CUADERNOS DE SEGURIDAD

NÚM. 351 | MARZO 2020 | 12€

cuadernosdeseguridad.com

Edita Peldaño

GRANDES EVENTOS Y CENTROS DE OCIO

Prevención y protección, pilares de la seguridad

INTEGRACIÓN DE SISTEMAS

Nuevas tecnologías, nuevos servicios

CIBERSEGURIDAD

La ciberinteligencia, clave para afrontar las nuevas amenazas

HOLA SIGNO

La línea icónica de lectores de control de acceso de HID Global

Conozca más sobre SIGNO en hidglobal.com/es/**signo**

HID

Powering **Trusted Identities**

STAFF

DIRECTOR ÁREA DE SEGURIDAD:
Iván Rubio Sánchez

REDACTORA JEFE DE SEGURIDAD:
Gemma G. Juanes

REDACCIÓN:
Laura Sala, Marta Santamarina

PUBLICIDAD:
Emilio Sánchez
publi-seguridad@peldano.com

IMAGEN Y DISEÑO:
Juan Luis Cachadiña, Adrián Beloki

PRODUCCIÓN Y MAQUETACIÓN:
Débora Martín, Verónica Gil,
Cristina Corchuelo, Lydia Villalba

DISTRIBUCIÓN Y SUSCRIPCIONES:
Mar Sánchez, 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
info@cuadernosdeseguridad.com

Precio: 12 €
Precio suscripción en España:
Un año (9 núms.) 98 €
Dos años (18 núms.) 174 €

Printed in Spain | Depósito legal: M-7303-1988 | ISSN: 1698-4269

Peldaño
Avda. del Manzanares, 196
28026 Madrid
peldano.com
914 768 000

Presidente: Ignacio Rojas / **Gerente:** Daniel R. Villarraso
Director de Desarrollo de Negocio: Julio Ros / **Directora de Contenidos:** Julia Benavides
Director de Producción: Daniel Rojas / **Director de TI:** Raúl Alonso
Directora de Administración: Anabel Lobato / **Director de Imagen & Diseño:** Eneko Rojas
Jefe de Producción: Miguel Fariñas

SEGURIDAD & COVID-19

La rápida propagación del virus COVID-19 ha sumido a España en un estado de crisis sanitaria, social y económica. Tras la declaración del estado de alarma a través de un real decreto que contempla medidas "inmediatas y eficaces", entre ellas el estado de confinamiento que se alargará hasta el 11 de abril, para proteger la "salud y seguridad de los ciudadanos", el Ministerio del Interior aprobó una orden ministerial con criterios de actuación para las Fuerzas y Cuerpos de Seguridad, entre cuyos objetivos está garantizar la acción concertada de las autoridades policiales, así como de la seguridad privada.

Una vez más, se pone de manifiesto el papel que cumple la seguridad privada y sus profesionales, en su colaboración y coordinación con la seguridad pública, en beneficio de la sociedad. Profesionales y empresas que en estos momentos de dificultad, contribuyen y cooperan, con su esfuerzo y plena dedicación, en restablecer la normalidad de un país convulsionado por una situación de emergencia sanitaria sin precedentes, en un compromiso ético inherente al sector de la seguridad privada. Compromiso de servicio permanente y apoyo al sector que comparte Grupo Peldaño, organizador de Plataforma de Negocio que, atendiendo a criterios de salud y responsabilidad, aplaza la celebración del evento a los días 27 y 28 de octubre. ✱

SUMARIO

SECURITY FORUM CAMBIA SUS FECHAS AL 27 Y 28 DE OCTUBRE

Security Forum, bajo el paraguas de Plataforma de Negocio, celebrará su próxima edición 2020 los días 27 y 28 de octubre, dejando atrás las fechas del 2 y 3 de junio anteriormente previstas.

Las circunstancias excepcionales requieren soluciones excepcionales. Las actuales sin duda lo son, y están poniendo a prueba la capacidad de resistencia de muchos profesionales y negocios en el ecosistema empresarial español.

Precisamente por esta razón, de ninguna de las maneras queríamos que nuestros visitantes y clientes se perdieran las oportunidades que les esperan en Plataforma de Negocio.

En este sentido, queremos transmitir un mensaje de calma a todos los profesionales que tuvieran en sus planes participar en el evento: Peldaño, grupo impulsor de Plataforma de Negocio, tiene en su estrategia de gestión una política de garantía de devolución. Ello implica que las inversiones de los clientes realizadas en Plataforma de Negocio están resguardadas y garantizadas al cien por cien por su política de devolución si se anulase el evento. Además, el cliente se habrá beneficiado de una campaña de comunicación asociada a su contratación en Plataforma de Negocio, y esta campaña de comunicación no tendrá ningún coste para el cliente.

Tenemos claro que en estos momentos es más importante que nunca ser parte de la solución y no parte del problema para nuestros clientes.

Nuestro equipo está desde ya a plena disposición de todos aquellos que necesiten aclarar temas relacionados con este cambio de fecha o cualquier otro aspecto del evento.

PREMIOS SECURITY FORUM 2020

Los Premios Security Forum 2020 también se ven afectados por este cambio de fecha. Por tanto, los premios tendrán lugar el día 27 de octubre durante la cena-cóctel que tendrá lugar este mismo día. Estos premios tienen la finalidad promover y potenciar la investigación, el desarrollo y la innovación de la industria de la seguridad en España.

Con el aplazamiento de Plataforma de Negocio, también ampliamos las fechas para poder presentar las candidaturas. Las memorias deberán ser recibidas hasta el 1 de septiembre. El fallo del jurado se llevará a cabo el día 15 de septiembre.

security forum

CCIB - BARCELONA | 27 - 28 OCTUBRE 2020

¿Qué tienen en común un director de seguridad, un CISO y un experto en sistemas de seguridad?

Que todos encuentran soluciones en Plataforma de Negocio.
Y lo hacen de forma gratuita.

Plataforma de Negocio une tecnología y profesionales influyentes para que las empresas afronten la transformación digital con las mejores herramientas.

Si buscas u ofreces soluciones reales para empresas, no te lo pienses.

Inscríbete gratis en
plataformadenegocio.es/securityforum

PLATAFORMA DE NEGOCIO

Impulsa: Peldaño

ACTIVA. COMPARTE. POTENCIA.
Tres eventos profesionales en un mismo espacio.

security forum | tecnohotel forum | contact forum

En paralelo, seguiremos trabajando duramente para que cuando el otoño asome por la puerta, el CCIB acoja una edición espectacular de Plataforma de Negocio. Agradecemos la comprensión de todos los afectados y mandamos mucho ánimo a todas las personas y entidades que están atravesando este duro bache.
A pesar del cambio de fechas, Security Forum sigue siendo la mejor opción para los profesionales y empresas que desean descubrir los últimos lanzamientos de la industria y las tendencias que marcarán el futuro del sector en las áreas de videovigilancia, integración de sistemas, control de accesos, seguridad lógica y seguridad física, IP/redes, entre otras.
La transformación digital, ingeniería social, la seguridad privada en un mundo globalizado, o las perspectivas de negocio de la seguridad privada en el s. XXI vertebran un completo programa en el Congreso Security Forum 2020 del que iremos informando puntualmente.

Para más info: securityforum.es ✱

Plataforma de Negocio 2020 presenta a sus embajadores

Plataforma de Negocio ha presentado a los seis embajadores que conformarán el comité asesor del evento en su edición 2020. La sede de Peldaño a las orillas del río Manzanares de Madrid ha sido el escenario en el que han coincidido Alfonso Castaño, Eduard Zamora, Fabián González, Rodrigo Martínez, Emilio Castellote y Ramón Cabezas, seis profesionales de prestigio, influyentes y reconocidos en sus respectivos sectores.
Este órgano asesor y de referencia será prescriptor del evento y embajador de la edición 2020. Colaborarán aportando ideas y su amplia experiencia en cada sector, potenciando la comunicación de esta ambiciosa iniciativa B2B que se celebrará en Barcelona el 27 y 28 de octubre.

PLATAFORMA
DE NEGOCIO

CCIB - BARCELONA

27 - 28 OCT 2020

La mejor plataforma para hacer negocios

plataformadenegocio.es

Impulsa: Peldaño

ACTIVA. COMPARTE. POTENCIA.
Tres eventos profesionales en un mismo espacio.

security forum | tecnohotel forum | contact forum

DIVERSIÓN Y OCIO ASEGURADOS

Directores y responsables de Seguridad analizan el momento actual de la seguridad en grandes eventos y centros de ocio

Quién no ha ido alguna vez a un macro concierto, un partido de fútbol o baloncesto, un congreso, una feria...? Grandes eventos, en recintos hoy en día multiusos, en los que se pueden llegar a congregar miles de personas. Instalaciones y espacios singulares, que acogen todo tipo de eventos y actividades, en los que la seguridad juega un papel fundamental para garantizar la diversión y disfrute del público, así como de los trabajadores del centro y de los propios protagonistas del evento.

Garantizar la seguridad es una de las máximas para el adecuado desarrollo de un gran evento, que requerirá la implantación de una serie de medios y medidas de seguridad en función de las características del mismo: público, recinto, horario, etc. El objetivo final es dotar de una seguridad integral, que aglutine la seguridad física del recinto, la seguridad interior y exterior. Y es que a la hora de garantizar la seguridad y la prevención en este tipo de celebraciones existen tres fases esenciales: Planificación, en la que se analizarán, entre otros aspectos los riesgos, normativa de aplicación,...; Intervención, fase en la que se hace efectivo el Plan de Seguridad que se ha elaborado previamente; y, finalmente, una etapa de Evaluación, donde se analizará la puesta en escena del plan y su gestión, con el objetivo de mejorar de cara a futuras intervenciones.

Y es que «una de las premisas fundamentales que no se debe producir en un evento multitudinario es la improvisación», señala Juan Carlos Ruiz, director de Seguridad del WinZink Center, en Madrid, para quien la seguridad interior de un gran recinto la compone el personal de seguridad, emergencias, y el propio staff, todo ello apoyado con una buena iluminación, «sistemas integrados de CCTV, contra incendios, antiintrusión, alarmas,

Pablo-heimplatz / Unsplash


pexels/pixabay

megafonía...», y sobre todo que estas medidas estén operativas y en buen funcionamiento.

PREVENCIÓN, LO PRIMORDIAL

Para Julián Suescum, director de Seguridad de Valencia C.F., lo primordial es la prevención, «todo lo que se trabaja antes del evento», por lo que desde el departamento de Seguridad que dirige, en estrecha colaboración con los CC. y FF. de Seguridad, se hace una valoración de los riesgos que se puedan dar durante el evento; de esta manera «podemos adoptar las medidas correctoras o preventivas con el fin de reducir al máximo los riesgos que hemos podido detectar», añade.

De la misma opinión se muestra Raúl Valera, director de Seguridad, experto en la elaboración/implantación de Planes de Seguridad, Emergencias y Autoprotección en grandes eventos, para quien «cada evento está vivo hasta la dispersión del público, y es diferente independientemente de que el número de espectadores y formatos sea incluso el mismo, por lo que hay que tratar cada evento específicamente». Por ello, algunas de las claves que nos ofrece a Cuadernos de Seguridad para garantizar la seguridad en un evento multitudinario, son prevención, proactividad, integración, coordinación y evaluación de todas y cada una de sus fases.

PROTECCIÓN CONTRA INCENDIOS

Pero también los incendios son uno de los riesgos que se pueden desencadenar en espacios/centros de ocio y grandes eventos. En el caso de España, los centros de ocio tienen que instalar obligatoriamente una serie de medidas de seguridad que son exigidas por el Código Técnico de la Edificación, CTE-DSBI, así como reglamentos de la comunidad autónoma, y en otros muchos casos, incluso ordenanzas municipales. Medidas a aplicar son, en palabras de Adrián Gómez, presidente de Tecnifuego –Asociación Española de Sociedades de Protección contra Incendios–, una debida compartimentación y habilitación para la evacuación, y en superficies de más de 10.000 m² la instalación de sistemas de detección, «rociadores automáticos y sistemas de evacuación de humos y, por supuesto, extintores, BIE, puertas cortafuego, hidrantes de exterior para uso de los bomberos, etc.»

Y no podemos terminar este artículo sin hacer referencia a la importancia de potenciar la cultura de prevención en este tipo de eventos, y fomentar la tolerancia cero ante la violencia en el deporte. «Los valores intrínsecos del deporte son en sí mismos incompatibles con la violencia... El deporte ha de entenderse como un factor de integración y no exclusión, fomentando el respeto a los derechos fundamentales y libertades públicas consagradas en la Constitución», asegura Fernando Bernal, director de Seguridad del Sevilla C.F. La verdad es que es necesaria una labor de concienciación y potenciación sobre la implantación en la sociedad de una cultura de prevención y seguridad en los grandes eventos. ✱

Western Digital®

Ni un punto ciego

Una gama amplia de soluciones de almacenamiento para la videovigilancia inteligente

Nos adelantamos al futuro. La seguridad inteligente está evolucionando más rápido que nunca. Esté preparado con nuestras soluciones de almacenamiento calibradas al milímetro y diseñadas para el vídeo inteligente. Nuestros productos ofrecen fiabilidad y durabilidad, son compatibles con las transmisiones múltiples y cuentan con capacidades escalables y funciones de análisis incorporadas, tanto para vídeos sin procesar e IA, como para puntos finales y sistemas en la nube; todo ello ofrecido por Western Digital.

Obtenga más información en
www.westerndigital.com/no-blind-spots.

IÑAKI GARMENDIA
GESTOR DE SEGURIDAD Y LOGÍSTICA. PALACIO EUSKALDUNA BILBAO

«Queremos que Euskalduna Bilbao sea un centro moderno, seguro y de gran calidad para los usuarios»

Texto: Gemma G. Juanes.
Fotos: Palacio Euskalduna Bilbao

Iñaki Garmendia, gestor de Seguridad y Logística, (en el centro de la imagen), junto a José Luis Roca y Fernando Díez, jefes de equipo del Servicio de Seguridad de Euskalduna Bilbao.

—«Nuestra principal misión como gestores de la Seguridad, es establecer y ejecutar los planes de acción necesarios, para que Euskalduna sea una instalación lo más segura posible», explica Iñaki Garmendia, Gestor de Seguridad y Logística del Palacio Euskalduna Bilbao, quien en esta entrevista con CUADERNOS DE SEGURIDAD, analiza los elementos clave a la hora de planificar la seguridad del centro, entre otros aspectos.

—A grandes rasgos, ¿podría explicarnos características concretas del Palacio Euskalduna, aforo, número de empleados, eventos que se realizan...?

—Somos un edificio singular ubicado en Bilbao, propiedad de la Diputación Foral de Bizkaia, cuya principal actividad es la de facilitar espacios de calidad para el desarrollo de diversas actividades de distinta índole (cultural, musical, congresual, empresarial, etc.).

Así mismo, damos el apoyo y asesoramiento necesario para que el evento programado se desarrolle con éxito durante su planificación y ejecución.

Cabe destacar, que la Bilbao Orkestra Sinfonikoa (BOS) tiene su sede aquí, magnífica institución musical, fundada en 1920, que dio su primer concierto en 1922. Además, destacar la Temporada de Opera de la ABAO, una de las más importantes y prestigiosas del Estado y de Europa.

Con dicha actividad, trabajamos para generar riqueza cualitativa y cuantitativa en nuestro entorno social sin generar gasto, es decir, siendo autosuficientes y con una gestión basada en la mejora continua.

Somos un equipo propio de 19 trabajadores y contratamos servicios auxiliares necesarios para el mantenimiento del edificio y dar el apoyo técnico y logístico necesario a nuestros clientes. Entre la plantilla de Euskalduna y las empresas colaboradoras, se mueven habitualmente de 50 a 100 trabajadores, con puntas que pueden llegar a los 500 trabajadores, si sumamos las empresas intervinientes en la organización y montaje de un gran evento, como puede ser una Junta de Accionistas de una gran empresa.

La singularidad del edificio y su diseño estructural nos permite realizar eventos simultáneos de distinta índole, manteniendo la independencia y singularidad de cada uno de ellos. Trabajamos para que el Euskalduna Bilbao sea el espacio donde se desarrollen actividades, aportando valor y reconocimiento internacional a nuestra sociedad tanto en el ámbito cultural, congresual y de

empresa, garantizando el rigor económico y la transparencia en la gestión.

Queremos que el Palacio Euskalduna sea una instalación moderna, segura, atractiva y de gran calidad para los usuarios.

Euskalduna constituye un gran complejo multifuncional de 58.200 m², con un aforo máximo simultáneo de hasta 10.000 personas (comprende personal interno y clientes). Cabe destacar que, disponemos de uno de los escenarios más grandes de Europa y fuimos reconocidos como mejor Palacio de Congresos del mundo en el año 2003. Por supuesto, seguimos trabajando para mejorar, día a día, y no bajar ni un milímetro el nivel.

El edificio combina las zonas dedicadas al uso público, a través de su Auditorium y de sus numerosas salas de congresos, salas de reuniones, salas de juntas, despachos, foyers y hall de exposiciones (4.200 m²), con las áreas de servicio, destinadas a almacenes, talleres, vestuarios, camerinos, salas de ensayos, oficinas, etc.

Por hacernos una idea del tipo de actividad y afluencia que tenemos en Euskalduna Bilbao, indicar que en 2018 se realizaron un total de 811 eventos, de los que 447 fueron Meetings & Events y 364 fueron representaciones culturales. Se realizaron un total de 38 Congresos, de los cuales el 53% fueron internacionales. Tuvimos un 90% de ocupación y recibimos 518.147 asistentes. Cabe destacar la incorporación del nuevo restaurante del Chef Eneko BILBAO by Patricia Urquiola, habiendo obtenido una estrella Michelin 5 meses después de su apertura.

«En un centro como Euskalduna Bilbao es crítico cooperar y estar en comunicación con los servicios públicos»

Presenta forma irregular y con una altura superior a 53 m. En él se diferencian claramente cuatro volúmenes:

1. Edificio Singular (vestíbulos, foyeres, salas, despachos, botiquín, restaurantes y cafetería, almacenes, vestuarios de hostelería y zonas técnicas).
2. Edificio Camerinos (salas de ensayo, vestuarios, camerinos y zonas técnicas).
3. Edificio Buque (auditorio, salas-escenario).
4. Zona Ampliación (hall exposiciones, salas, almacenes, zonas técnicas).

—¿Cuál es la estructura e infraestructura del área de Seguridad de Palacio Euskalduna?

—La gestión de los servicios encomendados a la empresa de seguridad es responsabilidad de la Dirección Técnica, de la cual dependo. La contratación de empresas de seguridad privada se realiza a través de oferta pública, en la que Euskalduna Bilbao establece los requisitos

que considera oportunos dentro del marco legal. En la actualidad el servicio de seguridad lo presta la empresa Prosegur.

El equipo humano básico de seguridad está compuesto por un jefe de equipo por turno (total 2), 2 puestos de control de acceso (Puertas) y un puesto en el Centro de Control. Además de estos puestos básicos, dependiendo de la tipología del evento y necesidades puntuales, se refuerza el servicio según necesidad. Todo el servicio es supervisado a su vez por un Inspector de servicio y apoyado por las noches por una Central Receptora de Alarmas y un Centro de Control externo. Aprovecho la ocasión para agradecerles y felicitarles por el gran trabajo que realizan y vienen realizando, gran equipo.

Nuestra principal misión como gestores de la seguridad, es establecer y ejecutar los planes de acción necesarios para que Euskalduna sea una instalación lo más segura posible, tanto para sus trabajadores, como para sus clientes, intentando que dicha cualidad sea valorada interna y externamente, aportando a la entidad mayor prestigio.

Una de las principales características que tenemos, y creo que nos diferencia, es que, dependiendo de las exigencias y necesidades de nuestros clientes, facilitamos la posibilidad de ampliar el servicio/dispositivo hasta donde consideren necesario, adaptando la seguridad de Euskalduna a la necesidad de seguridad de nuestros clientes.

En cuanto al Centro de Control, indicar que el mismo es compartido a propósito con el equipo de Mantenimiento, ya que, en un edificio de tal envergadura, es crítico que las incidencias y averías se comuniquen rápido al objeto de que se resuelvan lo antes posible. Así mismo, en un caso de emergencia, también consideramos importantísimo tener a disposición el equipo de Mantenimiento para actividades críticas que puedan hacer falta como es el corte de gas, electricidad, etc.

En cuanto a medios técnicos, creo que no disponemos de nada que no pueda tener cualquier otra instalación que requiera vigilancia y compartimentación de áreas. Contamos con cámaras de videovigilancia interiores y exteriores. Detectores de movimiento, contactos de puerta, centralita de incendios, centralita de ascensores, megafonía interior y disuasoria, control de acceso y sectorización interior del edificio.

Estos medios técnicos con el trabajo de planificación de eventos del equipo y el gran diseño arquitectónico, nos permite hacer de Euskalduna Bilbao un edificio multifuncional, y además, de forma simultánea.

—¿Podría explicarnos los medios y medidas de seguridad con que cuenta la instalación?

—Numero los más importantes:

1- Cabe destacar, de forma muy importante, la relación de cooperación y coordinación absoluta con los Servicios de Emergencias de Bilbao. Ertzaintza, Protección Civil, Servicios Sanitarios y distintos departamentos del Ayuntamiento de Bilbao.

Aprovecho la ocasión para agradecerles todo su apoyo y ayuda en el día a día. Creo que, en un centro como el nuestro, con tanta afluencia de público y diversidad de actividades, es crítico cooperar y estar en permanente comunicación con los servicios públicos de la ciudad. Realmente nos sentimos arropados.

2- Tenemos implantado desde 2008 un sistema de Gestión según OHSAS 18001 basado en una Política de Prevención de Riesgo. Este mismo año hemos sumado la certificación de Empresa Saludable.

3- Medios de detección y control de incendios pasivos y activos.

4- Medios anti-intrusión, sensores de movimiento, contactos de puerta, Seguridad 24 horas.

CIBERSEGURIDAD

Nuestro reto, tu tranquilidad

Apostamos por un tratamiento global de la ciberseguridad, **identificando** las amenazas existentes, **protegiendo** los activos, **detectando** intentos de ataque y, si se producen, **restableciendo** la situación lo antes posible, todo orquestado mediante los sistemas de gestión más exigentes.

¿Qué podemos hacer por ti?

- Descubrimos las **vulnerabilidades** existentes y nos aseguramos de que queden resueltas.
- Te mostramos como aprovechar las capacidades que **cloud** ofrece para detectar malware avanzado o parar ataques de denegación de servicio.
- Adoptamos la filosofía **SecDevOps**, para que tus procesos de desarrollo sean más ágiles y resilientes.
- Utilizamos **Inteligencia Artificial** para combatir el fraude de forma certera y totalmente personalizada.
- A través de **ciberinteligencia**, interpretamos adecuadamente la información a nuestro alcance para tomar las mejores decisiones en tiempo real.
- Te ayudamos a cumplir con la **legislación** vigente de tu sector para que consigas el óptimo nivel de ciberseguridad y privacidad.

marketing.TIC@gmv.com

gmv.com

gmv®
INNOVATING SOLUTIONS

5- Medios de identificación y control de trabajadores y visitantes. Principalmente de 2 tipos: Visuales (cámaras de videovigilancia) y de control de acceso (identificación y autorización de trabajadores y visitantes, según criterios de acceso establecidos por la Direccion).
6- Medios de control de aforos. Contadores automáticos que se activan cuando la entrada es libre o de venta continua de entrada.
7- Mantenimiento preventivo y correctivo continuo.

«Nuestra misión es establecer y ejecutar los planes de acción necesarios para que Euskalduna sea una instalación lo más segura posible»

8- Somos edificio cardio protegido, disponiendo de 5 desfibriladores semiautomáticos situados de forma estratégica en el edificio, y con un equipo de seguridad preparado para su utilización.
9- En el ámbito sanitario, indicar que disponemos de botiquín equipado fijo y personal sanitario profesional cuando el aforo supera las 2.000 personas. Este servicio se puede ampliar o completar a medida del cliente.
10- Disponemos de personal instruido en la evacuación de ocupantes y extinción de incendios, a los que entrenamos a través de simulacros anuales. El equipo de alarma y evacuación y el equipo de Primera Intervención está formado por un grupo de más de 50 personas. No todos intervienen a la vez, su presencia está supeditada a los espacios utilizados, la afluencia de personas y al tipo de actividad que se desarrolle.
11- Consideramos imprescindible la formación continua de los trabajadores, y valoramos aún más, la formación práctica.

Aunque lo hemos comentado antes, uno de los aspectos más importantes y que más trabajamos en Euskalduna respecto al funcionamiento del equipo de seguridad, es la gran necesidad de adaptación que debemos de tener para adecuar el nivel de seguridad a las necesidades de nuestros clientes.

Podemos decir que somos capaces de hacer de Euskalduna Bilbao, un edificio abierto donde el control de seguridad es mínimo y los visitantes se pueden mover libremente con total seguridad; un edificio cuyo acceso y movimientos internos están totalmente controlados asemejándose a una fortaleza.

—¿Cuáles considera que son los elementos clave a la hora de planificar una seguridad integral en instalaciones como las del Palacio Euskalduna?

—Como antes he comentado, es muy importante contar con una cooperación y comunicación continua con los servicios públicos de la ciudad. Es crítico disponer de una Evaluación de Riesgos real y actualizada al momento en que nos encontremos.

Tenemos riesgos básicos o propios de Euskalduna, generados por la actividad de las personas que trabajamos y por la propia instalación, y tenemos los riesgos asociados a nuestro cliente y su evento.

En cuanto a los riesgos básicos, establecemos planes de acción a corto y medio plazo al objeto de eliminar o minimizar los riesgos detectados.

En cuanto a los riesgos asociados a nuestro cliente y su evento, asesoramos de posibles soluciones según nuestra experiencia y facilitamos los medios materiales y humanos que se precisen. Así mismo, facilitamos la coordinación con los servicios de la ciudad, contacto con ayuntamiento, policía, protección civil, en caso de ser necesario.

Cuando hablamos de seguridad integral, debemos considerar y tener en cuenta todos los riesgos: Riesgos de Seguridad Lógica, Riesgos Laborales y Riesgos de Autoprotección.

Por último, pero no menos importante, destacaría la proactividad de la Direccion en el ámbito de la seguridad. Sin una Direccion implicada, no es posible hacer seguridad.

—¿Cómo se organiza la seguridad de un centro donde se celebran eventos de diferentes características y donde este factor es una de sus prioridades?

—Diferenciamos dos niveles de seguridad. Por un lado, tenemos la seguridad básica, que es la organización mínima que precisa la instalación para funcionar, y por otro lado, la seguridad del evento, que se adapta a las necesidades que nos marca el cliente en cada uno de los eventos, siempre garantizando el cumplimiento de lo establecido legalmente en esta actividad.

En cuanto a la simultaneidad de eventos de distinta índole, nos lo facilita el diseño del edificio y la planificación al milímetro que realiza el equipo Euskalduna Bilbao. Para entenderlo de forma sencilla, es como tener edificios independientes dentro de uno.

1-Tenemos la planta 0 con 4.200 m^2 de halles y 5 salas principales, que nos permite desarrollar un gran evento con capacidad para 3.000 personas, o diversos eventos pequeños compartiendo espacio de hall. Este espacio tiene salida directa a la calle a través de la misma planta y a través de la planta 1º y 2º donde se encuentran las puertas principales de acceso 1 y 2.

2- Tenemos un auditorio con capacidad para 2.200 personas cuyos accesos internos se encuentran repartidos de la planta 2º a la planta 7º, que nos permite tener espectáculos y reuniones de forma simultánea a la actividad de planta 0. Este espacio comparte salida en puerta 2 con la actividad de planta 0, pero también tiene su propia puerta de acceso y tres escaleras especialmente protegidas.

3- Contamos con un edificio de camerinos, individuales y colectivos, una cafetería interna que da cobertura al escenario principal y diversas salas de ensayo. Dispone de sus propios accesos exteriores, diferenciados de las indicadas anteriormente.

4- Dos restaurantes y una cafetería que cubren nuestro servicio de hostelería interna a los eventos y a su vez mantienen su propia actividad independiente a la de Euskalduna, ya que también cuentan con sus propios accesos exteriores. (Restaurante Eneko Bilbao con una estrella Michelin, Restaurante Jauregia y Cafetería Jauregia).

Doy un dato representativo que es parte del diseño estructural del edificio y hace posible en parte nuestra multifuncionalidad simultánea. Para un aforo máximo simultáneo de 10.800 personas, tenemos una capacidad de evacuación en salidas de 17.700 personas. Este dato también nos hace conscientes de las limitaciones que obligan las normas de autoprotección en cuanto al cálculo de evacuación de ocupantes.

—En un mundo globalizado, donde somos objeto de ciberamenazas, ¿están las instalaciones como las del Palacio Euskalduna expuestas y preparadas ante este nuevo tipo de amenazas?

—Sin duda, todos estamos expuestos a ciberataques y tenemos mucho trabajo en concienciarnos de la realidad y peligrosidad de este riesgo. En cuanto a si estamos preparados, en mi opinión creo que estamos en proceso de aprendizaje.

Creo imprescindible evaluar el estado de las empresas en este ámbito y animo a todas las empresas a realizar auditorías de sus sistemas informáticos a través de empresas especializadas. Debemos identificar puntos débiles y fuertes, y así establecer las acciones necesarias según los recursos disponibles.

En esta faceta también es muy importante el apoyo de servicios como el que nos aporta en Euskadi, el Basque Cibersecurity Center o asociaciones de profesionales de la seguridad como SAE (Segurtasun Adituen Euskal Elkartea).

En mi opinión, es imprescindible que las empresas atacadas compartan sus incidencias y que el conocimiento de expertos en la lucha de estos delitos, faciliten información y métodos de trabajo, para que todos en conjunto nos sintamos y estemos más protegidos.

El reto más importante al que se enfrenta la sociedad en este riesgo está en la concienciación de cada persona. En muchos casos, los ataques precisan de nuestra colaboración para hacer realmente daño. En este caso, la difusión de medidas preventivas de forma continua y actualizada es una herramienta muy potente para protegernos. Hay mucho camino por recorrer en poco tiempo. El desarrollo tecnológico actual crece exponencialmente, al igual que el riesgo que entraña.

—¿Cuáles son los grandes retos a los que se enfrentan hoy en día los responsables de seguridad de centros como el Palacio Euskalduna?

Yo destacaría los siguientes:

1. Reto de concienciar de la importancia que tiene evaluar riesgos y adoptar acciones que anulen o minimicen los mismos. ¡Que importante es comunicar riesgos, incidencias, accidentes, para poder investigarlos y así adoptar acciones que eviten su repetición!.
2. Reto de formar e instruir a un equipo humano para que, en caso de emergencia, o en el desarrollo de su trabajo, sepan responder a las distintas circunstancias de riesgo que se les planteen.
3. Reto de mantener controles periódicos de seguimiento que nos aporten datos de nuestra evolución y nos ayuden en la toma de decisiones con el objetivo de reducir y anular riesgos.
4. Reto de hacer cumplir la legislación y normativa en materia de prevención y seguridad.
5. Reto de hacer frente a nuevos riesgos como son:
   - El Yihadismo y el miedo que ello genera en la sociedad, «pánico espontáneo».
   - Los ciberataques.
   - Cambio climático y sus consecuencias.

En cuanto a nuestros propios retos:

1. Reto de seguir siendo centro de referencia europeo para la celebración de grandes eventos de índole cultural/musical, empresarial y congresual y así generar riqueza en la ciudad y en Euskadi.
2. Reto para que este barco en continua construcción, desde su dique, no pare. PROA Euskalduna Bilbao. Visitanos en: www.euskalduna.eus. ✱

MEDICIÓN INSTANTÁNEA DE **TEMPERATURA CORPORAL**

Eficiencia visible en tiempo real

PRECISIÓN DE MEDICIÓN ± 0.3°C

KIT BÁSICO

JQ-D70Z

Blackbody, proporciona una referencia de temperatura constante y precisa que la cámara utiliza para autocalibrarse y aumentar la precisión de la medición.

TPC-BF3221-TB7F8

Cámara híbrida con medición de temperatura que proporciona simultáneamente una imagen normal y una imagen térmica de la escena tomada.

DAHUA TECHNOLOGY IBERIA
Tel: 0034 - 91 764 98 62
Av. De la Transición Española 24, 4º-128108 Alcobendas (Madrid)
marketing.iberia@dahuatech.com

ALFONSO ILLESCAS
DIRECTOR DE SEGURIDAD DE IFEMA. MADRID

«Nuestro reto es armonizar el nivel de protección de personas, bienes e instalaciones que IFEMA requiere»

Texto: Gemma G. Juanes.
Fotos: IFEMA

Previsión, prevención, preparación y protección, son según Alfonso Illescas, director de Seguridad de IFEMA, los pilares sobre los que debe asentarse una adecuada seguridad en una instalación como es el Recinto Ferial IFEMA. Y es que, quién mejor que él, para explicar a CUADERNOS DE SEGURIDAD la estrategia de seguridad de un recinto que, con más de 200.000 m² cubiertos de exposición, recibe anualmente a 4 millones de visitantes.

—¿Cuál es la metodología de trabajo diaria que lleva a cabo el departamento de Seguridad del Recinto Ferial IFEMA?

—Se parte de un dispositivo fijo de seguridad/emergencias permanente y estable (24/7), en una planificación anual. Diariamente, se añade otra variable en función de la actividad que viene determinada por la dinámica del negocio (montajes, celebraciones, desmontajes,...), el tipo, características y circunstancias –internas y externas- de los eventos programados, sus confluencias, solapamientos, contextos, etc., dentro de una planificación específica focalizada por la concentración de dicha actividad en espacio (instalaciones contratadas –pabellones, auditorios, zonas exteriores, Palacio,....) y tiempo (fechas de contratación), y que suelen comprender periodos concretos de entre una y tres semanas.

La planificación de los servicios de seguridad/emergencias y de control de accesos afecta tanto a la previsión de recursos humanos, como a la disponibilidad de medios materiales y técnicos, así como a la configuración concreta de los sistemas de seguridad en función de los escenarios en los que hay que operar. Esta se lleva a cabo por el personal de IFEMA de la Dirección de Seguridad y Autoprotección, en donde se residencia su departamento de Seguridad, desde la que también se dirige y supervisa al personal que los ejecuta dependientes

de las empresas colaboradoras competentes, como: vigilantes de seguridad, detectives privados, medicina de emergencias (médicos, ATS), ambulancias, bomberos de empresa y control de accesos.

—¿Cómo ha variado la seguridad, en cuanto a estrategia y logística, en instalaciones como las del Recinto Ferial IFEMA?

—Los diseños de los dispositivos son más variados y dinámicos, más «a la carta», –aunque imperando siempre un criterio de integración–, derivado de la diversificación del tipo de evento que hoy en día se ofrece desde IFEMA. Más allá de ferias, exposiciones o congresos –ya de por sí diferentes y que requieren de un tratamiento específico y diferenciado-, el recinto acoge nuevos eventos de muy distinta naturaleza (conciertos «indoor» y «outdoor», festivales, eventos deportivos, espectáculos públicos de todo tipo –musicales, circos, eventos de ocio masivos...–), cada uno con sus especificidades, que determinan tratamientos particulares.

Hemos perfeccionado la gestión de la información para garantizar un análisis de los escenarios de operación preciso y, así, optimizar los recursos y medios materiales y técnicos disponibles, en una gestión eficaz y eficiente, asegurando el adecuado tratamiento que requiere el constante y significativo incremento de actividad, la multiplicación del número de eventos y la extensión de horarios más allá de los habituales. Anualmente nos visitan más de 4 millones de personas y el flujo de vehículos de todo tipo supera los 2 millones de unidades.

Ha habido una redefinición de procedimientos, una concienciación específica a los profesionales y una potenciación de sistemas de vigilancia y protección para enfrentar una particular amenaza, como son posibles ataques indiscriminados a personas e instalaciones.

Se ha apostado por referenciar actuaciones y procedimientos a estándares internacionales, a través de la certificación ISO 22320 en Gestión de Emergencias, comprometiendo con ello la prestación de un servicio de calidad y su mejora continua. También mediante el intercambio de información con otros grandes recintos europeos a través del Security Working Group de la European Major Exhibition Centres Association (EMECA), de la que IFEMA es miembro.

Carta al ecosistema profesional español

Estimados lectores, clientes y amigos de Peldaño,

Nuestro grupo de comunicación cumplirá treinta y cuatro años este mismo mes de marzo. Tres décadas y media en las que hemos sido testigos y relatores de muchas transformaciones, crisis, recuperaciones... en el ecosistema social y económico que nos rodea. Pero a diferencia de eventos anteriores, estos días **nos tocará superar por primera vez una situación inédita en nuestro país** y entorno inmediato.

Medios de comunicación, empresas, personas, administraciones y sociedad no tenemos misión más importante, en las semanas que siguen, que la de arrimar el hombro, ser solidarios y poner nuestro grano de arena para ayudar a derrotar la pandemia.

En el caso de Peldaño, **instaurar el teletrabajo de toda nuestra plantilla por primera vez en nuestra historia** ha sido el primer paso.

Hoy a través de Cuadernos de Seguridad, Gaceta Dental, Contact Center Hub, Panorama, Restauración News, Mab Hostelero, TecnoHotel News, DiffusionSport, AutoC y Entre Estudiantes, y anteayer con otras cabeceras que se quedaron por el camino, lo mejor que ha hecho Peldaño desde su nacimiento es **conectar a profesionales con la información de calidad que necesitan.**

Tened la firme convicción de que vamos a seguir haciéndolo durante esta crisis, aunque sea desde detrás de los escritorios de nuestras habitaciones. Además, ponemos nuestros canales a disposición de todos los clientes que necesiten comunicar las diferentes medidas que están adoptando en sus compañías en tan excepcionales circunstancias.

Como Presidente de Peldaño y en nombre de todos sus empleados os quiero hacer llegar este mensaje de cercanía, apoyo y calor: **cuidad de los vuestros y cuidaos mucho vosotros mismos**. Todo lo demás llegará a su debido tiempo.

Dentro de muy poco tiempo nos encontraremos y nos abrazaremos en esos eventos profesionales, plazas, bares o terrazas que tanto añoramos hoy. Celebraremos que hemos acabado con el COVID-19 y **recordaremos con orgullo estos días en los que todos tuvimos que parar para que todo pudiera seguir adelante.**

Mucha fuerza, compañeros.

IGNACIO ROJAS.
PRESIDENTE DE PELDAÑO

Sanitarios
Teleoperadores
Policías
Transportistas
Carteros
Farmacéuticos
Seguridad ciudadana
Periodistas
Cajeros
Panaderos
Limpiadores
Cuidadores
Carteros
Militares
Voluntarios

Y a todos los que estéis dándolo todo...

GRACIAS

#EsteVirusLoParamosUnidos

Peldaño

Comunicamos. Conectamos. Impulsamos.

IFEMA, en cifras

IFEMA cuenta con dos recintos en la capital española, Feria de Madrid, con más de 200.000 m² cubiertos de exposición, que reciben anualmente a 4 millones de visitantes y 36.000 empresas de todo el mundo; e, IFEMA Palacio Municipal, recientemente incorporada su gestión, con más de 30.000 m² útiles divididos en amplias zonas, y un Auditorio con capacidad para 1.812 butacas. A estos espacios se sumará un nuevo gran emplazamiento, con la ejecución del proyecto de ampliación de IFEMA Valdebebas. IFEMA acoge anualmente más de 700 convocatorias de todos los sectores, además de 120 ferias y congresos.

—¿Cuáles considera que son hoy en día los pilares sobre los que debe asentarse una adecuada seguridad en una instalación como el Recinto Ferial IFEMA?

—Previsión: o lo que es lo mismo, anticipación a las particularidades de un evento concreto que se va celebrar, a la situación del propio recinto en su conjunto en ese momento e, incluso, a coyunturas de ámbito regional, nacional o internacional que pudieran ser de afectación; todo ello en un entorno de gestión de la información adecuado y preciso.

Prevención: o capacidad para evitar la materialización de riesgos, en donde la actuación anticipada con ocasión de posibles indicadores y la disuasión, cumplen un papel protagonista.

Preparación: entendida como el diseño de procedimientos eficaces y adecuados (oportunos, proporcionados, congruentes), la disponibilidad de personal cualificado para llevarlos a cabo (selección, especialización, formación y entrenamiento) y de la capacidad tecnológica necesaria y acorde con las amenazas que hay que enfrentar.

Protección: es decir, la adecuada ejecución de actuación ante la manifestación de un riesgo, interviniendo, entre otros, aspectos fundamentales (intangibles) como la concienciación, motivación y disposición del personal operativo, y el compromiso y liderazgo de sus responsables.

—¿Se han llevado a cabo mejoras en cuanto a infraestructuras de Seguridad en el Recinto Ferial IFEMA?

—En los últimos tres años se han llevado a cabo tres ambiciosos proyectos de actualización, potenciación o innovación tecnológica en los ámbitos de la vigilancia y protección de personas, instalaciones y bienes:

-Sistema de CCTV: migración de tecnología analógica a digital con sustitución de la plataforma operativa, cámaras, etc., de última generación; incorporación de analíticas, incremento del número de cámaras tanto en interior de instalaciones como en exteriores, derivado de las necesidades detectadas, consecuencia de la actualización del análisis de riesgos y evaluación de las amenazas, así como de los nuevos tipos de evento que se celebran en el recinto.

-Sistema de Megafonía de Emergencias: sustitución, bajo estándares UN 54, del antiguo y parcial sistema de megafonía más orientado a uso comercial, así como su ampliación a todo el recinto ferial –cubriendo el 100% de los espacios interiores y exteriores-, asegurando su eficacia en cualquier situación.

-Sistema mecanizado de bolardos de seguridad: para protección de todos los accesos del recinto ferial y puntos críticos, frente a la amenaza de posibles ataques indiscriminados contra personas mediante empleo de vehículos.

—¿Qué retos debe asumir un responsable de Seguridad a la hora de implantar una estrategia de seguridad en un recinto de la singularidad de IFEMA?

—Con carácter general, el reto siempre es conseguir armonizar el nivel de protección de personas, bienes e instalaciones que un recinto de estas características requiere en cada momento y circunstancia, con los intereses comerciales y de negocio, sin menoscabo de la eficacia del primero y del resultado de los segundos.

Por otro lado, dado el momento en el que nos encontramos, nuestro particular reto es adaptar un nuevo modelo derivado de la ampliación del negocio. Inveteradamente IFEMA ha desarrollado su actividad en una única sede, asumiendo una gestión centralizada de la seguridad que, debiendo mantenerse, tiene que adaptarse a la gestión de nuevas e importantes instalaciones «periféricas» que se añaden al Recinto Ferial, como es el Palacio Municipal, dependiente de IFEMA desde hace un año, la ampliación en la zona Valdebebas con nuevos pabellones, auditorio, zonas exteriores, aparcamientos, etc., u otros posibles proyectos a determinar en su momento.

—Nuevas amenazas globales, ciberseguridad... ¿cuáles considera que son las claves para hacer frente a esta nueva era de la seguridad?

—En el ámbito de ciberseguridad, es básica la concienciación del usuario como una de las medidas más importantes con el fin de evitar incidentes. En este punto, trabajamos en la formación y la comunicación de instrucciones a toda la plantilla. Es importante también el concepto de security by design, para adoptar todas las medidas necesarias de disponibilidad e integridad en cada diseño del sistema informático, infraestructura, comunicaciones o aplicaciones.

Hay dos tipos de compañías: las que han sido atacadas y las que van a serlo. También hay que prestar especial atención a las medidas de resiliencia, actualización continua de los sistemas, así como adoptar medidas ante las amenazas persistentes avanzadas (APT), trabajando para evitarlas, en la medida de lo posible. De hecho, pensamos que existen dos tipos de compañías: las que han sido atacadas y las que van a serlo.

En el ámbito de la seguridad física las claves para enfrentar la amenaza terrorista internacional, amenaza global por excelencia, está en el escrupuloso cumplimiento de los principios en los que se basa el modelo de seguridad asumido («previsión, prevención, preparación y protección»), y en la mejor y permanente disposición para asegurar la total cooperación, colaboración y coordinación, con las instancias públicas competentes de seguridad y de protección civil.

—¿Qué tipo de relación, en cuanto a coordinación, colaboración, etc., existe entre el departamento de Seguridad y el resto de departamentos de IFEMA?

—La relación de coordinación y colaboración entre departamentos es permanente e intensa, cualificada por las características de cada uno de ellos y modulada por la frenética actividad del recinto y del negocio, que se inicia con la idea de un nuevo proyecto, pasando por su definición, hasta su ejecución (montaje, entrada de mercancía, celebración, salida de mercancía y desmontaje) y finalización. Todos los departamentos velamos por y convergemos en los intereses generales de IFEMA, en una misma unidad de acción y dirección.

—El pasado mes de diciembre se celebró en IFEMA la Cumbre del Clima, ¿qué supuso para el departamento de Seguridad la organización de este evento? ¿Cómo se articuló y organizó el dispositivo de seguridad?

—La COP-25 supuso para el departamento de Seguridad poner a prueba su capacidad para:

-Planificar de manera solvente en tiempo record, un dispositivo de seguridad de muy particulares dimensiones y características y diferenciado con respecto a experiencias anteriores.

-Ejecutarlo eficazmente y atendiendo en tiempo y forma todos los requerimientos cuantitativos y cualitativos que nos fueron exigidos, gracias al total compromiso de su personal y al de nuestras empresas colaboradoras (Vigilantes de Seguridad –Prosegur-, Detectives Privados –Kolb, Alian-, Sistemas de Seguridad –Saima, Proselec-, Medicina de Emergencias –Medycsa, ambulancias Ortigueira-, Bomberos de Empresa –Previnsa- y Control Comercial de Accesos –BCM.-).

-Compatibilizar la celebración de un evento de su complejidad y características, con la de otros eventos organizados en IFEMA que se desarrollaron en paralelo en el Recinto Ferial.

-Facilitar y favorecer la coordinación con el dispositivo de seguridad/ emergencias implantado en el marco establecido entre el Ministerio del Interior, NNUU y los órganos de Protección Civil competentes, adaptarse a sus requerimientos e indicaciones, colaborar permanentemente y mantener los niveles de vigilancia y protección fijados para el recinto, en el ámbito de sus competencias.

En ese contexto se articuló y organizó el dispositivo y la máxima expresión fue la constitución de un CECOR permanente mientras duró la celebración de la Conferencia, en el que estaban representadas todas las instancias competentes y a través del cual se coordinaron y encauzaron todas las actuaciones. ✱

AirSpace®
Make your space safer

¡CELEBRAMOS **EL RELANZAMIENTO DE AIRSPACE** CON **GRANDES PRECIOS EN SUS INNOVACIONES!**

AirSpace®
Make your space safer

Nuevo logo más simple y tecnológico adaptado a las nuevas tendencias: soluciones de IA, ciberseguridad, cloud, protección de privacidad y verticales especializadas.

20 AÑOS

20 años liderando el mercado de CCTV

24

Iluminación a todo color las 24h con sus cámaras HD FULLCOLOR Starlight 2, 5 y 8 MP

Compatibilidad total Plug&Play con DAHUA y HIKVISION con sus cámaras IP 2 y 5 MP

La mejor relación calidad-precio del mercado

3 años de garantía

Colaboración con los mejores fabricantes mundiales

Marca exclusiva de By Demes Group, el distribuidor nº1 en Iberia y de referencia internacional

Trato directo fabricante-distribuidor, para asegurar el mejor asesoramiento y soporte

by demes GROUP
El distribuidor líder en tecnologías de seguridad

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

ESPAÑA
Barcelona | Madrid | Canarias
www.bydemes.com

JUAN CARLOS RUIZ
DIRECTOR DE SEGURIDAD. WIZINK CENTER. MADRID

«El público es bastante receptivo a la hora de tomar conciencia de adoptar medidas de seguridad»

Texto: Gemma G. Juanes.
Fotos: G.G.J./WiZink Center

—«El objetivo es dotar de una seguridad integral en la que tanto el público, trabajadores como los propios protagonistas se vean seguros y protegidos en su espectáculo», así lo asegura Juan Carlos Ruiz, director de Seguridad del WiZink Center (Madrid), para quien una de las premisas fundamentales que «no se debe producir en un evento multitudinario es la improvisación». Ruiz Rabadán, desgrana para Cuadernos de Seguridad, los aspectos estratégicos de la seguridad de un recinto multiusos, en el que se llega alcanzar la asistencia mas de 17.453 personas.

—¿Cómo se organiza la seguridad de una gran instalación como es el caso del WiZink Center, donde este elemento es una de sus prioridades?

—El Wizink Center es un recinto multiusos, donde tienen cabida espectáculos deportivos, baloncesto, recinto oficial del Real Madrid y del Estudiantes, lugar donde se ha celebrado la Copa del Rey y Supercopa de Baloncesto, la Copa de España de Fútbol Sala, el campeonato del mundo de Freestyle, entre otros deportes. También se celebran eventos de carácter religioso, políticos, privados, corporativos, ferias de exposiciones y ventas.

Por otro lado, y en un número importante, se encuentran los conciertos donde se llegan a alcanzar las cifras más altas de visitantes: 17.453 personas.

Una de las máximas de la Dirección es la de garantizar la seguridad, para ello se requiere un tratamiento especial y específico para cada tipo de evento.

El objetivo es dotar de una seguridad integral en la que tanto el público, trabajadores como los propios protagonistas se vean seguros y protegidos en su espectáculo.

Para garantizar la seguridad en un espacio como el WiZink Center se ha de contar con una organización de base; llevando el ejemplo a un gran concierto de un reconocido artista, se debe de conocer el perfil del público que va a asistir, siendo un dato fundamental a la hora de realizar un plan de seguridad.

Cada concierto es distinto, dependiendo del público asistente, ya sea fanático, fenómeno fans, adulto, joven, infantil, etc.; los estudios y la estadística que se manejan en el departamento de Seguridad, hace que el

planteamiento de los dispositivos de seguridad y emergencias varíen de unos a otros y se ponga más énfasis en otros aspectos.

«Una de las premisas fundamentales que no se debe producir en un evento multitudinario es la improvisación»

Dentro de esta organización, se ha de contar con varios factores de importancia, como son los datos que ofrece el promotor del evento: el tipo de implantación del formato de la pista, que es el lugar donde se aglomeran más personas, el número de tickets vendidos, horarios, el mes del año, es también un dato relevante por la climatología.

Esta organización está compuesta por un departamento Técnico, otro de Producción, de Ticketing, Comercial, de Servicios, de Prevención de Riesgos Laborales, de Control de Accesos, de Seguridad, de Personal Auxiliar, de Informadores y Acomodación, de Personal Sanitario, entre otros. Todo lo expuesto se finaliza en un documento, denominado Plan de Seguridad, el cual se traslada a los Servicios de la Administración Pública.

—¿Cuáles considera que son los elementos fundamentales a la hora de plantear una seguridad integral en instalaciones del tipo de WiZink Center donde se celebran grandes eventos?

—Una de las premisas fundamentales que no se debe de producir en un evento multitudinario es la improvisación. La seguridad integral en un gran evento la conforma la seguridad física del recinto, seguridad interior y exterior.

La seguridad exterior es la que genera al público la sensación de una buena organización; es muy importante la gestión de las masas en el exterior, en las filas, en

los accesos, en la información y con una buena presencia y profesional del personal del recinto, que hacen que las miles de personas que se encuentran en el exterior entren al recinto de una forma ordenada, coordinada y segura.

La seguridad interior es la que se compone de todo el personal de seguridad, de emergencias y el propio staff. Todo ello se apoya con una buena iluminación, puertas en perfecto estado de apertura, sistemas integrados de CCTV, sistemas contra incendios, PCI, anti intrusión, alarmas, megafonía y una sala estratégicamente situada donde se controle todo lo expuesto, denominada UCO.

—¿Cuáles son los grandes retos a los que se enfrentan hoy en día instalaciones como el WiZink Center en cuanto a seguridad?

—En la actualidad el WiZink Center es el 4º recinto del mundo en venta de entradas y número de eventos celebrados según la revista internacional Pollstar. Este puesto supone un reto de conseguir una mayor y mejor seguridad, y crea una exigencia proactiva al departamento de Seguridad, aún mayor a la que ya teníamos, si cabe.

Para conseguir este objetivo se trabaja y se entrena en los riesgos más extremos que se pueden sufrir como avalanchas, incendios, ataques terroristas, etc.

—¿Cree que existe en la sociedad la concienciación de la necesidad de tomar medidas de prevención y seguridad por parte de los asistentes que acuden a grandes eventos?

—Sí que lo creo. El público es consciente de la situación actual de riesgo que existe, y es bastante receptivo a la hora de tomar conciencia de adoptar las normas y medidas de seguridad.

De hecho en las encuestas realizadas (que elaboramos después de cada evento al público asistente para recibir sus opiniones y poder mejorar nuestros servicios), la percepción de seguridad mostrada por el público es bastante alta, así como la aceptación de las medidas de seguridad.

—En un mundo globalizado, donde somos objeto de ciberamenazas y ataques virtuales, ¿están las grandes instalaciones como el WiZink Center también expuestas a este nuevo tipo de riesgos y amenazas?

—Las amenazas están siempre presentes y no hemos sido la excepción de ciberataques, ello nos ha hecho incrementar en soluciones para combatir estos ataques y para mantener una buena resiliencia ante estos.

—Hoy en día el sector de la Seguridad apuesta por la convergencia de la seguridad como un concepto integral, ¿cree que las instalaciones como el WiZink Center han sabido asumir este nuevo concepto?

—Sí. Creo en la convergencia en la seguridad. El concepto de seguridad se traslada a todos los extremos, como el de control de accesos, el de control de aforo, el sistema sanitario, el de prevención de riesgos laborales, el control de los trabajadores, la prevención, los ciber ataques, la falsedad de las entradas, etc.

—¿Reciben algún tipo de formación, en cuanto a seguridad y prevención, los trabajadores de WiZink Center?

—La base del buen funcionamiento de un gran evento, está en los trabajadores. Es fundamental la formación, por ello, al cabo de un año se realizan varios cursos enfocados al comportamiento, organización y control de

«La base del buen funcionamiento de un gran evento está en los trabajadores, la formación es fundamental»

masas, sobre el comportamiento del fuego y emergencias; primeros auxilios, empleo y uso del DESA; deontología profesional, y también se han añadido unos cursos relacionados con los delitos de odio y pautas de actuación ante el colectivo LGTBI, racismo y xenofobia y contra la libertad sexual.

—¿Qué relación en cuanto a cooperación y coordinación mantiene el departamento de Seguridad de WiZink Center y las Fuerzas y Cuerpos de Seguridad?

—La relación con las Fuerzas y Cuerpos de Seguridad es plena. La Delegación del Gobierno convoca reuniones precisamente para coordinar todo el operativo de seguridad, en el que se encuentra Policía Nacional, Policía Municipal, Samur-Protección Civil, Bomberos, Dirección de Seguridad del recinto, promotores y Seguridad Privada del evento.

Todos los participantes en la convocatoria, tienen un papel fundamental para el buen desarrollo del evento. Y todo ello está coordinado desde el CECOR, (Centro de Coordinación), tanto en el exterior como en el interior del WiZink Center. El papel de las Fuerzas y Cuerpos de Seguridad y de los Servicios de Emergencia son vitales para el buen desarrollo del mismo. ✱

FERNANDO BERNAL GARCÍA
DIRECTOR DE SEGURIDAD. SEVILLA FÚTBOL CLUB S.A.D.

«La formación continua y especializada de los responsables de seguridad de los clubes de fútbol es fundamental»

Texto: Gemma G. Juanes.
Fotos: Sevilla Fútbol Club S.A.D.

—«El principal objetivo de un departamento de Seguridad es crear unas condiciones óptimas de seguridad, generando una sensación de seguridad y control, que puedan ser percibidas por todos los usuarios de las instalaciones o servicios en este caso del Sevilla Fútbol Club», así lo asegura Fernando Bernal García, director de Seguridad del Sevilla Fútbol Club, quien en esta entrevista con Cuadernos de Seguridad desvela cómo se gestiona la seguridad de una instalación y sus profesionales, como es el Estadio de Fútbol Ramón Sánchez-Pizjuán, así como los factores fundamentales a la hora de planificar una estrategia de seguridad integral.

—Para comenzar, ¿podría explicarnos características concretas del Estadio Sánchez-Pizjuán: aforo, número de trabajadores, otros eventos que se realizan…?

—El estadio Ramón Sánchez-Pizjuán tiene un aforo total de 43.883 espectadores. El Sevilla Fútbol Club dispone de un número de empleados superior a los cuatrocientos trabajadores. Actualmente, el Estadio Ramón Sánchez-Pizjuán está siendo objeto de una profunda remodelación que en los próximos meses supondrá un aumento considerable del aforo para público general. Unido a esto se crearán en un corto plazo de tiempo nuevas zonas de hospitalidad y, cómo no, una mayor seguridad percibida al implementarse nuevos y modernos sistemas de seguridad, accesos mejorados e incremento de las puertas de salida para facilitar aún más los flujos de evacuación.

El estadio Ramón Sánchez-Pizjuán tiene tres usos principales. El primero, y fundamental para todo Club de Fútbol, es la organización de encuentros deportivos de competición nacional e internacional. Como segundo destino de las instalaciones del estadio, se celebran otro tipo de espectáculos y eventos que en corto plazo serán destinados al gran público, concretamente la celebración de conciertos de artistas de primer nivel. Finalmente tiene un uso de gestión y administración del Club, donde diferentes Direcciones y empleados del Sevilla Fútbol Club tienen su centro de trabajo habitual, al igual que la explotación de una de las tiendas oficiales del Club.

—¿Cuál es la estructura e infraestructura del área de Seguridad del Sevilla Fútbol Club?

—El departamento de Seguridad del Sevilla Fútbol Club está integrado por la Dirección de Seguridad con un director de Seguridad, miembro del Cuerpo Nacional de Policía en excedencia, perteneciente a las Unidades de Intervención Policial, y una jefa de Seguridad proveniente de la Seguridad Privada con más de diez años de experiencia. Unido a lo anterior y dependientes de la Dirección de Seguridad, cuatro personas más completan el departamento de Seguridad, cuyas funciones de control, planificación, asistencia, administración y gestión son esenciales para el funcionamiento del departamento. Fundamentales son las aportaciones de uno de esos cuatro miembros del departamento por sus conocimientos en materia de ticketing, atención a los abonados o socios, y monitoreo y estudio de redes sociales o webs. Junto a esto, es muy reseñable la experiencia y conocimientos en normativa federativa de otro de los miembros del equipo de seguridad, muy útiles en la organización, gestión y control de todos los encuentros de categorías inferiores que se disputan en las instalaciones del Sevilla Fútbol Club.

Igualmente, el director de Seguridad cuenta con la asistencia directa de un especialista en seguridad privada con más de 24 años de experiencia en el mundo de la seguridad referida al fútbol, a través de la empresa que presta los servicios propios de la seguridad privada para el Sevilla Fútbol Club.

—De manera general, ¿podría explicarnos los medios y medidas de seguridad con que cuenta el Estadio Ramón Sánchez-Pizjuán?

—Todas las instalaciones del Sevilla Fútbol Club disponen de medidas de seguridad que garantizan el buen funcionamiento de las mismas y las protegen de posibles accesos o intrusiones no deseados.

Haciendo una exposición de los medios con los que cuenta el estadio Ramón Sánchez Pizjuán, cabe destacar:

El circuito de cámaras de seguridad privada propiedad de la entidad y controladas por el departamento de Seguridad, que permiten analizar situaciones de emergencia que se pudieran producir y que junto al sistema de alarma anti intrusión contribuyen a generar una sensación de seguridad óptima. Están situadas

«Es objetivo de las Administraciones Públicas y Privadas contribuir a erradicar cualquier manifestación de violencia en el deporte»

en determinadas zonas sensibles y fundamentalmente orientadas al control durante los encuentros deportivos. Este circuito es independiente del sistema CCTV-UCO (Circuito Cerrado de Televisión), controlado por la Comisaría General de Seguridad Ciudadana de la Policía Nacional.
El Estadio dispone de un puesto de Control de Seguridad gestionado mediante la empresa de seguridad privada contratada por el departamento de Seguridad del Sevilla Fútbol Club, desde el que se coordina el dispositivo de seguridad prestado por vigilantes de seguridad en el estadio. Teléfonos fijos de línea segura permitirían la comunicación entre todas las secciones del Estadio en caso de emergencia o caída de las comunicaciones.
Escáneres de seguridad para el control de la paquetería o de los instrumentos con que se quiera acceder al Estadio, como es el caso de cámaras y equipos profesionales de los medios de comunicación. Un dispositivo de perros especializados en la detección de explosivos y artefactos pirotécnicos completan el sistema de control de acceso, junto a palas detectoras de metales en todas las puertas de acceso. Se han instalado sistemas de auto extinción de incendios que mejoran la seguridad en zonas especialmente sensibles.
También se dispone de EPI de primera intervención para los eventos deportivos. Un técnico especializado en la comprobación de la existencia o no de un incidente y determinar las primeras actuaciones a llevar a cabo. Este técnico especialista es contratado para los eventos deportivos del primer equipo del Sevilla Fútbol Club a través de la empresa de Seguridad Privada.
Sistema de cerraduras inteligentes y de seguridad completan los sistemas de seguridad del Estadio.

—¿Cuáles considera que son los elementos fundamentales a la hora de planificar una seguridad integral en instalaciones del tipo del Estadio Sánchez-Pizjuán?

—El principal objetivo de un departamento de Seguridad es crear unas condiciones óptimas de seguridad, generando una sensación de seguridad y control que puedan ser percibidas por todos los usuarios de las instalaciones o servicios en este caso del Sevilla Fútbol Club.
Son misiones principales de los departamentos de Seguridad proteger la integridad física de los usuarios de la instalación, la propia instalación y sus elementos, y la integridad o indemnidad de la propia institución deportiva o sociedad en el caso de un club de fútbol de primer nivel.
La protección de los usuarios del Estadio se realiza mediante un análisis de riesgos. El acceso controlado y seguro al recinto deportivo, la segregación en las gradas de aficiones que pudieran estar enfrentadas por diferentes cuestiones, dispositivos de Seguridad Privada suficientes, Servicios de Emergencias Sanitarios, contra incendios, y Fuerzas y Cuerpos de Seguridad suponen un mínimo para la protección de participantes y espectadores. La declaración de zona cardioprotegida o segura mediante el cumplimiento de las exigencias que suponen tal mención, son pluses de seguridad que han de ser próximamente concebidas como necesarias u obligatorias en relación a la seguridad de los espectadores y participantes del evento.
En relación a la protección del propio estadio deportivo, los nuevos sistemas de autoextinción de incendios, sistemas de CCTV y alarmas controlados mediante un centro de control existente en las propias instalaciones

y dirigidos por personal de seguridad privada habilitado para ello, dobles acometidas eléctricas que garanticen o minimicen los riesgos de los cortes de suministro eléctrico, sistemas de ayuda contra incendios como columnas secas, etc., suponen medidas que contribuyen a mejorar la seguridad de la propia instalación. Fundamental es realizar un exhaustivo control de acceso que permita conocer en todo momento número y localización del personal laboral que accede, y evitar accesos no permitidos o intrusiones que pueden generar una situación de alarma.

En relación a la protección de la propia Institución o Integridad y muy relacionada con la responsabilidad penal de las sociedades, es trascendente que el director de Seguridad pueda participar y colaborar en la adopción de medidas de autoprotección en materia de integridad y ejecución de las mismas, debiendo para ello estar en posesión de titulación y los conocimientos propios. La formación continua y especializada de los responsables de Seguridad de los clubes de fútbol de primer nivel es fundamental y esencial.

—¿Cómo se organiza la seguridad de una instalación donde se celebran grandes eventos deportivos y donde este factor es una de sus prioridades?

—A grandes rasgos, la seguridad integral y globalmente entendida para grandes eventos deportivos de primer nivel, puede estructurarse mediante el establecimiento de dos vertientes de un mismo dispositivo de seguridad:

Una primera fase de organización del evento concebido en sentido general sería el estudio y aplicación de un dispositivo de seguridad estable en el tiempo, por cuanto existen realidades o riesgos inherentes a todos los dispositivos. Las condiciones de acceso, permanencia y evacuación del estadio y la protección de las mismas, la disposición de los servicios de Seguridad Privada en los accesos, gradas o zonas a proteger por su especial vulnerabilidad, dispositivo de emergencias sanitarias, sistema de acreditación para personal laboral o Vips, y todas aquellas medidas preventivas y reactivas contenidas en el plan de autoprotección, suponen la base sobre la que se asienta la generalidad de la planificación de la seguridad de un evento deportivo de masas. Podría definirse como el común denominador y base de

todos los dispositivos de seguridad que cubrirán y protegerán los diferentes eventos que se realicen en el estadio de fútbol.

Una segunda fase de la organización de un evento concreto conlleva una labor de adecuación o implementación de nuevas o diferentes medidas de seguridad para adaptarlas a las necesidades o riesgos del particular y concreto encuentro de fútbol a disputar. Es en este aspecto donde la coordinación con las Fuerzas y Cuerpos de Seguridad y especialmente con el coordinador de Seguridad adquiere especial importancia. El coordinador de Seguridad es un miembro cualificado de las Fuerzas y Cuerpos de Seguridad al que la Ley 19/2007 de 11 de julio contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte atribuya importantísimas competencias en el marco de la seguridad del evento. Fechas previas al acontecimiento deportivo se produce una reunión entre el coordinador de Seguridad, el director de Seguridad y el resto de Servicios de Emergencia que participarán en el dispositivo y de la que se levanta un acta. En esta reunión previa se ponen de manifiesto los riesgos específicos que han sido detectados y que pueden afectar al encuentro de fútbol. Consecuentemente, y para prevenir o reaccionar ante los riesgos anteriormente descritos, se establecen en el dispositivo de seguridad para el

«Todas las instalaciones del Sevilla Fútbol Club disponen de medidas de seguridad que garantizan el buen funcionamiento de las mismas y las protegen de posibles accesos o intrusiones no deseados»

evento, medidas de seguridad especiales, tanto desde la Seguridad Pública como desde la Seguridad Privada. Si los riesgos para la seguridad del evento deportivo son especialmente significativos, el encuentro podría obtener la declaración por la Comisión Estatal contra la Violencia, el Racismo, la Xenofobia o la Intolerancia como de Alto Riesgo, con lo que el dispositivo de seguridad al evento habrá de reforzarse necesariamente en número y servicios. Afortunadamente, la seguridad del evento es hoy en día el principal aspecto a tener en cuenta en la celebración del mismo, quedando el resto de aspectos, incluso los deportivos, supeditados a la celebración del evento en un entorno seguro y que tenga las garantías suficientes en materia de seguridad para participantes y espectadores. También para los propios integrantes del dispositivo de seguridad.

—¿Cree que se debería potenciar una cultura de prevención y fomentar la tolerancia cero ante la violencia en el deporte?

—Los valores intrínsecos del deporte son en sí mismos incompatibles con la violencia, cualquiera que sea ésta la forma en que se produce. Es objetivo de todas las administraciones públicas, y debe serlo de las privadas, contribuir a erradicar cualquier manifestación de la violencia en el deporte, fundamentalmente cuando ésta pudiera tener connotaciones racistas, xenófobas o intolerantes.

La prevención de la violencia en el deporte ha de realizarse desde las edades más tempranas infantiles y juveniles. El deporte tiene un valor social como elemento educativo que desde el inicio de la progresión personal ha de estar presente con sus valores en la vida del

menor, siendo referente ético y estando radicalmente desvinculado de toda connotación violenta.

El Deporte ha de entenderse como un factor de integración y no de exclusión, fomentando el respeto de los derechos fundamentales y libertades públicas consagradas en la Constitución Española.

Por consiguiente, siendo importantes las políticas reactivas ante conductas violentas en el Deporte, lo son aún más las políticas educativas y de concienciación, que supongan una base de sensibilidad reactiva ante la violencia en el entorno deportivo y que signifiquen su rechazo conceptual desde las edades más tempranas.

—¿Cuáles son los pilares sobre los que debería asentarse una adecuada seguridad en una instalación deportiva de las características del Estadio Sánchez-Pizjuán?

—Se pueden considerar tres los ámbitos de responsabilidad y gestión de una razonable política de seguridad y control de una instalación deportiva destinada a un espectáculo de masas.

El primero de ellos es la propia seguridad, la integridad de la instalación o safety, que implica la construcción o adecuación de las instalaciones existentes a los requisitos legales y congruentes de seguridad. Hablamos aquí de la adecuación a la norma de la propia instalación en todo lo relativo a medidas de seguridad, cuyo último objetivo es que el acceso, la permanencia y la salida de la instalación se realice en condiciones de seguridad, aun en el caso de que pudiera haber producido algún incidente intencional o accidental. Puertas de acceso suficientes, CCTV, sistemas antiavalancha, sistemas anti incendios o de autoextinción, dobles acometidas eléctricas o puertas de evacuación, entre otras muchas, suponen el mínimo desde el que se han de generar las condiciones suficientes de seguridad para la celebración de un evento de las características de un encuentro de fútbol de alta competición. Todas estas medidas de seguridad y otras muchas han de estar contenidas en un plan de autoprotección de cuya ejecución es responsable el director de Seguridad del club de fútbol, por lo que el conocimiento del plan es de vital importancia.

Un segundo ámbito sería la tradicional concepción de la seguridad realizada por profesionales de la Seguridad Privada y destinada a la protección de la propia instalación deportiva, fundamentalmente de accesos no deseados o de todas las operaciones de seguridad relativas a los accesos, permanencia en el estadio y evacuación del mismo durante el dispositivo de seguridad. Se trata del dispositivo de seguridad privada conformado por los vigilantes de seguridad, perros especializados en la detección de artefactos explosivos o pirotécnicos y sus guías, jefes de seguridad y directores que participan del mismo. En este segundo ámbito de actuación es fundamental la estructura del dispositivo de seguridad que ha de ser jerarquizado y conocido.

En este segundo estadio de la seguridad de un estadio de fútbol o gran instalación para eventos, se incluyen a los Servicios de Emergencia Sanitarios que han de ser estructurados y controlados en cuanto a ubicación por el responsable de seguridad de la instalación. Estos servicios, como parte fundamentalmental del dispositivo de seguridad, han de contemplarse en el mismo y estar perfectamente comunicados y coordinados desde las unidades de control organizativo.

Un tercer eje de la seguridad de una instalación deportiva de primer nivel es la relativa a la ciberseguridad. Es trascendental proteger los sistemas de información que se contienen en los diferentes servicios informáticos. El bloqueo, siquiera por unos minutos, del funcionamiento de los equipos informáticos y, por ende, de la información que en ellos se contienen, conlleva la paralización de la actividad de la entidad deportiva. Cuando además se produce fuga de información mediante la intrusión en los sistemas, se produce una situación del vulnerabilidad cuya resolución en sentido positivo se hace muy difícil. Es por ello por lo que la ciberseguridad, en íntima relación y cooperación con los departamentos de IT, ha de ser uno de los objetivos y ejes de toda política de seguridad del departamento de Seguridad de toda institución, incluidos los clubes de fútbol. ✱

JULIÁN SUESCUM SEGURA
DIRECTOR DE SEGURIDAD. VALENCIA C.F.

«Para el Valencia C.F. es primordial reforzar y fomentar la tolerancia cero en el deporte»

Texto: Laura Sala.
Fotos: Valencia C.F.

«Los grandes retos a los que se enfrenta el Valencia C.F. sería la prevención de movimientos ultras dentro del mundo del fútbol». Son palabras del director de Seguridad del Club valenciano, Jesús Suescum, quién, a lo largo de esta entrevista, explica las prestaciones y las diferentes actuaciones en materia de seguridad que se llevan a cabo en el Estadio Mestalla durante la celebración de grandes eventos.

—Para comenzar, ¿podría explicarnos características del Mestalla (aforo, número de trabajadores, otros eventos que se realizan...)?

—Mestalla es un estadio con una capacidad actualmente para 50.000 espectadores. Durante un día de partido funcionamos con alrededor de 550 personas con dependencia directa del departamento de Seguridad (Seguridad Privada, Auxiliares de Seguridad, Voluntarios, Dispositivo Sanitario de Cruz Roja y empleados de Club).
En Mestalla se puede realizar cualquier tipo de evento, desde conciertos hasta reuniones de trabajo de diversa magnitud. En los últimos años hemos albergado conciertos, Monster Jam, carreras populares, encuentros de empresarios, reuniones de empresas, jornadas de formación de diversa índole, actos de graduación universitarios, etc.

—¿Cuál es la estructura e infraestructura del área de Seguridad del Valencia C.F.?
El Valencia C.F. cuenta con un departamento de Seguridad compuesto por 7 personas, todas ellas empleadas del Club. Cada miembro del departamento se especializa en una función específica dentro del dispositivo el día de partido.
A su vez, cada una de las diversas empresas que participan en los eventos en Mestalla tienen coordinadores y personal de supervisión para apoyar las funciones de los diversos colectivos.

—De manera general, ¿podría explicarnos los medios y medidas de seguridad con que cuenta la instalación?
—Mestalla cuenta con todos los medios y medidas de seguridad que requieren las diversas normativas de

aplicación. Tiene una Unidad de Control Operativo (UCO), que cuenta con un sistema de CCTV que controla al cien por cien el interior y exterior del estadio con cerca de 200 cámaras y con un sistema de grabación digital, comunicaciones, sistema contra incendios, y megafonía interior y exterior, un sistema de control de accesos mediante tornos, y grupos electrógenos que garantizan el correcto funcionamiento de la instalación en el supuesto de fallo eléctrico. Así mismo, el Club cuenta con sistema de detección de incendios y alarmas en las dependencias más críticas del estadio. También contamos con sistemas de detección de metales portátiles y desfibriladores semiautomáticos ubicados estratégicamente en el interior del estadio.

En cuanto a las medidas de seguridad cabría resaltar el registro de todas las bolsas, mochilas, bolsos y demás objetos, así como registros selectivos a los espectadores. Tanto en la zona de afición rival como en la zona de nuestra Grada de Animación los registros se realizan a todas las personas que acceden.

Se trabaja también en la prevención y la información en el entorno, tanto de los empleados del Club y de las diversas empresas que participan en los dispositivos, como con información a los espectadores que pudieran asistir a los eventos a través de redes sociales, e incluso con envíos de correo electrónico personalizados con información relativa a los objetos que pueden o no acceder al estadio y a los comportamientos que se deben tener en un evento deportivo.

—¿Cómo se organiza la seguridad de una instalación donde se celebran grandes eventos deportivos y donde este factor es una de sus prioridades?

—Para nosotros, lo primordial es la prevención, todo lo que se trabaja antes del evento. Obviamente, en cualquier evento de estas dimensiones la prioridad debe ser la seguridad del espectador y de todas las personas que componen los diversos servicios que se realizan. Para ello, desde el departamento de Seguridad de la entidad, en estrecha colaboración con los Cuerpos de Seguridad del Estado, se valoran todos los riesgos y escenarios posibles que se pueden dar durante el evento. A raíz de este trabajo pre-evento podemos adoptar medidas correctoras o preventivas con el fin de reducir al máximo los riesgos que hemos podido detectar. No obstante, en este tipo de eventos siempre hay un porcentaje de factor sorpresa, para este tipo de coyunturas el personal que trabaja en un evento está instruido para poder

Equipo del departamento de seguridad del Valencia C.F. en el Estadio Mestalla.

reaccionar y activar los mecanismos necesarios dentro del dispositivo para poder hacer frente a cualquier tipo de situaciones, previstas o no.

—¿Cree que se debería potenciar una cultura de prevención y fomentar la tolerancia cero ante la violencia en el deporte?

Obviamente. Para nosotros es primordial reforzar y fomentar la tolerancia cero en el deporte. De hecho, el Club ha tomado medidas muy severas en nuestra Grada de Animación con el fin de erradicar la violencia y los comportamientos no deseables en nuestro Estadio. También, desde hace varias temporadas, el Club trabaja junto al CNP en talleres orientados tanto a jugadores como a padres en nuestra Academia, con el fin de trasmitir valores deportivos a nuestro colectivo y evitar comportamientos antideportivos.

—¿Cuáles son los grandes retos a los que se enfrentan hoy en día los responsables de seguridad de los grandes estadios deportivos como el Mestalla?

—Bajo nuestro punto de vista, los grandes retos a los que nos enfrentamos serían la prevención de movimientos ultras dentro del mundo del fútbol, así como alcanzar un mayor control en la venta de entradas por Internet. Igualmente, es importante seguir trabajando en la formación e información para poder prevenir el mayor número de situaciones que se puedan producir.

—¿Cuáles son los pilares sobre los que debería asentarse una adecuada seguridad en una instalación deportiva de las características del Mestalla?

—Es crucial una buena relación con los Cuerpos de Seguridad del Estado con el fin de compartir adecuadamente la información de manera bidireccional. También es vital una buena planificación en el desarrollo de los eventos, tener una infraestructura acorde a la instalación, una buena preparación de los recursos humanos que participen, así como suministrarles a ellos unos medios físicos acordes a su función. Todo ello teniendo un dispositivo de seguridad claro y conocido por las partes y muy definidos los protocolos de actuación ante el máximo posible de eventualidades. ✱

NUEVO CATÁLOGO

MARZO 2020

TBK VISION

CCTV

Enjoy the experience!

www.tbkvision.com info@tbkvision.com Tel.: +34 96 159 46 46

RAÚL VALERA TENA*
DIRECTOR DE SEGURIDAD. EXPERTO EN ELABORACIÓN/IMPLANTACIÓN DE PLANES DE SEGURIDAD, EMERGENCIAS Y AUTOPROTECCIÓN EN GRANDES EVENTOS.

«La prevención, proactividad y coordinación son clave para garantizar la seguridad en un evento»

Texto: Gemma G. Juanes.
Fotos: G.G.J./ R.V.T.

—Desde su experiencia durante años como director de la Dirección de Seguridad y Emergencias y del departamento de Seguridad de Madrid Destino, ¿cómo se organiza la celebración de un gran evento de ocio o cultural en las instalaciones municipales?

—En primer lugar, quiero dar las gracias al equipo del CNP de Red Azul, destacando a Ana, Ramón, y al gran maestro Julio Camino, por su inestimable apoyo, así como a los diferentes Servicios Públicos y Privados de Seguridad y Emergencias, y a otros posibles implicados en la coordinación de los eventos que he gestionado; y en especial al equipo de Cuadernos de Seguridad por difundir esta entrevista, y apoyarme en los numerosos congresos y jornadas en los que venimos coincidiendo.
En relación a la pregunta, ante la falta de regulación y homogeneización normativa en materia de eventos, espectáculos públicos y actividades recreativas (por ejemplo, no hay una clasificación de lo que se considera un gran evento, excepto en el ámbito internacional, pero sin marcar cifras), se redactaron diferentes instrucciones internas a seguir de obligado cumplimiento en cada evento, con el fin de estar coordinados los diferentes implicados e interlocutores. Siendo obligatorias reuniones previas y posteriores de coordinación y evaluación de cada evento en base a una memoria descriptiva exigida al organizador para evaluar la viabilidad, dando traslado de las diferentes normas internas y normativa de aplicación de obligado cumplimiento; además, una vez mantenidas las reuniones internas, se

trasladaba, previamente al evento, toda la información de interés a Delegación de Gobierno, Red Azul (programa bidireccional de comunicación con CNP), Direcciones Generales y Oficina de Actos en Vía Pública, dependientes de la Coordinación General de Seguridad, Salud y Emergencias, o a otros posibles entes públicos o privados que pudieran verse implicados o afectados por alguna de las fases del evento, manteniendo reuniones de coordinación en su caso.

Igualmente, impartíamos a todo el personal implicado en el desarrollo y celebración de los diferentes eventos, briefings previos al inicio de cada evento, en el que se convocaba a organizadores, servicios sanitarios, personal de seguridad y auxiliar de servicios, mantenimiento y limpieza, a fin de explicar los códigos de comunicación, el material disponible, puntos de reunión exterior, medidas a tomar en caso de emergencia y evacuación (confinamiento, conato, emergencia parcial o total), con entrega de trípticos y control de firmas con carácter previo al inicio del evento. Todo ello, independientemente de la implantación de cada Plan de Autoprotección o Medidas de Emergencia específicas, formación teórica y práctica, real y efectiva, simulacros y evaluaciones.

—Madrid también es escenario de otro tipo de eventos multitudinarios como es la Cabalgata de Reyes, Fiestas Patronales, ... ¿cómo varía la metodología de trabajo en cuanto a seguridad y emergencias? ¿Con qué efectivos contaba?

—Además teníamos el encargo por parte del Ayuntamiento de Madrid de la gestión de las grandes fiestas y campañas municipales multitudinarias, como Cabalgata de Reyes, fiestas patronales de San Isidro, Veranos de la Villa, Campaña Navideña o Año Nuevo Chino, entre otras, y de los espectáculos con pirotecnia que suelen poner el broche final.

Dependiendo de la memoria (y tipología del evento) indicada anteriormente, del análisis de la información, y de las reuniones de coordinación mantenidas con los diferentes implicados internos y externos, llevábamos a cabo la planificación, en materia de actividades de seguridad privada, analizando posibles riesgos y normativa de aplicación, referidos a gestión documental, autorizaciones, y protección frente a todo tipo de riesgos.

Los efectivos de los diferentes dispositivos se establecían en base al marco competencial de cada implicado, si bien, como buena práctica aplicábamos la normativa más restrictiva a nivel nacional en materia de seguridad

«Cada evento está vivo hasta la dispersión del público, y es diferente independientemente de que el número de espectadores y formato sea incluso el mismo»

privada, e implementábamos dispositivos sanitarios también en las fases de montaje y desmontaje de estructuras eventuales, temporales o efímeras.

—¿Qué medidas o mejoras en cuanto a seguridad en eventos se han implantado en Madrid durante su trayectoria profesional en Madrid Destino y han llevado a la capital a ser pionera en este aspecto?

—Madrid Destino es una empresa pionera a nivel nacional en medidas preventivas y buenas prácticas en la seguridad de grandes eventos. En lo que respecta a nuevas tecnologías, puedo destacar:

Instrucciones internas en diferentes ámbitos, estaciones meteorológicas en eventos al aire libre en los escenarios y espectáculos piromusicales y pirotécnicos, recomendaciones en redes sociales y webs, vídeos y recomendaciones interpretados en lengua de signos y subtitulados, mensajes de megafonía, configurados pregrabados de alarma, evacuación parcial y total, confinamiento y fin de actividad. Carpas o módulos para el personal prestatario del servicio de vigilancia y auxiliar, de protección climatológica y calefactores complementados con iluminación adicional en espacios exteriores, señalización complementada con lonetas y banderolas en altura de señalización y ubicación, sistema SARF de intervención, comunicación bidireccional y control remoto de los equipos de sonido de las diferentes carrozas en Cabalgata, escenarios, casetas e incluso atracciones de feria, junto con la instalación de botones tipo seta manual de comunicación remota con los servicios privados y públicos de emergencias sanitarias y seguridad pública, entre otros. Sistema autónomo portátil de megafonía crítica, drones para supervisión de montajes en altura en espacios cerrados, vallados de interposición, etc.

Como novedad, nos encontrábamos inmersos en un nuevo proyecto de innovación tecnológica de una empresa madrileña (DN1N1), de control automatizado de afluencia de personas no intrusivo, es decir, sin necesidad de portar entradas físicas o uso de lectores de códigos, dispositivos que permitieron en las pruebas efectuadas y en tiempo real disponer de cifras de asistentes por puntos de acceso.

Instalación y puesta en marcha de sistema anti intrusión con tecnología de video vigilancia IP de última generación, complementado con un sistema de control de accesos inteligente.

Llevamos a cabo la primera Cabalgata con carrozas cardioprotegidas dinámica de la historia, con instalación de desfibriladores con soporte gráfico en las carrozas, en colaboración con Proyecto Salvavidas, y botiquines de control de hemorragias severas en los escenarios de eventos al aire libre, espectáculos pirotécnicos, y en todos los edificios municipales indicados.

Y destacar que, gracias a las aportaciones de mis compañeras de accesibilidad e innovación, los eventos son cada vez más accesibles e inclusivos con mochilas vibratorias para personas sordas y bucles magnéticos, entre otras innovaciones para personas con discapacidad.

—Siempre ha destacado la falta de un marco normativo en el sector de los eventos, ¿cómo se suple esta carencia? ¿Qué aspectos cree que se deberían recoger en esa normativa?

—Efectivamente, es algo en común que acusamos los implicados en los eventos, (#normativaunificadaparaeventosya). Voy a tratar de explicarlo, -fuera del ámbito deportivo y profesional de máxima categoría el cual se encuentra bastante regulado y actualizado- cronológica y normativamente hablando en base a la jerarquía de las fuentes, nos podemos remontar en primer término a la Orden de 1935 por la que se aprueba el Reglamento de Espectáculos Públicos que, pasando al texto constitucional actual, ya en la Constitución Española de 1978 se expone en el título I, de los derechos y deberes fundamentales, el derecho al ocio, a la vida y a la integridad física, y en el título VIII la asunción y distribución de competencias a nivel estatal y por parte de las Comunidades Autónomas. Si nos remontamos a 1982 encontramos el Real Decreto 2816/1982, por el que se aprueba el Reglamento General de Policía de Espectáculos Públicos y Actividades Recreativas, aún en vigor y de aplicación en algunas CCAA, que no han legislado en esta materia, como es el caso, si mal no recuerdo, de Ceuta y Melilla, por ejemplo.

Por otro lado, varias comunidades han aprobado diferentes leyes en materia de espectáculos públicos y actividades recreativas, e incluso las han desarrollado reglamentariamente. Algunas de ellas disponen de normativa muy específica que hace referencia por ejemplo a dispositivos sanitarios o número de vigilantes y controladores de acceso por aforos, y otras han desarrollado leyes que a día de hoy y muchos años después siguen a expensas de desarrollo reglamentario, como sucede en nuestro caso en Madrid donde la conocida como LEPAR (Ley de Espectáculos Públicos y Actividades Recreativas) es de 1997. Si bien es cierto que en los últimos años se han publicado en nuestra comunidad actualizaciones normativas de criterios de mínimos mediante decretos, respecto a la obligatoriedad de instalación y formación sobre desfibriladores o registro de datos de planes de autoprotección, a modo de ejemplo, aspectos y novedades a tener en cuenta como complemento a la nueva Ley del Sistema Nacional de Protección Civil de 2015 o de la Norma Básica de Autoprotección, a pesar de ello, queda mucho por regular. Los denominados «técnicos competentes» pendientes de definir y clasificar o profesionalizar, así como tipos de vallados, cálculos de aforo restrictivos y progresivos en porcentajes, según campo visual, cuadros de dispositivos sanitarios para eventos y obligación en usos de tipo 3, aclaraciones normativas, sobre la aplicación del decreto del 97 de obras de construcción (Ana Alonso de Prevent Event está en constante lucha para mejorar en la prevención), zonas de protección acústica para menores, obligación de cctv y centros de coordinación en eventos en recintos al aire libre, puntos de violencia sexual en el ocio (aquí destaco a Anna Almécija por

Riesgos y amenazas

—Con una visión profesional, ¿han variado los riesgos y amenazas en los grandes eventos en los últimos años?

—Rotundamente sí, tanto por el uso de nuevas tecnologías como por amenazas externas activas intencionadas que todos conocemos, y vienen sucediéndose por desgracia en diferentes ciudades europeas, e incluso españolas.

#SEJUEGACOMOSEENTRENA, como diríamos Pedro Merodio y yo al finalizar cualquier jornada: formación, formación y formación, tanto teórica como práctica; así como señalamos otros profesionales del sector como José Cruz, Javier Revuelta o Angel Dieste y yo mismo, la seguridad no es un gasto, es una inversión.

su gran aportación al sector), y un largo etc. Gracias a diferentes congresos y jornadas, vamos compartiendo buenas prácticas, mejorando y aprendiendo unos de otros, como en los Congresos de Seguridad en Eventos organizados, por ejemplo, gracias a Olga Sánchez y Carlos Moreno, Pedro Merodio y Moisés Álvarez, Anna Almécija o Eduardo Martín de ASPEC, entre otros.

—¿Cree que los ciudadanos valoran las medidas de seguridad y prevención que se implantan en los eventos multitudinarios, o se trata de un hecho que pasa desapercibido?

—La concienciación de la ciudadanía, asistentes a eventos, e incluso de algunos organizadores, no ha sido fácil, pero por desgracia ante diferentes tragedias o accidentes sucedidos, a la constancia e implicación que venimos implantando de buenas prácticas los profesionales del sector y servicios públicos, y al constante traslado de difusiones y recomendaciones previas en redes sociales, webs, pantallas, mensajes de megafonía, canales de venta, etc, a seguir antes, durante, después y en caso de emergencia en los eventos, creo que todos valoramos muy positivamente estas medidas preventivas y proactivas.

—¿Cuáles son las claves para mantener o garantizar la seguridad en un evento multitudinario?

—Cada evento está vivo hasta la dispersión del público, y es diferente independientemente de que el número de espectadores y formato sea incluso el mismo, y por ello hay que tratar cada evento específicamente, aunque tengamos antecedentes del mismo. Las claves son: reuniones previas, análisis documental, perfil de asistentes,

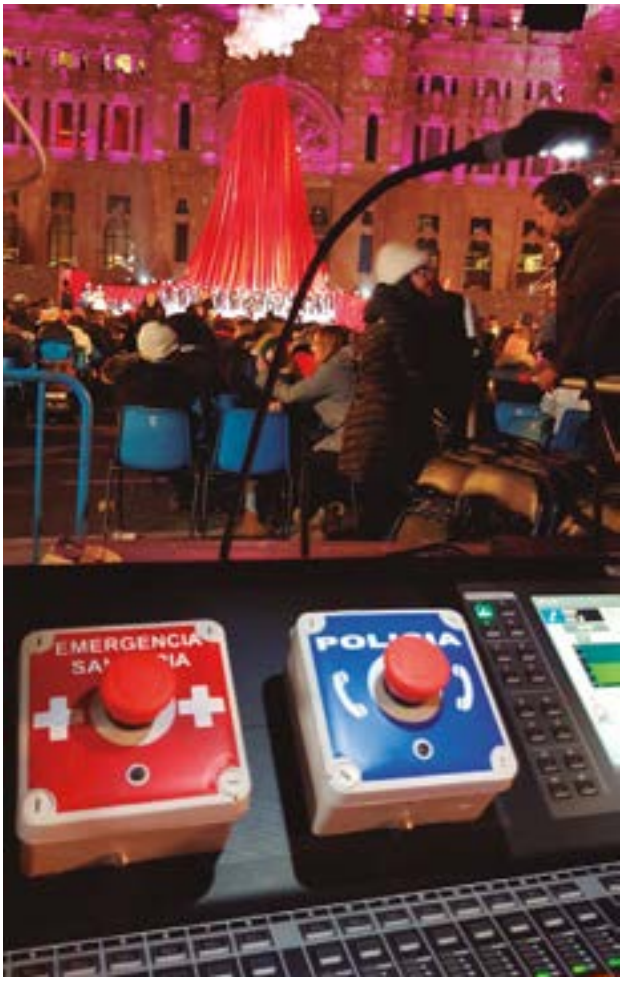
riesgos previsibles, reuniones de coordinación, briefings previos para ponerse cara todos los implicados, implantación de los diferentes planes elaborados, formación teórica y práctica, real y efectiva, simulacros, evaluaciones posteriores, códigos claros de comunicación..., todo ello partiendo de la memoria y pasos que he indicado anteriormente, destacando la prevención, proactividad, integración, coordinación y evaluación en todas sus fases.

—Y para finalizar ¿qué recomendaciones darías a todos aquellos ciudadanos que habitualmente acuden a eventos multitudinarios?

—Las recomendaciones serían:

Antes del evento: Utilice el transporte público y acuda con antelación suficiente; asista bien alimentado e hidratado. Lleve bebida y alimentos para los niños; utilice ropa cómoda y adecuada y protectores solares o prendas de cabeza, para protegerse del calor, la lluvia o el frío; lleve siempre calzado apropiado y cerrado, ya que el mayor número de heridas en las concentraciones se produce en los pies; debe llevar documento de identidad. En caso de personas que puedan necesitar apoyo, prepare una ficha con los datos personales y al menos un teléfono de contacto, preferentemente de móvil; en caso de seguir un tratamiento médico o padecer algún tipo de enfermedad, acuérdese de llevar la medicación y el informe, etc.

Durante el evento: Esté atento a las indicaciones del personal de seguridad y de la organización; infórmese de las salidas de emergencia o vías de evacuación existentes; en caso de nieve o lluvia utilice capuchas y chubasqueros antes que paraguas; no descuide sus objetos personales y cuide de sus pertenencias; asegúrese



de que las personas que puedan necesitar apoyo llevan los datos para poder contactar con su familia en caso de extravío; mantenga siempre el control y contacto visual sobre los menores; en caso de emergencia contacte con los miembros de la organización y de los servicios de emergencias o comuniquen con el 112, etc.

En caso de emergencia: Informe de las anomalías y atienda las recomendaciones del personal de organización y de los servicios de emergencia; colabore cumpliendo las instrucciones y recomendaciones sin interferir en las labores de socorro; si debe evacuar, salga en calma y con orden al punto de encuentro establecido. Evite retroceder; no empuje, no corra, no grite. Todo ello provoca alarma y reacciones peligrosas para todos. ✱

*Raúl Varela ha sido director de Seguridad y Emergencias de Madrid Destino (Ayuntamiento de Madrid) —julio 2015/febrero 2020—.

SEGURIDAD PRIVADA & GRANDES EVENTOS

Una buena planificación y organización con capacidad de adaptación y de respuesta, gestionada por un equipo humano profesional, clave del éxito de la seguridad en los grandes eventos.

EDUARDO TÉLLEZ RUIZ
DIRECTOR DE OPERACIONES. PYCSECA

La organización de grandes eventos está supeditada a las características peculiares de cada evento, lo cual supone un esfuerzo extraordinario para las empresas en la gestión y contratación de recursos, al igual que disponer de una capacidad de adaptación a los requerimientos y peculiaridades operativas, lo cual hace único y excepcional cada evento, aunque bien es cierto que hay unas pautas comunes que son coincidentes en todos.

Como ejemplo vamos a ver un evento que reúne todas esas características singulares y diferenciadoras, como es el caso de la DANONE Nations Cup, la cual tiene una repercusión internacional, una política interna muy específica por parte de la organización, los participantes en el torneo son jugadores menores (entre 10 y 12 años), de diferentes nacionalidades y culturas, etc.

LA PLANIFICACIÓN

Sin duda, una buena planificación es la clave del éxito, de ella dependerá que lo desarrollado sobre el papel, se pueda poner en práctica sobre el terreno, por lo que es indispensable una coordinación entre los diferentes departamentos que participan (logística, alojamiento, catering, dirección de Seguridad, etc.).

En todos los eventos siempre existe una gran probabilidad de que surjan cambios, debido a imprevistos o requerimientos sobrevenidos, por lo tanto, es clave en todo esto la capacidad de respuesta y adaptación de la empresa de seguridad / servicios, para dar cobertura a esas nuevas necesidades, cumpliendo siempre con los criterios marcados por la Dirección de Seguridad del evento.

LA COORDINACIÓN

Es fundamental, que exista una coordinación entre la Dirección de Seguridad del evento, la empresa de seguridad y las diferentes instituciones competentes, (Seguridad Ciudadana, Agentes Locales, Emergencias, etc.), lo que da paso a motivar las reuniones con la Junta Local de Seguridad. Desde aquí se acuerdan los recursos o dispositivos públicos que considere necesarios la administracion, para garantizar el correcto desarrollo a nivel de seguridad y emergencias.

Estas acciones dan lugar a la creación del CECOR, (Centro de Coordinación) desde donde se materializa la coordinación de los recursos disponibles, se establece la Sala de Crisis y se aplican, en caso necesario, los planes de contingencia.

LOS COORDINADORES

En un evento de estas características, donde durante 10 días es necesario dar cobertura a más de 7.000 horas entre Vigilantes de Seguridad (armados, sin arma, unidades caninas de explosivos y defensa), Auxiliares de Servicios, etc., realizando servicios en diferentes ubicaciones y espacios, requiere una serie de una gran cantidad de medios humanos y materiales, los cuales deben ser gestionados por parte de los coordinadores, que se encargarán de formar y gestionar al equipo humano que tiene a su cargo, gestión de equipos de comunicaciones, medios materiales, etc., haciendo cumplir los procedimientos generales del evento y los específicos de cada puesto.

SELECCIÓN Y CONTRATACIÓN

Debido al gran volumen de contratación necesario y añadiendo la peculiaridad de una exigencia indispensable para todos los operativos, al tener que trabajar con menores, siendo indispensable la exigencia del Certificado de Delitos de Naturaleza Sexual, emitido por el Ministerio de Justicia, se consideró necesario la creación de una oficina móvil de contratación y selección, con dependencia directa de servicios centrales, que ayudó a gestionar de manera rápida y ordenada los procedimientos necesarios para la selección, contratación y reparto de uniformidad correspondiente.

Esta exigencia del Certificado de Delitos Sexuales, dificulta enormemente la planificación operativa en dos sentidos básicamente:

• No existe una disponibilidad inmediata del personal.

-El personal, aunque cumpla con el perfil necesario, no se puede contratar hasta obtener el Certificado de Delitos Sexuales.

• La planificación de recursos extraordinarios , se supedita a una exigencia del evento.

-En caso de ampliación de servicios, hace necesario tener a personal de reserva en cartera con dicho certificado.

En este pequeño resumen sobre la organización desde el punto de vista de seguridad privada de grandes eventos, queremos destacar, una buena planificación y una organización con capacidad de adaptación y de respuesta, gestionada por un equipo humano profesional, como clave del éxito. ✱

ENTRENA COMO TRABAJAS, TRABAJA COMO ENTRENAS

La celebración periódica de simulacros se convierte en una herramienta imprescindible en la prevención y gestión de incidentes armados y especialmente donde el flujo de usuarios es constante

DAVID CREVILLÉN. CEO. GRUPODC SOLUTIONS
BEATRIZ GUTIÉRREZ . DEPARTAMENTO DE INVESTIGACIÓN. GRUPODC SOLUTIONS.

Cuando hablamos de centros comerciales el imaginario colectivo reconoce espacios amplios e interconectados por escaleras mecánicas, con diversas plantas, zonas de restauración, comercios, en algunos casos incluso varias salas de cine y, especialmente, una multitud tanto de usuarios de todos estos servicios como de trabajadores deambulando por todo el espacio. Las propias actividades que se realizan en el centro condicionan que tanto las medidas de seguridad como la percepción de amenaza de los usuarios sean escasas. Esta doble característica se ajusta al concepto de «soft targets» u objetivos blandos, y representa una serie de problemas específicos de seguridad, que van de la protección de activos y bienes a la protección de activos humanos, que en este caso son tanto los propios trabajadores como los usuarios, un volumen de población variable en el tiempo, que pueden conocer o no las instalaciones, con diversas formaciones y características, y que por tanto, por su heterogeneidad, dificultan su protección, especialmente frente a la nueva casuística de incidentes armados que se ha producido en Europa en la última década en forma de ataques terroristas.

Este tipo de incidentes van a reunir, a su vez, una serie de características, que podemos resumir en dos elementos: la maximización del número de víctimas y el dinamismo de las acciones. Ello conlleva el incremento del número de bajas por unidad de tiempo y en consecuencia provoca que los tiempos de respuesta por parte de los primeros intervinientes policiales y sanitarios deban ser lo más breves posibles para poder limitar el número de muertos y heridos. Por ello, el tiempo es una de las variables más importantes en términos de respuesta, y casos –aunque no todos de naturaleza terrorista- como Columbine y sucesivos incidentes de características similares han mostrado que los mecanismos clásicos de perimetrar, establecer puestos de mando, contener la amenaza y esperar a los equipos de intervención, si bien son válidos en otro tipo de incidentes, no son adecuados por el incremento en el tiempo de respuesta que suponen. La mejor respuesta, por tanto, es aquella que proporcione un modelo

preestablecido basado en la coordinación, de modo que cada actor conozca las acciones básicas a realizar en este tipo de incidentes. Siguiendo esta lógica, la celebración periódica de simulacros y ejercicios se convierte en una herramienta imprescindible en la prevención y gestión de incidentes armados en objetivos blandos y especialmente en aquellos donde, por sus especiales características, el flujo de usuarios es constante, reduciendo las posibilidades de proporcionarles formación, y aumentando la necesidad de que los intervinientes encargados de la seguridad conozcan los protocolos de respuesta y los apliquen de forma no solo eficiente, sino también rápida, a través de la mejora del conocimiento entre los intervinientes y, por ello, de su coordinación inter-agencias.

Pese a que el ámbito de las simulaciones es extensísimo, metodológicamente se pueden establecer una serie de apuntes útiles para su realización. En primer lugar, se debe tener en cuenta el alcance, puesto que la logística no es la misma para un ejercicio de simulación en sala o un ejercicio table-top, que para un ejercicio multiagencia, donde se van a emplear instalaciones, vía pública y

«Dependiendo de las restricciones de escenario físico y tiempo disponible, lo deseable es realizar varios ensayos previos al simulacro»

un elevado volumen de participantes que cubrirán todo el espectro de intervinientes, tanto inmediatos como policiales y sanitarios. Ello puede conllevar un control añadido de la información en un vecindario determinado para que no se produzcan sobresaltos, modificación en los horarios del centro comercial u organización donde se celebra, cortes de tráfico, etcétera, que deben ser convenientemente coordinados, en su caso, a nivel municipal.

Definido el alcance, uno de los objetivos que no se deben perder de vista es el entrenamiento de los intervinientes inmediatos -miembros de la organización, especialmente seguridad privada, pero también personal administrativo, comercial y, de gran importancia, mantenimiento,

David-Klein-Unsplash

por su especial conocimiento de las instalaciones-, y de los primeros intervinientes que van a proporcionar la primera respuesta. Pese a que es fundamental también que todos ellos conozcan los protocolos de respuesta de los equipos de intervención, deben ser conscientes de que siempre existe un intervalo de repuesta, que media entre el inicio del incidente -en este caso, simulado- y la llegada de los equipos de respuesta táctica, y que en un incidente activo las víctimas se van a seguir produciendo en estos momentos, por lo que las acciones llevadas a cabo en este lapso son fundamentales.

Algunos aspectos genéricos que se deben adaptar a cada caso concreto son los siguientes:

1.- Formar un equipo de diseño del simulacro. Puesto que la idea clave de la celebración de ejercicios simulados es mejorar los canales de coordinación entre los distintos intervinientes, para así mejorar los tiempos de respuesta y la eficacia de la misma, el diseño del ejercicio debe ser también conjunto entre todos los implicados en el mismo, tanto el personal de la propia organización donde se celebra, como intervinientes policiales y de emergencias, variables según las jurisdicciones. Una figura que resultará también de gran utilidad, durante el desarrollo del ejercicio, es el coordinador de role play o controladores, cuya función principal es dinamizar el desarrollo del mismo, corregir posibles disfunciones, vigilar que los escenarios discurren de forma

«La idea clave de la celebración de simulacros es mejorar los canales de coordinación entre los intervinientes, para así mejorar los tiempos de respuesta y eficacia de la misma»

realista, etcétera, para lo que tiene que dominar de antemano tanto instalaciones como sectores de participantes, como el propio diseño del escenario.

2.- Diseño del escenario. Para que éste sea realista, resulta de utilidad basarlo en casuística previa, sobre la experiencia de ataques realizados en objetivos similares a aquél con el que trabajamos. Ataques como el de Westgate Mall (Nairobi, Kenya, 2013), o mucho más reciente, Walmart de El Paso (Texas, 2019), pueden proveer de información y datos útiles, si bien la casuística de ataques en objetivos blandos es mucho mayor, y la cantidad de After Action Reports generados es ingente, y por tanto, disponible para su uso a la hora de elaborar un diseño adecuado. Se debe prestar especial atención al número de víctimas aproximado, patrones lesionales y distribución de víctimas, conforme a los parámetros del tipo de ataque seleccionado y de la configuración del propio escenario físico. Otro aspecto a tener en cuenta es el nivel de coordinación y entrenamiento previo entre los distintos intervinientes: si éste es bajo, el resultado del ejercicio va a arrojar bastantes fallos, lo cual, lejos de representar un problema, es una gran oportunidad para identificar fallos y poder buscar medidas correctivas. El diseño realista del escenario debe buscar precisamente eso.

3.- Aspectos relacionados con la ejecución. Dependiendo de las restricciones de escenario físico y tiempo disponible, lo deseable es realizar varios ensayos previos al simulacro. Si estamos trabajando un enfoque multi-agencia, una recomendación útil es que cada agencia practique de forma separada sus competencias, por ejemplo, seguridad privada practicará las nociones básicas TECC[1] , evacuaciones y confinamientos en caso de incidente armado activo, los intervinientes policiales practicarán aspectos tales como la formación de equipos de contacto y rescate, extracciones o formación y protección de un nido de heridos (CCP), y los intervinientes sanitarios practicarán triaje, extracción del CCP a zona segura, primera asistencia para los patrones lesionales específicos seleccionados de acuerdo con el escenario, y triaje para evacuación. Posteriormente, se procederá a la celebración del simulacro multiagencia, donde en este caso, efectivamente, todo el espectro de intervinientes realizará el simulacro de forma coordinada a lo largo de toda la cadena asistencial, desde el protocolo «corre-escóndete-lucha/llama» y la asistencia inicial a víctimas, a la neutralización de la amenaza, extracción y evacuación, con los pasos asistenciales intermedios requeridos. Una práctica recomendable es combinar estos dos estadios de práctica con la realización por parte de los intervinientes participantes de cuestionarios que puedan medir el conocimiento previo, entre ejercicios y post-ejercicio multiagencia, de modo que se pueda cuantificar el progreso en la familiarización con los protocolos de respuesta.

4.- La figura del evaluador. El evaluador es una figura externa a las organizaciones participantes, cuya función principal es nutrirse de los datos que se generan durante el ejercicio, apoyado en esta tarea por los controladores del ejercicio. Para ello, el evaluador debe de conocer previamente las instalaciones, actores participantes, protocolos de actuación de cada una de las entidades y, especialmente, tiempos esperados de respuesta. Todo ello se puede complementar con los mencionados cuestionarios post-ejercicio. La recolección de todos estos datos se revertirá, convenientemente codificada y sistematizada, en el Informe Post-Ejercicio, que se elaborará como elemento final del simulacro. Aunque el número de evaluadores puede ser variable, se recomienda que se limite al mínimo necesario para que sea funcional y que se nutran de la información proporcionada por los controladores, para reducir el número de actores que no participan directamente en el desarrollo del ejercicio.

En conclusión, la realización de simulacros no se trata de «quedar bien», sino todo lo contrario, se trata de quedar todo lo mal posible, porque esos fallos representan vulnerabilidades que, en un escenario real, no van a afectar a figurantes, sino a personas también reales, compañeros de trabajo, usuarios, clientes, proveedores, etcétera. Es un cambio de mentalidad necesario para que los ejercicios simulados sean efectivos. Por otra parte, aunque la experiencia de años realizando simulacros de autoprotección y emergencias representan un acervo de gran valor para las organizaciones, los incidentes armados activos presentan una serie de condicionantes específicos en cuanto a amenaza, gestión del escenario y patrones lesionales resultantes, que obligan a replantear el modelo de respuesta, y por tanto, el modelo de simulaciones. Varios son los centros comerciales que ya se han mostrado conscientes de esta necesidad, pero el camino por recorrer todavía es largo, aunque hayamos empezado a caminar. ✱

1.- Tactical Emergecy Casualty Care Guidelines (2015), donde a nivel de intervinientes inmediatos, prima el control de hemorragias masivas exanguinantes con torniquetes y medios de fortuna, y el manejo de la vía aérea.

COMUNICAR LA SEGURIDAD EN EVENTOS (I)

Los responsables de la seguridad de eventos deben conocer cómo la comunicación puede ser de ayuda para el desarrollo de sus funciones.

CARLOS MORENO CLEMENTE.
CODIRECTOR DEL «CONGRESO COMUNICACIÓN Y SEGURIDAD EN EVENTOS» DE LA UCM. DOCTOR EN COMUNICACIÓN, PUBLICIDAD Y RRPP. MÁSTER EN DIRECCIÓN DE SEGURIDAD PRIVADA.

Probablemente a los viajeros habituales ya no les sorprenda y ni tan siquiera presten la requerida atención cuando, antes de emprender un vuelo, se les proporcionan las normas de seguridad. Esa especie de ritual previo al despegue es un claro ejemplo de comunicación de la seguridad, ¿pero qué ocurre con la comunicación de la seguridad en eventos?

Los eventos se han convertido en motores sociales y económicos, permitiendo también intercambios culturales y políticos, además de oportunidades para el ocio y el entretenimiento. Algunas de las propias características de los eventos, como pueden ser la congregación de un gran número de personas, la presencia de personalidades relevantes o reconocidas, la atracción que generan sobre los medios de comunicación o la propia repercusión y trascendencia del acontecimiento, los pueden convertir en vulnerables desde el punto de vista de la seguridad. A través de la comunicación de la seguridad, en un sentido amplio del concepto, se puede modificar el contexto en que se desarrollará el evento, mejorando la prevención y la protección del mismo.

Los responsables de la Seguridad de eventos deben conocer cómo la comunicación puede ser de ayuda para el desarrollo de sus funciones. La sociedad actual interconectada obliga a mantener un continuo análisis comunicativo para identificar y reducir riesgos, en pro de una mejor experiencia de visitantes y participantes. Bajo el concepto de comunicación de la seguridad se engloban múltiples aspectos como puede ser la comunicación entre las partes interesadas, la comunicación interna o la propia comunicación con los asistentes, todos ellos relevantes para reforzar la cultura de la seguridad en el contexto de los eventos.

COMUNICACIÓN ENTRE PARTES INTERESADAS PARA CONOCER MEJOR EL EVENTO E IDENTIFICAR SUS RIESGOS.

Etimológicamente, la palabra comunicación deriva del vocablo latín commūnicātiō que se refiere a la acción de compartir, es decir, poner algo en común. Precisamente, es gracias a la comunicación que podemos poner sobre


Tijs van Leur/Unsplash

«A través de la comunicación se puede modificar el contexto en que se desarrollará el evento, mejorando la prevención y la protección del mismo»

la mesa información que puede ser de interés común y, en el contexto de la seguridad, toda aquella información que permite un mejor análisis de riesgos.

Muchos de los eventos se caracterizan por ser «eventos únicos», es decir, destacando por su propia singularidad. En estos casos, es aún más importante que fluya toda la información posible entre organizadores, participantes, instituciones, responsables de la seguridad y la movilidad y el resto de partes interesadas, desde la fase de conceptualización del evento. Es probable que, gracias a este intercambio de información o gracias a una frase que empiece con un «quizá no sea importante» pronunciada por una de las partes, se pongan de relieve elementos a considerar desde la seguridad que contribuyan a la prevención.

Por tanto, gracias al compartir con las demás partes interesadas o relevantes de un evento la información más objetiva, pero también aquello que creemos o podemos sentir al respecto del evento, estaremos reforzando la seguridad desde la fase más preventiva. Puede parecer algo obvio, pero ese intercambio previo de información es un elemento crítico, ya que enmarcará el tipo de evento sobre el que se debe planificar la seguridad y el resto de elementos que la compongan, así como contribuirá a la identificación de los posibles riesgos y amenazas. Los responsables de la seguridad de un evento deben conocer las características del mismo y los objetivos por los que se celebra, algo que no es siempre fácil de lograr plenamente.

La comunicación entre el grupo de interés debe ser eficiente y la información que se intercambie debe ser «inteligible» por las partes. Por consiguiente, será necesario despojarla de jergas o tecnicismos, de manera que los interlocutores puedan interpretar los mensajes recibidos para analizarlos desde su perspectiva, como ocurre en el caso de la seguridad.

Desde otro ángulo, Eric S. Stuart[1] apunta que los medios de comunicación y los mensajes de marketing que

los organizadores o promotores hacen circular en la fase previa de un evento pueden afectar significativamente tanto al número de asistentes a esos eventos, como impactar sobre su estado de ánimo y comportamiento. El autor menciona que es un fenómeno en crecimiento, aunque no nuevo, y refiere un concierto de Fat Boy Slim, en 2002, en la playas de Brighton donde se esperaban unas 60.000 personas y que fue valorado inicialmente por las autoridades como un evento con bajo perfil de riesgo, desconociendo toda la comunicación que se iba a realizar a través de medios de comunicación e internet en una promoción sin precedentes en la ciudad. La cifra de asistentes alcanzó las 250.000 personas, creando problemas durante todo el día, empeorando la situación al combinarse la alta concentración de personas con la subida de la marea que reducía el espacio disponible para la celebración evento. Acciones comerciales como dejar caer elementos promocionales en un evento que no incluyan un análisis de la seguridad pueden acabar con incidentes como ocurrió las pasadas navidades en un centro comercial de Sidney donde se soltaron globos con premios en su interior, provocando heridos entre los asistentes que se golpeaban y aplastaban por obtenerlos.

En caso de que se produzcan incidentes como los descritos, también es importante destacar que los seres humanos hemos convertido la comunicación en un eje social que favorece las relaciones interpersonales. Es gracias a la confianza que genera el intercambio honesto de información por ese referido bien común como es el seguro desarrollo de un evento, que también se desarrollan relaciones y vínculos entre las partes interesadas. Todas esas relaciones comunicativas basadas en la confianza entre los interlocutores son de gran ayuda a la hora de gestionar cualquier imprevisto o cualquier crisis que se pueda producir en el transcurso del evento.

Sin duda, existe también un riesgo comunicativo en caso contrario, especialmente si se producen incidentes, ya que cada una de esas partes o grupos de interés pueden querer gestionar de manera independiente la situación, lo que genera, según Luis Serrano[2], «nuevos factores de riesgo de un escenario altamente digitalizado en el que cada uno de esos stakeholders se ha convertido en un medio de comunicación en potencia», siendo necesario «identificar la capacidad de influencia y de generación de informaciones falsas que poseen».

COMUNICACIÓN INTERNA Y CONCIENCIA DE LA SEGURIDAD

Dado que la seguridad afecta de manera transversal a todo lo que ocurre en un evento, la comunicación interna de la seguridad debe diseminarse y llegar a todos los componentes del evento, especialmente a aquellos que forman parte de la organización.

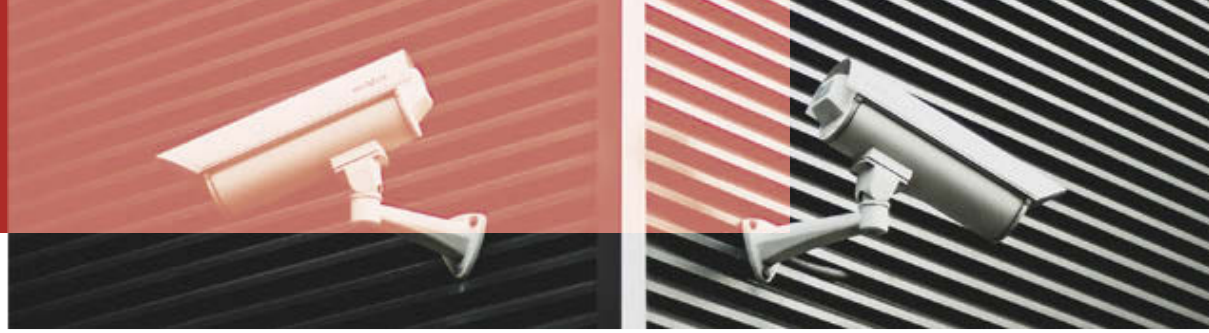
Muchos son los miembros que participan en la organización del evento, abarcando desde la dirección hasta el staff o voluntarios, a los que se debe llegar con el fin de crear una mayor consciencia de la seguridad. Para la seguridad y la prevención, una detección temprana de cualquier riesgo o amenaza puede aportar un mayor tiempo y capacidad de reacción, por lo que multiplicar los 'ojos' que miran debe ser una de las prioridades para los responsables de la seguridad.

En ningún caso se trata de suplir las funciones y cometidos asignados al personal de seguridad o servicios de emergencia, sino que consiste en llegar a compartir la conciencia de la seguridad y facilitar los canales de comunicación interna en materia de seguridad a todos los miembros de la organización. El objetivo de los responsables de la seguridad de un evento debe ser comunicar al resto de personal de otras áreas cómo pueden contribuir con la seguridad gracias a sus acciones, y cómo reaccionar en caso de que se produzca un incidente de seguridad, para mitigar el impacto del mismo.

No se trata de algo nuevo, pero sí es algo sobre lo que se debe insistir y amplificar en muchos casos. Por ejemplo, gran parte del personal que trabaja para un evento conoce cómo actuar en caso de una evacuación o para contener un conato de incendio. Pero conviene reflexionar acerca de cuándo recibieron la última formación sobre estos conceptos o ampliar los ámbitos en los que han sido formados, incluyendo, por ejemplo, la detección de casos de violencia sexual que se pueden producir en el contexto de eventos musicales u otras celebraciones multitudinarias.

1.- Stuart, E. S. (2012). The effect of high-speed communication on crowd attendance and behaviour at events. Journal of Crowd Safety and Security Management, Vol. 2 Núm. 2, 14-21

2.-Serrano, L. (2019). Metodología de crisis. Una propuesta de gestión de crisis para un escenario digitalizado. Disponible en: http://luisserranor.com/metodologia-de-crisis-una-propuesta-de-gestion-de-crisis-para-un-escenario-digitalizado/.



Redstone

Soluciones de seguridad

Electrónica de red

Análisis de vídeo

Control de accesos

RFID

Intrusión

CCTV

Mayorista oficial:

deister electronic · VAELSYS · Canon · Panasonic · wavestore Innovation with integrity · OPTEX · MOBOTIX · HIKVISION

redstone.com.es · comercial@redstone.com.es · 911722802

LOS PROTOCOLOS DE SEGURIDAD CONTRA LA VIOLENCIA SEXUAL EN GRANDES EVENTOS

La formación es el punto de partida para poder prevenir las agresiones sexuales.

ANNA ALMÉCIJA CASANOVA
ABOGADA Y CRIMINÓLOGA. DIRECTORA DE SEGURIDAD PRIVADA

Artistas, asistentes, el personal... todas las personas que acuden a un evento multitudinario, -especialmente en un entorno de ocio festivo como puede ser un concierto, un festival, etc.- pueden ser víctimas de violencia sexual. Además de las conductas que se pueden producir en el propio evento –tocamientos, comentarios groseros, seguimientos, acoso, etc.-, estos espacios son lugares de captación y acercamiento a personas que pueden encontrarse en situación de vulnerabilidad por la ingesta de alcohol u otras sustancias, y que son acompañadas al exterior y agredidas sexualmente en aparcamientos, parques, viviendas, etc.

No se trata de criminilizar la noche, ni los espacios festivos, sino de buscar soluciones y garantizar un ocio y un entorno de trabajo seguro, luchando contra este problema con la planificación de acciones concretas en diferentes ámbitos: prevención, detección de este tipo de conductas, intervención y la atención a las personas afectadas.

Uno de los instrumentos que debe incluir un plan contra la violencia sexual es un protocolo de actuación, que será un procedimiento operativo que ha de servir para que todo el personal sepa identificar la conducta que ha detectado -o de la que le han advertido- y actúe de manera correcta, tanto en relación a la persona afectada como ante la persona agresora.

1. PREVENCIÓN

La formación es el punto de partida para poder prevenir la violencia sexual. Los contenidos deben cubrir tres ámbitos: sensibilización, conceptos jurídicos y procedimientos operativos para actuar ante determinadas conductas. Para activar el protocolo de actuación el personal ha de saber identificar qué es y qué no es una violencia sexual, superar los mitos que hay en torno a ella, entender conceptos como el consentimiento, contar con cifras y datos sobre estos comportamientos, distinguir qué comportamiento es delito, qué es infracción administrativa o qué conducta no está legalmente tipificada, pero ante la cual podemos intervenir para garantizar el bienestar de asistentes y trabajadores, y que ese comportamiento inadecuado no vaya a más.

«Es imprescindible que el personal de seguridad privada que presta servicio en el evento reciba, además, una formación lo más completa posible sobre violencia sexual»

Christian Bertrand/Shutterstock

Todo el personal de la organización puede sufrir o detectar una conducta que constituya violencia sexual y debe saber cómo actuar, por eso todos deben recibir una formación aunque sea mínima. Y teniendo en cuenta que los contenidos obligatorios de formación para aspirantes a vigilantes siguen sin incluir los delitos contra la libertad e indemnidad sexuales, es imprescindible que el personal de seguridad privada que ha de prestar servicio en el evento, reciba, además, una formación lo más completa posible sobre este tema. No solo vigilantes, sino también el/la directora de Seguridad, coordinadores, etc. Y por las funciones que desempeñan en los acontecimientos, también deberían contar con conocimientos más extensos el personal de control de acceso y auxiliares.

El compromiso de un evento contra la violencia sexual debe visibilizarse a través de cartelería, vídeos, mensajes en redes sociales... Eso también es prevención, ya que ayuda a crear un entorno seguro para trabajadores y asistentes, y puede ser disuasorio para el potencial agresor, que así sabrá que en ese recinto se actúa ante conductas indebidas.

En coherencia con el plan, en el evento no deberían realizarse prácticas sexistas, por ejemplo, en el control de acceso: no hacer pagar entrada a las mujeres y sí a los hombres es una discriminación que vulnera el principio de igualdad. Tampoco pueden imponerse códigos de vestimenta diferente a mujeres y hombres, ya sean asistentes o trabajadores. Asimismo, debe revisarse la cartelería, flyers... con la que se promociona el evento, o el contenido de la página web para evitar imágenes que cosifiquen a la mujer o contengan expresiones sexistas.

Además, el personal de control de acceso tiene una misión muy importante: del mismo modo que no deben permitirse indumentarias, símbolos... con mensajes de odio, racistas, xenófobos, homófobos, etc., tampoco deben permitirse mensajes sexistas o denigrantes para la mujer. Y en cuanto que las condiciones de acceso lo son de permanencia, en el caso que dentro del recinto se detecte a alguien con ese tipo de indumentaria, se debe actuar.

Es esencial adoptar medidas de prevención situacional. Para ello hay que hacer un recorrido por el recinto por donde se desarrolla el evento y sus entornos para detectar riesgos y buscar soluciones para combatirlos: mejorar la señalética, buena visibilidad (ver y ser visto), implantar sistemas que permitan pedir ayuda en entornos alejados de la multitud o por el contrario

Román Kosolapa/Shutterstock

excesivamente ruidosos (pulsadores de alarma, etc). En los espacios que puedan ser más problemáticos –como los lavabos– además, de otras medidas, habrá que contar con la presencia –tan próxima como se pueda– de personal de seguridad.

También forma parte de la prevención, un plan de movilidad específico y adecuado que garantice una salida segura por parte de asistentes y trabajadores, evitando el paso obligado por zonas aisladas, esperas en paradas de transporte público poco seguras, etc. Es importante que en la página web del evento o por las redes sociales se informe de la hora de finalización del evento y de las alternativas de transporte para que trabajadores y asistentes puedan planificar cómo van a realizar la vuelta a casa.

2. DETECCIÓN E INTERVENCIÓN

La formación ha de servir al personal para saber detectar una violencia sexual, identificar ante qué tipo de conducta están (delito, infracción...) y si deben intervenir directamente o a quién deben avisar para que intervenga (al vigilante de seguridad, al responsable de protocolo contra las violencias sexuales, etc).

En este punto el protocolo operativo de actuación debe ser muy claro para realizar la actuación correcta, y en la formación se deben haber planteado las diferentes situaciones ante las que el personal se puede encontrar para actuar en el caso de que se dé un comportamiento indebido. Por ejemplo, establecer el procedimiento a seguir si hay que expulsar o llamar la atención a alguien porque está siendo pesado con otra persona, para evitar grandes enfrentamientos o problemas (quién lo hará, qué se le dirá, cómo se actuará si se niega, etc.).

3. ATENCIÓN A LAS PERSONAS AFECTADAS

Todo el personal de un evento puede encontrarse en la situación de ser el primero en atender a una persona que acaba de sufrir una violencia sexual, y esa primera atención hasta que llegue la ayuda especializada –criminólogos, psicólogos o la propia policía– puede ser determinante de cómo esa víctima viva la experiencia que acaba de pasar: su recuperación psicológica, que decida denunciar o no, que quiera recibir atención médica, etc. Por ello, es muy importante recibir también formación específica en este ámbito sobre qué decirle, qué no, cómo no revictimizarle, cuál ha de ser nuestra actitud –empatía, escucha activa, no juzgar...–, hay que conocer los recursos que existen para ayudar a esa persona, así como una información básica que pueda resolver las preguntas que nos plantee.

Es recomendable que en el evento exista una persona responsable del protocolo contra las violencias sexuales que pueda gestionar esas situaciones y dar una primera atención de calidad a la víctima.

En grandes eventos también es conveniente tener un punto estático de información y atención, llevado por personal especializado o con formación suficiente, donde se puedan dirigir las personas afectadas por violencia sexual o que deseen realizar alguna consulta sobre el tema. ✱

LA SEGURIDAD DIGITAL EN EVENTOS MUSICALES Y DEPORTIVOS

La tecnología avanza y nosotros como profesionales debemos avanzar con ella ya que nos dará ventajas para mejorar la calidad de nuestros eventos y para prever posibles ciberataques.

HELENA BATLLE VICENTE
PERITO JUDICIAL Y FORMADORA

Klaus Schwab ya dejó claro que estamos en la 4ª revolución industrial y que casi todo lo que hacemos en nuestra vida diaria tiene un mínimo componente digital.
En el mundo de los grandes eventos, sean del tipo que sean, la seguridad digital es de vital importancia ya que las comunicaciones y la maquinaria de estos eventos depende de ordenadores e internet en el 90% de los casos. Esta seguridad es responsabilidad de todos, desde el señor que monta el escenario hasta el fan que compra una entrada para acudir a ver el espectáculo.

¿POR QUÉ LOS EVENTOS MULTITUDINARIOS SON TAN SUSCEPTIBLES A CIBERATAQUES?

En mis clases y en mis conferencias mucha gente me pregunta por qué los grandes eventos son tan susceptibles de tener ciberataques. Sensibles lo somos todos dependiendo del objetivo de éste y los motivos pueden ser variados: Retos, vandalismo, robo, ciber-activismo, hacktivismo, secuestro de información, dinero, terrorismo...
Uno de los casos de mayor repercusión fue en las Olimpiadas de invierno 2018. El ataque inicial afectó principalmente a todos los sistemas de tecnología y la conexión a Internet que sería utilizada por los periodistas para hacer la transmisión a sus respectivos países. También imposibilitó al público que había adquirido sus entradas online imprimir sus reservas. Estos problemas se extendieron por un par de días. El causante de esto fue Olympic Destroyer, creado con la finalidad de eliminar las instantáneas de los sistemas, los registros de eventos e intentar usar PsExec y WMI para avanzar en el entorno. Su comportamiento es similar al de Bad Rabbit, ransomware que ocasionó grandes problemas en Europa del Este durante el tercer trimestre de 2017.

BRECHAS DE SEGURIDAD DIGITAL EN LA PRODUCCIÓN DE UN EVENTO

Es típico e incluso tiene cierta lógica pensar que los ataques criminales en los eventos se realizan el mismo día de esa actuación y ese partido en concreto. Esa es una

Stuart Miles/Shutterstock

«En el mundo de los grandes eventos, sean del tipo que sean, la seguridad digital es de vital importancia»

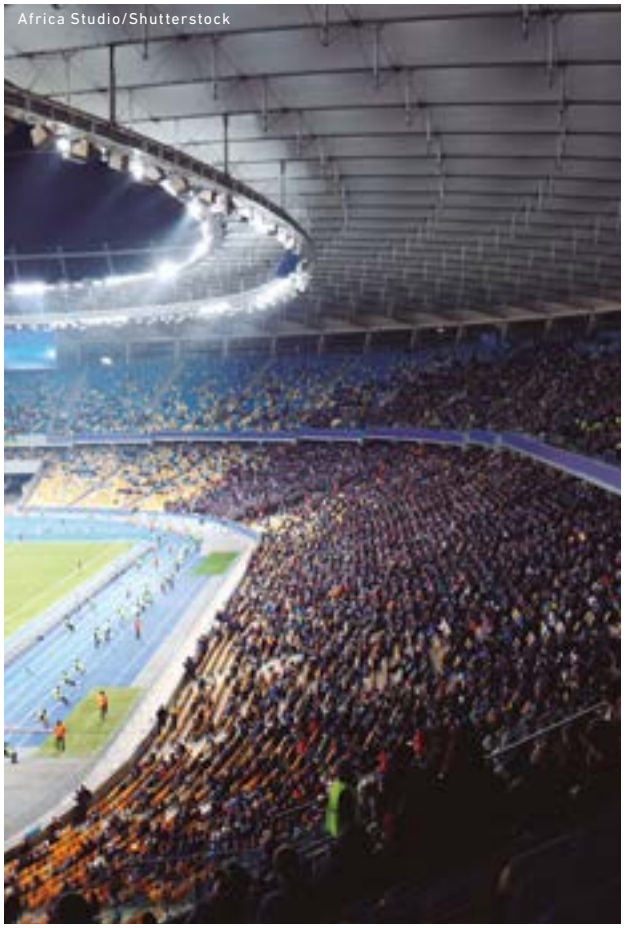
concepción errónea ya que atacar un evento no es sólo provocar un incidente durante el mismo, puede ser también denegar el acceso al público como comentábamos antes cuando hablábamos de las olimpiadas de invierno, dificultar las comunicaciones o provocar que el evento no se pueda realizar. Desde el minuto 0 en el que empezamos a crear y planificar el evento ya podemos tener agujeros sensibles a que nos puedan atacar a nivel informático. La evaluación del sitio donde se va a organizar, la evaluación de riesgos, durante la información y/o formación del personal, la estrategia de vigilancia..., todos ellos son puntos vulnerables a ciberataques que tenemos que controlar y monitorizar.

¿CÓMO INFLUYE LA TECNOLOGÍA EN LA SEGURIDAD DE GRANDES EVENTOS?

No nos damos cuenta, pero hemos integrado la informática a nuestro día a día de manera que no sabemos vivir sin nuestro móvil, y muchas puertas se abren con tarjeta en vez de con la llave dentada de siempre.

En los grandes eventos están presentes los últimos avances tecnológicos, aunque algunos lleguen a pasar inadvertidos.

A gran escala el control de servidores para que siempre haya información a tiempo real, y a nivel más de consumidor en las compras de entradas y en los controles de acceso, siendo una de las últimas novedades las pulseras de prepago, dando al trabajo de control de seguridad grandes ventajas. La precisión de conteo gracias a su sistema de hypertracking, con un sistema de detección de personas que funcione por detección de patrones, el control en accesos libres o desordenados y/o la posibilidad de poder funcionar en cualquier ambiente (interno o externo), evitar que se cuelen entradas falsas... son avances que nos permiten además de seguridad, confort y confianza con nuestros consumidores finales. La ventaja de este tipo de tecnología es que casi todo el software se puede utilizar fácilmente desde cualquier plataforma (móvil, ordenador, tablet...). Otro factor a tener en cuenta es que tenemos que combinar todo el sistema de seguridad digital a la normativa española y según en qué casos a la europea (sí la famosa RGPD), aspecto que nos puede traer algún que otro quebradero de cabeza, como pasó en su día con los sistemas de reconocimiento facial. Gales puso en marcha en 2017 durante la final de la Champions League, un sistema de reconocimiento facial para evitar el acceso a potenciales criminales a eventos deportivos. Un 92% de las 2,297 personas detectadas como criminales, y a las que se les impidió acceder al espacio, no tenían antecedentes e incluso se catalogó como criminal a un ministro asistente al acto. Ya lo dijo Javier Sánchez Monedero, investigador en el Data Justice Lab de la Universidad de Cardiff en su momento: «Las herramientas de vigilancia y big data, más que predecir comportamientos de personas sirven para la gestión de los recursos de seguridad. La resistencia a


Africa Studio/Shutterstock

«En los grandes eventos están presentes los últimos avances tecnológicos, aunque algunos lleguen a pasar inadvertidos»

estas tecnologías se plantea a menudo desde los derechos sociales, pero rara vez usamos una razón estadística: es imposible que la mayoría de estas propuestas funcionen».

LA IMPORTANCIA DE LA FORMACIÓN Y DE LOS PLANES «B» EN LA SEGURIDAD PRIVADA Y EN LOS GRANDES EVENTOS

Bruce Schneier, criptógrafo, experto en seguridad informática, y escritor, además de jefe tecnológico de Counterpane Internet Security, afirma que, si pensamos que la tecnología puede solucionar nuestros problemas de seguridad, está claro que no entendemos ni de tecnología ni de seguridad. En mi experiencia como informático y como perito puedo afirmar que el 95% de los casos en los que he colaborado alguien apretó un botón que no debía en el momento equivocado, con malas, buenas intenciones o simplemente por ignorancia o falta de información.

Los planes «B» deberían ser incluidos en la seguridad de grandes eventos como punto obligatorio. Pequeños detalles como protocolos manuales escritos en papel guardados en una funda en el bolsillo del uniforme, llevar dobles SIM en los móviles, baterías autónomas de bolsillo, contar con una compañía de internet por cable y por satélite, etc., pueden ayudarnos a parar un posible ataque sin que casi se perciba su impacto.

La tecnología avanza y nosotros como profesionales debemos avanzar con ella, ya que nos dará ventajas para mejorar la calidad de nuestros eventos y para prever posibles ciberataques. Por eso creo firmemente que es muy importante la formación y la especialización de los profesionales de la Seguridad Privada. Se trata de una oportunidad única para crear nuevas profesiones y/o especializaciones en este sector y de estar preparado a lo que vendrá, ya que se prevé que los ciberataques se van a acrecentar en la próxima década especializándose en temas como la inteligencia artificial, los suministros o los datos en tráfico. ✱

VIGILANCIA CAMUFLADA EN EVENTOS

Los servicios de Seguridad no uniformada son aquellos que, prestados por personal de seguridad sin uniforme, garantizan la misma en eventos como ferias, hoteles, exposiciones y espacios análogos.

RAFAEL GUERRERO
DIRECTOR GRUPO AGENCY WORLD INV

Para contemplar el asunto que titula este artículo con un punto de vista global trataré de abordar desde las perspectivas teórica, práctica y legal los llamados Servicios de Seguridad no uniformada, siendo aquellos que, prestados por personal de seguridad sin uniforme, garantizan la misma en eventos tales como ferias, hoteles, exposiciones y espacios análogos. Dicha seguridad no uniformada o camuflada convive y se opera tanto desde el sector privado como del público con metodología y recursos muy similares. Un ejemplo de ello es la dotación humana que ambos disponen, es decir, el personal de uniforme y el personal de paisano, ya sean agentes de uno u otro. En el caso del sector privado la ley otorga esa función a los detectives privados.

En este sentido, la Ley 05/2014 deja claro que los detectives privados formamos parte del Plan de Seguridad, aportando personal de seguridad como empresa externa y en la fase de ejecución.

Con esta combinación de esfuerzos y estrategias se pretende delimitar un entorno seguro, exento de riesgo y que por tanto requiere un análisis riguroso de éste. Para tal fin, se llevarán a cabo acciones de vigilancia que respeten los derechos, libertades y propiedades de los asistentes. Este cometido se sirve de la seguridad e investigación privadas en cuanto a las medidas preventivas que se apliquen y lógicamente a las practicadas en tiempo real, así como de las posteriores al suceso, que de acontecer, se demanden.

Así lo corrobora la Ley Seguridad Privada en su artículo 2.1, especificando que «la seguridad privada son actividades, servicios, funciones y medidas de seguridad realizadas o prestadas por, entre otros, despachos de detectives privados y personal de seguridad privada, cuyo fin es garantizar la seguridad de las personas, proteger su patrimonio y velar por el normal desarrollo de sus actividades».

«La Ley 05/2014 deja claro que los detectives privados formamos parte del Plan de Seguridad, aportando personal de seguridad como empresa externa y en la fase de ejecución»

EL DETECTIVE PRIVADO EN MATERIA DE SEGURIDAD EN EVENTOS

La seguridad jurídica que se proporciona al cliente se formaliza a través del contrato de prestación de servicios. Según el Artículo 48: «Los detectives privados prestarán su servicio realizando las averiguaciones necesarias para la obtención de información, tendente a garantizar el normal desarrollo de las actividades que tengan lugar en ferias, hoteles, exposiciones, espectáculos, certámenes, convenciones, grandes superficies comerciales, locales públicos de gran concurrencia y ámbitos análogos». Estas actividades se ejecutan sin distintivos ni identificación exterior. El detective privado se identificará solo cuando sea preciso o a requerimiento de los ciudadanos o de los agentes de la autoridad mostrando la correspondiente TIP.

No es necesaria la autorización previa de Seguridad Privada, aunque el profesional contratado estará dado de alta en el Registro de Detectives Privados de la D.G.P.

El detective privado es considerado, por consiguiente, personal de seguridad y está cubierto por el seguro de Responsabilidad Civil Profesional correspondiente.

Al tener un ámbito específico de actuación, se aplican los planes de riesgos laborales a los detectives conforme a las instrucciones del cliente.

El detective privado colabora activa y complementariamente con la empresa de seguridad asignada.

EL DISPOSITIVO DE SEGURIDAD COMBINADA

El departamento de Seguridad que se establece para este tipo de operativos responde a un determinado esquema de mando (de mayor a menor autoridad): director de Seguridad, delegados del director, empresas colaboradoras, empresa de seguridad, empresa de detectives privados.

Este es el equipo multidisciplinar que se enfrenta y resuelve los denominados actos antisociales, tales como: riesgos derivados de acciones de carácter delincuencial, robos, hurtos, vandalismo, altercados, amenazas físicas y verbales, violencia de género, reventa de entradas, manifestación no autorizada o similares, consumo y venta de estupefacientes, y posibles atentados de carácter indiscriminado vinculados al terrorismo internacional.

Para el buen desarrollo de ese cometido, la vigilancia camuflada se antoja imprescindible pues facilita las

funciones preventivas, la presencia y observación, la obtención de información de cualquier comportamiento sospechoso y, llegado el momento, la actuación proporcionada para evitar males mayores siempre en estrecha colaboración con la empresa de seguridad y con las Fuerzas y Cuerpos de Seguridad del Estado, en aras de ofrecer al cliente y a los asistentes una solución de forma conjunta bajo la supervisión de dichas autoridades, quedando el personal civil, incluido el detective privado, a su disposición. De ahí que habitualmente se habilite en el seno de la organización un CECOR (Centro de Coordinación) con teléfono directo para todos los participantes en el dispositivo de seguridad.

FASES EN UNA VIGILANCIA CAMUFLADA EN EVENTOS

Todas ellas son preceptivas e importantes. El error o fallo en una puede provocar graves consecuencias en las posteriores.

Fase 0 | Zona Segura: Inspección perimetral de todo el recinto a fin de detectar «agujeros» de seguridad.

Fase 1 | Inicio y Acceso: Especial atención a perfiles sospechosos, reventas, consumo y venta de alcohol, sustancias prohibidas en parkings, delincuencia habitual y elementos terroristas.

Fase 2 | Celebración: Vigilancia discreta sobre las zonas de público, escenario, aseos, portones, zonas vips, barras, etc. Vigilancia de las salidas de emergencia, de desplazamientos de aforo, ante toma de fotografías no consentidas, ante toma de datos personales mediante subterfugios. Especial atención a situaciones de posible acoso o violencia sexual.

Fase 3 | Finalización y Desalojo: Se orienta específicamente a la salida ordenada y segura del público. Detección de sospechosos de haber cometido actos antisociales.

INFORME Y CONCLUSIONES

Para finalizar con la tarea encomendada por el cliente, se redactará y presentará un informe detallado al mismo con todas las actuaciones realizadas. Asimismo, el detective privado valorará la experiencia objetivamente, teniendo en cuenta aciertos y déficits para mejorar las futuras prestaciones de este servicio. ✱

GESTIÓN DE ALARMAS REMOTAS Y TELEGESTIÓN

LLUIS MARÍN.
COORDINADOR DEL COMITÉ DE FABRICANTES DE DETECCIÓN.
TECNIFUEGO

En el pasado, en general, eran impensables los efectos que iba a tener el desarrollo de las tecnologías de la información en nuestras vidas, en la forma de relacionarnos en nuestro entorno privado o profesional.

Hace ya algunos años que la digitalización afecta a nuestro entorno, privado y profesional, transformando el modo en que nos relacionamos o trabajamos. La digitalización nos trae una capacidad de gestión inconmensurable que, con el IoT, el 5G y el Big Data, cambiará de forma radical nuestra percepción del valor de los bienes, de los productos y de los servicios.

En este nuevo escenario, un sector tan regulado como la detección de incendios se va a ver arrastrado a cambios profundos. Cambios que ni siquiera ahora podemos prever pero que llegarán en breve con esta ola de innovación. Con toda seguridad, esta evolución nos traerá precisión, seguridad, protección, calidad, y un entorno más agradable y eficiente.

Con la llegada de las nuevas tecnologías se han ampliado las posibilidades de servicios disponibles sobre los Sistemas de Detección y Alarma de Incendios (SDAI) a través de las conexiones remotas que aportan:

- mejoras en la seguridad de las personas y bienes,
- un incremento sustancial de la fiabilidad del sistema,
- rapidez y efectividad en el mantenimiento,
- reducción de costes de operativos,
- mejora en la calidad del servicio,
- mejora de la eficiencia energética

Con la publicación del RIPCI (RD 513/2017), en el anexo II, se reconoce esta nueva realidad puesto que acepta la conexión remota a un centro de gestión de servicios de mantenimiento, con el fin de facilitar las tareas de mantenimiento y gestión del sistema, así como proporcionar servicios añadidos. Por otro lado, se hace mención a la transmisión de alarmas de incendios.

Debido a que estas nuevas prestaciones no han podido ser claramente reflejadas en el RIPCI (RD 513/2017), a continuación, se realiza un análisis sobre las diferentes posibilidades de servicio existentes.

QUÉ SE HACE EN OTROS PAÍSES

En el área de servicios, hoy, ya existen plataformas cloud para el soporte en el mantenimiento y diversos fabricantes ya han desarrollado soluciones propias de software de servicio.

En otro ámbito, la asociación europea, Euralarm, ha trabajado recientemente en un estudio en un grupo de países de la Unión Europea, sobre el impacto de las falsas alarmas de los sistemas de detección. Aunque no hay un estándar común, la información revela un alto nivel de conexión directa de los sistemas de detección y alarma con los servicios de emergencia, centros receptores de alarma de incendio u otro tipo de plataformas (cerca de un 90%). Cada país ha aplicado diferentes soluciones, según su tradición, experiencia y conocimiento.

Se evidencia que los equipos conectados facilitan el control de los sistemas, hacen posible el seguimiento del libro de registro, permiten el análisis para la mejora y la aplicación de medidas preventivas o correctoras, y promueven un mantenimiento más eficaz posibilitando la supervisión y auditoría.

MISIÓN DE UN SDAI

Gestión local

La misión de un SDAI se centra en la vigilancia y aviso de incendio de un local, edificio o instalación a sus ocupantes con el fin de preservar la vida humana.

Entre las funciones del Equipo de Control e Indicación (ECI) de un SDAI, se encuentra la de centralizar la información y el acceso al sistema. Es por ello que este equipo debe situarse dentro de la instalación en un lugar accesible, tanto para el personal responsable del edificio, como para la asistencia de los bomberos, y con el fin de que puedan interactuar adecuadamente con el sistema.

En muchos casos, por el uso, la geometría, distribución, o tamaño de la instalación es difícil cumplir con este requisito, por lo que se pueden recurrir a varias soluciones.

- Uso de repetidores de información integrados en el SDAI que permiten el acceso a la información y control desde distintos puntos de la instalación.
- Uso de software de control, además de las ventajas de los repetidores, facilitan el control de la instalación mediante información adicional, como por ejemplo gráficos, datos o planos sinópticos de la misma.
- Integración del SDAI en el sistema de gestión del edificio SCADA (Supervision Control And Data Acquisition - Supervisión, control y adquisición de datos) que interacciona de manera independiente con los diferentes sistemas existentes en la instalación. En este caso los sistemas de protección contra incendios tendrán un nivel de prioridad máximo. (R.D. 513/2017 Anexo I Punto 1).

Todas estas soluciones se entienden desde la perspectiva de que el personal responsable del edificio o los bomberos puedan tener acceso al SDAI en la instalación.

En el caso en que se usen sistemas de transmisión de alarma a otros sistemas fuera de la instalación, no exime de la responsabilidad de la propiedad, explotador y/o usuario con respecto a las acciones necesarias que se deban tomar localmente para la protección de las personas y bienes.

El plan de emergencia y autoprotección debe integrar los sistemas de gestión local y determinar las acciones que deben tomarse frente a cualquier circunstancia de riesgo o falta de protección.

Conexión Remota

Además de estas conexiones locales del SDAI, el sistema puede tener conectividad con otros sistemas fuera de la instalación. A este tipo de comunicaciones es a lo que nos referimos como conexión remota. Existe gran variedad de sistemas con conexión remota con posibilidad de realizar diferentes funciones. Dentro de esta diversidad de comunicaciones, conceptualmente se pueden dividir en tres:

a) Telegestión

Acceso remoto al SDAI para ofrecer servicios enfocados principalmente al mantenimiento del sistema.

La telegestión no debe causar ninguna disminución de

Existe gran variedad de sistemas con conexión remota con posibilidad de realizar diferentes funciones

la efectividad del SDAI sobre la vigilancia y aviso de incendio en la instalación.

Posibles servicios pueden ser:

– Conexión y actuación directa sobre el SDAI, permitiendo soporte a distancia en tiempo real, bien por parte de una empresa instaladora/mantenedora o por parte de responsables del SDAI que no se encuentren físicamente en la instalación.
– Acceso a la información de mantenimiento con el que planificar estas actividades con la finalidad de asegurar la disponibilidad del SDAI.
– Vigilancia en general del sistema, donde poder recibir eventos informativos con la finalidad de facilitar el mantenimiento y gestionar los recursos del servicio de forma eficiente, actualizar el sistema o dar soporte remoto para la configuración.

Es preciso implementar medidas específicas de seguridad cuando se realicen acciones de escritura sobre el SDAI, verificar la corrección de los cambios y debe ser posible el retorno a la configuración anterior.

Cuando el fin de la telegestión sea el de facilitar las tareas de mantenimiento y gestión del sistema, deben realizarse a través de una empresa mantenedora de PCI debidamente habilitada. (R.D. 513/2017 Anexo II Punto 10).

b) Centro Receptor de Alarmas de Incendio (CRI)

Centro de recepción y supervisión de alarmas de incendios remoto, con el cual se pueden contratar diferentes niveles de servicios de vigilancia de los sistemas de detección y de alarma de incendios.

Las instalaciones pueden externalizar un servicio de vigilancia en estos centros en base a comunicaciones eficaces de acuerdo con lo que esté contratado. Si el CRI acepta la responsabilidad de vigilar el SDAI y responder de los eventos de alarma ante los servicios de emergencias/bomberos, con protocolos de actuación adecuados, la conexión remota debe tener una disponibilidad y fiabilidad alta en la que es exigible el cumplimiento de la norma EN 54-21 a los equipos de transmisión.

c) Integración Remota

Sistema de gestión del edificio (SCADA) deslocalizado. Un ejemplo puede ser un SCADA de una gran empresa que pueda gestionar edificios situados por todo el país desde su sede central. Esta es una conexión informativa para la gestión integrada de otros servicios en los edificios y que no se produzcan actuaciones contradictorias. Las posibilidades de interacción están sujetas a las necesidades técnicas y económicas del proyecto, y deberán tener una fiabilidad adecuada al servicio de vigilancia que vayan a realizar. De la misma manera que en los SCADA locales, el sistema de protección contra incendios tendrá un nivel de prioridad máximo.

CONCLUSIONES

El estado del arte de las tecnologías permite nuevas posibilidades de gestión de los SDAI que pueden generar dudas en su aplicación. Por ello se ha de tener en cuenta lo siguiente:

Los equipos de transmisión del SDAI deben cumplir con la norma EN 54-21 cuando los CRI acepten la responsabilidad de vigilar el SDAI y responder de los eventos de alarma ante los servicios de emergencias/bomberos.

Los equipos de transmisión del SDAI no precisarían cumplir con la norma EN 54-21, cuando se integre la información del SDAI con otros sistemas o se utilice como medio de información para finalidades de mantenimiento e inspección.

En todos los casos estas comunicaciones no deben afectar a la integridad del sistema. ✱

INCORPORAR LA TECNOLOGÍA RADAR CON OTROS SISTEMAS

JOAN BALAGUER
DIRECTOR COMERCIAL. GRUPO IPTECNO

Conscientes de la necesidad de incorporar la tecnología radar en proyectos donde nos encontramos con otros sistemas PSIM o VMS, Magos en colaboración con nuestra compañía ha desarrollado integraciones con los VMS más usados del mercado, de forma que las alarmas puedan ser gestionadas de igual forma que las generadas por otros dispositivos integrados al sistema y de manera cómoda para el operador.

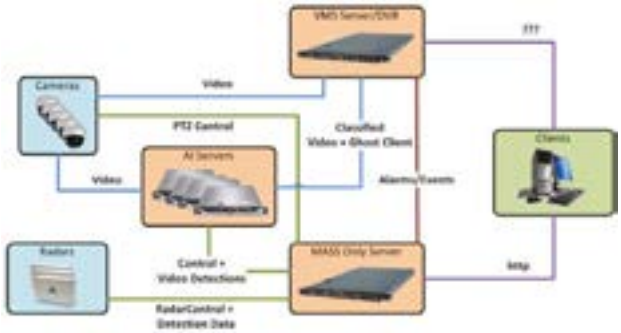
Actualmente el software de gestión de Magos, denominado MASS, en su versión 3 ya incorpora plugins de integración con diversos fabricantes de VMS y software de CRA.

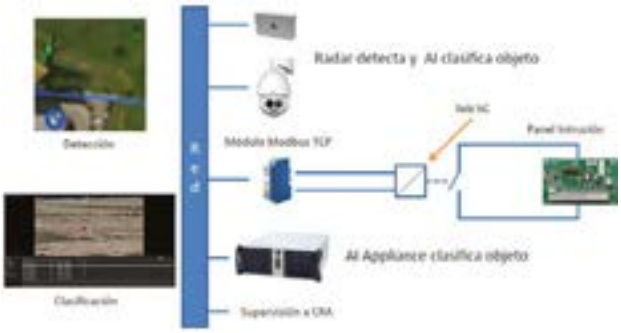
En esta versión se integra también la funcionalidad de clasificación de objetos mediante videoanálisis, que reside en un servidor industrial MASS AI Appliance, que asociado a domos PTZ controlados por el radar, realiza la clasificación de objetos detectados entre humano, animal, vehículo de cuatro ruedas o vehículo de dos ruedas, cuyo resultado puede aplicarse al filtro de alarmas correspondiente de MASS, para que solamente determinados objetos generen señales de alarma contra los dispositivos integrados, bien sea un VMS o una CRA.

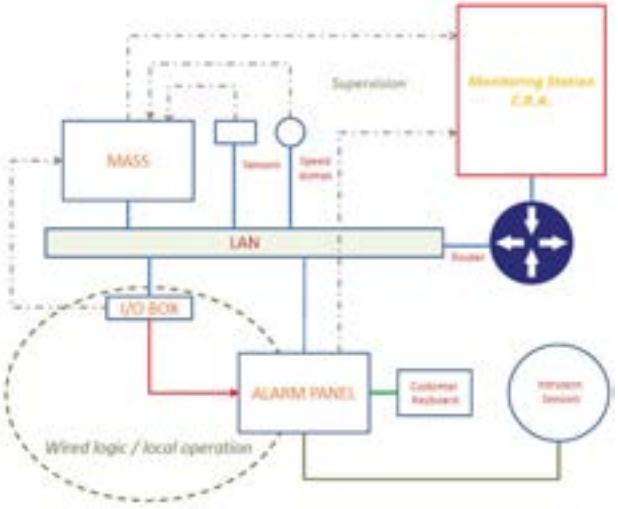
La integración con VMS se realiza mediante las correspondientes llamadas según el API de cada uno de ellos y basta con configurar los parámetros típicos en el interfaz del plugin, tales como dirección IP, puerto y demás características propias de ese software en concreto. De esta manera la gestión de vídeo, GUI y las alarmas

de MASS quedan integradas en el VMS correspondiente. La integración con sistemas de detección de intrusión se realizan mediante dos procesos en paralelo, por una parte un módulo compatible ModbusTCP conectado a la red se encarga de convertir las señales de alarma en cierre o apertura de contactos en el I/O Box, que a su vez se conectan a las zonas de alarma correspondientes del panel de intrusión, por lo que es compatible con cualquier marca y modelo. Por otra parte se envían vía IP señales de latido y supervisión del sistema hacia la receptora (CRA), de manera que el latido nos confirma el funcionamiento del MASS, que es un servicio de Windows o Linux según convenga, y por otra parte se supervisa el funcionamiento de todos los radares y domos PTZ del sistema, así como del propio módulo ModbusTCP (i.e. Adam, Barionet, etc.).

La supervisión del funcionamiento de estos dispositivos en CRA se ha integrado y probado satisfactoriamente en Manitou, de Bold Technologies, a quien agradecemos su inestimable colaboración. Magos/Iptecno da un paso adelante como sistema desantedido localmente para su instalación en ubicaciones sin sala de control local ni operador local. ✱







LA CIBERINTELIGENCIA, CLAVE PARA AFRONTAR LAS NUEVAS AMENAZAS

Se está librando una nueva guerra fría, pero en esta ocasión en el ciberespacio.

CARLOS JAVIER SEISDEDOS
RESPONSABLE DE CIBERINTELIGENCIA. INTERNET SECURITY AUDITORS

2019 ha sido un año convulso en el ámbito de la ciberseguridad, poniendo en evidencia la magnitud del problema al que se enfrentan las organizaciones en términos de seguridad de la información y de sus activos. Los últimos informes del Ministerio del Interior sobre la criminalidad de 2019 señalan que, únicamente en el último año, los ciberdelitos en España aumentaron un 36%.

Hablando con algunos amigos responsables de la ciberseguridad en grandes empresas tengo la percepción de que cada vez resulta más complicado mantener el nivel de seguridad requerido, debido a que la transformación digital avanza a pasos agigantados en entornos empresariales y particulares, nuestra superficie de exposición continúa aumentando exponencialmente gracias a elementos como la expansión/migración de muchas organizaciones al cloud, la proliferación de nuevas tecnologías como el 5G o la digitalización de los entornos industriales, lo que supone nuevas oportunidades para las actividades relacionadas con la cibercriminalidad, ciberterrorismo y ciberespionaje.

Se está librando una nueva guerra fría, pero en esta ocasión en el ciberespacio, con ataques esponsorizados por Estados y dirigidos hacia objetivos donde los resultados tienen importantes connotaciones en el tablero de la geopolítica internacional.

La ciberinteligencia es fundamental para hacer frente a esta creciente amenaza, ya que las medidas tradicionales de ciberseguridad no consiguen mitigar los nuevos tipos de amenazas. Las organizaciones cada día invierten más recursos en securizar sus servicios e infraestructuras. Los ciberdelincuentes aprenden, mutan y se adaptan, y observamos cómo, cada vez más, utilizan técnicas de ingeniería social para lograr llegar a sus objetivos, ya que son conscientes que las personas son el eslabón más débil en cualquier cadena de seguridad u organización.

Podemos ver un ejemplo de esta estrategia en lo sucedido a Jeff Bezos, el fundador y director ejecutivo de Amazon que, aun siendo la persona más rica del mundo y disponer de los mejores equipos de ciberseguridad,

«Los ciberdelincuentes utilizan técnicas de ingeniería social para lograr llegar a sus objetivos, ya que son conscientes que las personas son el eslabón más débil en cualquier cadena de seguridad u organización»

fue víctima de espionaje digital sin que su organización pudiera evitar caer en manos de los cibercriminales.
Amazon sufrió un ataque dirigido, donde el vector principal de ataque no fueron sus servidores ni equipos, fue su director ejecutivo. No fue un ataque extremadamente elaborado, pero sí efectivo, donde los criminales realizaron un ataque al eslabón más débil mediante técnicas de ingeniería social.
El mecanismo fue muy simple, los criminales conocían/orquestaron una cena entre Jeff Bezos y un príncipe heredero de Arabia Saudí, donde al finalizar el encuentro se intercambiaron los números de teléfono. Hasta aquí bien, pero unas semanas más tarde, Bezos recibió un archivo de vídeo que su nuevo amigo le había enviado mediante la aplicación Whatsapp y donde Bezos, confiado por el origen del mensaje, lo abrió provocando que se instalara un malware en su terminal que exfiltró información durante 10 meses, con tasas de salida diarias de información de 4,6 gigas, hasta que fue detectado en febrero de 2019.
La ciberseguridad busca detectar indicadores y elementos para así avanzar, permitiéndonos elaborar estrategias y mitigar los ataques de los criminales, aunque como hemos visto, los cibercriminales se han dado cuenta que engañar a una persona es mucho más fácil que identificar y explotar una vulnerabilidad de una infraestructura, por lo que el principal vector de entrada a nuestros equipos ya no es una vulnerabilidad en nuestro dispositivo, sino que somos nosotros mismos.
En este punto entra en juego la Ciberinteligencia, debiendo ser un proceso proactivo, una evolución a los sistemas de ciberseguridad tradicionales, que suelen ser reactivos, que debe ser capaz de detectar indicadores de la preparación de un ataque convencional y paralelamente concienciar a nuestras organizaciones sobre este nuevo escenario.
La ingeniería social puede describirse como el arte de convencer, influir o manipular a una persona, grupo de personas o colectivos, apelando a la curiosidad, el altruismo, vanidad o temor para que una persona haga algo que, en condiciones normales, y sin nuestra interacción no realizaría. Al menos son cuatro los principios básicos y de orden psicológico que nos hacen proclives a un ataque de ingeniería social: todos queremos ayudar, tendemos a confiar en los demás, no nos gusta decir 'No' y a todos nos gusta que nos alaben. Si a estos elementos le añadimos dos elementos extras como son la urgencia y la autoridad, vemos un aumento de los ataques denominados Estafa del CEO.
Aunque los métodos de ingeniería social darían para escribir un libro, es interesante y necesario conocer sobre qué parámetros actúa, tanto para saber aplicarla cuando se requiera, como para saber defendernos de ella, ya que es y creo que cada vez más, una de las formas más comunes de hackear a las personas, y que resulta frustrante para los especialistas en ciberseguridad, ya que no se puede prevenir los sistemas únicamente mediante la tecnología, haciendo falta concienciación y educación de los usuarios para conseguir una seguridad ampliada. ✱

LA SEGURIDAD DE LOS EXPATRIADOS

Enseñanzas del nuevo Coronavirus 2019-nCoV.

EDUARD ZAMORA PERAL
DIRECTOR Y CONSULTOR DE SEGURIDAD. PRESIDENTE DE SECURITY FORUM*

Desde que a finales de diciembre de 2019 se confirmó la existencia de personas afectadas por neumonías de origen desconocido en Wuhan (China), finalmente diagnosticadas como portadoras del denominado «Nuevo Coronavirus 2019-nCoV», ha habido una cascada de sucesos relacionados con esta infección, que enmarcada en un mundo cada vez más globalizado, ha provocado una afectación a las rutinas de vida, desplazamientos y trabajos de las empresas multinacionales y, por ende, a las funciones y responsabilidades de las Direcciones de Seguridad Corporativas, tengan o no delegadas estas funciones en otros ámbitos de sus empresas, como puede ser en muchos casos los departamentos de Prevención de Riesgos Laborales, en muchas ocasiones ubicados orgánicamente bajo el paraguas de Recursos Humanos.

Pero antes de profundizar en esas responsabilidades y en cómo se debieran coordinar las mismas, hagamos una breve exposición del riesgo ante el que nos encontramos y de la propia idiosincrasia del virus, que pese a que su mortalidad afecta básicamente a personas mayores o afectadas previamente de alguna enfermedad que debilite su sistema inmunitario, lo cierto es que, de manera acertada, se está haciendo un trabajo preventivo importante para evitar el contagio y la expansión por los cinco continentes.

El periodo de incubación es de 14 días y si a ello sumamos la notable expansión de la población china por todo el mundo, se motiva que el riesgo de contagio en una multitud de países sea muy alto, especialmente si atendemos a que la reciente celebración del Año Nuevo Chino provoca un altísimo índice de desplazamientos de la población china que visita a a sus familiares en sus ciudades de origen, en esta festividad.

El regreso a los países de residencia conlleva un elevado riesgo de diseminación de casos puntuales que, de no controlarse correctamente en sus puntos de destino, dado el alto nivel de contagio del virus, amenazan con una más que probable extensión de la infección por muchos países, muy alejados del foco inicial en China, incluida España.

MEDIDAS DE PREVENCIÓN SANITARIAS

Las medidas de prevención que nos facilitan las autoridades sanitarias son de los más genéricas (lavarse las manos con frecuencia, tapar boca y nariz al estornudar, utilizar guantes desechables en registros e inspecciones, uso de mascarillas especialmente en instalaciones frecuentadas por pasajeros provinientes de países con afectación, mantener distancia con personas que

«En muchas entidades se evidencia falta, o insuficiencia de políticas efectivas de protección de empleados, expatriados o que viajan puntualmente, en casos como estos»

parezcan presentar síntomas compatibles con la afectación, comunicar casos sospechosos, etc.). Todas ellas, por genéricas, no pueden por sí mismas anular posibles contagios. Se hacen precisas medidas más profundas y efectivas, como la suspensión de viajes a zonas de riesgo o desde ellas, la cuarentena de todo viajero proviniente de países de riesgo, etc. Y es aquí donde retomamos el comentario que dejé a medias en el primer apartado de este artículo, en donde trataba de las responsabilidades dentro de las empresas en la contención de la expansión de los posibles contagios y las medidas organizativas y preventivas aplicables a cada una.

Hunters-Race / Unsplash.

En muchas entidades se evidencia falta, o insuficiencia de políticas efectivas de protección de empleados, expatriados o que viajan puntualmente, en casos como estos. En otras, que pese a disponer de unas buenas medidas no se dan las mejores prácticas de coordinación entre los diversos ámbitos afectados dentro de la propia entidad.

Que las empresas especializadas en estas ayudas y asesoramiento van a hacer su agosto es indudable, como ocurre siempre que se evidencia cualquier situación de crisis grave, con la prestación de servicios, consultoría o asesoramiento en seguridad. Pero ello no es criticable si todos actúan con profesionalidad y sin alarmismos o medidas extremas que pudieran pecar a todas luces de innecesarias.

MEJORAR LA GESTIÓN DE LOS RIESGOS

Querría ahora centrar mis comentarios en cómo el Coronavirus habrá enseñado a mejorar la gestión de estos riesgos en las grandes empresas, las de mayor globalización y dispersión de centros de trabajo o empleados por diversos países del mundo.

Con frecuencia todas ellas tienen consistentes medidas o procedimientos para estos casos, pero en igual frecuencia pecan de falta de lideraje en su coordinación o en la determinación de criterios y medidas drásticas que posibiliten minimizar al máximo los riesgos para sus empleados y, por añadidura, para los países donde habitan o trabajan.

Aplaudo la aplicación de drásticas resoluciones, como prohibir los viajes, tanto de entrada como de salida de esos países de riesgo; ausencia de eventos clave de su sector; obligar a retorno forzoso de desplazados o

«Si algo provocará esta crisis es el reconducir hacia las Direcciones de Seguridad Corporativas el lideraje de gestión que les corresponde, por su visión transversal de todas las "seguridades"»


Ryoji-Iwata / unsplash

expatriados y, cuando ello no sea viable, extremar las medidas organizativas y de aislamiento de sus entornos. Pero todavía merece mayor reconocimiento que la capacidad de resiliencia de las entidades lleve a que incidentes como estos sirvan para que internamente se reordenen competencias, responsabilidades y liderajes sobre la totalidad de estas medidas aplicables, habitualmente dispersas en varios ámbitos de la entidad.

El desfase de publicación de este artículo desde la fecha en que lo escribo no permite una mayor aproximación a los resultados finales de esta crisis de salud mundial, que esperemos no llegue a sus peores previsiones. Pero sí permite ya conocer, de inicio, muchas deficiencias reales en numerosas entidades, en cómo gestionan una crisis de este tipo y en cómo tienen organizadas sus medidas preventivas y la coordinación interna de los diversos ámbitos afectados por las mismas (Recursos Humanos, Gestión de Eventos, PRL, Operaciones o Seguridad Corporativa).

Estoy convencido de que si algo provocará esta crisis es el reconducir hacia las Direcciones de Seguridad Corporativas de cada entidad el lideraje de gestión que considero les corresponde, por su visión transversal de todas las «seguridades» de la entidad.

DIRECCIÓN DE SEGURIDAD CORPORATIVA

Todo el proceso debe ser liderado y coordinado por y desde la Dirección de Seguridad Corporativa, donde se contará con expertos especialistas en esa gestión y coordinación de seguridad globalizada, que permita minimizar el impacto para los empleados de la compañía y para sus entornos de trabajo, familias, ciudades y países que pueden verse afectados.

Estos expertos deben trabajar, conjuntamente con los responsables de los planes estratégicos de la compañía, en la implantación de medidas organizacionales preventivas y reactivas, en procedimientos de coordinación de todo ámbito con funciones relacionadas con los desplazados o expatriados.

La globalización creciente de nuestras entidades debe ir acompañada por la globalización de la responsabilidad de gestión y coordinación de la seguridad global de una compañía, que debe recaer, sin duda, en su Dirección de Seguridad Corporativa. ✱

*Eduard Zamora es también Abogado, Master en PRL y diplomado en Gestión de la Seguridad y Presidente de ADSI.

EL TRIVIAL DE LA INFORMACIÓN

Son muchas y diversas las noticias, preocupaciones o amenazas que incumben a la información de cualquier país medianamente ubicado en el tablero geopolítico mundial.

PEDRO BARCELÓ
DIRECTOR DE SEGURIDAD CLUB DE MAR, MALLORCA.
GRADUADO EN SEGURIDAD Y CIENCIAS POLICIALES

No es precisamente trivial la cuestión de la información. Por todos son conocidos los diversos Servicios de Información que actúan en nuestro país y, también, cómo no, al otro lado de nuestras fronteras, aunque de éstos quizás sabemos más a través del celuloide.

Por lo que ya podríamos hablar de una división primaria del tratamiento de la información, la interior y la exterior, ambas de naturaleza diferente, pero condenadas a complementarse al mismo tiempo, y desde hace algo más de dos décadas, su crecimiento exponencial las ha expansionado por nuestro planeta globalizado, en donde todo tiene repercusión fuera de las fronteras del epicentro del problema. Las réplicas de un atentado cuya «zona 0» se encuentra a miles de kilómetros de nuestro hogar, llegan, invaden y afectan a nuestra zona de confort como si de un tsunami se tratase. Son algunas de las ventajas de la globalización...

Son muchas y diversas las noticias, preocupaciones o amenazas que incumben a la información de cualquier país medianamente ubicado en el tablero geopolítico mundial. El nuestro, por fenómenos exógenos y endógenos, se ha convertido en un objetivo, ahora también legítimo para grupos terroristas de corte yihadista.

AMENAZAS DIRECTAS

Especialmente en el año 2019 que acabamos de lacrar, en el que hemos recibido un aumento considerable en el número de amenazas directas a nuestro país, ya sean como consecuencia de la detención, en la localidad madrileña de Parla, de un integrante de su frente mediático a través de su «cibercalifato», en esa red del terror que, mediante una continua guerra psicológica, pretende complementar sus otras acciones directas en el teatro de operaciones, o por el siempre socorrido alegato de recuperación de «Al Ándalus» e incluso amenazas directas de Dáesh, como sucedió en la pasada nochevieja, contra nuestra icónica Puerta del Sol, buscando siempre la multiplicadora visualización mediática mediante un mega atentado.

Acabamos de tocar el Talón de Aquiles de la Información, el terrorismo que es la prioridad de todos y cada uno de los servicios de información españoles.

Hablar de actividad contraterrorista no es fácil, ni siquiera prudente. Aunque actualmente los expertos se

prodigan por los platos, foros, tertulias o conferencias con el manual bajo el brazo de «Cómo ser un espía en un fin de semana y no morir en el intento». Tampoco defiendo la mitificación del agente de información, pues mi pregunta sería: ¿Quién no es informador o quién no posee información de interés para cualquier servicio?

Y ésta es la parte más sustancial de la información, en la era de la tecnología digital con posibilidades prácticamente ilimitadas por parte de algunos gobiernos, el uso de la más alta y sofisticada tecnología al servicio de los servicios de inteligencia, indica que los resultados de tan ingente arsenal, no son suficientes para acabar con el terrorismo, si todo ello no va acompañado de la –en muchas ocasiones infravalorada- fuente viva.

COMPLETAR EL PUZLE

Ahí es donde entramos y encajamos todos como piezas, para solucionar y completar el puzle, independientemente del servicio, unidad o colectivo al que pertenezcamos.

Cada organismo estatal, comunitario o local maneja «un quesito» de información, desgraciadamente en muchos casos, demasiado aislado, ubicado en un silo que no es compartido, ni volcado o contrastado con el resto de «quesitos» mediante vasos comunicantes, que tienen información sobre el mismo problema.

Si no hay ente que pueda visualizar todos los quesitos en su conjunto, no hay inteligencia, como resultado de tanta información analizada.

Y esta sí que es la clave de bóveda de tanta información, la dovela central para crear inteligencia útil y actualizada para usarla contra una amenaza que en muchas ocasiones se presenta intangible, pero que desgraciadamente nos afecta a todos.

La seguridad privada no queda excluida ni mucho menos de esta ingente labor. Es más, tanto por parte de la Policía Nacional como de la Guardia Civil, a través de sus respectivos programas RED AZUL y COOPERA, de colaboración con la Seguridad Privada, coordinan, gestionan, alimentan y también forman a un colectivo que resulta fundamental para conseguir una «Seguridad Integral» tanto en ámbito público como privado.

Por lo que animo desde esta revista, que resulta una ventana profesional e imprescindible para todos los que formamos parte del sector de la Seguridad, a colaborar mediante los diversos canales de comunicación reseñados, a trasladar de cuanta información sea de interés a nivel de contraterrorismo especialmente, sin dejar de lado otros aspectos que por nuestra labor diaria seamos conocedores en cuanto a seguridad ciudadana se refiere, como pueden ser, por poner un ejemplo, los relacionados con robos, estupefacientes o con otra lacra que golpea cobardemente a nuestra sociedad como es la violencia de género y la trata de seres humanos.

Formemos parte de esta manera, participando en nuestra propia defensa, resultando parte activa en nuestra principal labor diaria... que es la prevención y protección.

No hay por lo tanto información trivial, resultando siempre aconsejable compartirla con los profesionales que puedan analizarla y explotarla o incluso descartarla.

Difícilmente podremos ganar esta partida... si no contamos con todos los «quesitos informativos» en el mismo «cubilete» del analista. ✱

NUEVOS TIEMPOS, NUEVAS NECESIDADES: SEGURIDAD E INTELIGENCIA

JORGE GÓMEZ
VOCAL DE INTELIGENCIA DE ADISPO Y AIMCSE

La gran revolución tecnológica, la globalización y la crisis económico-social han generado una sociedad muy compleja, una sociedad que cohabita con el caos producido por los cambios constantes y la velocidad vertiginosa de los mismos. Nuestras empresas desarrollan sus labores comerciales inmersas en esta sociedad del cambio que ha traído, sin duda, nuevas oportunidades, pero también nuevas amenazas.

Este cambio profundo, que afecta a la sociedad en su conjunto, impacta especialmente en los profesionales del mundo de la seguridad, que debemos adaptarnos a las nuevas circunstancias con rapidez, para así poder aportar a las empresas una labor profesional a la altura de lo que los nuevos escenarios nos exigen.

Nuestra profesión, la seguridad privada, cobra una especial relevancia en estos escenarios de incertidumbre actuales. Se están produciendo continuamente situaciones que alientan la cooperación publico-privada. La seguridad pública debe proteger los intereses nacionales dentro y fuera de sus fronteras, y la privada los intereses de las empresas en los mismos escenarios. La necesidad creciente de colaboración es innegable porque la seguridad privada no deja de ser, a la postre, un complemento de la seguridad pública, pero aportando al sector privado unas condiciones de seguridad adecuadas al desarrollo de sus actividades.

SEGURIDAD, EL BIEN MÁS PRECIADO

Me gustaría recordar que la seguridad es el bien más preciado de nuestras democracias. Basta viajar a países con índices de inseguridad elevados para darse cuenta de lo importante que es tener seguridad. Cuando no existe seguridad todo lo demás se complica, incluida la libertad del propio individuo. Para darnos cuenta de la importancia de la seguridad público-privada podemos observar cuantas personas de las Fuerzas y Cuerpos de Seguridad del Estado y cuantos miembros de seguridad privada velan porque nuestra seguridad esté garantizada en aeropuertos, estaciones de ferrocarril, estaciones de autobuses, en todo tipo de eventos y en un sinfín de servicios que se prestan cada día.

En cuanto a las empresas privadas, lanzadas por efecto de la crisis y la globalización al mercado exterior, necesitan, en mi opinión, de un binomio inseparable: Seguridad e Inteligencia. La Seguridad nos permitirá llevar a cabo acciones para proteger nuestro patrimonio, nuestro conocimiento, nuestra información, nuestros empleados, etc. La Inteligencia, en cambio, está más orientada a la acción ofensiva y nos permitirá, entre otras cosas, obtener información de nuestro entorno competitivo, analizarla y convertirla en informes de inteligencia que sirvan para ayudar a las personas encargadas de tomar decisiones

NUEVOS RETOS Y NUEVAS AMENAZAS

No podemos enfrentarnos a los nuevos retos, a las nuevas amenazas, aplicando soluciones antiguas, que antes nos valieron pero ahora no. Es necesario que los profesionales de la seguridad e inteligencia aportemos un plus a nuestras empresas, demostremos profesionalidad con mayúsculas, seamos líderes de nuestros equipos y sepamos generar soluciones nuevas y creativas. Para ello, queridos compañeros, debemos prepararnos constantemente, sin perder ni un minuto, nuestras empresas lo demandan y la sociedad también.

En relación con lo anterior, creo que nos encontramos en un momento vital en el que debemos afrontar un cambio en la formación indispensable para nuestro futuro, para dignificar nuestra profesión y para que ocupemos el lugar que nos corresponde. Desde mi humilde opinión, creo que los planes formativos del personal de seguridad privada deberían contener asignaturas de inteligencia, un alto contenido en nuevas tecnologías, asignaturas relacionadas con el liderazgo y la gestión de equipos, relaciones internacionales y, por supuesto, prepararnos para la gestión de riesgos. Estos planes, más completos que los actuales, generarían, sin duda, profesionales a la altura de los nuevos retos y, para llevar a cabo estos cambios en nuestra formación, es necesario implicar a todos los organismos, tanto públicos como privados.

Sin duda la universidad es vital a la hora de establecer planes formativos correctos y algunas universidades, como la Rey Juan Carlos de Madrid o el Colegio Universitario LASALLE, han iniciado proyectos interesantes al respecto. Nosotros, por supuesto, debemos estar prestos a colaborar con estos proyectos para así poder volcar en los planes formativos nuestra experiencia adquirida, nuestra veteranía y la visión real desde el punto de vista de las empresas en las que prestamos servicios y sus necesidades.

Creo que estamos en un momento histórico impresionante y tenemos la suerte de poder participar en él. No debemos perder la oportunidad de aportar seguridad e inteligencia al mundo que tenemos y al que nos vendrá, todos nos lo agradecerán.

Esperando no haber sido demasiado crítico, y habiendo pretendido abordar un tema de importancia suma como es el de nuestra formación, creo que el objetivo estará cumplido si solamente algunas de las ideas aquí vertidas son objeto de reflexión por parte de nuestro colectivo. ✱

«Es necesario que los profesionales de la seguridad e inteligencia aportemos un plus a nuestras empresas y sepamos generar soluciones nuevas y creativas»

Markus-Spiske-TaKB-4F58ek / unsplash

KINGSTON

Nuevo SSD centros de datos

Kingston Digital Europe Co LLP, una división de Kingston Technology Company Inc., referente mundial independiente de productos de memoria y soluciones tecnológicas, ha anunciado el lanzamiento del DC1000B M.2 NVMe. Este nuevo SSD es ideal para servidores que disponen de dos ranuras M.2 NVMe para arranque de sistema, con el objetivo de preservar las valiosas bahías de la unidad 2.5" de carga frontal para el almacenamiento de datos adicionales. El DC1000B está diseñado en un factor de forma 2280, que incluye protección contra la pérdida de alimentación in situ y que ofrece una durabilidad de 0.5DWPD4 para una mayor vida útil. Esta nueva unidad de Kingston cuenta con un increíble rendimiento, llegando a alcanzar velocidades de hasta 3.2GB/s y 205K IOPS2. Asimismo, está diseñado para desarrollar funciones de arranque, así como para aplicaciones de caché y registro de usuario. El DC1000B es un SSD NVMe M.2 (2280) de alto rendimiento que utiliza la última interfaz Gen 3.0 × 4 PCIe con 3D TLC NAND. El DC1000B ofrece a los centros de datos una solución de arranque óptima, con la seguridad de que están adquiriendo un SSD diseñado para uso en servidores. Esta unidad es ideal para su uso en servidores de montaje en bastidor de gran volumen como unidad(es) de arranque interna, así como en sistemas construidos especialmente para este fin, en los que se necesita una unidad SSD M.2 de alto rendimiento que incluya protección contra la pérdida de alimentación.

VISIOTECH

Seagate SkyHawk AI, el siguiente paso a los discos duros

A diferencia de los discos duros para ordenadores de escritorio que están pensados para un uso discontinuo durante unas 8 horas al día; en CCTV, por su criticidad, se deben utilizar discos duros específicos para videovigilancia, como la serie SkyHawk de Seagate, que están diseñados para trabajar de forma continua las 24h del día, con hasta 180 TB al año y un promedio de fallo por encima de 110 años. Estos discos duros están optimizados para soportar las cargas de trabajo habituales de los NVR y DVR, con una escritura durante un 90% del tiempo y un 10% para la lectura de grabaciones, pudiendo trabajar de forma individual o conjunta con más de 16 HDD.

Seagate da un paso más allá con la serie SkyHawk AI, creados para mejorar el rendimiento y la fiabilidad en el análisis de datos, permitiendo hasta 32 flujos simultáneos de metadatos de IA y una tasa de hasta 550 TB al año. Con capacidades de hasta 16 TB en una sola unidad e incorporando, al igual que la serie SkyHawk, sensores de vibración internos que aseguran su perfecto funcionamiento de forma conjunta, incluso con más de 16 discos duros en un mismo dispositivo.

BY DEMES GROUP

Software Security Control Center

By Demes Group, distribuidor de referencia en tecnologías de seguridad en Iberia y a nivel internacional, ha presentado Security Control Center (SCC), como la evolución del software DVR Control Center (DCC), una aplicación gratuita que permite a instaladores o centrales receptoras controlar el estado de todos los grabadores de sus clientes en la red local o desde Internet. Se instala en PCs con S.O. Windows y controla eventos de sistema de los grabadores o cámaras offline. Entre los beneficios más destacados de DCC se encuentran el control de equipos Hyundai, Hikvision y Dahua por IP fija, IP dinámica con DDNS y P2P; el control de parámetros (desconexión de grabadores, pérdidas de vídeo y oclusión de cámaras, alerta por visualización de cámaras en negro y grabaciones correctas por canal); visualización de cámaras en directo y grabaciones por fecha; además de exportación de informes personalizables o descarga de certificado de visualización de cámaras.

Y es que el nuevo software SCC permite, además, la gestión remota de videoporteros Dahua y monitorización de centrales de incendio convencionales Honeywell. Entre sus aspectos novedosos respecto a los videoporteros Dahua, SCC recibe las llamadas, visualiza las imágenes y realiza la comunicación de audio bidireccional; acciona los relés de las puertas principal o secundaria; además de disponer de multi-operador para atender varias llamadas simultáneas.

HANWHA TECHWIN

Cámara Box con zoom Wisenet X-Lite

La última incorporación a la gama de cámaras Wisenet de Hanwha Techwin es una cámara clásica económica de 2 megapíxeles con zoom de 32 aumentos.

La cámara Wisenet X-Lite XNZ-L6320 es la sustitución directa de la exitosa cámara con zoom Wisenet SNZ-6320, si bien cuenta con un tamaño y un precio más ajustado que su predecesora (XNZ-6320).

La cámara Wisenet XNZ-L6320 es una cámara día/noche, con filtro mecánico (ICR), y un amplio rango dinámico (WDR) de 120 dB, a fin de obtener imágenes claras en escenas que contienen una combinación compleja de zonas muy luminosas y muy oscuras. A diferencia del WDR convencional, que captura imágenes tomando 2 imágenes con diferentes niveles de exposición, la cámara Wisenet XNZ-L6320 utiliza 4 imágenes con diferentes niveles de exposición para producir una imagen más clara.

Principales prestaciones:

-Soporta los algoritmos de compresión H.265, H.264 y MJPEG, así como WiseStream llt.

-Análisis de vídeo inteligente (IVA) incorporado, que incluye manipulación, merodeo, detección direccional, detección de desenfoque, detección de niebla, línea virtual, etc.

Clasificación de sonidos: Análisis de audio, que reconoce sonidos críticos como gritos, cristales rotos, disparos y explosiones,y genera una alerta.

ZKTECO

Atlas, controladoras multipuertas

La controladora multipuerta ATLAS es la primera solución de acceso de Zkteco en plataforma Linux que incorpora una aplicación web embebida para su gestión, eliminando así la necesidad de instalación de ningún software de gestión de control de acceso y funcionando de manera completamente autónoma.

La controladora puede trabajar en modo primaria y secundaria, y puede conectar con lectores RFID y biométricos. ATLAS ofrece una configuración y escalabilidad rápidas y fáciles, lo que permite lograr un alto rendimiento y menores costes de instalación, mantenimiento y de programación fuera del sitio, gracias a que poseen PoE por defecto y comunicación vía Wi-Fi de forma opcional, prescindiendo de la necesidad de desplegar redes adicionales de cableado.

El sistema habla por sí mismo cuando se instala y utiliza. Es fácil de usar sin demasiadas instrucciones ni entrenamiento previo, simplemente accediendo desde su navegador e incluye una herramienta de ayuda en línea para resolver de forma rápida y sencilla cualquier duda durante el proceso de instalación. Entre sus muchas funcionalidades destacan las de control de acceso avanzadas como la función antiretorno, la creación de mapas, control y monitorización del estado de puertas, bloqueo y desbloqueo global, multiverificación, apertura de primera tarjeta y de múltiples tarjetas, etc.

ATLAS es la solución ideal para proyectos de tamaño medio con distintos accesos, que requieren sistemas sin complejidades, escalables y con acceso en remoto. ATLAS se ha instalado con gran éxito en colegios, edificios públicos, hospitales, oficinas, museos colegios y universidades.

JOHNSON CONTROLS

EntraPass v8.20, seguridad más unificada

Johnson Controls Building Technologies & Solutions ha anunciado el lanzamiento del nuevo EntraPass v8.20, un software de seguridad que simplifica aún más la forma en que los usuarios acceden de forma remota a la app de gestión de accesos EntraPass go.

Con EntraPass v8.20, los usuarios de la aplicación móvil EntraPass go Pass obtienen capacidades de búsqueda mejoradas y otras actualizaciones eficientes para ofrecer acceso remoto y en tiempo real. Las solicitudes de EntraPass go Pass ya no se adjuntarán a un SmartLink seleccionado, eliminando la necesidad de configurar cada conexión de manera individual. Los usuarios ahora podrán acceder a cualquier conexión entrante con pocos o ningún obstáculo.

La funcionalidad mejorada de búsqueda de usuarios/tarjeta es también una mejora significativa de EntraPass v8.20. Los operarios de seguridad podrán buscar un perfil, mientras mantienen abierto el menú de búsqueda, consiguiendo eliminar la necesidad de comenzar cada búsqueda de nuevo. Esto resuelve el problema de tener que volver a abrir el menú de búsqueda si un operario ha hecho clic en el perfil equivocado.

FERRIMAX

Security Smart Lockers: taquillas inteligentes

Ferrimax ha presentado las Security Smart Lockers, sus nuevas taquillas inteligentes en las que, además de guardar objetos, se puede cargar el móvil o recibir compras online. Esta innovadora solución ofrece una serie de ventajas tanto para el punto de instalación como para los usuarios: seguridad, ahorro de gastos de gestión, ahorro de tiempo y colabora con el medio ambiente. Las necesidades de la sociedad actual, en constante evolución tecnológica, han provocado abrir el abanico de las soluciones de seguridad. Ferrimax cuenta con más de 40 años de experiencia en el sector de la seguridad, desarrollando y fabricando todo tipo de productos de seguridad física. Las cajas fuertes y puertas acorazadas son los productos más visibles para el gran público, pero también cuentan con experiencia en el diseño y ejecución de proyectos de gran envergadura en clientes para los que el grado de exigencia en seguridad es máximo.

Ferrimax ha diseñado los Security Smart Lockers: taquillas inteligentes para guardar objetos, cargar el móvil o recibir compras online.

-Security Box Point: guarda tus pertenencias en un lugar seguro. Taquillas para guardar tus objetos de valor en gimnasios, escuelas, hoteles,...

-Security Charge Point: carga tu móvil y otros dispositivos electrónicos en un punto seguro.

-Click & Collect Empresa: punto de entrega de paquetes totalmente seguro, que permite recoger paquetes de compra online en la propia empresa.

-Eco Mail Box: punto de conveniencia para recibir compras online mediante una red municipal.

VANDERBILT

SPC Connect 3.0, solución basada en cloud

Vanderbilt, proveedor de sistemas de seguridad de última generación, ha lanzado la última versión de SPC Connect, la solución de detección de intrusos que se gestiona de forma remota y está basada en la nube.

Esta última versión 3.0, incluye una interfaz de usuario completamente revisada y se centra en operaciones de usuario más intuitivas.

Alexander Scheffold, gerente de Producto de Vanderbilt, dijo que «con este lanzamiento, creemos que la evolución de SPC Connect ha alcanzado un nuevo nivel». Y añadió: «Uno de los objetivos de Vanderbilt es proporcionar sistemas de intrusión de última generación a nuestros clientes con una amplia gama de ventajas.

HIKVISION

Récord de reconocimientos para sus cámaras térmicas

Hikvision, proveedor mundial de soluciones globales de seguridad, ha conseguido el reconocimiento internacional de su tecnología térmica y termográfica, al erigirse ganador en distintos certámenes y premios de reconocido prestigio a nivel internacional.

Los certámenes organizados por ESX Innovation Awards 2019 (USA), así como los Detektor International Award (EMEA), han premiado las cámaras IP Minidomo térmicas DS-2TD1217-x/V1, destacando sus altas prestaciones y rendimiento en cuanto a detección de incendios, su capacidad de detección de alarmas, y su capacidad bi-spectrum, gracias a la cual, es posible visualizar imágenes visibles y térmicas en formato Picture in Picture, o mediante fusión de imágenes de doble espectro, que crea una imagen única híbrida más detallada.

Por su parte, los PSI Premier Awards 2019 (UK), han reconocido en la categoría de Producto CCTV del año, a las cámaras IP térmicas Bullet DS-2TD2617-3/V1, poniendo de relieve su capacidad en cuanto a defensa perimetral, su excelente adaptabilidad ambiental, y la precisión y fiabilidad en la detección de alarmas.

Otro de los dispositivos premiados, esta vez en los GIT Security Award (EMEA), concretamente en la categoría de protección ante fuego y explosiones, han sido las cámaras IP termográficas Bullet Antideflagrante DS-2TD2466T-25X, con certificación ATEX a prueba de explosiones. Para finalizar, los premios internacionales Security & Fire Excelence Awards 2019, han reconocido como producto innovador del año a la cámara IP térmica Bullet DS-2TD2136/V1, de nuevo gracias a su precisa y fiable detección de alarmas, su capacidad de defensa perimetral de largo alcance, y su alta adaptabilidad al entorno, pudiendo ofrecer imágenes de alta calidad en entornos con oscuridad total, y ante condiciones climáticas adversas (lluvia, nieve, niebla, etc.).

TECNIFUEGO

Nueva norma UNE en la señalización contra incendios

Se ha publicado la Norma UNE 23033-1:2019 en base a los pictogramas y criterios de la Norma UNE-EN ISO 7010. La actualización de esta norma supone un gran avance en el campo de la señalización contra incendios, ya que busca la uniformidad a nivel europeo de los pictogramas, lo que supone un aumento de la seguridad en caso de incendio.

La nueva Norma UNE 23033-1:2019 incorpora también otras modificaciones importantes:

- Incorporación de criterios de diseño. Para que las formas, colores y tamaños de la señalización estén perfectamente definidos.
- Aumento del catálogo de señales de protección contra incendios. Se regularizan sistemas que carecían de señalización normalizada.
- Eliminación de señales de evacuación. La Norma UNE 23034, actualmente en revisión, incorporará de forma exclusiva este tipo de señalización.
- Regulación de balizamientos de seguridad. Para un mayor grado de visibilidad de los sistemas de protección contra incendio, y para el marcaje de áreas o superficies.
- Inclusión de anexos normativos. Se regula la señal de hidrante y el cálculo del tamaño de la señalización en función de su distancia de observación.
- Etc.

GUNNEBO & FERRIMAX

Acuerdo de colaboración para el mercado español

Gunnebo confía en un modelo de comercialización y distribución de su línea de cajas fuertes chubbsafes en colaboración con la empresa española Ferrimax. Este acuerdo va en línea con la estrategia adoptada por la unidad de negocio de Gunnebo «Safe Storage» de apostar por la diferenciación entre la venta directa e indirecta.

El pasado mes de noviembre Gunnebo anunció un primer acuerdo con la empresa británica Insafe, consolidando este modelo de distribución para su implementación en otros países como España. Ferrimax, nuevo partner de Gunnebo, se posiciona como una de las empresas líderes en el mercado español de cajas fuertes.

«Con Ferrimax como distribuidor exclusivo contamos con el mejor partner para relanzar las ventas en el mercado español y posicionar a Gunnebo como proveedor líder en la comercialización de cajas fuertes, bajo la marca Chubbsafes», comenta Stefan Syrén, presidente de Gunnebo, CEO y SVP de la Unidad de Negocio Safe Storage

«Ferrimax posee más de 40 años de trayectoria en el sector de cajas fuertes y supone, para nosotros, una gran oportunidad de formar parte de un acuerdo internacional con una empresa como Gunnebo. Juntos seremos capaces de ofrecer la mejor experiencia para el cliente, basada en una amplia y completa gama de productos y un profundo conocimiento del mercado español», Antonio de la Casa, CEO de Ferrimax.

SECURITAS

La compañía refuerza su área de PCI con la adquisición de SCI

Securitas ha asumido el control, a través de su filial Securitas Seguridad España, de la empresa española SCI Protección Incendios. Esta compañía, ubicada en Badalona, cuenta con 20 años de experiencia en servicios de mantenimiento e instalaciones de Protección Contra Incendios (PCI) con una importante presencia en clientes industriales y del sector hotelero en el noreste del país.

Facturación de 2 millones de euros en 2019

La compra de SCI, que facturó 2 millones de euros en el año 2019, se suma a la reciente integración de la compañía de tecnología de seguridad Techco, para duplicar la presencia de Securitas en el mercado de la protección contra incendios.

Para Carlos A. Chicharro, director de Protección contra Incendios en Securitas Seguridad España, «la compra de SCI nos permite seguir profundizando en actividades y mercados muy relevantes para nuestra actividad. Ahora contamos con un área de PCI capaz de competir no solo con empresas especializadas en ingeniería, instalación o mantenimiento, sino que además, al integrarse con el resto de servicios con personas de Securitas, nos permite aportar un valor esencial con la atención y supervisión continuada de los sistemas de PCI. En definitiva, seguimos desarrollando la oferta más completa del mercado para la protección de empresas e instituciones».

INCIBE

017, nuevo número para consultas en ciberseguridad

El Instituto Nacional de Ciberseguridad (INCIBE) ha puesto en marcha el 017, el nuevo número –disponible todos los días del año, en horario de 9 a 21 horas–, que sustituirá al antiguo número de seis cifras y que ayudará a resolver asuntos relativos a dudas o consultas sobre ciberseguridad, privacidad, confianza digital, uso seguro y responsable de Internet y tecnología de forma gratuita y todos los días del año.

Este servicio es de alcance nacional, gratuito, confidencial y accesible, y está dirigido tanto a los menores y su entorno como a los ciudadanos en general que utilizan Internet, y al colectivo de empresas y profesionales que utilizan Internet y las tecnologías para el desempeño de su actividad y sus negocios.

Los usuarios del 017 recibirán atención y orientación en temáticas relativas a:

- En el caso de las empresas: cuestiones como la organización de la ciberseguridad en la empresa y principales problemas asociados a la protección de los datos e incidentes de seguridad que puedan producirse.
- En el caso de ciudadanos: la protección de dispositivos, conexiones, privacidad, tipos de fraudes e infecciones por virus y programas maliciosos.
- En el caso del entorno del menor: los padres y educadores recibirán asesoramiento psicosocial, técnico y legal sobre situaciones de riesgos y conflictos de los menores en Internet, etc.

INFORME

España, quinto país en Europa que más invierte en IoT... ¿Y en Security IoT?

España se sitúa en quinta posición como país que más invierte en IoT, por detrás de Alemania, Reino Unido, Francia e Italia. Además, se prevé que mercado de IoT en España crezca un 18% durante 2020 hasta alcanzar los más de 23 millones de euros. Pero, ¿y el Security IoT? ¿Invierten las empresas en mejorar la seguridad a través de esta nueva tecnología?

El estudio sobre el IoT elaborado por la profesional del EAE Business School, Cristina Gallego, revela que el 69% de las organizaciones que adoptan tecnologías de IoT han creado o planean crear nuevas políticas de seguridad diseñadas específicamente para abordar las necesidades y desafíos relacionados con este avance.

Los motivos que llevan a las compañías españolas a invertir en tecnología IoT son: la automatización de los procesos (26%) y la reducción de los costes operacionales (24%). Sin embargo, muchas organizaciones reconocen que encuentran dificultades para abordar este tipo de iniciativas, como son los costes iniciales (29%), las preocupaciones relacionadas con la seguridad (25%).

Brecha digital

Existe una brecha digital entre generaciones y zonas geográficas que poco a poco se va subsanando debido a iniciativas a nivel global y local. Un total de 65 ciudades españolas forman parte de la red de Smart Cities españolas. Según detalla Cristina Gallego en su estudio, Barcelona es, junto a Singapur y Londres, una de las ciudades más inteligentes del mundo.

El informe también indica que existen proyectos que se desarrollarán en nueve comunidades autónomas para convertirse en inteligentes. Las más beneficiadas son Canarias, con ayudas por 12,6 millones; la Comunidad Valenciana, por 12,3 millones; e Islas Baleares, con 10,06 millones.

ISMS FORUM

Protocolo de actuación frente a incidente en proveedor

La Asociación ha constituido recientemente un grupo de trabajo formado por responsables de seguridad de la información y continuidad de negocio, con el objetivo de responder a la necesidad de hacer frente al problema de la gestión de un incidente de seguridad que esté afectando a un proveedor de la organización. Esta prestación se realiza con acceso a sus instalaciones, a sus redes o sistemas.

Cuando el incidente en este proveedor es grave, la gestión del mismo por parte del proveedor involucra a la entidad que debe saber cómo actuar ante esta situación.

El documento ofrece una guía rápida de recomendaciones de coordinación con el proveedor afectado por el incidente, así como de medidas de monitorización, contención y vuelta a la normalidad en la propia entidad.

Este protocolo debe ser adaptado a las peculiaridades de la infraestructura y organización de cada entidad e integrada en el Plan de Respuesta a Incidentes específico de la misma; es por ello, que sus contenidos deben ser tomados como un ejemplo.

KASPERSKY

La privacidad, la gran olvidada en plena era digital

En un mundo cada vez más interconectado, en el que compartir información online es una práctica habitual, ¿ha muerto la privacidad?. El 56% de los internautas cree que la privacidad total es imposible en el mundo actual. Nueve de cada diez (89%) consumidores acceden a la red varias veces al día.

Así lo revelan los datos de un estudio de Kaspersky. Internet se ha convertido en una parte esencial de casi todo lo que hacemos -desde comprar y ver películas a cambiar de trabajo, socializar o gestionar las finanzas personales.

Nuestro comportamiento online también influye en el tipo de contenidos que visualizamos, como la publicidad personalizada, que percibimos como una invasión de nuestra privacidad total. En este contexto, ¿se puede considerar a Internet un lugar seguro o una zona de conflicto?

La investigación de Kaspersky muestra que una de cada tres personas (32,3 %) no sabe cómo proteger plenamente su privacidad online, y algunas no se creen con suficiente poder como para defenderse ante posibles ataques. Más preocupante aún, más de uno de cada diez (13%) ha perdido interés en informarse sobre cómo mejorar aún más su privacidad.

El concepto la privacidad online puede ser complejo, sin embargo, el impacto financiero e incluso emocional del mal uso de los datos online puede tener un gran alcance y sus efectos pueden perdurar durante varios años. Según datos de Kaspersky, más de la cuarta parte (26%) de los usuarios ha sufrido intrusiones a sus datos privados, una cifra que alcanza el 31% en el caso de los jóvenes entre 16 a 24 años. Para el 24% de estas personas, sus datos privados o secretos fueron robados o manipulados. Cerca de la mitad (46%) de los usuarios sufrieron accesos no autorizados a sus datos personales a través de sus cuentas online.

PROTECCIÓN CONTRA INCENDIOS

El sector de SCI nota la desaceleración económica

Como el resto de los sectores industriales, el de la seguridad contra incendios, está observando una desaceleración en el crecimiento, que se hace notar en la facturación global en torno a un 3% durante 2019, alcanzando los 2.781 millones de euros.

El sector industrial está expuesto al contexto internacional más que otros sectores, y los últimos indicadores apuntan a una ralentización de la actividad de fábrica. Por lo que las perspectivas para 2020 están en esta misma línea de desaceleración.

Los datos del INE, sobre el Índice de Producción Industrial (IPI), un indicador de carácter coyuntural que mide la evolución conjunta de la cantidad y de la calidad, sin tener en cuenta la influencia de los precios, también revelan esta tendencia, situando el crecimiento interanual en un 2,1%. En este sentido, y como riesgos para la economía española, están el entorno de desaceleración económica de la Unión Europea y las tensiones políticas en el mundo. Si bien la cifra de negocio venía mejorando desde 2015 en torno a un crecimiento del 7 %, en estos momentos la tendencia es de desaceleración.

Desde TECNIFUEGO, Asociación española de Sociedades de Protección contra Incendios, se está trabajando en un estudio más completo del sector que tenga en cuenta los diferentes equipos y sistemas, la manufactura y la instalación y mantenimiento.

CNP

La Policía Nacional celebra su 196 aniversario

El ministro del Interior, Fernando Grande-Marlaska, presidió el acto de conmemoración del 196 aniversario de la creación de la Policía Nacional, celebrado en el Complejo Policial de Canillas. Lo hizo acompañado del secretario de Estado de Seguridad, Rafael Pérez, y del director general de la Policía, Francisco Pardo.

En 1824, una Real Cédula creaba la Policía General del Reino. Se trata del primer antecedente de la actual Policía y ya recogía como principal función de los agentes «el servicio público de seguridad, garantizando el bien y la seguridad pública». Se han cumplido ya 196 años velando por la seguridad.

Funciones que convierten a la Policía Nacional en «un pilar básico de la democracia», según Grande-Marlaska que, en su intervención, subrayado también la de «velar porque podamos seguir ejerciendo nuestros derechos y libertades con plenitud y desde el respeto a la diversidad, la dignidad de la persona y todas sus expresiones», así como el carácter vertebrador de la Institución. Fernando Grande-Marlaska animó a la Policía Nacional a «mirar hacia el futuro con decisión». Y, entre los retos de la nueva etapa que se abre en el Ministerio del Interior, ha subrayado la lucha contra la violencia de género –«ese mal que tanto nos repugna»– la ciberseguridad o la delincuencia globalizada que «exige respuestas globales y coordinadas que cuenten con la máxima cooperación internacional».

ASSA ABLOY

José María Camacho, nuevo responsable de Desarrollo de Clientes Estratégicos

ASSA ABLOY Entrance Systems, la empresa de referencia en soluciones de acceso automatizado para un flujo eficaz de mercancías y personas, ha anunciado el nombramiento de José María Camacho López como responsable de Desarrollo de Clientes Estratégicos y Jefe de Ventas de su División Peatonal.

José María Camacho será el responsable de dirigir y desarrollar el equipo de ventas de obra nueva de la División Peatonal, así como de la relación directa con clientes estratégicos de la compañía. Entre sus responsabilidades está la de seguir apoyando y priorizando los valores que definen a ASSA ABLOY: sostenibilidad, seguridad, innovación, fiabilidad y comodidad de su gama de completas soluciones de acceso.

Camacho atesora una amplia y notable experiencia de más de 10 años en diversos sectores. Ha trabajado para reconocidas empresas del sector de accesos y de soluciones tecnológicas, responsabilizándose de la gestión de clientes estratégicos e impulsando las ventas y rentabilidad de los productos.

INFORME ACCENTURE

Sólo el 17% de las organizaciones se consideran líderes en ciberesiliencia

A pesar de los altos niveles de inversión en tecnologías avanzadas de ciberseguridad en los últimos tres años, menos de una quinta parte de las organizaciones están deteniendo de forma eficaz los ataques cibernéticos, así como encontrando y reparando las vulnerabilidades lo suficientemente rápido como para reducir el impacto.

Es una de las conclusiones del Tercer Estudio Anual del Estado de Resistencia Cibernética realizado por Accenture. Este informe se basa en una encuesta realizada a más de 4.600 profesionales de seguridad empresarial en todo el mundo y explora hasta qué punto las organizaciones priorizan la seguridad, la efectividad de los esfuerzos actuales de seguridad y el impacto de las nuevas inversiones relacionadas con la seguridad.

El estudio identificó un grupo de «líderes» de élite –el 17% de la muestra- que logran resultados significativamente mejores de sus inversiones en tecnología de seguridad cibernética que otras organizaciones. Estos «líderes» se caracterizan por estar entre los de mayor rendimiento en al menos tres de las cuatro categorías: detener ataques, encontrar brechas, arreglarlas y reducir el impacto de éstas.

Y por otro lado, se identifican un segundo grupo denominados «no líderes» –compuesto por el 75% de los encuestados– que tienen un desempeño promedio en términos de resistencia cibernética, pero lejos de ser rezagados.

Por ejemplo, el grupo de los «líderes» tenían cuatro veces más probabilidades de detectar una violación en menos de un día (88% frente a 22%). Y cuando las defensas fallan, el 96% de los líderes arreglaron las infracciones en 15 días o menos, mientras que casi dos tercios (64%) de los «no líderes» tardaron 16 días o más en remediar una infracción.

ALARMA Y CONTROL

GAROTECNIA
D.G.P. con el nº 2.276
Avda. Leonardo Da Vinci 8, 202-203.
Parque Empresarial Carpetania
28906 Getafe (Madrid)
Tel: 91 684 77 67

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

GESTIÓN DE VISITAS

PECKET
Las visitas a tu empresa gestionadas de forma inteligente
+34 91 476 80 00
info@pecket.es
www.pecket.es

CONTROL DE ACCESOS ACTIVO

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

BIOSYS
(Sistemas de Tecnología Aplicada)
C/ Cinca, 102-104
08030 BARCELONA
Tel. 93 476 45 70
Fax. 93 476 45 71
comercial@biosys.es - www.biosys.es

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

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

insidesales@hidglobal.com
www.hidglobal.mx

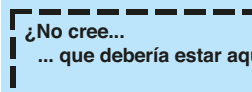
Avda. Roma, 97
08029 BARCELONA
Tel.: 93 439 92 44

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

Pol. Lanbarren - C/Arkotz 9
20180 Oiartzun (Gipuzkoa)
Spain
Tl: +34 943 344 550
www.saltosystems.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

PROTECCIÓN CONTRA INCENDIOS

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

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

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

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

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

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

PROTECCIÓN CONTRA INTRUSIÓN. ACTIVA

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

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

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

DAITEM
Calle Miguel Yuste, 16, 28037 Madrid
91 375 08 04
www.daitemspain.es

TELECOMUNICACIONES

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

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

comercial@alai.es • www.alaisecure.com

VIGILANCIA POR TELEVISIÓN

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

¿No cree...
... que debería estar aquí?

El directorio es la zona más consultada de nuestra revista.

Módulo: 660€/año*

Más información:
Tel.: 91 476 80 00
e-mail: publi-seguridad@epeldano.com
* Tarifa vigente 2020

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.
C/ Hierro, 2B
28850 Torrejón de Ardoz

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

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

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.
Av. Transición Española 24, 4ª Izq.
28108. Alcobendas.
Madrid

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

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

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

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

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

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

EUROMA
C/ Emilia 55, local 4.
28029 Madrid
Telf.: 91 571 13 04
Fax: 91 570 68 09
euroma@euroma.es
www.euroma.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

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

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

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

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

INSTALACIÓN Y MANTENIMIENTO

VIGILANCIA Y CONTROL

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

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

FUNDADA EN 1966

INSTALACIONES A SU MEDIDA

ISO 9001

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

SECURITAS SEGURIDAD ESPAÑA
C/ Entrepeñas, 27
28051 Madrid
Tel.: 912 776 000
email: info@securitas.es
www.securitas.es

CAPITULO 143 – ESPAÑA
143 CHAPTER - SPAIN

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

Asociación Española de Ingenieros de Seguridad
Avda. del Brasil Nº 29, Centro de oficinas
28020 – Madrid
aeinse@aeinse.es
www.aeinse.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 2020

TRANSPORTE Y GESTIÓN DE EFECTIVO

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

CENTRALES DE RECEPCIÓN Y CONTROL

MATERIAL POLICIAL

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

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

Certificación: ISO 9001

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

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

¿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 2020

CUADERNOS DE SEGURIDAD

Suscríbase

RELLENE SUS DATOS CON LETRAS MAYÚSCULAS (fotocopie este boletín y remítanoslo)

DATOS PERSONALES

Empresa: ..... Cargo/Dpto.: .....

D./Dña.: ..... CIF/NIF: .....

Dirección: ..... C. P.: .....

Localidad: ..... Provincia: ..... País: .....

Teléfono: ..... E-mail: .....

Actividad empresarial: .....

FORMA DE PAGO

☐ Adjunto cheque nominativo a nombre de Ediciones Peldaño, S. A.

☐ Con cargo a mi cuenta corriente o libreta de ahorros:

IBAN: ..... Entidad: ..... Oficina: ..... DC: ..... Número de cuenta: .....

☐ Tarjeta de crédito (VISA y MasterCard):

...../...../...../..... Fecha de cad.: ...../.....

☐ Transferencia bancaria a Ediciones Peldaño, S. A., en La Caixa:

IBAN	ENTIDAD	OFICINA	D.C.	NÚMERO DE CUENTA
E S 8 0	2 1 0 0	3 9 7 6	2 1	0 2 0 0 1 0 7 8 9 7

Firma:

TARIFAS (válidas durante 2020)

ESPAÑA

☐ 1 año: **98€** (9 números) ☐ 2 años: **174€** (18 números)

EUROPA

☐ 1 año: **130€** (9 números) ☐ 2 años: **232€** (18 números)

RESTO

☐ 1 año: **140€** (9 números) ☐ 2 años: **252€** (18 números)

* Precios con IVA incluido

☐ Deseo recibir Newsletters de información sectorial.

☐ MIS DATOS NO SERÁN CEDIDOS A TERCEROS. Deseo recibir comunicaciones de promociones y publicitarias.

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**

ENVÍA EL CUPÓN DE SUSCRIPCIÓN A:
Ediciones Peldaño, S. A.
Avda. del Manzanares, 196 | 28026 MADRID
Más información: 902 35 40 45

Peldaño
Si lo prefieres, llámanos o envíanos un email a **suscripciones@peldano.com** y nosotros nos encargamos de gestionarlo.

pecket

Send. Scan. Meet. pecket.es

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

TOTAL SOLUTION PROVIDER

CCTV | Intrusion | Intercom | Access Control

El futuro de la seguridad pasa por la convergencia de todos los elementos de seguridad (CCTV, Intercom, Intrusión, Control de Accesos) en lo que llamamos Internet of Security Things. Hikvision, como Total Solution Provider, es el fabricante que ofrece mayores garantías de interoperabilidad, con dispositivos basados en inteligencia artificial y algoritmos de deep learning desarrollados por nuestro equipo de más de 16.000 ingenieros de I+D en todo el mundo.

Hikvision Iberia
Calle de la Almazara, 9
28760 Tres Cantos, Madrid
T +34 91 7371655
info.es@hikvision.com

www.hikvision.com/es