

Nueva Generación en Detectores de Intrusión

Los sistemas de intrusión siempre han jugado un papel importante en la protección de las empresas y las instalaciones industriales para mantenerlas a salvo y con los más altos estándares de seguridad.Las aplicaciones comerciales e industriales requieren una gama completa de detectores profesionales para niveles de seguridad de Grado 2 y Grado 3. Dichos detectores deberían ofrecer una fiabilidad extremadamente alta e inmunidad a falsas alarmas, incluso en los entornos industriales más exigentes tanto en interiores como en exteriores.

La gama de detectores de grado comercial incluye detectores volumétricos montados en pared para diversas condiciones ambientales, detectores de techo para diferentes alturas, así como detectores sísmicos, de golpes y de rotura de cristales para aplicaciones de alta seguridad.

¿Qué novedades hay en la tecnología de detección?

Cuando se trata de detectores de movimiento (volumétricos), los detectores de infrarrojos pasivos (PIR) y detectores de doble tecnología (DT) con tecnologías PIR y de microondas, siguen siendo los sensores dominantes en la industria de la alarma de intrusión. En términos de detección, existen 2 parámetros principales que definen la calidad de detección: las tasas de captura y de falsas alarmas. Los algoritmos de detección, la óptica y la elección de los componentes electrónicos definen la calidad de los detectores y los parámetros de rendimiento. Los detectores de nueva generación, sin embargo, no sólo son superiores en términos de diseño de algoritmos, óptica y electrónica, sino que también lucen mejor.

En la era actual, cuando los diseñadores de interiores y los propietarios de casas son muy exigentes acerca del aspecto de cualquier elemento en el hogar o la oficina, los fabricantes de alarmas de intrusión se ven obligados a invertir mucho dinero y esfuerzo en el diseño con formas modernas y elegantes.

Rendimiento superior PIR

Los detectores PIR (infrarrojo pasivo) recogen la energía IR de los objetos cálidos y la traducen al movimiento utilizando lentes especiales junto con el procesamiento digital. Para obtener la máxima eficacia de la detección PIR, la lente debe tener una forma parabólica / convexa.

Sin embargo, debido a consideraciones de fabricación, los detectores PIR típicos están equipados con lentes planas, basadas en la tecnología Fresnel, que simula la curvatura parabólica / convexa. La lente Fresnel consiste en una serie de surcos concéntricos grabados en la superficie de la lente.

El uso de la tecnología Fresnel es muy bueno, de hecho, y está implementado en la mayoría de los detectores PIR. Sin embargo, los detectores con lente parabólica / convexa real proporcionan una mejor eficiencia de la señal IR.

Los detectores modernos, que representan las últimas tecnologías, están diseñados con lentes convexas para proporcionar una recepción de la señal IR más eficientemente. Esta eficiencia se traduce en una mayor relación señal / ruido y, en consecuencia, en niveles sin precedentes de rendimiento de captura e inmunidad a falsas alarmas.

Además, el hecho de que la lente frontal y la zona inferior (fluencia) se fabriquen en una sola pieza utilizando una tecnología de fabricación única, maximiza el área de la superficie de la lente, lo que aumenta aún más el nivel de la señal IR.

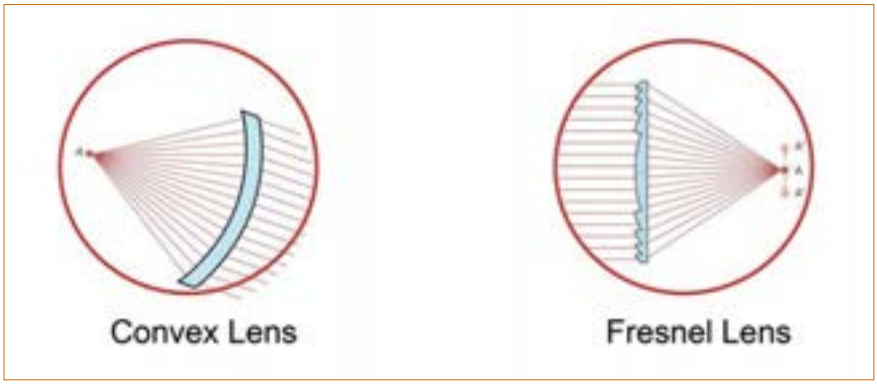
Rendimiento superior de microondas

La mayoría de los detectores de doble tecnología tradicionales están utilizando el rango de frecuencia de banda-X para el canal de microondas. El microondas de banda-X funciona en el rango de 12 GHz.

Los detectores de nueva generación utilizan microondas de banda-K con frecuencias más altas en el rango de 24 GHz.

Debido a la mayor frecuencia, el microondas de banda-K tiene la ventaja de una menor penetración de la pared («sangrado»), por lo que aquellas personas que caminan en un pasillo fuera de la habitación protegida no pueden provocar falsas alarmas.

Por lo tanto, el microondas de banda-K reduce drásticamente las falsas alarmas del canal de microondas, en comparación con el microondas de banda-X, considerándose una solución altamente fiable en la detección actual de doble tecnología.



> «Las empresas pueden disfrutar de estos detectores por un precio asequible

Nueva Generación de detectores

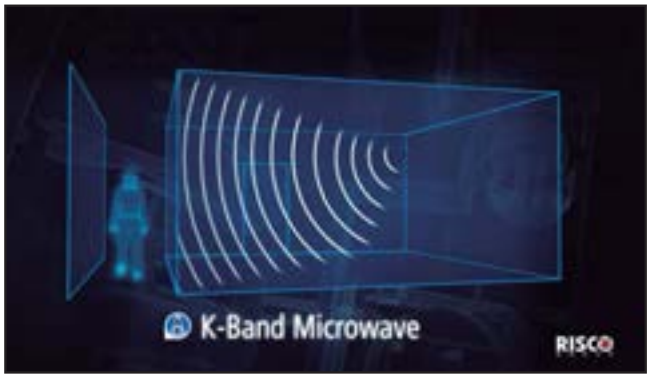
Los detectores que implementan esta combinación de rendimiento superior de PIR y microondas están a la vanguardia de las tecnologías de detección de alarmas de intrusión.

Tales detectores de vanguardia presentan un gran avance en las tecnologías de detección tradicionales y ofrecen un nivel superior de rendimiento de captura y de inmunidad a falsas alarmas.

Anteriormente, los detectores de banda-K eran significativamente más caros en comparación con los detectores de banda-X tradicionales y, por lo general, se reservaban para las aplicaciones de mayor seguridad. Hoy en día, los sensores de movimiento de banda-K tienen precios competitivos y proporcionan un rendimiento de última generación.

Un precio asequible hace que estos detectores de nueva generación estén disponibles no sólo para aplicaciones comerciales e industriales de alto nivel, sino que ahora todas las empresas pueden disfrutar de los beneficios de los niveles de seguridad más altos combinados con la más avanzada inmunidad contra falsas alarmas, independientemente de su tamaño y presupuesto. ●

Fotos: Risco



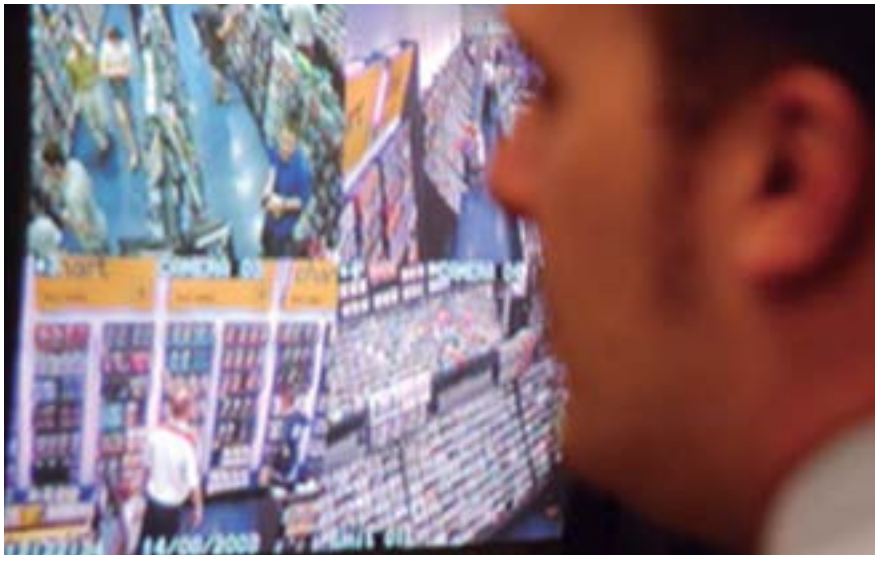
Contactos de empresas, p. 8.

ALEJANDRO GUTIÉRREZ. DIRECTOR DEL ÁREA CUSTOMER EXPERIENCE. JOHNSON CONTROLS

De CRAs a Centro de Gestión Integral de Seguridad

La idea primigenia de una Central Receptora de Alarmas es relativamente sencilla. A través de ella, la compañía de seguridad gestiona las conexiones de los sistemas de seguridad de sus abonados mediante una comunicación 24/7 para proporcionarles seguridad en caso de intrusión. Como gestores de uno de los principales centros de recepción de alarmas de España nuestra labor principal es asegurar las instalaciones de nuestros clientes. Sin embargo, el entorno empresarial evoluciona y cada vez requiere de más valor añadido en los servicios de los que dispone, y somos conscientes de la necesidad de trascender nuestra misión principal para ofrecer al mercado un conjunto de servicios que aporten un valor más allá de la simple detección de intrusiones y, en su caso, el aviso a los cuerpos de seguridad.

ACTUALMENTE, la evolución de la tecnología ha permitido la implantación de sistemas basados en protocolos de internet, que mejoran significativamente las prestaciones tradicionales de los sistemas analógicos, y permiten gestionar todos los datos recibidos de forma mucho más eficaz y eficiente. Sobre esta capa, eminentemente tecnológica, se construyen toda una serie de servicios que permiten elevar el valor de la Central Receptora de Alarmas para que ofrezca soluciones más personalizadas a las necesidades específicas de cada cliente.



Aunque el gran reto de las CRAs sigue siendo mejorar su eficacia a la hora de verificar las señales de alarma que reciben, las capacidades tecnológicas actuales le permiten dar un paso al frente y convertirse en socio estratégico de la empresa, a través de la configuración de servicios de valor añadido para los clientes. Abordarlo requiere integrar los sistemas de seguridad conectados a la central, y añadirles una capa de servicios realizados a distancia, orientados al mantenimiento y gestión remota de sus instalaciones. La gran velocidad de las transmisiones a través de protocolos IP y el mayor ancho de banda disponible actualmente permiten desarrollar estos nuevos servicios.

Estos servicios remotos deben tener como objetivo principal contribuir a que la empresa esté lista para cumplir con todos los requisitos internos, regulatorios y de sus clientes. Así, la CRA ha de tener capacidad para identificar las

amenazas potenciales de cualquier instalación a la que esté conectada, de forma que pueda fortalecer sus capacidades y reducir al mínimo la posibilidad de que se registren incidentes que puedan afectar a su operativa. Y, en caso de que se produzcan, ofrecer a la empresa la respuesta adecuada para su resolución, minimizando el impacto que pueda tener en la organización. Es decir, proporcionar al cliente todos los servicios asociados a la continuidad de utilización de sus instalaciones durante y después de cualquier incidente.

Vídeo Vigilancia

Un buen ejemplo de cómo extender los servicios asociados a la recepción de alarmas podemos encontrarlo en los servicios asociados a la vídeo vigilancia como servicio. Este tipo de servicios gestiona de forma centralizada todos los procesos de monitorización y gestión de las instalaciones de los clientes, incluyendo control de zonas sensibles, apertura y cierre de puntos de acceso, recepción de mercancías o control horario de los empleados. Pero a estos datos se pueden sumar muchos más, procedentes de los puntos de control disponibles en las instalaciones, y así se pueden controlar, desde el mismo punto central, los sistemas de climatización e iluminación, el funcionamiento de ascensores y cualquier otro subsistema que proporcione información sobre el centro.

Con todo ello, se pueden diseñar servicios personalizados, adaptados a las necesidades de cada cliente, para mejorar sensiblemente tanto la seguridad como la gestión de los recursos, al tiempo que se optimiza la operativa general

«Las capacidades tecnológicas actuales permiten a las CRAs dar un paso al frente y convertirse en socio estratégico de la empresa»

de negocio y se analizan los costes generales de mantener la instalación en funcionamiento. Este tipo de soluciones, altamente escalables tanto en la variedad de servicios que prestan como en el número de instalaciones a los que puede aplicarse, permite desarrollar, entre otros, distintos servicios de valor añadido:

• Asistencia a través de vídeo: Ayuda al personal de la organización dando apoyo mediante seguimiento de CCTV mientras por ejemplo los vigilantes salen del parking por la noche. También permite hacer análisis y realizar informes. También puede realizar mapas de calor que permitan identificar las zonas de mayor tráfico de personas, y permite incluso hacer un conteo del número de personas que entra y sale del recinto.

• Auditorías: Permite realizar chequeos remotos del seguimiento de procedimientos internos. La CCTV permite seguir el proceso de caja de manera remota. Por otro lado, hace posible la verificación de indicadores clave de desempeño (KPI).

• Ayuda al cliente: 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: La CCTV ofrece la posibilidad de apoyar las descargas desatendidas de material de los transportistas y seguimientos personalizados de transporte de fondo. También permite verificar el trabajo realizado por las contratas de limpieza y mantenimiento de manera remota.

Continuidad de negocio

Con la finalidad crítica de asegurar la continuidad del negocio de sus clientes, las Centrales Receptoras de Alarmas deben contar con la estructura necesaria para dar servicio en los procesos y operativas de negocio, gestionando adecuadamente los sistemas de TI de la compañía y protegiendo su información. Esto es crucial para mantener la confidencialidad, integridad y disponibilidad de la información de la compañía, de forma que se asegure que solo los usuarios autorizados tienen acceso a la información y a los activos asociados.

En Johnson Controls mantenemos un fuerte compromiso con la innovación y con la aportación de valor añadido a las relaciones con nuestros clientes, para poder ofrecerles las mejores soluciones basadas en sistemas de información eficientes. Así, ofrecemos nuevas posibilidades de integración de productos, instalación y servicio en los ámbitos de seguridad, protección contra incendios, sistemas de control y proyectos de climatización. La combinación de todas estas fortalezas, y su gestión a través de un punto centralizado de atención a las necesidades de cada cliente, nos permite suministrar la cartera más completa de servicios asociados al control total de las instalaciones de los clientes. ●

Fotos: Johnson Controls

Contactos de empresas, p. 8.

ENJOY SAFER TECHNOLOGY™

ADAPTA TU EMPRESA A LA NORMATIVA DE PROTECCIÓN DE DATOS

PROVEEDOR Nº 1 DE LA UNIÓN EUROPEA EN CIBERSEGURIDAD EMPRESARIAL

MADE IN EU

ventas@eset.es
96 291 33 48

www.eset.es

MARILUZ CEJAS. RESPONSABLE SAT BARCELONA DE BY DEMES GROUP

«No hay mayor satisfacción que ayudar al cliente que está al otro lado del teléfono»

La tecnología la atrajo desde pequeña y a los 10 años de edad ya estaba programando. Desde hace 11 años trabaja en el campo de la seguridad electrónica, un mundo aún predominantemente masculino en el que mujeres como Mariluz Cejas van abriéndose camino. La responsable técnica de By Demes explica en esta entrevista los retos de futuro de la compañía y las tendencias tecnológicas de un campo en el que continúa aprendiendo cada día para hacer frente a nuevos retos.

Como responsable técnica de By Demes, ¿cuáles son los objetivos de la compañía en este ámbito?

—Los objetivos de By Demes en este ámbito son claros y muy bien definidos, y son dar la respuesta más rápida de la manera más eficiente y eficaz a los clientes que se ponen en contacto con nosotros para resolver cualquier duda o incidencia técnica que se les plantee. Para ello, se han implementado una serie de procedimientos y estrategias para mejorar nuestro servicio post-venta, y que están dando muy buenos resultados.

—¿En qué proyectos está actualmente trabajando?

—Principalmente estoy muy implicada con el seguimiento de incidencias, mejoras, controles de calidad y todas aquellas herramientas que hemos puesto al servicio de nuestro cliente para que aumente su nivel de satisfacción con nuestro departamento técnico, como los cursos on-line, por ejemplo.

Solución de detección de fuego forestal de SR7, formada por cámaras térmicas instaladas en unidades Pan-Tilt para un control panorámico 360º de hasta 15 km de radio.

—¿Qué aspectos considera imprescindibles a la hora de elegir un sistema electrónico de seguridad?

—Lo principal, a mi parecer, es la estabilidad en las comunicaciones, ya sea con el cliente final o bien con la central receptora.

Igualmente, es muy importante que el sistema que decidamos instalar sea flexible, que admita elementos cableados y un vía radio estable, el cual nos avise en caso de intento de inhibición. Esto sólo lo pueden ofrecer fabricantes que llevan años en el mercado, con importantes ingenieros en sus filas dedicados a mejorar el rendimiento de los

sistemas e innovar con soluciones IoT, pero sin sacrificar lo más importante, que es la seguridad del cliente final.

—¿Qué tecnologías cree que serán tendencia a corto plazo?

—Como he dicho anteriormente, lo que ya tenemos pero que se encuentra en desarrollo y creciendo a una velocidad sorprendente es la tecnología IoT. Consiste en que un grabador, por ejemplo, nos pueda dar la temperatura y humedad de cada una de las estancias de nuestro domicilio, nos avise cuando haga más calor de lo estipulado y a su vez nos encienda el aire acondicionado, si eso pasara dentro de un horario determinado. Eso ya está aquí y es real.
Las soluciones térmicas van a dar mucho de qué hablar también, sobre todo a la hora de detección de intrusión, pero más aún para la detección precoz de conatos de incendio, algo que en nuestro país está a la orden del día.
Y por último el Deep Learning. Dispositivos capaces de determinar si lo que nos ha generado la alarma ha sido un vehículo, una persona, o bien la rama de un árbol, sin necesidad de intervención por parte de ningún operador, lo cual nos ayuda a reducir el número de falsas alarmas y a aumentar la utilidad y eficacia de nuestros sistemas.

—En un plano más personal, ¿cuál es su impresión al pertenecer profesionalmente a un sector tradicionalmente masculino?

—Es cierto que muchos clientes se sorprenden de que sea una chica la que les contacte, e incluso algunos dicen que «ya era hora», pero en definitiva te das cuenta de que debemos dejar de lado las discriminaciones positivas y/o negativas y admitir que cuando alguien es profesional, su género es irrelevante.
Por el momento y siendo sincera, no he sufrido ningún tipo de discriminación, ni mala cara en los 11 años que llevo en el mundo de la seguridad electrónica, todo lo contrario. Me da pena que no seamos más, por lo que desde aquí animo a todas las chicas a no tener miedo a trabajar en este sector y demostrar todo su potencial.

Equipo del SAT de By Demes Barcelona.

—¿Por qué ha escogido el mundo de la tecnología para su futuro?

—Desde pequeña me ha atraído la tecnología. Con 10 años ya estaba programando y mis padres siempre me han motivado a dedicarme a lo que me gusta, pese a que en aquellos años la gente dijera que «eso es para chicos».
Lo bonito que tiene el mundo de la tecnología es que no se detiene, que cada día hay cosas nuevas, que jamás vas a dejar de aprender y que nunca te va a dejar de sorprender.

—¿Qué es lo que más le gusta de su profesión?

—Lo que más me gusta de mi profesión es el poder solucionar problemas y no parar de aprender. Me encantan los retos, cada incidencia que se plantea lo es para mí, y no hay mayor satisfacción que ayudar a quien está al otro lado del teléfono y poderme felicitar a mí misma y crecerme por ello. ●

Fotos: By Demes

Contactos de empresas, p. 8.

ENRIQUE BILBAO LÁZARO. DIRECTOR TÉCNICO DE CUEVAVALIENTE INERCO.

La Dirección de Obra en la instalación de Sistemas de Seguridad

Una función necesaria no demasiado conocida ni recogida por la legislación de Seguridad Privada

La instalación de un Sistema de Seguridad de una cierta entidad (plantas industriales, edificios de oficinas, hospitales, estadios, centros penitenciarios, etc.) es un proceso complejo, que se conjuga con la instalación de otros Sistemas: climatización, electricidad, comunicaciones, etc., con afecciones cruzadas entre estas actividades y una imprescindible coordinación. Cambios en el avance de la obra, arquitectónicos, de usos, de nuevas circulaciones, obligan a la adopción a su vez de retoques en la instalación proyectada.

ESTE tipo de Sistemas de Seguridad abundan en España, y están lógicamente sometidos a la legislación aplicable de Seguridad Privada. Muchos de ellos se corresponden con los centenares de Instalaciones Críticas, por lo que también son aplicables a ellas las disposiciones legales de Protección de Infraestructuras Críticas.

Responsabilidades

Estos Sistemas de Seguridad de una cierta complejidad se contratan con empresas de Seguridad autorizadas para la actividad de instalación y mantenimiento de Sistemas de Seguridad, de acuerdo con el artículo 5.f de la Ley de Seguridad Privada, al disponer de un Centro de Control normalmente como parte del Sistema.

Esta contratación se realiza habitualmente mediante un concurso basado en un Proyecto del Sistema realizado previamente, sobre el que las empresas instaladoras calculan y ajustan sus ofertas.

El resultado es que la empresa instaladora adjudicataria del contrato consiguiente debe ejecutar una instalación de acuerdo con un Proyecto que no ha realizado, sino que le ha venido impuesto por la Propiedad.

Sin entrar en este artículo en las contradicciones de esta situación en su fase de Proyecto, que sería materia para otro artículo al respecto, la Ley establece que en la ejecución y puesta en marcha del Sistema de Seguridad hay dos responsabilidades en juego.

Por una parte, el director de Seguridad que operará ese Sistema, según el artículo 36.1 a, b, c, d, e y f, tiene la responsabilidad final del estado y funcionamiento del Sistema implantado, y de su coherencia con los riesgos evaluados y con su adecuación a la legislación y normativa técnica aplicable.

Por otra, la empresa instaladora del Sistema, según lo establecido en el artículo 51.7 «…serán responsables de su correcta instalación, mantenimiento y funcionamiento…».

Esta doble responsabilidad está pendiente de aclarar y delimitar en el desarrollo reglamentario de la Ley que, como es conocido, lleva más de tres años sin publicarse tras la entrada en vigor de la Ley.

Mundo real

En cualquier caso la realidad es tozuda y, por la cuenta que le trae, la Propiedad (a la que debe pertenecer el director de Seguridad si es que ha sido nombrado durante la ejecución del Sistema) necesita garantizar que el Sistema de Seguridad, como el resto de los Sistemas de la obra, ha de ser instalado y puesto en funcionamiento según el Proyecto con el que se adjudicó, vigilando tanto sus prestaciones y calidad de los materiales instalados, como que la medición resultante se ajuste al presupuesto adjudicado.

Por lo tanto, en el «mundo real» las instalaciones de Sistemas de Seguridad se rigen por las mismas buenas prácti-

cas técnicas de la ingeniería de instalaciones de las obras, bajo la responsabilidad final de la Dirección Facultativa de la obra.

Como ocurre con otras especialidades la Dirección Facultativa cuenta por un lado con la subcontratación a ingenierías especializadas del control de la obra (ascensores, climatización, etc.) y con la interlocución con la Propiedad que, en algunos casos, tiene su propia supervisión de la obra en temas sensibles como las redes informáticas o… la Seguridad.

El resultado final de esta situación «de facto» es que inevitablemente existe una actividad necesaria de Dirección de Obra de la instalación del Sistema de Seguridad que se realiza por ingenieros especializados pertenecientes a la Propiedad, a una empresa de Ingeniería o por un ingeniero en ejercicio libre de la profesión, no considerados con suficiente claridad en la Ley de Seguridad Privada ni en el borrador del Reglamento, aún no aprobado.

Dirección de obra eficaz y rentable

Haciendo abstracción de las contradicciones regulatorias de esta actividad, el hecho es que la Dirección de Obra de las instalaciones de Sistemas de Seguridad, es una actividad necesaria, que se lleva a cabo habitualmente con mayor o menor eficacia y que, sin duda, se seguirá demandando y ejecutando.

Fundamentalmente la actuación del ingeniero o ingenieros que lleven a cabo la tarea de Dirección de Obra del Sistema se puede desglosar en las siguientes actividades:

Conocimiento profundo del Proyecto del Sistema de Seguridad a ejecutar

Normalmente el Proyecto lo ha realizado su empresa o incluso el mismo

ingeniero, ya sea como empleado de una empresa de ingeniería, empleado de la Propiedad o ingeniero autónomo.

Visado del encargo de la Dirección de Obra

No siempre es necesario este trámite, pero sí es aconsejable en el caso de haber sido visado en un Colegio Profesional de Ingeniería (Industrial, Telecomunicación) el Proyecto.

Replanteo de la instalación al inicio de la Obra

Esa reunión inicial, de la que se levanta acta por el ingeniero de Dirección de Obra, se realiza con la empresa adjudicataria (instaladora de Seguridad), con el fin de disipar dudas que puedan aparecer inicialmente y solicitar los primeros documentos de la obra: plan de trabajos, documentos de Seguridad y Salud, listado de trabajadores con los correspondientes permisos y certificados, etc.

Reuniones periódicas de supervisión de la obra

Pueden (y suelen) ser conjuntas con otras especialidades de la obra, debido a la necesaria coordinación con otros oficios como canalizaciones, redes de datos, planes de albañilería y obra civil, etc. Estas reuniones deben servir también para supervisar la correcta instalación del Sistema, la disposición de elementos según lo especificado en el Proyecto, aclaración de dudas, autorización de cambios en función de cambios de la obra, etc. Lógicamente acompañadas de las correspondientes actas y mediciones para, en su caso, certificación parcial de la instalación para su facturación.

Pruebas parciales

Durante las reuniones periódicas se suelen presentar los resultados de las pruebas aisladas de los elementos que se van instalando, con el fin de que en las pruebas finales no haya que recurrir a pruebas individuales de sensores o cámaras de televisión, por ejemplo. El protocolo de dichas pruebas y los resultados de las mismas han de ser supervisados por la Dirección de Obra.

Entrega y puesta en marcha (Commissioning)

Las reuniones finales que se precisan para la entrega definitiva del Sistema son lógicamente de gran importancia, de cara a garantizar a la Propiedad que el Sistema responde a lo proyectado, que las facturas correspondien-

tes son adecuadas y que el Sistema va a operar correctamente.

En estas reuniones se deben realizar por la Dirección de la Obra las siguientes actividades:

• Supervisión de las pruebas de funcionamiento de todo el Sistema, incluyendo la correcta parametrización del software del Sistema de Control. Esta revisión se puede hacer de forma aleatoria según la norma ISO 2859.1:1999.

• Supervisión de los detalles de instalación: marcado de cableados, estado de canalizaciones y cajas de conexión, tomas de tierras, etc.

• Revisión de la documentación final de la instalación: planos «as built», esquemas de conexionado, manuales de operación, manuales técnicos de los elementos (esta documentación permitirá libertad de contratación del mantenimiento a la Propiedad).

• Revisión de la documentación legal de la instalación: certificado de la empresa de Seguridad instaladora, libro de mantenimiento, etc.

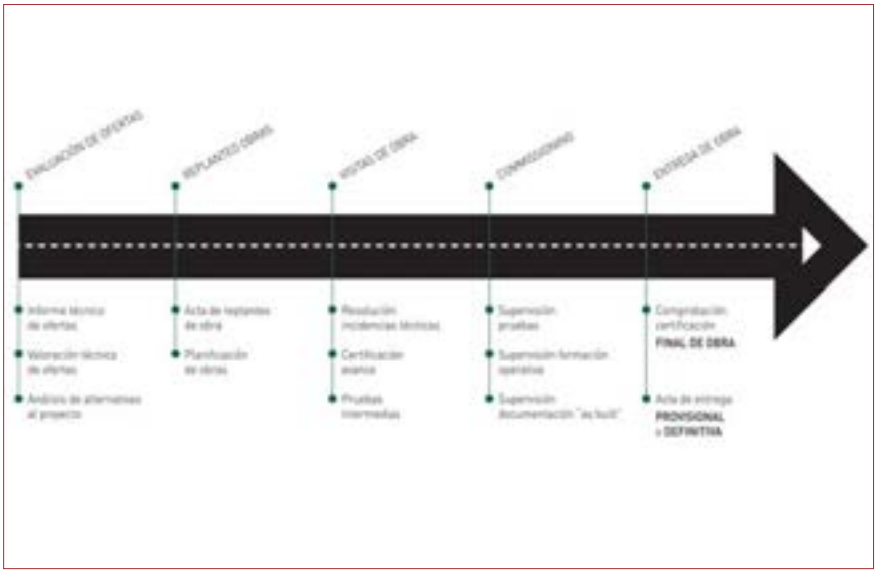
• Supervisión de la formación a impartir por la empresa instaladora a los vigilantes y operadores del Sistema de Seguridad.

• Revisión de la certificación final y de la facturación correspondiente a la Propiedad.

• Redacción de la relación de detalles a corregir.

• Firma del acta de recepción provisional.

En algunas ocasiones, cuando la ingeniería que realiza la Dirección Facultativa es de propósito general, no realizada por especialistas de Seguridad, la actividad de Entrega y Puesta en Marcha, o Commissioning, se contrata de forma separada con especialistas en ingeniería de Sistemas de Seguridad, para garantizar al menos la fase final de la ejecución del Proyecto.



Conclusiones

La realización de todas estas actividades descritas de Dirección de Obra es determinante, garantizando que el sistema funcione correctamente con las calidades, las prestaciones y la operativa definidas en el Proyecto durante el tiempo suficiente que garantice a la Propiedad un retorno de la inversión. Resultan pues de una gran eficacia para la Propiedad, y la repercusión de su coste en el montante total de la inversión es muy inferior a los ahorros conseguidos en la ejecución de la instalación.

En Cuevavaliente INERCO tenemos la fortuna de contar con la confianza de muchos clientes, en España y en Iberoamérica, que han contratado nuestros servicios en Dirección de Obra de instalaciones complejas de todo tipo: edificios en altura, centros logísticos, centros hospitalarios, fábricas, instalaciones energéticas, centros penitenciarios, etc.

> «La empresa instaladora del Sistema, según el artículo 51.7 de la Ley de Seguridad Privada ...será responsable de su correcta instalación, mantenimiento y funcionamiento...»

Es de especial satisfacción sentir la utilidad del trabajo de nuestros ingenieros en este terreno.

Sería importante para la regulación de esta actividad que el futuro Reglamento estableciera la necesidad de que se acreditaran como Ingenieros de Seguridad no sólo los que prestan sus servicios en las empresas instaladoras, sino todos aquellos que lo hacen (y lo van a seguir haciendo) en los Proyectos y Dirección de Obras ajenos a esas empresas, contratados por los usuarios de la Seguridad en sus plantillas laborales, o a través de empresas de ingeniería o como ingenieros autónomos. ●

Fotos: Cuevavaliente Inerco

Contactos de empresas, p. 8.

ESPAÑA BRASIL CHILE COLOMBIA MÉXICO PERÚ PORTUGAL ESTADOS UNIDOS

Independencia de fabricantes y empresas de seguridad

cue>a>aliente

INERCO

DEPARTAMENTOS DE SEGURIDAD

Análisis de Riesgos, Auditorías,
Implantación de Sistemas de Gestión,
Determinación de métricas de Seguridad,
Redacción de procedimientos.

Asesoramiento para cumplimiento de legislación PIC a Operadores Críticos

INGENIERÍA DE SISTEMAS

Realización de Proyectos de Sistemas de Seguridad
Dirección de Obra de instalaciones de Sistemas de Seguridad

+300 proyectos de seguridad

www.**cuevavaliente**.com info.cuevavaliente@inerco.com +34 **918 047 364**

ÓSCAR PASCUAL SANZ. DIRECTOR DE OPERACIONES-ESPAÑA. ADVANCE SECURITY BUSINESS GROUP

La problemática del análisis de riesgos en zonas críticas y países de alto riesgo

El papel de la inteligencia estratégica y prospectiva

«Las metodologías de análisis habituales resultan ineficaces ante los riesgos extremos de muy baja probabilidad. No basta con trabajar únicamente con los riesgos más probables, hay que considerar también los más peligrosos en un entorno dinámico y cambiante. El papel de la Inteligencia Estratégica y Prospectiva cobra en estos casos una especial importancia».

EL Análisis y Gestión de Riesgos para la Seguridad de Organizaciones que operan en Zonas Críticas o Países de Alto Riesgo, es algo que difiere tanto en la teoría como en la práctica de los planteamientos y condicionantes habituales.

Un entorno hostil, dinámico, desequilibrado y hasta cierto punto desconocido, la presencia de terrorismo extremista, crimen organizado, narcotráfico, blanqueo de capitales, etc., todo ello en un ambiente con factores potenciadores tales como la pobreza, conflictos religiosos y político-sociales… configura unos escenarios de riesgo con características muy cercanas al modelo «Cisne Negro» enunciado por Nassim Nicholas Taleb en su ensayo «El cisne negro: el impacto de lo altamente improbable» (2007).

El Análisis de Riesgos como punto de partida para cualquier planificación en seguridad, no resulta eficaz ante riesgos de impacto extremo pero con ínfima probabilidad o probabilidad imposible de estimar. Por este motivo, vamos a ver cómo la protección de personal expatriado, infraestructuras ferroviarias, energéticas, fábricas e instalaciones sensibles - tanto públicas como privadas- obligan no sólo a un estudio pormenorizado del contexto, sino obligatoriamente al empleo de Hipótesis de Inteligencia.

Trabajar desplazado en estos países es cada vez más común, llegándose incluso a tratar la figura del expatriado como perfil de vida laboral. Ya no se requiere pertenecer a una gran multinacional, sino que cualquier empre-

sa puede tener intereses en estas Zonas Críticas, bien directamente o como subsidiaria de otra matriz. Bajo estas circunstancias, escenarios de riesgo con similares causas y actores, se plantean también en el ámbito público en sus diferentes instalaciones oficiales y diplomáticas, tales como consulados, embajadas, etc.

La Inteligencia como «herramienta de apoyo para la toma de decisiones» resulta ahora imprescindible por su capacidad de reducir la incertidumbre, en el proceso de Análisis de Riesgos orientada a la detección de vulnerabilidades y como «herramienta de prevención y alerta».

Las amenazas «previsibles» se gestionarán como «Escenarios de Riesgo» en los que actuaremos sobre los aspectos de prevención y mitigación. Las «imprevisibles» o de sorpresa estratégica, por su impacto extremo pero probabilidad despreciable, se gestionarán como «Escenarios de Desastre», reduciendo con ello al máximo su impacto potencial.

Al igual que a nivel empresarial tenemos el Plan de Continuidad de Negocio (BCP), elaborado tras el correspondiente Análisis de Impacto (BIA), en el plano de la Seguridad Integral dispondremos también de Planes de Contingencia, compuestos por otros complementarios entre sí, tales como el de alarma, emergencia, evacuación, confinamiento, repatriación… siempre bajo las limitaciones impuestas por el ritmo de la «eficacia operativa» y el factor «tiempo de reacción».

Y aunque el objetivo principal sea la prevención, hemos de decir que una reacción oportuna, prevista y organizada disminuirá sin duda la magnitud del daño que el adversario pretenda causar en nuestra Organización. No olvidemos que hay vidas humanas sobre el tablero. Incluso opciones como la transferencia del riesgo, aunque en ocasiones deben realizarse, pierden en gran parte su efectividad como forma de gestión.

Estimación del Riesgo

Si bien la UNE-ISO 31000: Gestión del riesgo. Principios y Directrices, define el riesgo como «Efecto de la incertidumbre sobre la consecución de los objetivos» y por tal motivo incluye tanto «amenazas» como «oportunidades» para las Organizaciones, es evidente que desde el punto de vista de la seguridad, se estudia exclusivamente la vertiente negativa de la incertidumbre, es decir, únicamente la posibilidad de que se materialicen las amenazas a que se encuentran expuestas.

Por tanto para nuestra dirección y gestión de la seguridad podemos afirmar que «riesgo es la contingencia de que un bien sufra un daño». Recordemos que el riesgo es un aspecto cuantificable y medible en términos adimensionales, con valores que si bien relativos, nos sirven para comparar tras su análisis los diferentes tipos entre sí.

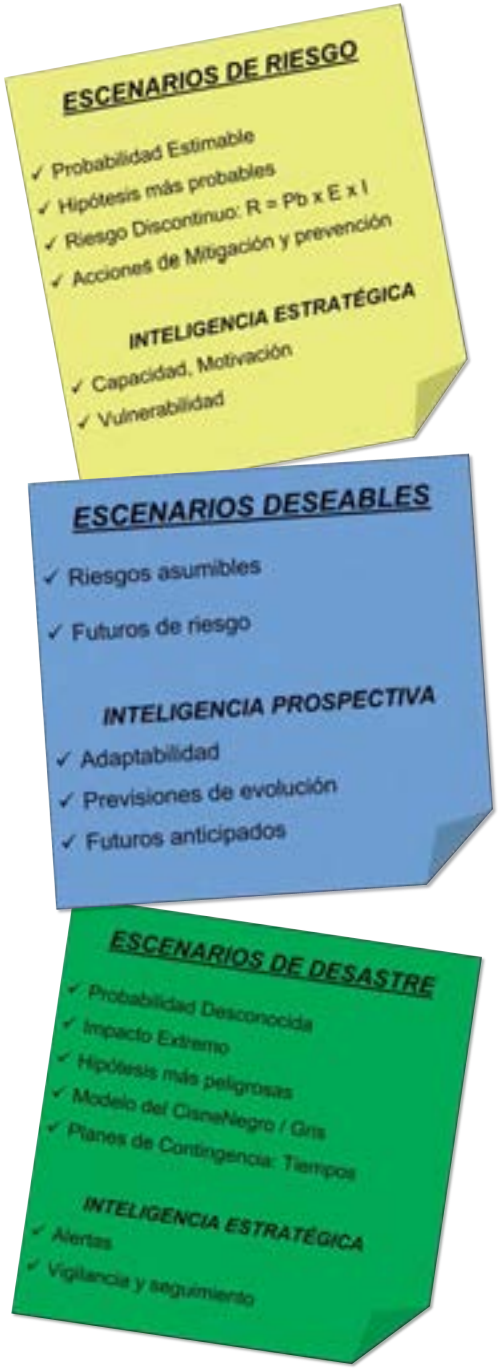
Todas las metodologías de análisis tanto específicas como genéricas, cuantitativas, cualitativas o mixtas, pasando desde la matriz probabilidad-impacto, Método Mosler, William T. Fine, Kinney, Magerit o hasta la técnica más compleja, se basan en realizar el producto de la «probabilidad de materialización» de una amenaza (Pb), por el valor de la «magnitud del Impacto» (I) o daño producido.

Su expresión matemática R = Pb x I resulta acorde con lo indicado en la ISO-GUÍA 73:2009, apartado 3.6.1.8: «el nivel de riesgo se ha de interpretar en términos de combinación de consecuencias y probabilidad».

Problemática

El sistema lleva implícito un problema que resulta especialmente grave en Zonas Críticas o Países de Alto Riesgo: ¿Qué ocurre con los eventos de muy alto impacto pero muy baja probabilidad?

Desde agresiones oportunistas hasta las más meticulosamente planificadas, existe un heterogéneo abanico de amenazas: secuestros, extorsiones, terroristas suicidas, asaltos organizados, búsqueda indiscriminada de víctimas,



empleo de artefactos tipo NRBQ... tácticas no convencionales que aumentan la peligrosidad con sus rápidos y continuos cambios, bajo la potencialidad que le otorga al adversario un habitual dominio del terreno y con ello la facilidad de obtener información de explotación inmediata.

Cuando la probabilidad de un suceso es muy baja o prácticamente nula, por elevado que sea el posible impacto, el citado proceso matemático de cálculo (cuyo resultado tenderá siempre a cero), llevará bien a que el nivel de riesgo estimado sea finalmente bajo, pasando desapercibido, o bien a que no se justifique la adopción de las correspondientes medidas de seguridad que podamos proponer.

Estamos ante lo que algunos autores denominan «Cisne Gris», un suceso conocido o que sabemos que puede ocurrir, que causaría daños enormes, pero cuya probabilidad de ocurrencia es prácticamente despreciable (en el caso del «Cisne Negro» aunque con un impacto igualmente extremo, no se concibe la posibilidad de que pueda ocurrir el evento hasta que éste no se ha producido).

Si tuviésemos una cantidad ilimitada de recursos económicos y de capacidad de estudio, podríamos intentar controlar casi todos los eventos razonables, pero este supuesto es inalcanzable.

La figura de un analista de riesgos con conocimientos y plena conciencia sobre las limitaciones metodológicas de sus análisis y los puntos críticos a vigilar, resulta la clave de un Plan de Seguridad acertado o de una auditoría eficaz.

No basta con trabajar bajo las hipótesis más probables, se deben contemplar obligatoriamente las hipótesis más peligrosas. Una probabilidad muy baja no presupone suprimir una amenaza del estudio, hay que potenciar la consideración de los eventos de alto impacto pese a su escasa probabilidad.

Por ello el Análisis de Riesgos ya no debe basarse en meros estudios de información puntual, estadísticas e historiales, sino en las hipótesis de inteligencia elaboradas por los correspondientes órganos especializados.

La Seguridad no debe de ser únicamente reactiva, sino esencialmente preventiva y toda la planificación debe contemplar no ya el momento actual, sino los posibles escenarios futuros. Es la única forma de reducir la aparición de sucesos inesperados, en los que su inmediatez y rápido desarrollo, supere nuestra capacidad de adaptación en los plazos de tiempo exigidos por la operatividad y eficacia.

Las amenazas evolucionan y la seguridad debe ser proactiva apoyándose para ello en un sistema de inteligencia estratégica y prospectiva.

La mitigación del riesgo y el resto de acciones de gestión se orientarán a modificar los escenarios futuros de riesgo, reduciendo los escenarios de desastre mediante estrategias de seguridad que comienzan en el presente y nos llevan a situaciones futuras lo más favorables posible y acordes a la «apetencia al riesgo» soportada por nuestra Organización.

El papel de la Inteligencia

Surge por todo ello la siguiente cuestión: ¿en qué parte de la apreciación del riesgo juega la Inteligencia un papel más significativo?

Cierto es que la inteligencia sirve de apoyo a la decisión en todas las facetas de la Seguridad, pero referidos al Análisis de Riesgos, debemos estudiar por separado cada factor de nuestra ecuación anterior (R = Pb x I) para justificar en qué factores cobra mayor importancia.

La probabilidad (Pb) de que se materialice la amenaza, será función de la Capacidad del adversario (C), su Motivación (M) y la Vulnerabilidad (V) de nuestro sistema de protección y seguridad. Pb: f (C, M, V)

Dos factores dependerán del adversario (Capacidad y Motivación) y un tercer factor dependerá sobre todo de nuestra propia planificación en seguridad (Vulnerabilidad).

Son principalmente el estudio de la Capacidad (C) y la Motivación (M) los que como componentes de la amenaza, sujetos a continuos cambios, obligan a realizar un estudio del contexto basado en Hipótesis de Inteligencia. Precisaremos no sólo del habitual «informe riesgo-país», como situación actual del entorno, sino de informes de inteligencia sobre capacidades operativas, grado y tipo de motivación del adversario e hipótesis sobre su posible desarrollo estratégico.

Cierto es que frente las múltiples posibilidades que aporta la considera-

ción de las diferentes informaciones y fuentes, la elaboración de inteligencia utiliza en ocasiones metodologías analíticas tales como la Matriz de Análisis Estructural MIC MAC o el Análisis de Hipótesis ACH, etc., pero ambas disciplinas, «Elaboración de Inteligencia» y «Análisis de Riesgos», son totalmente diferentes. Nunca un Análisis de Riesgos elabora Inteligencia, sino que debe utilizar los productos perfilados por ésta, pasando en todo caso a constituir una «necesidad» más a cubrir con su ciclo de funcionamiento.

Por otro lado la determinación de la Vulnerabilidad (V) como componente del primer factor de la ecuación, se corresponde a los estudios previos para la elaboración del Plan de Seguridad, la fase de verificación de su ciclo PDCA o bien a una posible auditoría del mismo (siempre considerando la planificación en su globalidad: seguridad de instalaciones, información, personal expatriado, etc.).

La valoración del Impacto (I), abarcará el posible daño a todos los activos, desde la vida e integridad de las personas como bien prioritario, hasta los bienes muebles e inmuebles, pasando por los importantísimos activos inmateriales (información, pérdida de confianza de clientes, de terceras partes interesadas o de los propios trabajadores), imagen de la compañía, cotización en bolsa si la hubiera, responsabilidad social, etc.

Riesgos discontinuos

Pero al gestionar riesgos tan elevados como los existentes en estas situaciones, surge un último problema que solventar. La discontinuidad a la Exposición (E) ante la situación de riesgo.

Dado que debemos optimizar los medios humanos y materiales para mitigar el riesgo, no parece correcto simplemente comparar entre sí un valor numérico de un nivel «muy alto», proporcionado por una situación que se produce tan sólo muy esporádicamente, con un valor «alto» que se produce con otra situación pero esta vez de forma continuada.

De nuevo la matemática parece poco eficaz e inclinaría la balanza hacia el nivel de riesgo «muy alto» frente al segundo caso, cuyo riesgo si bien es menor en magnitud (alto), su nivel de exposición permanente debería obligar a atenderlo o a dedicar un esfuerzo organizacional posiblemente por encima del primero.

Por ello pasamos ahora a incluir el término «Criticidad» (Cr) que dependerá del valor de la Exposición (E) y del impacto (I). C: f (E, I)

Métodos de análisis como William T. Fine (1971) o el método Kinney (1976), ya contemplan el factor de la «exposición al riesgo» como un elemento de estimación del riesgo discontinuo. La expresión del riesgo discontinuo en función del grado de Exposición (E) queda así:

R = Pb x I x E o bien R = Pb x Cr siendo el valor Cr tal y como se ha dicho, la magnitud de la criticidad.

Ambas metodologías están bastante extendidas en el ámbito de la prevención de riesgos laborales (PRL) siendo además William T. Fine muy empleado como modelo de análisis Mixto Cuantitativo-Cualitativo en seguridad. Originalmente se basó en estudios empíricos sobre heridos producidos en el ámbito Naval Norteamericano, siendo publicado en 1971 bajo el título «Mathematical Evaluation for Controlling Hazards» por su Naval Ordnance Laboratory.

En zonas críticas o países de alto riesgo, se deben emplear metodologías diseñadas para el análisis del riesgo discontinuo, tomado como base cualitativa no únicamente nuestro propio estudio del contexto, el cargo empresarial, cultura organizacional, necesidades laborales, etc. sino las hipótesis de inteligencia relacionadas con los factores abarcados por el concepto de probabilidad: capacidad del adversario, motivación y vulnerabilidades propias frente a sus capacidades operativas.

En cuanto a las vulnerabilidades propias, el concepto de la globalidad es el protagonista para la protección del personal expatriado. Un análisis completo debe incluir también sus posibles actividades y comportamiento durante el tiempo de ocio y descanso.

Ante el riesgo discontinuo, se recomienda adaptar el empleo de la Matriz Probabilidad-Impacto a un sistema del tipo Probabilidad-Exposición-Impacto o Probabilidad-Criticidad, y en el caso de metodologías tipo William T. Fine, adaptar cuidadosamente los «criterios explicativos de selección de los valores» de sus tablas, a nuestras necesidades prácticas.

Recordemos que ambos métodos

tienen un considerable grado de subjetividad y que lo importante no es el valor numérico final considerado de forma aislada, sino la posibilidad que supone la aplicación de un método idéntico para todos los riesgos.

Nuestro objetivo final tras la apreciación de los riesgos, es priorizarlos según su magnitud, para facilitar su gestión y en definitiva ponderar los medios y procedimientos de protección hacia unas vulnerabilidades u otras.

Por tal motivo el orden de prioridad resultante será equivalente, bien sea empleando el sistema matricial, que proporciona un desarrollo lineal de la función riesgo, o bien un sistema tipo William T. Fine, que emplea una escala logarítmica creciente, en la que a partir de la selección de un parámetro muy alto, los resultados se empiezan a disparar exponencialmente a la alza.

Propuestas

Como conclusión ante la problemática expuesta, podemos concluir como recomendaciones a la hora de analizar riesgos en Zonas Críticas:

• Complementar los estudios del contexto interno y externo de la organización con productos de inteligencia estratégica y prospectiva, que nos ayuden a alcanzar escenarios futuros sin desastres, ni interrupciones en las actividades desarrolladas.

• Estimar la probabilidad de materialización de las amenazas considerando la capacidad del adversario, su motivación y nuestras vulnerabilidades ante su operativa actual y tendencias futuras. De nuevo apoyados en la Inteligencia.

• Incluir la gestión del riesgo frente a eventos de muy alto impacto y muy baja probabilidad. Requiere una actitud proactiva del analista para que no sean suprimidos matemáticamente al aplicar las metodologías de análisis. Se debe alertar sobre estos tipos de riesgo, para que se proceda a incrementar su vigilancia, así como el componente reactivo de la seguridad. En este sentido hay que difundir, implantar y verificar los correspondientes Planes de Contingencia, de Repatriación, etc. que reduzcan al máximo el Impacto. Una amenaza puede sorprender respecto al momento de su materialización, pero los impactos sea cual sea su origen, deben estar previstos evitándose así un desastre.

• Emplear metodologías de análisis que consideren la exposición discontinua al riesgo.

• Vigilar los riesgos en tiempo real, especialmente los «cisnes grises», apoyados en los puntos críticos e indicios que nos proporciona la Inteligencia Estratégica y Prospectiva. ●

Fotos: shuterstock

Contactos de empresas, p. 8.

Asamblea General de Tecnifuego 2018

La Asamblea General de Tecnifuego 2018 aprobó cambios importantes que supondrán una mejora en el desarrollo de la asociación que ahora cumple 25 años. El primero es un cambio de nombre, que queda como Tecnifuego, Asociación Española de Sociedades de Protección contra Incendios y, en segundo lugar, una adaptación de los Estatutos y el reglamento de régimen interno para modernizar y actualizar la estructura asociativa, y de este modo ganar en dinamismo y eficacia en la gestión. Además, se ha planteado promover el asociacionismo hacia una Federación de asociaciones territoriales de empresas de seguridad contra incendios, con el fin de consolidar la unidad de criterios e intereses y estar más cerca de las administraciones locales.

El presidente de Tecnifuego, Adrián Gómez, hizo un análisis de la propia actividad sectorial-empresarial: «El futuro está en nuestras manos. Debemos trabajar intensamente por el futuro si queremos reforzar el sector y mejorar la competitividad. Para ello, debemos utilizar las herramientas que mejor manejamos, que son la especialización, la calidad y la formación continua. Hay que desenmascarar el falso mito de los que dan duros a pesetas. En seguridad contra incendios no se debe buscar el abaratamiento de costes sin más, la calidad, la especialidad, la eficacia priman para obtener la seguridad. Esas son las armas que debemos emplear para aumentar nuestra presencia en el mercado, y hacerlo entender a los que participan en las contratas».

El presidente informó de la necesidad actual de apoyarse en un equipo de gobierno para avanzar, actualizar y modernizar la Asociación: «Van a ser unos años de intensa actividad que requieren una concentración en el trabajo, en manos de un equipo de socios expertos en las grandes áreas que conforman la Asociación, protección activa y protección pasiva». A continuación, Marta Peraza, secretaria general de Tecnifuego, hizo un repaso de las actividades principales detalladas en la Memoria 2017, por bloques de actividad. Del área técnica que promueve el desarrollo normativo y la adecuación del sector a la realidad, destacó las actividades de los Comités sectoriales, el apartado de certificación AENOR, calificación de Cepreven y el de normalización UNE, donde Tecnifuego ocupa la secretaría técnica, y que ha tramitado 8 normas durante 2017; así como la presencia en los comités europeos de normalización. En comunicación, sobresale el aumento del tráfico web en un 80 por ciento (visitas y usuarios), y los datos aportados por la auditoría externa sobre las notas publicadas que alcanza a más de 2 millones y medio de audiencia, y más de 160.000 euros en valoración económica. En formación y divulgación, mencionó la celebración de los clásicos Días del Fuego (celebrados en Murcia, Madrid y Barcelona).

Marta Peraza informó también de los convenios de colaboración con entidades afines, para reforzar las acciones de interés común, como AES, ASEPAL, CEPREVEN, APTB, y AMPIMEX.

A destacar dos porcentajes muy positivos, uno económico, el aumento de la facturación del sector durante 2017 en un 7 por ciento, hasta alcanzar 2.600 millones de euros. Y otro asociativo, aumento del número de asociados en un 10 por ciento, hasta los 143 asociados.

Dentro de las actividades de 2018, la secretaria general de Tecnifuego enumeró las jornadas divulgativas junto a Cepreven para informar sobre las novedades del RIPCI y su Guía de aplicación, las jornadas formativas para asociados, la jornada sobre incendios forestales, y la celebración del 25 aniversario de Tecnifuego, que se ha enfocado en tres grandes acciones, una lúdica, que se celebró en el Casino de Madrid, en el mes de febrero, donde se homenajeó a personalidades y a los asociados más veteranos. Otra, formativa, a través de becas para asociados en el Curso Europeo Superior de Seguridad contra Incendios, que se impartió en abril y mayo. Y otra de sensibilización, con una campaña nacional para concienciar al usuario final de la necesidad de PCI en el hogar, bajo el eslogan «Los incendios matan. La protección es posible», fundamentada en notas de prensa, artículos, convocatorias de prensa, como el desayuno de trabajo entre expertos y medios especializados que se realizó en mayo sobre rociadores, y el que se hará en septiembre sobre la importancia de la instalación de protección pasiva.

Risco Group y Hommax Sistemas, innovación constante

Hommax Sistemas, como distribuidor oficial de Risco Group, afronta el segundo semestre del año introduciendo interesantes novedades gracias a la constante evolución tecnológica que caracteriza a la compañía internacional. El acuerdo, firmado a principios de año, forma parte de la estrategia de crecimiento de Risco Group, consolidando así su presencia en el sur de Europa.

Risco Group es una marca mundialmente reconocida especializada en el desarrollo de soluciones de seguridad basadas en la nube. Junto con vídeo verificación, monitorización y automatización, ofrece sistemas de seguridad innovadores, de alta calidad y fiables. Gracias a su aplicación para dispositivos móviles, ofrece a los usuarios un acceso remoto a sus sistemas de seguridad y permite el autocontrol, dirigiéndose a una tendencia creciente en la industria.

Su objetivo, proporcionar a los clientes tecnologías de última generación, un servicio personalizado y una atención al cliente de calidad que, apoyada por la comercialización constante de Hommax, sea coherente con los valores de la compañía.

Los productos de Risco Group, así como los de su distribuidor Hommax Sistemas (www.hommaxsistemas.com), cumplen con las normas internacionales y pueden presumir de ser innovadores, flexibles, rentables y de fácil utilización e instalación. Además, la marca ha actualizado recientemente Risco Cloud, una plataforma diseñada para que los instaladores puedan gestionar los paneles ubicados en la nube, así como configurar la utilización de los dispositivos Smarthome y las cámaras IP VUpoint.

Secure&IT: Ciberseguridad para empresas: prevenir, detectar y detener ataques

Que la tecnología nos facilita mucho la vida es un hecho. Pero, que genera grandísimos quebraderos de cabeza en cuanto a la seguridad y la privacidad también lo es. No existe ningún dispositivo electrónico conectado a la red que sea 100% seguro y este hecho se ha convertido en un arma para los ciberdelincuentes. Los datos hablan por sí mismos: el Instituto Nacional de Ciberseguridad (INCIBE) registró 120.000 incidentes el año pasado, lo que demuestra que España es uno de los más atacados por los ciberdelincuentes.

El equipo de Secure&IT trabaja en el desarrollo de tecnologías que ayudan a las empresas a prevenir, detectar y detener intrusiones en sus sistemas: la sonda de red Big Probe y el Big SIEM.

La sonda es una tecnología encargada de monitorizar la Red y detectar intrusiones, es decir, es una especie de «espía» que analiza la red y detecta ataques y malware. Usa motores de búsqueda de comportamiento de malware y ataques, propios y de terceros. Pero, además, en el caso de la Big Probe hay que añadir que se alimenta de un reconocimiento propio de patrones de ataque, una característica que la hace adaptable y flexible.

La sonda por sí sola no tendría ningún sentido, la Big Probe trabaja conjuntamente con el Big SIEM, que es el encargado de determinar si un evento de seguridad es una alerta o no. Esta tecnología lleva a cabo un análisis en tiempo real de los eventos de seguridad generados por los equipos y los programas informáticos. La particularidad del Big SIEM es que, además, determina cuáles de esos eventos suponen una alerta de seguridad y, una vez detectada, se hace un tratamiento de esa alerta en el Centro de Operaciones de Seguridad (SOC) de Secure&IT.

Las empresas y su apuesta por la ciberseguridad

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 de seguridad de la información, que trabajan para prevenir estos delitos, también avanzan en la tarea.

Detnov: acuerdo de distribución con Securiton

DETNOV ha firmado un acuerdo de distribución para España con el fabricante suizo Securiton, especializado en sistemas de detección de humo por aspiración.

Securiton es una prestigiosa marca reconocida internacionalmente por su amplia gama de productos de detección de humo de alarma temprana, basada en las más avanzadas tecnologías de detección, impresionando por su alto rendimiento, fiabilidad y durabilidad. El nuevo acuerdo alcanzado permitirá a los clientes de Detnov disfrutar de una oferta competitiva en toda la gama de productos Securiton, con amplio stock permanente y un servicio técnico comercial de calidad. El director comercial de Detnov, Eugeni Mulà, ha valorado positivamente el acuerdo alcanzado y ha asegurado que reforzará la capacidad de innovación en el mercado español de ambas marcas y contribuirá a su crecimiento.

Leo Jakob, regional Export manager de Securiton estuvo presente en las oficinas de Detnov para realizar la formación al equipo comercial de Detnov. La gama SecuriRAS ASD está compuesta por 3 modelos diferentes 531/532/535 utilizados según el tipo de instalación a proteger, pudiendo cubrir superficies de hasta 5.760m^2 con un único detector y distancias de tuberías de hasta 400 metros. Todos los detectores disponen de sus certificados europeos EN54-20, así como otras certificaciones internacionales (UL, VDS, FM).

Asamblea 1/2018 del Comité Técnico de Normalización 108

La sede del GEO, en Guadalajara, fue escenario el pasado 26 de junio, de la Asamblea 1/2018 del CTN108, que en esta ocasión celebraba su 35 aniversario.

En las instalaciones del GEO, y tras una calurosa bienvenida por parte de los mandos que personificó el Comisario Jefe del GEO, Javier Nogueroles (en la foto 1), explicó la forma de trabajar de este cuerpo de élite de la Policía Nacional, y que estuvo acompañado por el Comisario Javier Galván, de la Unidad Central de Seguridad Privada, y por el presidente del CTN108, Javier Ruiz. Los vocales tuvieron ocasión de disfrutar de una exhibición a cargo de esta unidad de élite de la Policía Nacional.

Posteriormente tuvo lugar la reunión, en la que, después de una presentación a cargo de Javier Ruiz y Manuel Sánchez, conmemorativa del 35 aniversario del Comité, intervinieron los coordinadores de los cinco grupos de trabajo (cajas fuertes, blindajes, cerraduras, dispositivos de maculación y protecciones perimetrales: Ester Balibrea, Francisco Moreno, Iñigo Ugalde, Eugenio Barranquero y José Miguel Ángel, respectivamente), así como el del Sub Comité 79 de seguridad electrónica, Antonio Escamilla, para explicar la actividad de los mismos. Además, se revisaron los cinco acuerdos pendientes de cumplimiento desde la última Asamblea, la 2/2017, celebrada el pasado 21 de noviembre en Valencia.

El Centro Vasco de Ciberseguridad inaugura sus instalaciones

El Centro Vasco de Ciberseguridad (BCSC), inauguró el pasado 18 de julio sus nuevas instalaciones, en un acto que contó con la presencia del Lehendakari Iñigo Urkullu y de tres miembros de su Gobierno: las consejeras de Desarrollo Económico e Infraestructuras (Arantxa Tapia), Educación (Cristina Uriarte) y Seguridad (Estefanía Beltrán de Heredia); además, también asistieron la viceconsejera de Administración y Servicios Generales (Nerea López-Uribarri), representando al departamento de Gobernanza Pública y Autogobierno. El director del Centro, Javier Diéguez, fue el encargado de mostrar las dependencias, ubicadas en el Parque Tecnológico de Álava y explicar los pormenores de su funcionamiento.

La importante presencia institucional en el acto de presentación evidencia el compromiso del Gobierno Vasco con esta iniciativa de país, integrada en el Grupo SPRI y cuyo objetivo es generar cultura de ciberseguridad en Euskadi. Así, el Lehendakari señaló que es un proyecto tecnológico fundamental para garantizar la seguridad en el mundo de una empresa vasca cada vez más digital e internacional. «Es un proyecto profesional y muy capacitado. Un núcleo de inteligencia al servicio de la seguridad y, por lo tanto, la competitividad», añadió el Lehendakari.

El BCSC está en funcionamiento desde octubre de 2017, y sus principales objetivos son los de dinamizar la actividad y fortalecer el sector empresarial relacionado con la ciberseguridad; posicionar Euskadi como referente internacional en esta materia; y promover la cultura de la seguridad informática en la sociedad vasca. En este sentido, el Lehendakari señaló que quieren generar un entorno competitivo para la atracción de potenciales inversores y tecnologías capaces de dar servicio a mercados globales. «Contamos con potencial suficiente para convertir Euskadi en un Hub de referencia europeo en Cyberseguridad», ha matizado el Lehendakari.

Junto a esta dimensión empresarial, BCSC se constituye así mismo como equipo de respuesta ante ataques informáticos que puedan poner en riesgo tanto a las empresas como a la ciudadanía de Euskadi, y colabora estrechamente con la Ertzaintza para la dotación de herramientas que ayuden en la persecución de ciberdelitos. De hecho, la policía vasca cuenta con una sala propia y presencia permanente de agentes en la sede del Centro. Desde el punto de vista educativo y de formación, el Centro Vasco de Ciberseguridad cuenta con una sala específica de laboratorio donde llevar a cabo proyectos innovadores y cuenta, además de con su propia plantilla, con la colaboración de personal investigador de la corporación tecnológica Tecnalia y los centros Vicomtech (tecnologías multimedia), Ikerlan (innovación industrial) y BCAM (matemáticas aplicadas), además de un técnico de ciberseguridad que actúa como enlace con la sociedad informática del Gobierno Vasco EJIE. A este equipo se unirán en breve tres estudiantes de informática con beca dual.

El Centro está presente en las mesas de inteligencia competitiva de 11 Clusters sectoriales del País Vasco, y colabora con asociaciones empresariales y cámaras de comercio para promover acciones de concienciación empresarial en la materia. Colabora asimismo con otros agentes relevantes de la Administración Pública Vasca como Izenpe, o la Agencia Vasca de Protección de Datos, o el Eustat o Izenpe, así como con asociaciones profesionales y ciudadanas que operan en Euskadi.

La coordinación con otros organismos similares que operan en el Estado y a escala internacional ha sido una clara vocación del Centro Vasco de Ciberseguridad desde el momento de su creación. En este sentido, el próximo otoño está previsto su ingreso como miembro de pleno derecho de FIRST (Forum of Incident Response and Security Teams), el foro de equipos de respuesta a incidentes informáticos más importante a nivel mundial.

Contactos de empresas, p. 8.

HikCentral, el nuevo sistema de gestión VMS que unifica todas las soluciones de Hikvision

Hikvision, el proveedor mundial de referencia de productos y soluciones innovadoras de videovigilancia, ha lanzado HikCentral, un nuevo sistema de gestión de videovigilancia (VMS) que facilita el control de una amplia variedad de dispositivos de seguridad en diferentes escenarios, de forma escalable.

HikCentral ofrece a los usuarios diferentes funciones operativas, entre las que se incluyen: gestión de visualización y reproducción en directo, búsqueda inteligente de imágenes y gestión de alarmas. Con dos opciones para elegir -una solución basada en servidor y una solución de software - HikCentral se adapta a cualquier necesidad o infraestructura.

Para ofrecer la máxima flexibilidad, HikCentral pueden utilizarlo hasta tres clientes:

- Un cliente de control: el más completo, ideal para la operativa del día a día;
- Un cliente web: diseñado para dar acceso a través de otros dispositivos;
- Un cliente móvil: con acceso remoto en vivo desde cualquier lugar.

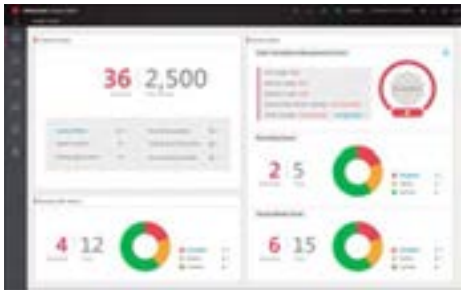
De esta forma, los usuarios pueden estar siempre actualizados.

El sistema está diseñado para ofrecer la máxima eficiencia y facilidad de uso: gracias al software precargado –con un paquete de instalación muy ligero- y la licencia preactivada se instala y configura muy rápidamente. Una vez concluido el proceso, detecta automáticamente los dispositivos, sincroniza los nombres de las cámaras y los programas de grabación de los dispositivos.

HikCentral es una plataforma unificada que combina la videovigilancia, lectura de matrículas (Automatic License Plate Recognition ALPR), sistemas de Punto de Venta (Point Of Sale, POS) e integración de sistemas de terceros en una sola solución.

El sistema está diseñado con un alto nivel de escalabilidad de forma que puede dar la respuesta más adecuada tanto a la gestión centralizada que debe realizarse desde una sede central como a cada una de sus sucursales. Para lograrlo emplea servidores de RSM (Removable Storage Manager). Con copias de seguridad de almacenamiento de un solo punto y de varios puntos, utilizando RAID y SAN híbrido, el sistema tiene una gran cantidad de contingencias. También está integrado con la tecnología del proveedor de soluciones de alta disponibilidad, Rose Replicator Plus, para proporcionar a la solución un alto nivel de fiabilidad.

HikCentral, el paso siguiente al iVMS 5200 de Hikvision, es una gran herramienta de gestión para todo tipo de aplicaciones en múltiples industrias, soportando una amplia gama de canales.



Fujitsu: el sistema de autenticación biométrica Fujitsu PalmSecure alcanza el millón de unidades

Fujitsu Limited y Fujitsu Frontech Limited han anunciado que las ventas acumuladas de su sistema Palm Secure, basado en sensores de autenticación de lectura de las venas de la palma de la mano, fabricados y vendidos por las dos compañías, ha superado el millón de unidades.

Alrededor de 73 millones de personas en aproximadamente 60 países de todo el mundo, interactúan con esta tecnología a diario como una medida de seguridad para una amplia gama de tareas de autenticación personal, incluso para cajeros automáticos, inicios de sesión de PC y gestión de entrada de salas.

La autenticación de las venas de la palma de la mano es un método de verificación biométrica que puede confirmar con precisión e instantáneamente la identidad de un individuo, mediante la lectura de los patrones de venas de la palma de la mano, sin contacto directo.

JABLOTRON
CREATING ALARMS

Únase a la familia JABLOTRON

Jablotron, empresa tecnológica internacional y especialista en seguridad con departamento R&D propio, inicia nuevos cursos de formación.

Aumente sus conocimientos, conviértase en nuestro socio certificado y aprenda como se instala correctamente este sencillo e innovador sistema de alarma.

Cursos básicos

16 de Octubre	Sevilla, España
24 de Octubre	Vigo, España JI
13 de Noviembre	Barcelona, España
12 de Diciembre	Vigo, España JI

Cursos avanzados

6 de Septiembre	Vigo, España JI
18 de Octubre	Barcelona, España
15 de Noviembre	Alicante, España
21 de Noviembre	Vigo, España JI
10 de Diciembre	Faro, Portugal
12 de Diciembre	Lisbon, Portugal
14 de Diciembre	Braga, Portugal

JI Jablotron Iberia

Regístrese en +34 986 095 364, **iberia@jablotron.cz**

www.jablotron.com

Dallmeier: Panomera S8 Ultraline, otro récord en resolución y rango dinámico

Ya desde 2011, la patentada tecnología de sensores multifocal de Dallmeier está permitiendo una amplia videoprotección de vastas áreas en numerosos estadios de fútbol, perímetros, aeropuertos y espacios municipales en todo el mundo. La nueva serie «Ultraline» de Panomera® ofrece una resolución efectiva extraordinariamente alta para este tipo de aplicaciones. Dallmeier presenta el primer modelo de la nueva serie, la Panomera® S8 Ultraline, que proporciona hasta 190 megapíxeles a 30 ips.

El concepto Panomera® ha revolucionado la tecnología de vídeo: hasta ocho sensores en una cámara hacen posible captar superficies y distancias enormes con una calidad de resolución sin precedente.

El primer modelo de la nueva serie Ultraline, la Ultraline S8, dispone de un excelente rango dinámico de 130 dB UWDR (efectivo) y se manifiesta en un efecto Panomera® extremo. Proporciona una resolución superior a 125 px/m hasta una distancia de 160, 104 o 82 m, posibilitando el reconocimiento de personas en toda la distancia. La identificación de personas (250 px/m) es soportada, dependiendo del modelo, hasta una distancia de 46 m y la observación (62 px/m) incluso hasta una distancia de 322 m, lo que corresponde a una escena inmensa de más de 26.000 m² con profundidad de campo continua.

El sistema de sensores multifocal capta y almacena todas las áreas de la escena con la máxima resolución en el detalle, sin tener importancia si los operadores en modo vivo se concentran en una zona determinada (zoom de detalle múltiple) o si se representan detalladamente zonas de interés a base de Video Content Analysis (seguimiento automático múltiple).

Como todas las cámaras Dallmeier, el nuevo modelo de Panomera® también es producido íntegramente en Alemania en la fábrica de Dallmeier en Regensburg. Esto en sí mismo es un aspecto esencial de la estrategia de protección de datos y seguridad de datos del fabricante, ya que con ello se impide, por ejemplo, el acceso no autorizado por puertas traseras. En total 14 funciones, tales como la configuración de zonas de privacidad, «people masking» o la última tecnología de autenticación y cifrado en la cadena de procesamiento de las soluciones Dallmeier, garantizan que se cumplan las altas exigencias del RGPD en cuanto a protección de datos y seguridad de datos.

Johnson Controls: nuevos rociadores colgantes Tyco Early Suppression Fast Response (ESFR)-22

Johnson Controls ha presentado sus nuevos rociadores colgantes Tyco® Early Suppression Fast Response (ESFR)-22, que vienen a ampliar la línea de rociadores para espacios de almacenamiento de Tyco. Se puede instalar los ESFR-22 en espacios con techos de hasta 13.71 m altura y alturas de almacenamiento de hasta 12.19 m sin necesidad de instalar rociadores dentro de las estanterías. El sistema también puede instalarse con una distancia máxima de 457 mm entre el deflector y el techo.

Los rociadores ESFR-22 se usan exclusivamente en techos para proteger principalmente, entre otras, las siguientes aplicaciones de almacenamiento:

- La mayoría de materiales comunes, encapsulados o no, incluyendo plásticos sin expandir guardados en cajas.
- Plásticos expandidos sin caja (a la vista).
- Algunos métodos para el almacenamiento de neumáticos de caucho, rollos de papel, líquidos inflamables y aerosoles.

El modelo ESFR-22 cumple con las normas de instalación de la National Fire Protection Association (NFPA) y FM Global (FM Approvals) aplicables al adecuado diseño de un sistema de rociadores automáticos que use rociadores ESFR.

Dahua lanza el Servidor de Reconocimiento Facial Distribuido DHI-IVS-F7500-P

Dahua Technology, un proveedor destacado de soluciones en la industria mundial de videovigilancia, ha presenta su servidor DHI-IVS-F7500-P de reconocimiento facial distribuido impulsado por inteligencia artificial, implementado sobre todo en proyectos de grandes poblaciones: ciudad segura, gestión de seguridad de vías principales de tráfico o plazas, análisis comerciales para cadenas de supermercados, etc.

Como plataforma de datos masivos de gestión de rostros, el servidor de reconocimiento facial Dahua DHI-IVS-F7500-P puede analizar flujos de imágenes como datos estructurales y almacenarlos en una base de datos distribuida. Además, con una excelente tecnología de motor de búsqueda de comparación de imágenes, incluso admite la búsqueda difusa de datos masivos de rostro humano y brinda resultados en cuestión de segundos.

Detección y reconocimiento facial de alta eficiencia

Compatible con el módulo GPU P4 integrado de alto rendimiento y los algoritmos avanzados de aprendizaje profundo de Dahua, el servidor DHI-IVS-F7500-P de reconocimiento facial distribuido puede detectar rostros humanos con una precisión superior al 90%, junto con sus características faciales detalladas como la edad, género, expresión y gafas, que ayudan a identificar las diferencias individuales.

Comparaciones potenciadas con alarma proactiva

Después de recopilar los datos de la cara, el servidor de reconocimiento de rostros de Dahua DHI-IVS-F7500-P también ofrece comparación de imágenes estáticas y dinámicas. La comparación dinámica admite la transmisión de imágenes de 100 canales en tiempo real (aproximadamente 8,5 millones de imágenes de procesamiento) y 300,000 comparación de control de rostro

Biblioteca de registro flexible y completa

Para una mejor compatibilidad con la comparación de rostros, el nuevo servidor de reconocimiento de rostros mejora la capacidad de almacenamiento de 300,000 imágenes de rostros humanos de su base de datos registrada para alertas de personas buscadas. Además, puede agregar, eliminar, modificar y consultar la información personal en la biblioteca registrada si es necesario cambiar algo, y también permite la importación / exportación por lotes de las imágenes y el archivo comprimido de la biblioteca.

Hanwha Techwin: cámara multidireccional Wisenet P de dos canales

La última incorporación a la serie de cámaras Premium Wisenet P, fabricadas por Hanwha Techwin, dispone de dos cámaras de videovigilancia en una sola unidad.

La cámara PNM-7000VD puede capturar imágenes Full HD de 2 megapíxeles de las zonas adyacentes con la ayuda de dos lentes separadas. La incorporación de dos lentes de 2,4 mm consigue un ángulo de visionado de 270°, lo que convierte a la PNM-7000VD en una solución ideal para la supervisión de grandes espacios abiertos - aparcamientos de coches, centros comerciales y almacenes -. Además, admite la compresión H.265 y, dependiendo del campo de visión requerido, los integradores de sistemas pueden elegir la instalación de lentes de 2,8, 3,6 o 6 mm. La PNM-7000VD dispone del mejor amplio rango dinámico (WDR) del mundo (150 dB), de corrección de la distorsión de la lente (LD), así como de la tecnología de estabilización digital de imágenes para proporcionar imágenes optimizadas en cualquier situación. También incluyen enmascaramiento de privacidad y dirección, detección facial, niebla, línea virtual, aparición y desaparición de objetos, merodeo y detección de manipulación de la cámara.

Hikvision ofrece soluciones asequibles para combatir hurtos en el pequeño comercio

En una era de competencia feroz, gracias al e-commerce y a las grandes cadenas, el comercio minorista está más obligado que nunca a ser eficaz y rentable. Ofrecer al consumidor el mejor servicio y reducir, todo lo posible, las pérdidas. Según un estudio de la Asociación de Fabricantes y Distribuidores (Aecoc), los comercios españoles perdieron, en 2017, un total de 1.800 millones de euros por hurtos de clientes y empleados y errores de gestión.

Los propietarios de pequeños comercios necesitan reducir al mínimo los costes y, al mismo tiempo, mantener la eficiencia en asuntos tan relevantes como la vigilancia y los sistemas de seguridad. Para ayudarles en esta difícil tarea, Hikvision ha trasladado las últimas innovaciones a productos más asequibles en cuanto a precio.

Productos como el mini PanoVu ofrecen, por un coste accesible, una cobertura asequible y flexible de una amplia zona. Con este equipo, los propietarios pueden ver un espacio amplio –incluso toda la tienda- con una sola cámara.

Nuevos avances tecnológicos, como las mejoras en Wide Dynamic Range (WDR) y el modelo LightFighter de Hikvision les permiten monitorizar zonas poco iluminadas o demasiado iluminadas. Estos equipos distinguen claramente la silueta de personas sobre un fondo con mucha luz y permiten controlar la actividad incluso en un rincón oscuro del establecimiento o en un callejón trasero durante la noche.

La facilidad de uso es otra de las grandes ventajas de estos sistemas. Dado que los propietarios de pequeños comercios no pueden dedicar mucho tiempo ni mucho presupuesto a la instalación o configuración de los equipos, Hikvision ha diseñado para ellos equipos intuitivos, fáciles de operar y de instalar. La naturaleza «plug and play» de las cámaras y la flexibilidad de las soluciones, incluidos los grabadores y monitores de vídeo en red, por ejemplo, ofrecen soluciones sencillas.

Las salidas HDMI y el software VMS permiten al propietario visualizar o grabar fácilmente las señales de la cámara, tanto por su tranquilidad como por si necesitaran utilizarlo como prueba en un juicio (en caso de robo). También pueden emplear el software para ver las imágenes en su teléfono móvil, lo que resulta muy útil si están fuera de las instalaciones o en el almacén, por ejemplo.

Los equipos que ofrece Hikvision para el comercio minorista incluyen también funciones inteligentes que activan una alerta, por ejemplo, si alguien cruza una línea predeterminada, o incluso se mueve en un área determinada. De esta manera, el propietario puede concentrarse en aquello que verdaderamente le importa y no necesita visualizar constantemente un área concreta. Como lo habitual en pequeños comercios es que no haya personal de seguridad visionando las imágenes de forma continuada, este tipo de funciones inteligentes de alerta, y las funciones de grabación, se convierte en herramientas especialmente útiles.

Por supuesto, las soluciones pueden ser extremadamente flexibles, ofreciendo más o menos equipos y avances tecnológicos, dependiendo de las necesidades de cada instalación y de cada propietario. Desde múltiples opciones de cámaras y grabadores hasta monitores, dispositivos de control de acceso y tecnología para leer matrículas: Hikvision puede ofrecer una solución de seguridad inteligente de cualquier medida.

Los pequeños comercios tienen necesidades específicas para mantener seguros sus locales, sus bienes y sus empleados. La tranquilidad es importante en este mercado, ya que a menudo tienen todo invertido en el negocio y es un riesgo personal. Pero utilizando la solución sencilla adecuada, Hikvision puede ayudar a crear entornos seguros, reducir las pérdidas y hacerlo con un presupuesto muy ajustado.

Risco Group: nuevo módulo KNK/Modbus

RISCO Group, especialista global en soluciones integradas de seguridad, ha anunciado el lanzamiento del nuevo módulo KNX/Modbus. KNX y Modbus son protocolos de uso común en Sistemas de Automatización de Edificios y Sistemas de Gestión de Seguridad dentro de los principales mercados de RISCO Group. El módulo KNX/Modbus permite a los paneles de alarma de RISCO interactuar con los sistemas de automatización de edificios y los sistemas de gestión de seguridad, que utilizan el protocolo KNX o Modbus.

El módulo traduce las señales del protocolo CS de RISCO Group al protocolo KNX o Modbus y viceversa a través de IP.

El módulo KNX/Modbus es adecuado para diversas aplicaciones: sistemas de automatización de edificios en instalaciones comerciales e industriales, sistemas de gestión de seguridad o domótica en instalaciones residenciales.

El módulo KNX/Modbus permite a los integradores utilizar paneles de alarma de RISCO como parte de un sistema de automatización de edificios totalmente integrado: controlar el panel de alarma a través de un sistema de gestión utilizando el protocolo KNX o Modbus, incluidos los comandos, como armado/desarmado parcial o total, salidas programadas o anulación de zonas; usar la integración con el sistema de alarma para escenarios, como encender luces en caso de un evento de intrusión o armado y desarmado automático programado; y aprovechar los detectores/dispositivos de los sistemas de alarma como activadores de otros sistemas como HVAC, iluminación o persianas.

Se recomienda que el módulo KNX/Modbus sea instalado por integradores, que están especializados en los entornos KNX/Modbus.

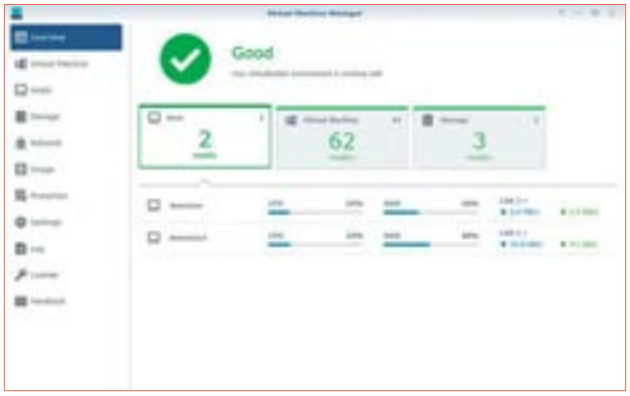
El módulo KNX/Modbus es compatible con las soluciones ProSYS Plus, LightSYS y Agility de RISCO Group.

Synology: Virtual Machine garantiza la seguridad en entornos de virtualización

Synology® Inc. ha anunciado el lanzamiento oficial de Virtual Machine Manager Pro para atender a las necesidades de los usuarios profesionales. VMM Pro permite que los servidores NAS de Synology ejecuten varias máquinas virtuales como Windows, Linux y Virtual DSM.

VMM Pro ayuda a los usuarios a integrar y administrar múltiples NAS de la marca a través de su clúster virtual, distribuye de forma flexible los recursos de hardware, facilita la migración de máquinas virtuales entre hosts sin interrupción y permite realizar instantáneas y replicaciones regulares para hacer copias de seguridad de máquinas virtuales, con el objetivo final de construir un entorno seguro de virtualización.

Synology se dedica a crear soluciones potentes y fáciles de utilizar para sus usuarios. «Virtual Machine Manager ha conseguido grandes elogios con su última versión, y más de 130.000 usuarios de servidores NAS de Synology lo han descargado e instalado en sus dispositivos en el transcurso de un año. Con el clúster extremadamente flexible de Virtual Machine Manager Pro, ayudamos a los encargados de TI a crear fácilmente un entorno de virtualización profesional y eficiente en los servidores NAS. Además, como esta aplicación mejora la eficiencia de los flujos de trabajo, también protege las máquinas virtuales críticas», explica Chen Feng Wang, Product Manager de virtualización en Synology.



Contactos de empresas, p. 8.

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

ALARMA Y CONTROL

PYRONIX

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

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

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

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

FUNDADA EN 1966

INSTALACIONES A SU MEDIDA

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

ISO 9001

CONTROL DE ACCESOS ACTIVO

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

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

BIOSYS
(Sistemas de Tecnología Aplicada)

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

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

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

DORLET S. A. U.
Parque Tecnológico de Álava
C/Albert Einstein, 34
01510 Miñano Mayor - ALAVA - Spain
Tel. 945 29 87 90 • Fax. 945 29 81 33
e-mail: comercial@dorlet.com
web: http://www.dorlet.com

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

DETECCIÓN DE EXPLOSIVOS

COTELSA
Basauri, 10-12, Urb. La Florida
Ctra. de La Coruña, Aravaca
28023 Madrid
Tel.: 915 662 200 - Fax: 915 662 205
cotelsa@cotelsa.es
www.cotelsa.es

TARGET TECNOLOGIA, S.A.
Ctra. Fuencarral, 24
Edif. Europa I - Portal 1 Planta 3ª
28108 Alcobendas (Madrid)
Tel.: 91 554 14 36 • Fax: 91 554 45 89
info@target-tecnologia.es
www.target-tecnologia.es

SISTEMAS DE EVACUACIÓN

OPTIMUS S.A.

C/ Barcelona 101
17003 Girona
T (+34) 972 203 300

info@optimus.es
www.optimusaudio.com

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

PROTECCIÓN CONTRA INCENDIOS. ACTIVA

detnov

C/ Alguer nº8 08830 Sant Boi de Llobregat (Barcelona)

Tel: +34 93 371 60 25
Fax:+34 93 640 10 84

www.detnov.com
info@detnov.com

bydemes

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

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

aguilera

GRUPO AGUILERA

FABRICANTES DE SOLUCIONES PCI DETECCIÓN Y EXTINCIÓN DE INCENDIOS

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

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

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

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

pefipresa

PEFIPRESA, S. A. U

INSTALACIÓN Y MANTENIMIENTO DE SISTEMAS DE SEGURIDAD Y CONTRA INCENDIOS

www.pefipresa.com

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

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

PROTECCIÓN CONTRA INCENDIOS. PASIVA

DICTATOR Española

DICTATOR ESPAÑOLA
Mogoda, 20-24 • P. I. Can Salvatella
08210 Barberá del Vallés (Barcelona)
Tel.: 937 191 314 • Fax: 937 182 509
www.dictator.es
dictator@dictator.es

PROTECCIÓN CONTRA INTRUSIÓN. ACTIVA

bydemes

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

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

RISCO GROUP
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

PROTECCIÓN CONTRA ROBO Y ATRACO. PASIVA

AGA
LA INDUSTRIA DE LA CERRAJERÍA
ALTA SEGURIDAD

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

expocom

SOLUCIONES INTEGRALES DE TELECOMUNICACIONES Y SEGURIDAD

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

VIGILANCIA POR TELEVISIÓN

HIKVISION

HIKVISION SPAIN

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

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

Hanwha Techwin Europe Ltd

Avda. De Barajas, 24, Planta Baja, Oficina 1
28108 Alcobendas (Madrid)España(Spain)
Tel.: +34 916 517 507

www.hanwha-security.eu
hte.spain@hanwha.com

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

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

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

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

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

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

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

ASOCIACION ESPAÑOLA
DE SOCIEDADES DE PROTECCION
CONTRA INCENDIOS
C/ Doctor Esquerdo, 55. 1º F.
28007 Madrid
Tel.: 914 361 419 - Fax: 915 759 635
www.tecnifuego-aespi.org

DAHUA IBERIA, S.L.

C/ Juan Esplandiú 15 1-B. 28007
Madrid

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

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

dallmeierspain@dallmeier.com
www.dallmeier.com

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

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

A Western Digital® Company

WD ESPAÑA
4 boulevard des Iles
92130 Issy les Moulineaux · Francia
florence.perrin@wdc.com
Tel.: 615 235 013
www.wdc.com

ASOCIACIONES

ADSI - Asociación de Directivos
de Seguridad Integral
Gran Via de Les Corts Catalanes, 373 - 385
4ª planta (local B2)
Centro Comercial **Arenas de Barcelona**
08015 Barcelona
info@adsi.pro • www.adsi.pro

Expertos en VIDEOVIGILANCIA

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

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

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

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

www.aecra.org

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

MATERIALES, SISTEMAS Y SERVICIOS DE SEGURIDAD

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

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

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

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

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

ASOCIACIÓN DE JEFES DE SEGURIDAD DE ESPAÑA

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

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

CENTRALES DE RECEPCIÓN Y CONTROL

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

INSTALACIÓN Y MANTENIMIENTO

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

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

MATERIAL POLICIAL

SABORIT INTERNATIONAL
Avda. Somosierra, 22 Nave 4D
28709 S. Sebastián de los Reyes (Madrid)
Tel.: 913 831 920
Fax: 916 638 205
www.saborit.com

VIGILANCIA Y CONTROL

SECURITAS SEGURIDAD ESPAÑA
C/ Entrepeñas, 27
28051 Madrid
Tel.: 912 776 000
email: info@securitas.es
www.securitas.es

¿No cree... ... que debería estar aquí?

El directorio es la zona más consultada de nuestra revista.

Módulo: 660€/año*

Más información:
Tel.: 91 476 80 00
e-mail: publi-seguridad@epeldano.com
* Tarifa vigente 2018

TRANSPORTE Y GESTIÓN DE EFECTIVO

LOOMIS SPAIN S. A.
C/ Ahumaos, 35-37
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 2018)

ESPAÑA

❑ 1 año: 98€ ❑ 2 años: 174€ (IVA y Gastos de envío incluido)

EUROPA

❑ 1 año: 130€ ❑ 2 años: 232€ (Gastos de envío incluido)

RESTO

❑ 1 año: 140€ ❑ 2 años: 252€ (Gastos de envío incluido)

CLÁUSULA DE PROTECCIÓN DE DATOS. De conformidad con el nuevo 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 (GDPR/RGPD) y la legislación de vigente aplicación le informamos que sus datos serán incorporados a un fichero titularidad del editor, EDICIONES PELDAÑO, S.A. como Responsable del Tratamiento y que serán tratados con la finalidad de gestionar los envíos en formato papel y/o digital de la revista, de información sobre novedades y productos relacionados con el sector, así como poder trasladarle a través nuestro, publicidad y ofertas que pudieran ser de su interés.
EDICIONES PELDAÑO, S.A., en calidad de editor de los contenidos y como RESPONSABLE DEL TRATAMIENTO, le informa que los datos personales proporcionados por Ud. y demás información aportada mediante la cumplimentación del presente formulario, serán tratados debidamente y en cumplimiento de las obligaciones legales vigentes. Más información de nuestra política de datos en **https://www.peldano.com/aviso-legal/ Condición 4.**
Siempre podrá ejercitar los derechos de acceso, rectificación, cancelación, oposición, portabilidad y olvido puede dirigirse a EDICIONES PELDAÑO, S.A., Avda. Manzanares, 196, 28026 Madrid, o bien al correo electrónico **distribucion@peldano.com**

❑ Deseo recibir Newsletters de información sectorial.

❑ MIS DATOS NO SERÁN CEDIDOS A TERCEROS. Deseo recibir comunicaciones de promociones y publicitarias.

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@peldano.com • www.cuadernosdeseguridad.com

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

DEEP LEARNING

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

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

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