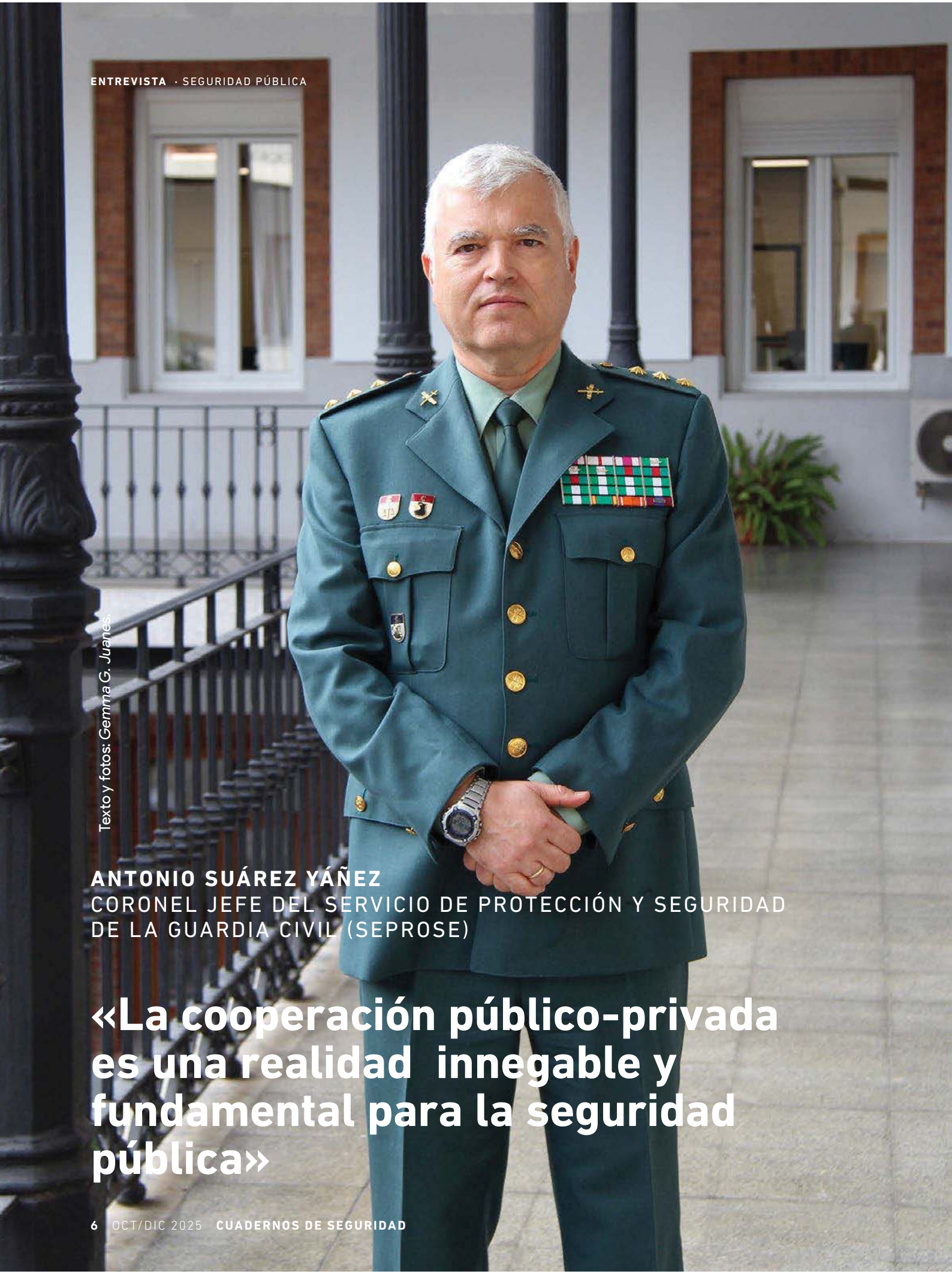


Texto y fotos: *Gemma G. Juanes*.

ANTONIO SUÁREZ YÁÑEZ
CORONEL JEFE DEL SERVICIO DE PROTECCIÓN Y SEGURIDAD DE LA GUARDIA CIVIL (SEPROSE)

«La cooperación público-privada es una realidad innegable y fundamental para la seguridad pública»

«POTENCIAR LA COMUNICACIÓN BIDIRECCIONAL Y COLABORACIÓN CON EL SECTOR PRIVADO E INICIAR EL PROCESO DE DIGITALIZACIÓN TOTAL TANTO DE CONTROL ADMINISTRATIVO COMO DE GESTIÓN DE HABILITACIONES, SON DOS DE LOS OBJETIVOS MARCADOS POR EL CORONEL ANTONIO SUÁREZ YÁÑEZ TRAS ASUMIR LA JEFATURA DEL SEPROSE DE LA GUARDIA CIVIL. EN ESTA ENTREVISTA CON CUADERNOS DE SEGURIDAD DESGRANA LAS PRIORIDADES Y PROYECTOS DE CARA A 2026.

—Tras su nombramiento como responsable del Servicio de Protección y Seguridad (SEPROSE) de la Guardia Civil, ¿qué objetivos y líneas estratégicas se ha marcado?

—La verdad es que esta pregunta, aunque parece sencilla, es bastante compleja de responder, sobre todo por la panoplia de responsabilidades internas y externas asociadas a la seguridad que tenemos en el Servicio.

Sintéticamente, el objetivo general que me he marcado es el de alcanzar una mejora sustancial en cantidad y calidad en tres grandes ejes:

1. Las colaboraciones que se realizan con el sector privado a través de los programas COOPERA y PLUS ULTRA, en las que vamos a incrementar en la medida de lo posible nuestro nivel de participación en eventos, la dinamización de las jornadas sectoriales a través de los grupos de coordinación y hacer una revisión sobre los productos de comunicación que difundimos.

2. Seguridad privada. En la vertiente de acciones de control administrativo de la seguridad privada responsabilidad de la Guardia Civil, así como de la dirección operativa de la seguridad privada bajo responsabilidad de la Guardia Civil y de aquella que se encuentra en su demarcación.

En cuanto al control administrativo de Guardas Rurales, instructores de tiro de seguridad privada y centros de formación, se está trabajando en líneas de mejora para ser más cercanos, agilizar y facilitar trámites, mejoras normativas específicas y la realización de labores de control o inspectoras más eficaces.

Sobre la dirección operativa de la seguridad privada, quiero hacer una campaña de sensibilización a todas nuestras unidades territoriales para que tengan muy presente en el desarrollo de sus servicios a cualquiera de las figuras de seguridad privada contempladas en la Ley, tanto durante los servicios ordinarios de seguridad ciudadana como en circunstancias excepcionales, ya que contamos con unos colaboradores excepcionales con vocación de apoyo a las Fuerzas y Cuerpos de Seguridad que desgraciadamente infrautilizamos, en la mayoría de los casos por desconocimiento. Y de ese desconocimiento en gran parte o en su totalidad, yo soy el responsable.

3. El control técnico asociado a edificios e instalaciones cuya protección está encomendada a la Guardia Civil. Incrementando en cantidad y en calidad los estudios de seguridad, teniendo a un equipo técnico perfectamente formado para infraestructuras críticas y actualizado en medios técnicos de seguridad y tendencias normativas.

—¿Cuáles son actualmente las prioridades y proyectos de cara a 2026 para el SEPROSE?

—Para el 2026 espero materializar los siguientes proyectos:

-Ámbito de colaboración con el sector privado:

• Realización de al menos 2 jornadas sectoriales por año para poder abordar de forma eficaz la problemática común y una respuesta más adecuada.

• Organización de 2 visitas al año a Unidades de la Guardia Civil para fomentar el conocimiento mutuo.

• Ofrecer al sector la capacidad de formular denuncias digitalmente y de manera centralizada a través de su representante legal vía la Cibercomandancia, sobre cualquier delito sin autor conocido del que sean víctimas, sea en el ciberespacio o delitos físicos producidos en demarcación del Cuerpo.

- Ámbito gestión administrativa de la seguridad privada:

• Iniciar el proceso de digitalización total, tanto de control administrativo como de gestión de habilitaciones.

- Ámbito de control técnico de edificios e infraestructuras:

• Tener una formación técnica actualizada, tanto en medios técnicos como en la nueva normativa a implantar en materia de ciberseguridad y de resiliencia, y también la realización de un minucioso seguimiento a documentos dimanantes de la Agencia Europea de Protección de Datos.

—Existe una clara apuesta de la Guardia Civil por la seguridad privada plasmada desde hace años en programas de colaboración como COOPERA y Plus Ultra. ¿Cómo se potenciarán en los próximos años estos programas de colaboración?

—Estos programas han estado tan bien diseñados desde el año 2021 que perduran hasta nuestros días en plena vigencia, y desde luego la Guardia Civil va a seguir apostando por ellos.

Como en todos los aspectos de la vida siempre hay margen de mejora; a la vista de la experiencia adquirida a esta fecha, desde el SEPROSE vamos a apostar por fomentar el conocimiento mutuo para mejorar la eficacia desde ambos mundos. Hoy por hoy la cooperación público-privada es una realidad innegable y fundamental para la seguridad pública y esta cooperación nos permite poder mantener nuestro estilo de vida.

Además, quiero potenciar la comunicación bidireccional con el sector y hacerles partícipes de los éxitos conseguidos gracias a la colaboración, y también de los aspectos en los que debemos de seguir trabajando.

En lo que concierne a Plus Ultra tengo varias iniciativas del departamento sobre la mesa, es quizás el campo que mayor capacidad de evolución ofrece, pero la complejidad de avanzar en este campo radica en la volubilidad geopolítica que estamos viviendo. Son tiempos convulsos, en los que las expansiones internacionales de nuestras empresas a países occidentales nos preocupan menos a nivel securitario; se da por garantizada la seguridad de la inversión y del personal, no obstante, los nuevos "nichos de mercado" apuntan en otra dirección y francamente es muy complicado dar con la "tecla" que nos permita contribuir a facilitar información al inversor nacional para que pueda hacer un correcto balance riesgo-beneficio.

«El sector de la seguridad privada tiene vocación colaborativa con todas las FCS y eso se palpa en el trato diario»

—¿Cómo valora la colaboración actual entre el SEPROSE y las empresas y profesionales de seguridad privada? ¿Qué mecanismos de coordinación son los más eficientes?

—Excepcional. Como ya he mencionado, este sector en particular tiene vocación colaborativa con todas las FCS y eso se palpa en el trato diario.

El mejor mecanismo de coordinación es el trato diario o frecuente y la confianza mutua. Lamentablemente la coordinación debe de estar por encima de las relaciones personales (aunque esto lo facilite mucho), y nosotros a través del programa COOPERA fundamentalmente estamos manteniendo estos mecanismos, aunque no de forma exclusiva.

—Con una visión general, ¿qué valoración haría de

la situación actual en la que se encuentra el sector de la seguridad privada?

—Personalmente y en su conjunto, creo que el sector goza de una excepcional salud con un prometedor futuro.

Las circunstancias en las que actualmente se encuentran las FCS unido al reto demográfico que involucra a la mayoría de los países de la UE, advoca forzosamente en una mayor asunción de competencias por parte del sector.

Vuelvo a dar mi opinión, el desafío en este punto creo que radica en garantizar unos servicios profesionales y de calidad orientados a la confianza del cliente, y también a la búsqueda de personal cualificado que pueda asumir estos cometidos.

-¿Qué aspectos cree que se deberían potenciar o mejorar en el sector de la seguridad privada (formación, especialización, tecnología...)?

—Mi impresión es que se debe de abordar un proceso global de ensalzamiento del sector, fomentando la calidad de los profesionales con una buena formación y selección, trabajando en generar un sentimiento de vocación corporativa, buscando el talento y conservándolo, y haciendo buenas campañas divulgativas a la sociedad civil para que pueda valorar el gran trabajo que se realiza y que revierte en la ciudadanía.

Otro aspecto de mejora en el que llevo pensando varios meses, y espero muy pronto poder afrontarlo como prioridad es la comunicación. Me explico: desde el sector de la seguridad privada hacia la Guardia Civil, tenemos el 062, o los números de los COS que permiten participar cuantas incidencias se consideren necesarias, sin embargo, a la inversa, en alguna ocasión suele costarnos mucho poder contactar de forma directa y ágil con el personal desplegado para prevenir o advertir sobre determinadas situaciones, riesgos o emergencias, o también, para requerir su inmediata colaboración en caso necesario.

-En un entorno de riesgos en constante evolución, ¿cuáles considera que son las principales amenazas (físicas o híbridas) a las que se enfrentan hoy las Infraestructuras Críticas bajo su demarcación, y cómo las aborda el SEPROSE?

—Las principales amenazas son ambas. La seguridad física es un desafío constante sobre el que siempre vamos a trabajar, es imposible asumir la seguridad de una infraestructura crítica sin tener en cuenta una acción física. El mayor riesgo desde mi punto de vista consiste en anclarse en el pasado, acomodarse y no evolucionar nuestros planes, tanto en prevención como en reacción a la realidad o las nuevas tendencias.

Las acciones físicas directas (robos, sabotajes o atentados) que pueden perpetrarse sobre una infraestructura crítica, de un modo u otro pueden ser relativamente

previsibles, sin embargo, las acciones indirectas, que no tienen como finalidad perturbar el funcionamiento de esa infraestructura, aunque puedan hacerlo (robo de cobre, de maquinaria, de chatarra, de fluido de cualquier tipo o de combustible), tienen una evolución más rápida en función de diversos parámetros (precio del cobre, combustible, etc.), y esto implica evaluar riegos cada vez que se informa de estos cambios de tendencia delictiva a través de nuestras unidades de inteligencia.
En lo que toca a las amenazas híbridas, no queda otro remedio que formarse e informarse continuamente, para poder dotarse de medios que nos permitan por un lado poder investigar, prevenir y combatir este tipo de delitos, y por otro saber que las infraestructuras bajo nuestra responsabilidad están dotadas de una buena capacidad de defensa ante este tipo de amenazas.

—Mirando hacia el futuro, ¿qué cambios o mejoras normativas considera que son necesarios para optimizar la capacidad de respuesta y protección del SEPROSE en el ámbito de las infraestructuras críticas?
—Todavía estamos a la espera de la trasposición nacional de las directivas NIS2 y CER que consideramos fundamentales para acometer esa capacidad de respuesta y protección, y esperemos que esto ocurra pronto. En su actual redacción, parece necesario al menos un desarrollo reglamentario que precise cómo abordar determinados aspectos que en el borrador de las leyes de trasposición se enumeran de forma genérica.
Y sí, también coincido en la clamorosa opinión del sector para proceder a una actualización de la Ley de Seguridad Privada y a un nuevo reglamento de desarrollo, a poder ser de fecha posterior a la Ley a la que está vinculado.
Aunque para ambos casos pienso que un exceso regulatorio en este ámbito puede contribuir a una prematura obsolescencia normativa. ✱

TARGET TECNOLOGIA

TU SOCIO EXPERTO EN SISTEMAS DE SEGURIDAD Y EMERGENCIA

Security & Safety

Inspección por Rayos X

Inspección de personas

Detección de explosivos y narcóticos

Equipamiento especial

Sistemas anti-embestida

Defensa

Equipamientos NRBQe

Material de Campamento y Emergencias

Robótica pesada y sistemas autónomos (UGV)

Drones

Sistemas anti-dron

Dron autónomo y cautivo

Servicios

Alquiler de equipamiento

Mantenimiento

Asesoramiento

Consultoría

target-tecnologia.es

JULIO ALCOCER. MANAGER DE SEGURIDAD ESPAÑA. DIA

«Nuestra prioridad es garantizar una experiencia de cliente fluida, donde la seguridad actúe como un elemento de protección invisible»

Texto: Gemma G. Juanes.
Fotos: DIA

«Para mejorar la eficiencia operativa y la satisfacción del cliente, es fundamental que nuestras iniciativas de seguridad se integren de manera fluida y discreta en el flujo de trabajo diario de nuestros empleados», explica Julio Alcocer, manager de Seguridad España de Dia, red de tiendas de proximidad con 2.300 tiendas, 1.500 franquicias y 14.000 empleados en España.

En esta entrevista con Cuadernos de Seguridad, donde aborda la estrategia de seguridad de la compañía, y la importancia de fomentar una cultura de seguridad, Alcocer asegura que «la concienciación y la responsabilidad en materia de seguridad deben ser compartidas por todos los miembos de la organización».

—Hoy en día, ¿cómo está estructurado el departamento de Seguridad de Dia? ¿Cuál es su infraestructura?

—Con el fin de fortalecer nuestra conexión con el negocio, el departamento de Seguridad de Dia ha adoptado una estructura horizontal, marcando un hito en nuestra evolución organizativa. En el corazón de esta nueva configuración se encuentra una unidad de dirección central, que no solo coordina las estrategias de seguridad a nivel global, sino que también colabora estrechamente con los directores de Seguridad delegados.

Estos directores, a su vez, son piezas clave en el engranaje, ya que gestionan una dirección operativa que replica con exactitud la estructura de las delegaciones de Dia. Esta duplicación no es casual; busca asegurar una coherencia y una integración sin fisuras de las políticas y procedimientos de seguridad en todas nuestras operaciones, desde la sede central hasta el último punto de venta.

La implementación de esta estructura horizontal permite una comunicación más fluida y una toma de decisiones ágil, eliminando barreras jerárquicas innecesarias. De esta manera, cada director de Seguridad delegado se convierte en

un punto de contacto vital para las necesidades específicas de su región, asegurando que la seguridad no sea un ente aislado, sino una parte intrínseca y proactiva del día a día del negocio. Este enfoque no solo mejora la eficiencia operativa, sino que también fomenta una cultura de seguridad compartida, donde cada miembro de Dia se siente parte de la protección de nuestros activos y operaciones.

—Actualmente, ¿cuáles son los puntos básicos en los que se basa la estrategia de Seguridad de Dia?

—Los puntos básicos son:

Para mejorar la eficiencia operativa y la satisfacción del cliente, es fundamental que nuestras iniciativas de seguridad se integren de manera fluida y discreta en el flujo de trabajo diario de nuestros empleados. Queremos que la gestión de la seguridad sea una parte intuitiva y sin esfuerzo de sus responsabilidades, liberándolos de cargas administrativas innecesarias y permitiéndoles concentrarse en sus tareas principales. Esto no solo optimizará su productividad, sino que también contribuirá a un ambiente de trabajo más seguro y eficiente.

Al mismo tiempo, es crucial que las medidas de seguridad que implementemos sean imperceptibles para nuestros clientes. Nuestra prioridad es garantizar una experiencia de cliente fluida y sin interrupciones, donde la seguridad actúe como un elemento de protección invisible que respalda la confianza y la integridad de sus interacciones con nosotros. Queremos que los clientes perciban la seguridad como un pilar fundamental de nuestro servicio, sin que ello implique una intromisión en su experiencia o en su percepción de la eficiencia de nuestros procesos.

—¿Cree que hoy en día los departamentos de Seguridad forman parte de la estrategia empresarial y comercial de las compañías?

—Aunque tradicionalmente los departamentos de Seguridad no han sido considerados el núcleo del negocio de las compañías, su rol está experimentando una transformación significativa. Cada vez más, estos departamentos se integran de manera profunda como parte estratégica de la operativa empresarial, dejando de ser meros centros de costo para convertirse en motores de valor añadido.

Esta evolución se manifiesta en su capacidad para aportar soluciones que mejoran sustancialmente la eficiencia y la productividad general de la organización. La seguridad ya no se percibe únicamente como una barrera o un mecanismo de contención de riesgos, sino como un facilitador que optimiza procesos, protege activos críticos y permite la innovación con mayor confianza. Este valor, que antes podía ser subestimado, se reconoce y se exige con una fuerza creciente en el panorama empresarial actual.

En este contexto de cambio, un elemento fundamental y de vital importancia hoy en día es la

«La seguridad se está consolidando como un pilar estratégico que impulsa la competitividad y la resiliencia de las empresas modernas»

colaboración. La seguridad no puede operar de forma aislada; requiere una interconexión constante y fluida con todos los demás departamentos de la empresa. La colaboración se convierte en la piedra angular para:

-Identificar riesgos emergentes: Trabajando conjuntamente con áreas como TI, Operaciones, Legal o Recursos Humanos, se puede obtener una visión holística de las vulnerabilidades y amenazas.

-Diseñar soluciones integrales: Las medidas de seguridad son más efectivas cuando se construyen con la participación y el conocimiento de quienes las van a utilizar o se verán afectados por ellas.

-Fomentar una cultura de seguridad: La concienciación y la responsabilidad en materia de seguridad deben ser compartidas por todos los miembros de la organización, no solo por el departamento especializado. La colaboración es clave para difundir este mensaje y asegurar su adopción.

-Optimizar la respuesta a incidentes: Una coordinación eficaz entre los distintos equipos es crucial para minimizar el impacto de cualquier incidente de seguridad, desde su detección hasta su resolución y el análisis post-mortem.

-Alinear la seguridad con los objetivos de negocio: La colaboración permite que las estrategias de seguridad estén perfectamente sincronizadas con las metas y prioridades estratégicas de la empresa, garantizando que las inversiones en seguridad respalden directamente el crecimiento y la sostenibilidad.

En resumen, la seguridad se está consolidando como un pilar estratégico que impulsa la competitividad y la resiliencia de las empresas modernas. La colaboración, interna y externa, es la clave para desbloquear todo el potencial de este departamento y asegurar que su contribución al negocio sea cada vez más significativa y tangible.

—Un elemento fundamental hoy en día es la colaboración y coordinación entre departamentos en aspectos de seguridad, ¿cómo se articula esta función transversal con las diferentes áreas de la compañía?

—Para ejercer esta función con fluidez, es fundamental ubicar al departamento de Seguridad en un área con acceso directo a otros departamentos clave. En el caso de Dia, esta área es la de Operaciones, lo que facilita la recopilación de incidencias de las tiendas y asegura un acceso constante al resto de los departamentos que brindan servicio al negocio. Esta ubicación estratégica permite una comunicación fluida y una coordinación eficaz, vital para una respuesta rápida y eficiente ante cualquier situación que afecte la seguridad.

Además, la integración del

AYR

Ecosistema inteligente de control de accesos y seguridad.

Visítanos en SICUR 26, stand 10B38
(espacio APECS). ¡Allí te esperamos!

int EGRA APP

works with the Google Assitant
WORKS WITH amazon alexa
Available on the App Store
ANDROID APP ON Google play

Ecosistema completo int EGRA

int LOCK PRO
int PASS
int ERPHONE
int NEX
int KEY PRO
int KEYPAD
int KEEP
int ALARM

+34 965 552 200
www.ayr.es

¡Descarga el catálogo! →

departamento de Seguridad dentro del área de Operaciones promueve una visión holística de los riesgos y las vulnerabilidades, ya que se encuentra en contacto directo con la realidad operativa de las tiendas. Esto no solo mejora la capacidad de reacción ante incidentes, sino que también contribuye a la implementación de medidas preventivas más robustas y adaptadas a las necesidades reales del negocio. La colaboración interdepartamental se ve reforzada, permitiendo que la seguridad no sea solo una función reactiva, sino una parte integral de la estrategia operativa de la empresa.

—¿Qué tendencias emergentes en seguridad considera que tendrán un mayor impacto en el futuro del sector de grandes superficies?

—La integración de sistemas es un pilar fundamental en la estrategia de cualquier organización moderna. Permite la unificación de diversas plataformas y aplicaciones (como las de detección, análisis y toma de acciones) que, de otro modo, funcionarían de forma aislada. Este proceso no solo optimiza la eficiencia operativa, sino que también facilita una visión holística de los datos, lo cual es crucial para la toma de decisiones informada.

La gestión y el análisis del dato son componentes interdependientes que se benefician enormemente de la integración. Una vez que los sistemas están interconectados, los datos fluyen libremente, eliminando silos de información y garantizando que los equipos tengan acceso a la información más relevante y actualizada. Esto permite:

-Detección proactiva: La capacidad de detectar anomalías, tendencias o patrones emergentes en tiempo real, lo cual es vital para la seguridad, el rendimiento y la satisfacción del cliente.

-Análisis profundo: La consolidación de datos de múltiples fuentes posibilita un análisis más completo y sofisticado, revelando insights que serían inalcanzables con sistemas fragmentados. Esto incluye análisis predictivos, prescriptivos y diagnósticos.

-Toma de acciones estratégicas: Basándose en los análisis generados, las organizaciones pueden tomar decisiones más rápidas y precisas, optimizando procesos, mitigando riesgos y capitalizando nuevas oportunidades.

El objetivo final de esta integración y gestión de datos es potenciar la capacidad de una organización para adaptarse, innovar y prosperar en un entorno cada vez más complejo y basado en datos.

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

—La demanda de un personal de seguridad altamente capacitado y especializado es cada vez mayor. Las empresas y organizaciones buscan profesionales que no solo posean habilidades básicas de vigilancia, sino que también estén familiarizados con las últimas tecnologías de seguridad, la gestión de crisis, los protocolos de emergencia y la atención al cliente. Esta profesionalización implica:

-Formación continua: Inversión en programas de capacitación avanzados que cubran desde el uso de sistemas de videovigilancia

inteligentes hasta la ciberseguridad y la respuesta ante amenazas emergentes.

-Certificaciones y acreditaciones: La obtención de certificaciones reconocidas a nivel nacional e internacional valida las competencias del personal y garantiza un estándar de calidad.

-Desarrollo de habilidades blandas: La comunicación efectiva, la empatía y la capacidad de desescalar situaciones conflictivas son tan importantes como las habilidades técnicas.

-Carrera profesional: Establecer rutas de carrera claras para el personal de seguridad, lo que incentiva la permanencia y el desarrollo a largo plazo.

Abordar estos desafíos requiere un enfoque multifacético que incluya la mejora de las condiciones laborales, la inversión en programas de formación atractivos, la promoción de la profesión de seguridad como una carrera de valor y la optimización de los recursos mediante la tecnología sin comprometer la calidad del servicio.

—¿Cree que es necesario vincular a los empleados en la importancia del papel de la seguridad en la compañía y potenciar la concienciación?

—Es fundamental realizar formaciones continuas sobre el correcto uso de los sistemas. Sin una buena política de comunicación que explique los beneficios de aplicar las pautas de seguridad y los procedimientos que se establecen, la adhesión por parte de los usuarios será mínima. Es crucial que estas formaciones no solo se centren en el "cómo", sino también en el "por qué", destacando las implicaciones positivas para la eficiencia operativa y la protección de datos sensibles, tanto a nivel individual como organizacional. La comunicación debe ser bidireccional, permitiendo a los empleados expresar sus dudas y ofrecer retroalimentación, lo que fomenta un sentido de propiedad y responsabilidad compartida en la seguridad de la información.

—¿Qué papel juega la seguridad en la experiencia de cliente en este tipo de establecimientos?

—Nuestro objetivo primordial es forjar un ambiente donde tanto nuestros valiosos asociados como nuestros estimados clientes se sientan completamente seguros. Esta seguridad es la piedra angular sobre la cual construimos una experiencia de servicio y compra inigualable y verdaderamente placentera. Sin embargo, la clave reside en que esta seguridad se perciba de manera inherente, que se sienta en cada interacción, en cada rincón de nuestras instalaciones, sin que sea una medida obvia o visible que pueda generar inquietud o incomodidad.

Buscamos que la seguridad sea una sensación intrínseca, un telón de fondo imperceptible pero omnipresente que permita a todos desenvolverse con total tranquilidad y confianza. Queremos que la protección sea un pilar tan fundamental que su presencia se dé por sentada, permitiendo que la atención se centre plenamente en el disfrute del servicio y la satisfacción de la compra, sin distracciones ni preocupaciones. Esta aproximación sutil pero efectiva a la seguridad es lo que nos permitirá garantizar una experiencia verdaderamente superior y memorable para todos. ✱

JAVIER VILLARUBIA SÁNCHEZ. SECURITY MANAGER I LOSS PREVENTION. MEDIAMARKT ESPAÑA

«Buscamos que cada cliente disfrute de la tecnología y acceda a nuestros servicios con total libertad, en un entorno seguro y confiable»

Texto: Gemma G. Juanes.
Fotos: MediaMarkt

«La seguridad juega un papel absolutamente fundamental en la experiencia del cliente y en MediaMarkt la concebimos como un auténtico facilitador de confianza». Así lo asegura Javier Villarubia Sánchez, Security Manager de MediaMarkt España, en esta entrevista con Cuadernos de Seguridad, en la que aborda los puntos clave de la estrategia de seguridad de la compañía, así como aquellas tendencias emergentes en seguridad que, bajo su punto de vista, tendrán un mayor impacto en el futuro del sector de grandes superficies.

—Hoy en día, ¿cómo está estructurado el departamento de Seguridad de MediaMarkt? ¿Cuál es su infraestructura?

—El departamento de Seguridad de MediaMarkt está diseñado para dar respuesta integral a las necesidades de seguridad de la compañía. Está estructurado en tres áreas clave:

1. Área de Operaciones de Seguridad:
Dirige la operatividad diaria en nuestras tiendas: gestiona la relación con nuestros proveedores de seguridad, coordina la información delictiva, analiza riesgos, asigna recursos, crea procedimientos y resuelve incidencias. Para garantizar una cobertura eficiente, contamos con una organización regional en las zonas de Cataluña, Centro y Andalucía, que brinda soporte directo a las tiendas de MediaMarkt en España. Además, trabajamos en estrecha colaboración con nuestro Centro de Control de Seguridad para asegurar una respuesta rápida y coordinada ante cualquier eventualidad.
2. Área de Sistemas de Seguridad:
Enfocada en la mejora continua y la implementación de soluciones tecnológicas avanzadas que nos permiten prevenir y predecir riesgos en nuestras instalaciones. Nuestro objetivo es establecer un modelo estandarizado de sistemas que optimice costes sin comprometer

la seguridad: integramos tecnologías innovadoras que refuerzan la protección de nuestras instalaciones y garantizan un entorno seguro para nuestro equipo y para nuestros clientes.

3. Área de Gestión de Delitos Fraudulentos:

Centrada en investigar y prevenir fraudes relacionados con transacciones digitales. Trabajamos en coordinación con Unidades Especializadas de las Fuerzas y Cuerpos de Seguridad del Estado (FFCCSS) para combatir delitos tecnológicos, fraudes y ciberdelincuencia. Nuestro enfoque proactivo nos permite proteger a nuestros clientes y mantener la integridad de nuestros procesos comerciales.

—Actualmente, ¿cuáles son los puntos básicos en los que se basa la estrategia de Seguridad de MediaMarkt?

—Nuestra estrategia tiene un enfoque integral y proactivo, diseñada para proteger tanto el patrimonio de la compañía como la seguridad de las casi 7.000 personas que forman parte de MediaMarkt y de nuestros clientes. Todo ello se sustenta en un modelo predictivo y anticipativo, basado en procedimientos rigurosos y análisis continuos de riesgos, que nos permite identificar vulnerabilidades, implementar medidas preventivas y responder con agilidad ante cualquier eventualidad.

Uno de los pilares de la estrategia es la protección patrimonial integral, que abarca desde la cadena de suministro hasta la venta final al cliente. No nos limitamos a reaccionar ante incidentes: trabajamos con un enfoque preventivo mediante sistemas avanzados de monitorización, gestión continua de inventarios y tecnología de seguridad física y tecnológica. Además, cumplimos con todas las normativas aplicables en materia de seguridad, garantizando no solo la protección de nuestros activos, sino también el cumplimiento legal en cada uno de nuestros procesos.

El segundo pilar es la protección de las personas: empleados y clientes. Para ello, hemos desarrollado protocolos de seguridad laboral, formación continua en prevención de riesgos y sistemas que garantizan un entorno seguro.

—¿Cree que hoy en día los departamentos de Seguridad forman parte de la estrategia empresarial y comercial de las compañías?

—En un entorno cada vez más complejo y competitivo, la seguridad juega un papel clave en la experiencia del cliente, la reputación de la marca y la sostenibilidad del negocio.

Un departamento de Seguridad bien estructurado contribuye a minimizar las pérdidas desconocidas, como el fraude, el hurto o los incidentes operativos, lo que impacta directamente en la rentabilidad de la empresa. En el caso de MediaMarkt, garantizar la seguridad de nuestros clientes y equipo o la protección de las instalaciones físicas no solo reduce riesgos, sino

que también mejora la experiencia del cliente y fideliza su relación con la marca.

Además, la implementación de políticas y procedimientos de seguridad eficientes permite a las empresas anticiparse a posibles amenazas, optimizar recursos y reducir costes a largo plazo. Esto se traduce en una ventaja competitiva, ya que las compañías que integran la seguridad en su estrategia global están mejor preparadas para adaptarse a los cambios del mercado y responder a las expectativas de sus clientes.

Creo que los departamentos de Seguridad ya no son un área secundaria o reactiva, sino un componente estratégico que contribuye al crecimiento, la innovación y la sostenibilidad de las empresas. Su integración en la estrategia empresarial y comercial no solo protege el negocio, sino que también impulsa su éxito a largo plazo.

—Un elemento fundamental hoy en día es la colaboración y coordinación entre departamentos en aspectos de seguridad, ¿cómo se articula esta función transversal con las diferentes áreas de la compañía?

—La seguridad en MediaMarkt no opera como un área aislada, sino como un elemento transversal que requiere una coordinación constante y efectiva con múltiples áreas de la compañía. Por ello, nuestro departamento de Seguridad mantiene una política que integra y alinea los objetivos de seguridad con las necesidades estratégicas de la empresa, trabajando de la mano con otros departamentos clave para garantizar la protección integral del negocio.

«El departamento de Seguridad mantiene una política que integra y alinea los objetivos de seguridad con las necesidades estratégicas de la empresa»

Este trabajo en equipo se articula de varias maneras:

-Departamento de Auditoría: Trabajamos estrechamente para identificar posibles riesgos y vulnerabilidades en los procesos operativos, asegurando que las medidas de seguridad implementadas sean eficaces y cumplan con los estándares internos y externos.

-Inventarios: Colaboramos en la prevención y detección de pérdidas desconocidas, como el hurto o los errores en la gestión de stock, mediante la implementación de controles y procedimientos que optimizan la trazabilidad y la seguridad de los productos.

-PRL (Prevención de Riesgos Laborales): Coordinamos esfuerzos para garantizar la seguridad física del equipo, asegurando que las instalaciones cumplan con las normativas de seguridad y salud laboral.

-Departamento Legal: Mantenemos una comunicación fluida para abordar aspectos legales relacionados con la seguridad, como la gestión de incidentes, la protección de datos y el cumplimiento normativo.

-Atención al Cliente: Trabajamos

Hanwha Vision

Opciones de lente fija de hasta 60 mm

8fps o 30fps

Claramente preciso. Precisamente claro.

Soluciones de videovigilancia térmica QVGA de largo alcance con Inteligencia Artificial

juntos para resolver incidencias que afectan la experiencia del cliente, como fraudes en compras online o problemas de seguridad en tiendas, asegurando una respuesta rápida y eficaz.

-Relaciones Laborales: Colaboramos en la formación y concienciación de los empleados sobre políticas de seguridad, fomentando una cultura de prevención y responsabilidad compartida.

-Seguridad IT: Coordinamos esfuerzos para proteger la infraestructura tecnológica de la empresa, abordando amenazas como la ciberdelincuencia y garantizando la seguridad de los datos y sistemas.

En MediaMarkt, entendemos que la seguridad es un esfuerzo colectivo, y esta colaboración transversal es fundamental para alcanzar nuestros objetivos estratégicos y garantizar un entorno seguro.

—¿Qué tendencias emergentes en seguridad considera que tendrán un mayor impacto en el futuro del sector de grandes superficies?

—El futuro de la seguridad en el sector de grandes superficies está experimentando una transformación profunda, impulsada por la evolución tecnológica y la necesidad de adaptarse a nuevos desafíos. En este contexto, consideramos que las tendencias emergentes más impactantes serán la integración de sistemas de seguridad avanzados, la monitorización remota y la combinación inteligente de diferentes tecnologías. Estas herramientas no solo permiten una gestión más eficiente de los riesgos, sino que también optimizan los recursos disponibles, algo especialmente relevante en el sector de la seguridad donde la escasez de personal cualificado es una realidad.

Uno de los avances más prometedores es la inteligencia artificial (IA), que se está convirtiendo en un aliado estratégico para la seguridad. La IA tiene el potencial de revolucionar la forma en que abordamos la prevención y la detección de incidentes, permitiéndonos analizar grandes volúmenes de datos en tiempo real, identificar patrones de riesgo y anticipar amenazas antes de que se materialicen. En MediaMarkt, estamos analizando activamente cómo la IA puede ayudarnos a mejorar la protección de nuestros activos y optimizar nuestros procesos de seguridad.

A su vez, la monitorización remota y la interconexión de sistemas serán claves en el futuro, al facilitar la supervisión de múltiples puntos de venta y centros logísticos desde una ubicación centralizada, combinando tecnologías como videovigilancia, control de accesos y análisis de datos.

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

—Los retos a la hora de implantar una estrategia de seguridad son múltiples y requieren un enfoque estructurado, colaborativo y adaptable. Estos espacios con alta afluencia de público, diversidad de procesos operativos y activos valiosos exige no solo soluciones técnicas robustas, sino también una gestión integral que involucre a todos los niveles de la organización.

La detección y análisis de riesgos constituyen un pilar fundamental en nuestra estrategia. Ante cualquier amenaza, investigamos su origen y evaluamos su impacto en los distintos departamentos o procesos afectados. Con esa información, establecemos prioridades y diseñamos medidas que mitiguen el riesgo sin comprometer la operatividad del negocio. El objetivo es mantener un equilibrio entre seguridad y continuidad operativa,

evitando soluciones que resulten eficaces en teoría pero que generen bloqueos o interrupciones en la actividad diaria.

Otro reto esencial consiste en crear procedimientos claros y aplicables. No basta con desarrollar protocolos técnicamente sólidos: deben ser prácticos, comprensibles y fáciles de poner en marcha por todos los equipos. Muchas estrategias de seguridad fracasan precisamente en este punto: las brechas de seguridad suelen aparecer no por falta de herramientas, sino por desconocimiento o falta de adopción de los procedimientos. En MediaMarkt reforzamos este aspecto con formaciones específicas y acciones de sensibilización que garantizan que cada miembro del equipo conozca y asuma su papel en la seguridad colectiva.

La implantación y el seguimiento representan igualmente un factor decisivo. Una estrategia no se limita a su lanzamiento, sino que requiere un monitoreo constante para verificar su efectividad y adaptarla cuando sea necesario. Para ello recurrimos a indicadores de cumplimiento, auditorías internas y feedback continuo de los equipos de tienda para detectar posibles desviaciones o de mejora de procesos.

—¿Cree que es necesario vincular a los empleados en la importancia del papel de la seguridad en la compañía y potenciar la concienciación?

—Sí. El equipo representa el eslabón esencial y cohesionador que da sentido a toda la estructura y estrategia en MediaMarkt. Nuestras tres áreas y nuestros pilares estratégicos descansan, en última instancia, en la concienciación activa de cada una de las personas que forman parte del equipo.

Las personas somos capaces de detectar anomalías, comportamientos sospechosos o desviaciones de los procesos que un sistema automático podría pasar por alto. Por ello, un equipo concienciado es nuestra mejor herramienta para detectar problemas a tiempo.

Para que esta implicación resulte efectiva, ofrecemos formación constante, protocolos claros y seguros, y canales de comunicación seguros que garantizan tanto su protección como su compromiso.

—¿Qué papel juega la seguridad en la experiencia de cliente en este tipo de establecimientos?

—La seguridad juega un papel absolutamente fundamental en la experiencia del cliente y en MediaMarkt la concebimos como un auténtico facilitador de confianza. Nuestra estrategia se apoya en un principio esencial: proteger los productos y la información del cliente sin comprometer la accesibilidad, la comodidad ni la fluidez de la experiencia, independientemente de que la compra se realice en tienda, en la web o a través de la app.

Buscamos que cada cliente disfrute de la tecnología y acceda a nuestros servicios con total libertad, en un entorno seguro y confiable. Para lograrlo integramos soluciones discretas e inteligentes, como sistemas de videovigilancia modernos o sensores integrados, que refuerzan la protección de nuestros activos y garantizan la tranquilidad de quienes interactúan con MediaMarkt.

Además, existe una relación directa entre la seguridad y la satisfacción del cliente: la gestión eficaz de riesgos como el fraude, el hurto o los errores de inventario asegura la disponibilidad de los productos y fortalece la coherencia de la experiencia omnicanal.

En definitiva, no se trata solo de proteger, sino de crear un clima de confianza y normalidad en todos los puntos de contacto. Ese entorno seguro permite que la experiencia en MediaMarkt sea siempre positiva, segura y, sobre todo, memorable. ✱

BEATRIZ RIVADA RODRÍGUEZ. DIRECTORA DE SEGURIDAD. HIPER USERA

«Hoy en día los departamentos de Seguridad son una parte fundamental de la estrategia empresarial»

Texto y fotos: Gemma G. Juanes

Dice Beatriz Rivada Rodríguez, directora de Seguridad de Hiper Usera, que la «concienciación de la importancia que tiene la seguridad para los trabajadores es fundamental para el éxito de una estrategia de seguridad». Y es que ella lo tiene claro al explicar que «cuando los trabajadores se sienten integrados y con un papel importante para contribuir a un entorno seguro, se sienten más responsables y comprometidos».

Rivada Rodríguez ofrece en esta entrevista con Cuadernos de Seguridad su visión profesional ante los retos a asumir al implantar una estrategia de seguridad en una gran superficie, así como el papel que juega la seguridad en la experiencia de cliente en este tipo de establecimientos, entre otros temas.

—Actualmente, ¿cuáles son los puntos básicos en los que se basa la estrategia de seguridad de Hiper Usera?

—El departamento de Seguridad en Hiper Usera está integrado dentro de cada uno de los proyectos del negocio. Dentro de nuestros puntos prioritarios y estratégicos trabajamos para mejorar la capacidad de prevenir de manera rápida y exhaustiva los riesgos para el negocio y/o para las personas, con medios tanto de seguridad física, tecnológica como metodológica, actualizándonos en la medida necesaria según avanzan los niveles delincuenciales, creando procedimientos que sean capaces de generar una integración de todo el personal que lo componemos.

Una de las partes importantes dentro de la seguridad la adquiere nuestro departamento de IT, dado el riesgo económico y otros añadidos que podría suponer un ataque informático.

—¿Cree que hoy en día los departamentos de Seguridad forman parte de la estrategia empresarial y comercial de las compañías?

—Hoy en día los departamentos

de Seguridad son una parte fundamental de la estrategia empresarial. No estamos sólo ante una tendencia, sino una necesidad estratégica integral frente a los riesgos cada vez más crecientes y complejos que generan pérdidas e inseguridad dentro del negocio.

Los departamentos de Seguridad no sólo protegen los activos de las empresas, sino que se alinean también con sus objetivos comerciales estratégicamente con unas medidas de prevención de pérdida, mejorando el margen operativo.

Además, hay que señalar que nuestra implicación y presencia contribuye a una reducción de costes en los seguros, sin dejar de lado nuestros continuos análisis y planes de seguridad, que nos hacen responder de forma óptima ante crisis o amenazas emergentes o incluso se evitan.

—La seguridad integral es un elemento clave en la gestión de la protección de las instalaciones, ¿cree que facilita el trabajo de los directores de Seguridad contar con los sistemas de seguridad integrados?

—Contar con sistemas de seguridad integrados facilita notablemente el trabajo de los directores de Seguridad. De hecho, es uno de los elementos clave para una gestión moderna, eficiente y estratégica del sector de la seguridad.

La automatización de procesos, la visión en tiempo real, el optimizar los recursos ayuda a contribuir en una respuesta más rápida y eficiente, a poder realizar análisis con patrones de comportamientos, vulnerabilidades, medir las incidencias, evitar zonas ciegas y a ser garantes de una seguridad más próxima y eficiente en el negocio.

«La seguridad mejora la percepción de una gran superficie, fomentando la fidelidad y satisfacción del cliente»

—¿Qué tendencias emergentes en seguridad considera que tendrán un mayor impacto en el futuro del sector de grandes superficies?

—El sistema de cámaras con inteligencia artificial recopilando comportamientos y conductas nos aportará una mejora en el análisis de datos para que podamos anticiparnos a los riesgos y prevenir delitos antes de que ocurran, optimizando recursos y esfuerzos.

Poder contar con sistemas de alarmas inteligentes que coordinen una respuesta rápida activando automáticamente una comunicación con los servicios de emergencia.

La incorporación de una vigilancia aérea con el uso de los drones también ha sido un gran avance para garantizar la seguridad en zonas de difícil acceso o incluso para poder controlar una gran superficie.

Y, por supuesto, el contar con una ciberseguridad avanzada, para la protección de ciberataques, que en la actualidad es uno de los grandes riesgos para el negocio.

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

—Un responsable de Seguridad que pretenda implementar una estrategia en una gran superficie se enfrenta a varios retos importantes, como crear medidas de seguridad para evitar la gran diversidad de riesgos existentes, robos, vandalismos, incendios, o incluso alguna de tipo emergencia médica; medidas tecnológicas que debe ser diseñadas con el más mínimo detalle, con una planificación eficiente, debiendo integrarlas para que, en su conjunto, sean efectivas.

Otro de los retos que debe asumir es adaptar la seguridad a la gran afluencia de público que transita por las instalaciones, debiendo garantizar la seguridad tanto para los trabajadores como para los clientes, creando una percepción de confianza en el público sin llegar a generar una sensación de inseguridad o incomodidad con unas medidas restrictivas.

—¿Cree que es necesario vincular a los empleados en la importancia del papel de la seguridad en la compañía y potenciar la concienciación?

—No es necesario, es primordial.

«Cuando los clientes perciben que están en un entorno seguro y protegido disfrutan de su visita si van a realizar compras»

La concienciación de la importancia que tiene la seguridad para los trabajadores es fundamental para el éxito de una estrategia de seguridad. Cuando los trabajadores se sienten integrados y con un papel importante para contribuir a un entorno seguro, se sienten más responsables y comprometidos.

Es importante fomentar la participación activa, así como mantener una formación continua en materia de seguridad ya que no sólo dependemos de los sistemas, sino también de la actitud y compromiso de las personas.

—¿Qué papel juega la seguridad en la experiencia de cliente en este tipo de establecimientos?

—Cuando los clientes perciben que están en un entorno seguro y protegido disfrutan de su visita si van a realizar compras o a pasar un buen rato. Esto les impulsa a repetir la experiencia, consolidando a unos clientes que confían y se sienten seguros en el entorno. Además, cuando la presencia de la seguridad se hace visible transmite tranquilidad y dejan de preocuparse por los riesgos o peligros existes. En resumen, la seguridad no solo protege a las personas y bienes, sino que también mejora la percepción de una gran superficie, fomentando la fidelidad y satisfacción del cliente. ✱

Araelec

partner oficial

ZKTeco

Innovación biométrica y tecnología avanzada para un mundo más seguro

En Araelec, como partner oficial de ZKTeco, ofrecemos tecnología biométrica avanzada para la gestión segura de personas y espacios.

Desde reconocimiento facial y de palma hasta cerraduras inteligentes y plataformas en la nube, integramos sistemas fiables, escalables y adaptados a las necesidades de cada empresa.

GoTimeCloud

TECNOLOGÍA, PROTOCOLOS Y PERSONAS

El triángulo de la seguridad moderna en grandes superficies.

ISMAEL LÓPEZ. PRODUCT MANAGER VIDEO DE CASMAR

Las grandes superficies comerciales son entornos complejos que, por su naturaleza, requieren un enfoque integral de seguridad. Con una afluencia diaria masiva, accesos múltiples, diversidad de espacios de uso y una creciente exposición a amenazas físicas o digitales, proteger estos entornos es todo un reto.

Desde nuestra perspectiva como expertos en soluciones de seguridad, es fundamental entender que proteger estos espacios no solo implica la prevención de hurtos, sino también la gestión de emergencias, la ciberseguridad, el cuidado del personal y todo ello garantizando una experiencia satisfactoria y segura al cliente. La clave está en combinar la tecnología adecuada con una planificación estratégica y ejecutada por personal capacitado, como pilares de una protección eficaz.

PRINCIPALES RIESGOS Y DESAFÍOS

- Alta afluencia de personas: aumenta la probabilidad de robos, extravío de menores, emergencias médicas o altercados.
- Diversidad de espacios: tiendas, zonas de ocio y parking, restaurantes o áreas técnicas requieren soluciones específicas.
- Múltiples entradas y salidas: se dificulta el control perimetral y la gestión de accesos no autorizados.
- Amenazas digitales: ciberataques, uso indebido de datos y pérdida de información sensible.
- Emergencias complejas: incendios o actos violentos podrían afectar a cientos de personas en su evacuación o generar flujos de movimiento anómalos.

SOLUCIONES TECNOLÓGICAS

Existen múltiples propuestas de seguridad adaptadas a este tipo de entornos dinámicos:

- **Sistemas antihurto**

Tecnología RFID o etiquetas magnéticas con arcos de detección en salidas. Ideal para el control en tiendas sin comprometer la experiencia del cliente.

- **Control de accesos avanzado o aforo**

Lectores biométricos, tarjetas OSDP o códigos para restringir el acceso a zonas sensibles como almacenes, oficinas, CPD o el centro de control.

• **Alarmas y sensores**
Detección de intrusión, detección de incendios (con sus sistemas de extinción asociados), presencia de gases o movimientos no autorizados. Todos conectados a una plataforma central o CRA con respuesta inmediata.

•**Ciberseguridad y protección de datos**
Soluciones que incluyen firewalls, cifrado de datos, control de accesos digitales y protección frente a ransomware son medidas imprescindibles de resiliencia.

• **Videovigilancia inteligente (CCTV)**
Cámaras IP de alta resolución combinadas con análisis de vídeo detectan comportamientos anómalos (caída, luchas, personas corriendo, manos alzadas, etc.), intrusiones o aglomeraciones a tiempo real.
El uso de metadatos con múltiples atributos nos permite también realizar búsquedas de forma más eficiente mediante filtros específicos para identificar personas, vehículos u objetos de interés en un análisis forense con gran cantidad de datos.
Finalmente, la sala de control para monitoreo en tiempo real con su Videowall y con una plataforma de centralización que integre todos los sistemas, para toma de decisiones eficiente ante cualquier evento (PSIM tipo Vigiplus de Desico).

PROTOCOLOS Y PLANIFICACIÓN ESTRATÉGICA

Una buena tecnología debe estar respaldada por procedimientos claros y personal adiestrado. Los protocolos deben incluir:
• Planes de evacuación y emergencias integrados con los sistemas de seguridad.
• Formación continua para todos los agentes implicados en manejo de incidentes y uso del equipamiento.
• Simulacros periódicos y auditorías de seguridad.
• Coordinación estrecha con fuerzas de seguridad y bomberos locales.

GESTIÓN DEL RIESGO: UN PROCESO CONTINUO

La seguridad no se alcanza, es un proceso. Evaluar, planificar, implementar, revisar y mejorar son etapas cíclicas que deben aplicarse de forma continua:
• Identificación de riesgos físicos, operativos y digitales.

- Evaluación del impacto y la probabilidad de cada amenaza.
- Aplicación de medidas correctivas y de prevención.
- Monitorización de incidencias mediante software de gestión y análisis de datos.

UN ENFOQUE INTEGRAL DESDE LA DISTRIBUCIÓN

Casmar, como distribuidores especializados, nuestra misión no se limita a suministrar productos, sino a asesorar y proporcionar soluciones integrales adaptadas a cada cliente. Trabajamos de la mano con las mejores marcas, instaladores, ingenierías y responsables de seguridad para diseñar e implementar sistemas que se ajusten a las particularidades de cada gran superficie.

Contamos con un catálogo tecnológico insuperable con fabricantes líderes, soporte técnico especializado y capacidad logística para dar respuesta rápida a cualquier necesidad, desde pequeñas superficies hasta complejos centros comerciales.

Garantizar la seguridad en grandes superficies no es solo una cuestión de vigilancia. Es proteger personas, bienes, reputación y continuidad operativa. Esto se logra con tecnología avanzada de última generación, personal preparado, protocolos eficientes y una visión global estratégica.

«Las grandes superficies son entornos complejos que, por su naturaleza, requieren un enfoque integral de seguridad»

En un entorno donde los riesgos evolucionan constantemente, las soluciones de seguridad también deben hacerlo. Nuestra misión es aportar valor en cada etapa del proyecto, ayudando a nuestros clientes a anticiparse, adaptarse y protegerse apuntando a la excelencia y comprometidos con la seguridad integral en grandes superficies. ✱

casmar®
www.casmarglobal.com

Innovación que transforma la seguridad en soluciones más inteligentes

Descubre nuestras soluciones con IA

SANTIAGO RIAÑO SUÁREZ. HEAD OF SECURITY AT SANITAS AND BUPA EUROPE AND LATINAMERICA

«La seguridad es una responsabilidad compartida y todos debemos estar implicados»

Texto y fotos: Gemma G. Juanes.

Con una visión de futuro, Santiago Riaño Suárez, Head of Security at Sanitas and Bupa Europe and LatinAmerica, visualiza «hospitales inteligentes donde la seguridad esté plenamente integrada con la asistencia. La IA predictiva permitirá anticipar incidentes, los sistemas IoT monitorizarán en tiempo real todos los parámetros críticos y la robótica apoyará en rondas y vigilancia».

Y es que en esta conversación con Cuadernos de Seguridad, Riaño Suárez, explica qué tecnologías clave tienen ya implantadas en el área de Seguridad y los retos actuales a asumir por un responsable de Seguridad de una gran corporación sanitaria.

—¿Cuáles son los pilares básicos sobre los que se asienta la estrategia de seguridad de los centros y hospitales Sanitas?

—La estrategia de seguridad de Sanitas se fundamenta en cinco grandes pilares: la protección de las personas como prioridad absoluta; la continuidad asistencial, es decir, que la seguridad sea un facilitador del servicio sanitario y no un obstáculo; la gestión integral de riesgos; la incorporación de tecnología e innovación; y finalmente, el cumplimiento normativo unido al fomento de una verdadera cultura de seguridad en toda la organización.

—¿Qué retos debe asumir un responsable de Seguridad a la hora de implantar una estrategia de seguridad en función de la singularidad de cada centro Sanitas?

—El principal reto es adaptar un marco corporativo común considerando la gran diversidad de inmuebles, así como la realidad de cada instalación. No es lo mismo un hospital, con urgencias abiertas 24/7, que una residencia de mayores o unas oficinas comerciales. Los

hospitales requieren equilibrio entre accesibilidad y seguridad; los centros médicos y dentales demandan control de afluencia; las oficinas, protección de información sensible; y las residencias, medidas específicas para colectivos vulnerables. En definitiva, se trata de armonizar lo global con lo local.

«Trabajamos con un enfoque de concienciación en seguridad continua con los trabajadores de Sanitas»

—¿Qué acciones y programas lleva a cabo el departamento de Seguridad para concienciar a sus trabajadores de la importancia de la seguridad?

—Trabajamos con un enfoque de concienciación continua. Impartimos formación en protocolos de autoprotección, prevención de agresiones y respuesta ante emergencias. Además, realizamos campañas internas, simulacros periódicos y programas adaptados al rol de cada empleado. También fomentamos canales de reporte confidenciales, porque entendemos que la seguridad es una responsabilidad compartida y todos debemos estar implicados.

—Convivimos con tecnologías como el Big Data, la Inteligencia Artificial,... ¿están utilizando estas tecnologías en el departamento de Seguridad de Sanitas? ¿En qué aplicaciones se están implementando?

—Por supuesto, y cada vez con mayor intensidad. Nadie es ajeno a estas tecnologías y, sin duda, tenemos que ser capaces de aprovecharlas en nuestro beneficio. Por ejemplo, aplicamos analítica de vídeo con IA para detectar comportamientos anómalos, accesos indebidos o aglomeraciones. Con Big Data analizamos patrones históricos de incidentes para anticiparnos a riesgos recurrentes. Estamos también avanzando en control de accesos digitales y en algoritmos predictivos que nos permiten dimensionar recursos de seguridad según la estacionalidad o los picos de demanda asistencial.

—¿Cuál es hoy la mayor brecha entre la estrategia de seguridad definida por un director de Seguridad y su ejecución real dentro de la organización?

—La mayor diferencia suele estar en la cultura organizativa. Aunque las políticas y protocolos estén muy bien definidos, su efectividad depende de que todo el personal, especialmente el sanitario, las interiorice y aplique en su día a día. Otro punto es la heterogeneidad tecnológica: no todos los centros tienen el mismo nivel de infraestructura, lo que dificulta la aplicación de medidas homogéneas.

—Las agresiones a sanitarios son un riesgo hoy en día importante en los hospitales y centros sanitarios, ¿qué tipo de pautas, para la atención, gestión, seguimiento y resolución de las denuncias por violencia en el lugar de trabajo disponéis en Sanitas?

—Como no puede ser de otro modo, contamos con un protocolo corporativo específico. Incluye medidas preventivas como la formación en comunicación no violenta y la presencia de seguridad en áreas críticas. En caso de incidente, activamos una respuesta inmediata con botones de pánico y asistencia al profesional agredido. Después realizamos un registro formal, desde Sanitas se da apoyo legal y psicológico al trabajador, y hacemos seguimiento del caso hasta su resolución. Nuestro objetivo es proteger al profesional, pero también aprender de cada caso para mejorar y tratar de minimizar este tipo de riesgos.

—Con una visión de futuro, ¿cómo imagina la seguridad de los grandes centros hospitalarios en cuanto a tecnología e innovación?

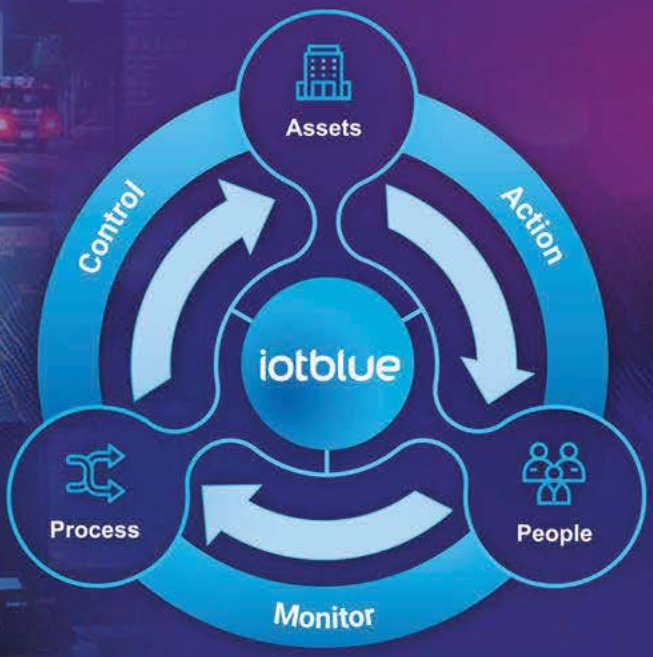
—Visualizo hospitales inteligentes donde la seguridad esté plenamente integrada con la asistencia. La IA predictiva permitirá anticipar incidentes, los sistemas IoT monitorizarán en tiempo real todos los parámetros críticos y la robótica apoyará en rondas y vigilancia. La ciberseguridad y la seguridad física estarán completamente unidas. Y todo ello con un enfoque de seguridad "invisible", que no incomode al paciente pero que garantice la máxima protección en el back-office. Nosotros ya estamos comenzando a implementar ese futuro en nuestros hospitales, recientemente hemos abierto el Hospital Blua Sanitas Valdebebas en Madrid, convirtiéndose en el hospital más digital de Europa y donde la seguridad ha ido alineada en todo momento con el resto de las áreas implicadas en el desarrollo y ejecución del proyecto. ✱

iotblue

Madrid - Cairo - Riyadh

El Sistema Operativo de tu sala de Control

La plataforma de gestión unificada que integra todos tus sistemas de seguridad y operaciones en una sola interfaz.



Inteligencia, automatización y resiliencia para infraestructuras complejas y críticas.

Integrate > Automate > Operate

Olvídate de los sistemas aislados.
Más que PSIM, iotblue integra todo (CCTV, SCADA, BMS, IoT...) para darte una visión 360° real y el control total que necesitas.

No dependas de soluciones cerradas.

Nuestra plataforma te ofrece la autonomía que necesitas.

INTEGRACIÓN TOTAL
Conecta cualquier sistema, de cualquier marca.

INTELIGENCIA REAL
Entiende el contexto, no solo alertas.

RESPUESTA ÁGIL
Automatiza protocolos y reduce errores.

GESTIÓN ÚNICA
Unifica seguridad, operaciones y mantenimiento.

No gestiones solo alertas. ¡Controla la situación!

Descubre por qué los centros de control más avanzados ya confían en iotblue.

Solicita tu demo en vivo.
www.iotblue.com

PASCUAL APARICIO SOTO. RESPONSABLE DE SEGURIDAD. HOSPITAL UNIVERSITARIO FUNDACIÓN ALCORCÓN (MADRID)

«La seguridad del futuro en los hospitales será más preventiva, más profesionalizada y más integrada en la misión asistencial»

Texto y fotos: Gemma G. Juanes.

«El mayor reto es lograr un equilibrio perfecto entre la protección y la misión asistencial; debemos proporcionar una protección plenamente efectiva sin entorpecer la atención al paciente», asegura Pascual Aparicio Soto, responsable de Seguridad del Hospital Universitario Fundación Alcorcón, durante esta conversación con Cuadernos de Seguridad, en la que hace hincapié en que los trabajadores del centro son conscientes de que «la seguridad está para protegerles y apoyarles, y nosotros sabemos que sin su colaboración diaria, la prevención sería mucho menos efectiva».

Y es que Pascual Aparicio explica, orgulloso, que en el centro sanitario «hemos fomentado una cultura de comunicación directa con Seguridad».

—¿Cuáles son los pilares básicos sobre los que se asienta la estrategia de seguridad del Hospital Universitario Fundación Alcorcón?

—La estrategia de seguridad del Hospital Universitario Fundación Alcorcón se construye sobre cuatro pilares sólidos, que conforman un sistema integral de protección adaptado a la complejidad de un gran centro sanitario.

-Prevención proactiva: partimos de un análisis exhaustivo de riesgos y del Plan de Autoprotección para anticiparnos y reducir la probabilidad de incidentes. Este enfoque nos permite identificar vulnerabilidades y poner en marcha medidas preventivas antes de que se materialice la amenaza.

-Integración tecnológica: el hospital ha realizado inversiones durante estos años para actualizar los sistemas de videovigilancia, intrusión y control de accesos. Ahora tenemos un centro de control más operativo que gestiona la información para tomar decisiones en tiempo real, esto nos permite reaccionar a los incidentes con mayor velocidad y precisión. También hemos ampliado las utilidades de las tarjetas identificativas, los profesionales pueden utilizarlas también en los servicios de parking, reprografía,

vending y dispensadores automáticos de vestuario.

-Cultura organizacional de seguridad: para que un hospital sea un lugar seguro, no es suficiente con invertir en tecnología y disponer de un equipo de vigilantes de seguridad. Necesitamos que cada persona —desde el equipo directivo hasta el personal de subcontratas— asuma que la seguridad es parte de su función diaria. Fomentamos esa mentalidad a través de la formación, comunicación interna y concienciación continua.

-Colaboración multidisciplinar: la seguridad hospitalaria es transversal y requiere trabajo en red. Coordinamos acciones con áreas clínicas, técnicas y de gestión, y mantenemos una colaboración fluida con las Fuerzas y Cuerpos de Seguridad, así como con los servicios de emergencia y con las distintas administraciones.

—¿Qué retos debe asumir un responsable de Seguridad a la hora de implantar una estrategia de seguridad en un centro sanitario de la singularidad del Hospital Universitario Fundación Alcorcón?

—El mayor reto es lograr un equilibrio perfecto entre la protección y la misión asistencial, debemos proporcionar una protección plenamente efectiva sin entorpecer la atención al paciente.

En la Comunidad de Madrid existen tres hospitales de referencia para la atención sanitaria a la población de centros penitenciarios, el Hospital Universitario Fundación Alcorcón es uno de ellos. Esto implica contar con módulos de custodia, medidas de seguridad y protocolos específicos para garantizar la seguridad sin comprometer la atención sanitaria.

Trabajamos en una infraestructura con actividad 24/7, por la que pasan más de tres millones de personas al año y situaciones de alta carga emocional. Las situaciones críticas pueden surgir en cualquier momento, y debemos estar preparados para actuar con rapidez, proporcionalidad y seguridad jurídica.

Otro punto a destacar es la gestión del helipuerto; hablamos de una instalación crítica cuyo fin es el traslado de pacientes que precisan de atención hospitalaria urgente. Cada segundo cuenta, la instalación debe estar siempre en condiciones óptimas para que las aeronaves puedan operar en ella. Esto implica tener un control estricto de los accesos para evitar intrusiones en una zona altamente sensible, una coordinación con los controladores aéreos y pilotos, y el estricto cumplimiento de los procedimientos sobre el estado del helipuerto, la vigilancia de obstáculos, la transferencia de pacientes, la corriente descendente y de emergencias. En resumen, el reto está en mantener un equilibrio perfecto entre la máxima seguridad y la fluidez operativa, porque un helipuerto hospitalario es mucho más que un punto de aterrizaje, es una puerta de entrada para salvar vidas.

—¿Qué papel ocupan actualmente los departamentos de Seguridad en la actividad

organizativa de los grandes centros sanitarios?

—Aquellos hospitales que disponen de un director de Seguridad al frente se han convertido en un elemento clave en la estructura organizativa de los grandes hospitales, con un papel que va mucho más allá de la vigilancia y el control de accesos, somos un valor para la organización. Nuestra función está plenamente integrada en la gestión estratégica y operativa, especialmente en dos ámbitos críticos: la continuidad de negocio y la gestión de crisis.

En cuanto a la continuidad de negocio, debemos garantizar que, ante cualquier incidente, la actividad asistencial continúe sin interrupciones. Esto implica coordinarse con todas las áreas del hospital, activar protocolos de contingencia y, sobre todo, anticipar riesgos para que el impacto sea mínimo.

El otro gran eje es la gestión de crisis. Un ejemplo reciente fue el apagón eléctrico que sufrimos este año. En un centro sanitario, la pérdida de suministro eléctrico es una situación de alto riesgo: pueden verse comprometidos equipos de soporte vital, sistemas de climatización, comunicaciones internas y externas, y la propia operativa hospitalaria. Durante una crisis, el departamento de Seguridad se convierte en el centro de mando operativo y de comunicaciones del hospital. Aportamos un valor añadido en estas situaciones como es la visión global del centro, la experiencia en gestión de incidentes complejos y como canal de información para la Dirección del centro.

Siempre tenemos en cuenta la protección de la reputación institucional, evitando que un incidente de seguridad afecte la imagen del centro y la confianza de los pacientes.

«El futuro de la seguridad hospitalaria combinará tecnología avanzada y unos recursos humanos especializados»

—¿Qué papel juegan los trabajadores del centro hospitalario en la organización de la seguridad teniendo en cuenta la fuerza laboral tan diversa?

—Son un elemento muy valioso para detectar y prevenir incidentes. La plantilla de un centro sanitario es extraordinariamente diversa: médicos, enfermería, técnicos sanitarios, personal administrativo, mantenimiento, limpieza, hostelería... Cada uno desarrolla su labor en entornos y horarios diferentes. Esa diversidad es, precisamente, una fortaleza para la seguridad. Los profesionales que trabajan en contacto directo con pacientes,

acompañantes o proveedores tienen la capacidad de detectar conductas anómalas o situaciones sospechosas antes de que escalen. Puede ser un comportamiento agresivo, una presencia no autorizada en zonas restringidas o cualquier señal de riesgo.

En el Hospital Universitario Fundación Alcorcón hemos fomentado una cultura de comunicación directa con Seguridad. Los trabajadores saben que cualquier incidencia, por pequeña que parezca, debe reportarse a Seguridad de inmediato. Y lo hacen porque confían en que su aviso será atendido de forma rápida, profesional y discreta.

Esta relación fluida nos permite actuar de manera preventiva, evitando que una situación potencialmente peligrosa llegue a convertirse en un incidente real. En la práctica, el personal del hospital se convierte en una red de observadores que amplían nuestra capacidad de cobertura mucho más allá de lo que puede abarcar un equipo de vigilancia por sí solo.

En definitiva, los trabajadores no son meros usuarios de la seguridad: son parte activa del sistema, ojos y oídos que, coordinados con nuestro equipo, hacen que el hospital sea un lugar más seguro para todos.

—¿Qué acciones y programas lleva a cabo el hospital para concienciar a sus trabajadores de la importancia de la seguridad?

—Disponemos de un plan de formación continua en emergencias, de formaciones específicas para determinadas unidades, realizamos simulacros, procedimientos específicos, disponemos de una Comisión de Catástrofes y el plan de emergencias está disponible en la intranet del hospital para todos los profesionales:

-En los cursos del plan de emergencias –que se imparte en colaboración con el Servicio de Bomberos de Alcorcón- pueden inscribirse todos los trabajadores del hospital. Hacemos varias sesiones al año para instruir al personal sobre cómo actuar en caso de producirse una emergencia y también damos una serie de recomendaciones de autoprotección con sujetos agresivos. Estos cursos incluyen prácticas de extinción con fuego real.

-Se realizan formaciones específicas en las unidades de nueva creación y en el centro de salud

mental adscrito a este hospital.

-Tenemos procedimientos para la atención sanitaria de la población reclusa y para la atención de pacientes en condición de detenidos que traen a Urgencias las FF. y CC. de Seguridad. Hemos realizado sesiones formativas en Urgencias difundiendo estos procedimientos, que incluyen numerosas medidas preventivas para los profesionales.

-Tenemos una Comisión de Catástrofes e Incidentes con Múltiples Víctimas, en el que hemos desarrollado un algoritmo para que, en el caso de ocurrir una catástrofe interna, los profesionales del hospital sepamos cómo organizar los recursos humanos y materiales. Lo pondremos en práctica próximamente.

En la última encuesta interna sobre la calidad del departamento de Seguridad, la rapidez de respuesta y la eficacia en la resolución de incidencias alcanzaron un 100 % de satisfacción positiva. Los trabajadores son conscientes de que la seguridad está para protegerles y apoyarles, y nosotros sabemos que sin su colaboración diaria, la prevención sería mucho menos efectiva.

—Con una visión de futuro, ¿cómo imagina la seguridad de los grandes centros hospitalarios en cuanto a tecnología e innovación?

—En un contexto donde los incidentes de seguridad van en aumento, la seguridad de los grandes centros hospitalarios evolucionará hacia un modelo híbrido, donde la tecnología y el factor humano se integren de forma mucho más profunda para ofrecer una protección inteligente, preventiva y adaptable.

En el futuro cercano, veremos una expansión del uso de inteligencia artificial. Los sistemas de videovigilancia pasarán de ser pasivos a ser proactivos, capaces de detectar comportamientos anómalos, aglomeraciones inusuales o accesos no autorizados en tiempo real, generando alertas automáticas al personal de seguridad. Además, la IA permitirá el análisis predictivo de incidentes, identificando patrones y anticipando riesgos antes de que se materialicen.

La robótica también tendrá un papel importante, se incorporarán robots de patrulla que podrán realizar rondas en zonas de baja afluencia o de acceso restringido, equipados con sensores térmicos, cámaras de 360º y sistemas de comunicación directa con el centro de control. Estos dispositivos no sustituirán a los vigilantes, pero les permitirán concentrarse en intervenciones de mayor complejidad, mientras las tareas repetitivas y de inspección se automatizan.

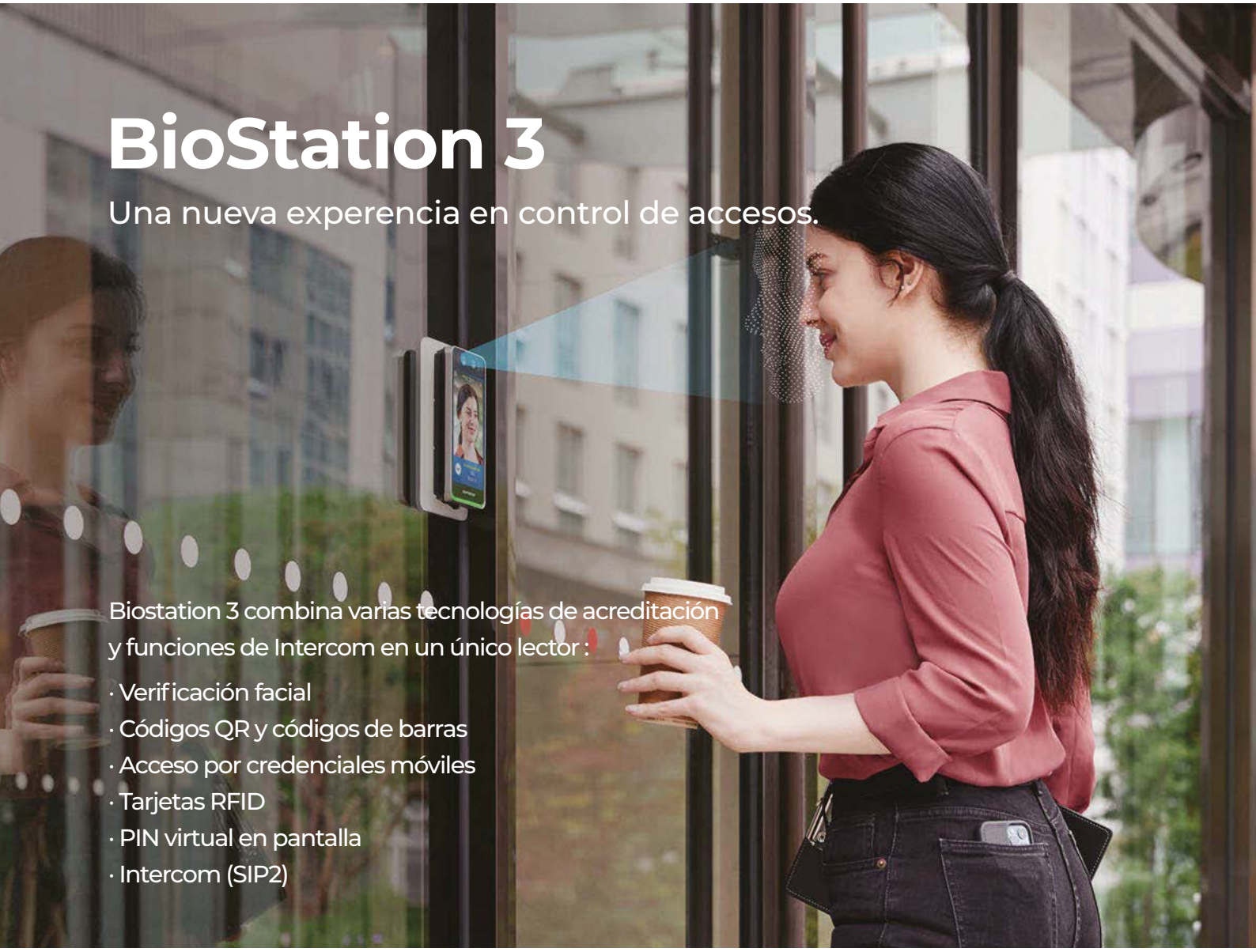
En cuanto a los drones, su potencial es especialmente relevante para el control perimetral, o la inspección rápida de instalaciones exteriores tras un incidente. Los drones podrían, por ejemplo, verificar en segundos la seguridad de un perímetro tras una intrusión, o asistir en la evaluación de daños tras una tormenta o incidente estructural.

El futuro de la seguridad hospitalaria combinará tecnología avanzada y unos recursos humanos especializados, porque necesitamos profesionales capacitados para utilizar todas las posibilidades que la tecnología nos ofrece.

En definitiva, la seguridad del futuro en hospitales será más preventiva, más profesionalizada y más integrada en la misión asistencial. ✱

BioStation 3

Una nueva experencia en control de accesos.



Biostation 3 combina varias tecnologías de acreditación y funciones de Intercom en un único lector :

- Verificación facial
- Códigos QR y códigos de barras
- Acceso por credenciales móviles
- Tarjetas RFID
- PIN virtual en pantalla
- Intercom (SIP2)

El procesador NPU, usando un algoritmo de IA, ofrece la mayor precisión y velocidad en la verificación facial

Plantilla de biometría “facial en el móvil”: los datos biométricos del usuario se almacenan en sus teléfonos personales y no se guardan en bases de datos de la compañía

Pequeño y potente — ligeramente más grande que un teléfono móvil

suprema
SECURITY & BIOMETRICS

Suprema Europe
366 Ter Vaugirard 75015 Paris France
T +33 1 84 73 29 43 **E** Sales_eu@supremainc.com
www.supremainc.com

NOS DIJERON QUE ÉRAMOS INFRAESTRUCTURAS CRÍTICAS… Y NOS LO CREÍMOS

SANTIAGO GARCÍA SAN MARTÍN.
PRESIDENTE DEL OBSERVATORIO DE SEGURIDAD INTEGRAL EN CENTROS HOSPITALARIOS (OSICH)

Era octubre del 2018 cuando nos cayó la jarra de agua fría (parece que ha pasado una eternidad después del COVID, La Filomena y el Blackout, pero solo hace 7 años): los grandes hospitales no se consideraban Infraestructuras Críticas.

La Comisión Nacional para la Protección de las Infraestructuras Críticas aprobó el Plan Estratégico Sectorial del Sector de la Salud y designó 24 nuevos Operadores Críticos (mayoritariamente Servicios de Salud de las Comunidades Autónomas), pero entre las infraestructuras designadas no se encontraba ningún gran hospital.

Esta decisión iba en contra de todo lo que se había hablado anteriormente y generó una enorme polémica. Si el sector salud es un sector estratégico y los grandes hospitales son las instalaciones más importantes del sector ¿por qué no eran designados?

La indignación, la incredulidad, el desconcierto y la sensación de desamparo en el sector de la seguridad en el ámbito sanitario eran evidentes. Todo por lo que habíamos trabajado durante años se nos escapaba en el último sprint, llegando a la meta.

INFRAESTRUCTURAS CRÍTICAS

Cuando preguntamos por qué no se consideraba a los grandes hospitales Infraestructuras Críticas, nos dijeron que “en la mayoría de los casos no se cumplía con los criterios de la Ley”. Cabe recordar un momento lo que dice la Ley 8/2011 de Protección de Infraestructuras Críticas al respecto:

Son Infraestructuras Críticas: “las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales”.

Siendo los criterios que lo determinan:

1. El número de personas afectadas (número potencial de víctimas mortales o heridos con lesiones graves y las consecuencias para la salud pública).
2. El impacto económico y el deterioro de productos y servicios.


FREEPIK/SENIVPETRO

3. El impacto medioambiental, degradación en el lugar y sus alrededores.
4. El impacto público y social, ... incluida la pérdida y el grave deterioro de servicios esenciales.

Entendiendo la Ley de Protección de Infraestructuras Críticas como un refuerzo a la continuidad en el funcionamiento de los servicios esenciales y de instalaciones críticas, que garantizan el normal funcionamiento de nuestra sociedad, sinceramente nuestro desconcierto fue todavía mayor, ya que a cualquier persona con la que hablábamos, no entendía por qué quedaban los grandes hospitales fuera de estos criterios (de hecho hay mucha gente que sigue pensando que todos los grandes hospitales son Infraestructuras Críticas designadas).

IMPACTO CRÍTICO SOBRE LA SALUD

Después de lo vivido estos años creo que ya nadie puede pensar que si un gran hospital deja de funcionar normalmente (total o parcialmente) esto no se traduzca en un impacto crítico sobre la salud no solo de los pacientes que tiene ingresados (con muertos directos en UCIS por ejemplo si no hay suministro energético), sino de los que acuden a urgencias tras un accidente de tráfico o a realizarse un TAC o Scaner urgentes, un impacto económico brutal sobre la actividad, un gran impacto sobre el medio ambiente (recordar la crisis de la gestión de residuos sanitarios en el COVID) y un impacto crítico sobre la opinión pública y el funcionamiento de las administraciones.

Recuerdo que en octubre de 2018 celebramos las XV Jornadas Técnicas de Seguridad en Centros Sanitarios del OSICH en el Hospital Príncipe de Asturias de Alcalá de Henares y en la mesa de Protección de Infraestructuras Críticas participó un representante del CNPIC. Al ser preguntado por lo que para nosotros era una gran incongruencia, nos dio un consejo que ha quedado marcado a fuego para la mayoría de los que estábamos allí: "Si consideran que los grandes hospitales son Infraestructuras Críticas, compórtense como si lo fuesen, independientemente de lo que diga la ley"... y eso hemos hecho estos años.

Ahora que se va a producir un cambio legislativo en España, transponiendo la directiva CER europea, más enfocada en potenciar la resiliencia de las organizaciones y la continuidad en el servicio para los ciudadanos, que en las amenazas de bomba y el terrorismo, y que parece que significará la designación de "de iure" y no solo "de facto" de los hospitales como Infraestructuras Críticas, podremos decir que nosotros siempre creímos en el sistema y nos comportamos siempre como si fuésemos parte del mismo, reforzando nuestras estructuras y mejorando la resiliencia de nuestras organizaciones, y eso es lo que nos ha permitido dar servicio a los ciudadanos en el COVID, en la Filomena y en el Blackout y poder seguir salvando vidas. ✱

BAUSSA ES RECONOCIDA ENTRE LAS 500 EMPRESAS LÍDERES DEL CRECIMIENTO EN ESPAÑA POR CEPYME

BAUSSA, referente en el sector de la seguridad, ha sido seleccionada como una de las **500 empresas líderes en crecimiento en España** por el proyecto **CEPYME500,** una iniciativa impulsada por la **Confederación Española de la Pequeña y Mediana Empresa (CEPYME).**

El programa CEPYME500 identifica y promueve a las 500 empresas españolas que lideran el crecimiento empresarial, reconociendo su capacidad para generar valor, empleo y competitividad. Este proyecto, impulsado por CEPYME, busca dar visibilidad y apoyo a las pymes que representan el motor de la economía española.

Asimismo, este reconocimiento que se concede anualmente, distingue a las pequeñas y medianas empresas que destacan por su **capacidad de crecimiento, innovación, generación de empleo y contribución al desarrollo económico nacional.** La selección se basa en rigurosos criterios económicos y financieros que reflejan la solidez y el potencial de las compañías más dinámicas del tejido empresarial español.

"Este reconocimiento es fruto del trabajo, dedicación y talento de todo nuestro equipo. Nos impulsa a seguir creciendo con responsabilidad, apostando por la innovación y la excelencia en cada proyecto", ha señalado Iñigo Ugalde Blanco, Director Comercial de BAUSSA.

El sello **CEPYME500** posiciona a BAUSSA dentro de un grupo selecto de pymes que impulsan la competitividad y el desarrollo económico del país, consolidando su papel como actor clave en el panorama empresarial español.

Desde su fundación en 1985, BAUSSA ha mantenido un crecimiento sostenido gracias a la innovación tecnológica, a su orientación al cliente y por supuesto a su expansión internacional. Con este sello, la empresa reafirma su papel como **motor de innovación y progreso** dentro de la seguridad. ✱


40 AÑOS SIENDO LA LLAVE
DE TU SEGURIDAD
BAUSSA
40
ANIVERSARIO
1985 - 2025
www.baussa.com
SEGURIDAD FÍSICA | SPIDER | FULL CONTROL

GESTIÓN INTELIGENTE DEL APARCAMIENTO EN HOSPITALES

Seguridad desde la entrada.

ALFONSO LORENZO ROBLEDANO,
DESARROLLO DE NEGOCIO DE HIKVISION

La llegada al hospital, ya sea como paciente, acompañante o profesional sanitario, marca el inicio de una experiencia que va más allá del acto médico. La primera impresión no se genera en la sala de espera ni en la consulta, sino en el acceso al recinto, especialmente en el aparcamiento.

Una gestión ineficaz del flujo de vehículos puede generar congestión, estrés y retrasos, afectando tanto a la percepción del centro como a su funcionamiento interno.

En los entornos hospitalarios, el aparcamiento no puede ser considerado un servicio accesorio. La puntualidad, la previsibilidad y la agilidad en los accesos son elementos clave para garantizar una atención adecuada y una experiencia digna.

Sin embargo, la realidad en muchos hospitales muestra sistemas anticuados: barreras manuales, tickets impresos, colas en la entrada y salidas lentas en los momentos de mayor afluencia.

RECONOCIMIENTO AUTOMÁTICO DE MATRÍCULAS Y ACCESO SIN CONTACTO

Una de las tecnologías que más ha transformado la movilidad en entornos urbanos e industriales es el reconocimiento automático de matrículas (ANPR, por sus siglas en inglés). Aplicada al entorno hospitalario, esta solución permite automatizar completamente el acceso al aparcamiento, sin necesidad de intervención del usuario. El sistema detecta el número de matrícula al aproximarse al punto de entrada y, si está autorizado, permite el paso sin detener el vehículo.

Este tipo de acceso sin contacto no solo agiliza el flujo, sino que resulta especialmente útil en contextos donde la higiene es prioritaria y donde se requiere minimizar el contacto físico, como durante una pandemia.

Además, la integración con los sistemas de gestión de pacientes permite reservar plazas de aparcamiento con antelación o dar prioridad automática a vehículos asociados a citas urgentes, ambulancias o transporte sanitario programado.

SEÑALIZACIÓN INTELIGENTE Y GUIADO EN TIEMPO REAL

Una vez dentro del recinto, el siguiente reto es encontrar plaza disponible de forma rápida. En hospitales de gran tamaño o con estructuras complejas, esta tarea puede convertirse en una fuente adicional de ansiedad. La instalación de sensores de ocupación y pantallas LED de guiado ayuda a dirigir a los conductores hacia las zonas libres en tiempo real, reduciendo el tiempo de búsqueda y evitando la circulación innecesaria dentro del complejo.

Este guiado dinámico no solo mejora la experiencia del usuario, sino que contribuye a una gestión más eficiente del tráfico interno, disminuyendo emisiones y ruido.

AUTOMATIZACIÓN DEL PAGO Y REDUCCIÓN DE TIEMPOS DE SALIDA

Otro de los puntos críticos en los aparcamientos tradicionales es la salida. Las colas en los cajeros automáticos o las barreras generan esperas innecesarias que pueden resultar especialmente incómodas para pacientes que acaban de recibir tratamiento o acompañantes que llevan horas en el centro.

Los sistemas de pago automático vinculados a la matrícula permiten abandonar el recinto directamente, ya que el cobro puede realizarse a través de aplicaciones móviles, códigos QR o plataformas integradas con el sistema hospitalario. El resultado es una salida fluida, sin esperas ni gestiones adicionales.

SEGURIDAD Y EFICIENCIA OPERATIVA

Además de mejorar la experiencia del usuario, estos sistemas aportan un valor significativo en términos de seguridad. La monitorización en tiempo real del flujo de vehículos permite detectar accesos no autorizados, identificar vehículos estacionados en zonas restringidas o controlar el cumplimiento de normativas específicas (como el uso de plazas para personas con movilidad reducida).

Los datos generados permiten a los responsables del centro sanitario analizar patrones de uso, prever picos de demanda y optimizar la asignación de recursos humanos y técnicos. Esto se traduce en una gestión más sostenible y racional del espacio disponible.

UN PUNTO DE FRICCIÓN CONVERTIDO EN VENTAJA OPERATIVA

Transformar el aparcamiento en un proceso automatizado, transparente y eficiente no es solo una mejora en comodidad: es una contribución directa a la calidad asistencial y al bienestar del paciente. Reducir el estrés previo a una cita médica, facilitar el acceso al personal sanitario o mejorar la seguridad de los accesos son beneficios que inciden en la operativa diaria del hospital. ✱

LA SEGURIDAD CONTRA INCENDIOS EN HOSPITALES Y RESIDENCIAS: UNA OBLIGACIÓN ÉTICA

ANTONIO TORTOSA. VICEPRESIDENTE DE TECNIFUEGO

En hospitales y residencias de mayores conviven personas con movilidad reducida, pacientes con enfermedades cognitivas o ciudadanos que dependen totalmente de los cuidados de otros. Estos espacios son especialmente vulnerables, y cualquier incidente puede tener consecuencias muy graves. Cada decisión en materia de prevención y protección no es solo técnica, sino que implica salvar vidas.

EXIGENTES REQUISITOS DE SEGURIDAD

El Código Técnico de la Edificación (CTE) lo deja claro: hospitales, clínicas y residencias tienen uso hospitalario, lo que significa que deben cumplir exigentes requisitos de seguridad. Se trata de edificios ocupados las 24 horas, con pacientes que, en muchas ocasiones, no pueden valerse por sí mismos. Cualquier incidente se convierte rápidamente en un riesgo muy alto. Por eso, la preparación no admite retrasos ni improvisaciones.

Las medidas básicas de protección no son complicadas, pero sí imprescindibles. La sectorización de los edificios permite crear zonas seguras donde el fuego no se propague, y las áreas de refugio facilitan que los ocupantes permanezcan a salvo hasta ser trasladados. Todo esto pierde sentido si el personal no está formado para actuar con rapidez y seguridad en caso de emergencia. La prevención es clave: planes de emergencia actualizados, simulacros periódicos y una cultura de seguridad que implique a todos los profesionales. Incluso elementos como cortinas, tapicerías o alfombras con reacción al fuego adecuada forman parte de esa cadena de protección.

TECNOLOGÍA, PAPEL FUNDAMENTAL

La tecnología también juega un papel fundamental. La combinación de detectores de humo y rociadores automáticos es la solución más eficaz que existe hoy en día. Los detectores permiten identificar el fuego en su fase inicial y activar alertas inmediatas, mientras que los rociadores ofrecen un tiempo vital para la evacuación e incluso pueden controlar o extinguir el incendio. Mantener


FREEPIK

libres de humo los pasillos y vías de escape es igualmente esencial: recordemos que el 75 % de las muertes en incendios se produce por inhalación de humo.

Cumplir la normativa es obligatorio. El CTE y el Reglamento de Instalaciones de Protección contra Incendios (RIPCI) establecen exigencias sobre materiales resistentes al fuego, extintores accesibles, bocas de incendio equipadas, sistemas de detección y alarma, y comunicación directa con los bomberos en edificios grandes. Pero cumplir la ley no debería ser el límite. Desde Tecnifuego defendemos ir más allá, adoptando soluciones que eleven el nivel real de seguridad. No se trata solo de normas: se trata de proteger vidas.

MANTENIMIENTO RIGUROSO Y POR EMPRESAS HABILITADAS

Igual de importante es asegurarse de que los sistemas instalados funcionen cuando más se les necesita. Un equipo de protección inactivo o mal mantenido es un riesgo añadido. Por eso, el mantenimiento debe ser riguroso y realizado por empresas especializadas y habilitadas, y las inspecciones periódicas de las autoridades competentes son esenciales para garantizar que todo funcione correctamente.

La seguridad contra incendios en hospitales y residencias es responsabilidad de todos: administraciones, gestores, personal sanitario y técnicos especializados. No es solo cumplir normas; es un compromiso ético con quienes más dependen de nuestra protección. Cada medida preventiva, cada sistema instalado y cada simulacro realizado puede significar la diferencia entre la vida y la tragedia.

«La seguridad contra incendios en hospitales es responsabilidad de todos: administraciones, gestores, personal sanitario y técnicos especializados»

Desde Tecnifuego seguiremos promoviendo la cultura de la prevención, el cumplimiento riguroso de la normativa y la adopción de soluciones avanzadas. Porque, al final, no hablamos solo de edificios seguros: hablamos de vidas que dependen de ello. ✱

EDGE AI: INTELIGENCIA AL BORDE Y LA IMPLEMENTACIÓN DEL AI ACT EN EUROPA

La Inteligencia Artificial al Borde (Edge AI) representa una de las transformaciones más importantes en la evolución tecnológica actual. Frente al modelo tradicional basado en grandes centros de datos, Edge AI traslada el procesamiento y la toma de decisiones a dispositivos locales, más próximos a donde se generan los datos. Este enfoque permite respuestas más rápidas, mayor control sobre la información y una gestión más segura de los sistemas inteligentes. En el contexto europeo, Edge AI surge como una vía estratégica para aplicar de forma práctica los principios del **AI Act,** la nueva regulación comunitaria sobre inteligencia artificial.

El **AI Act** establece un marco legal para garantizar que la IA en Europa sea ética, transparente y confiable. Clasifica los sistemas según su nivel de riesgo e impone exigencias más estrictas para aquellos de "alto riesgo". Edge AI se alinea naturalmente con estos objetivos porque su arquitectura distribuida facilita la trazabilidad, la supervisión y la protección de los datos personales, pilares esenciales del nuevo marco regulatorio.

Para Lorenz Baermann, CTO de **AltonaSpain,** Europa puede aprovechar este enfoque como un instrumento de **soberanía tecnológica.** El modelo de **Edge AI** ofrece **cuatro ventajas fundamentales** para cumplir el **AI Act.**

- Primero, permite **controlar el entorno tecnológico.** AI ejecutar los algoritmos directamente en el dispositivo o en redes locales, las organizaciones pueden mantener bajo su supervisión el hardware, el software y los datos utilizados. Esto simplifica las auditorías y la gobernanza interna exigidas por la normativa.
- Segundo, contribuye a **minimizar los riesgos de privacidad.** AI reducir la transferencia de datos hacia nubes externas, se evita la exposición de información sensible y se mejora el cumplimiento del Reglamento General de Protección de Datos (GDPR).
- Tercero, facilita un **ciclo de vida de la IA más transparente y gestionable.** La ubicación física de los dispositivos y su mantenimiento local hacen posible aplicar controles directos sobre las actualizaciones, las versiones del modelo y las medidas de mitigación de riesgo.
- Por último, potencia una **innovación alineada con la ética europea.** Las empresas que diseñen y desplieguen sistemas Edge AI "fiables desde su origen" podrán ofrecer soluciones certificables bajo el AI Act, reforzando así la confianza del mercado y su posicionamiento competitivo.

La **Edge AI** reduce la dependencia de infraestructuras de nube externas y promueve ecosistemas locales de hardware y software interoperables. Además, se integra con políticas comunitarias como la **Ley Europea de Chips** o los programas de supercomputación **EuroHPC**, que buscan fortalecer la capacidad digital propia del continente.

No obstante, el despliegue masivo de **Edge AI** presenta **retos significativos.** Algunos sistemas seguirán siendo considerados de alto riesgo y requerirán certificaciones específicas. Aún deben definirse estándares técnicos comunes y procedimientos de validación para garantizar la interoperabilidad y la calidad de los algoritmos. También será necesario desarrollar redes de soporte y

talento especializado que acompañen esta transición. Para el sector empresarial y profesional, **Edge AI** supone una oportunidad directa de **convertir la regulación en ventaja competitiva.** Las organizaciones que adopten soluciones distribuidas podrán automatizar procesos, optimizar operaciones y cumplir las normas europeas de manera más eficiente. En ámbitos como la **contabilidad** o la **auditoría,** la combinación de procesamiento local y supervisión humana permitirá integrar la IA de forma segura y transparente. Un ejemplo real es la reciente salida al mercadop de AltonaAlias que ofrece soluciones de **auditoria y cumplimento normativo.**

En conclusión, **Edge AI** ofrece a Europa una vía equilibrada entre innovación, protección y confianza. No se trata solo de una tecnología emergente, sino de una herramienta estratégica para materializar los principios del **AI Act** y consolidar un modelo de inteligencia artificial responsable, soberano y centrado en las personas. ✱

"LA NUEVA SEGURIDAD", HILO CONDUCTOR DEL VII CONGRESO DE SEGURIDAD PRIVADA EN EUSKADI

Más de 200 profesionales asisten al encuentro para conocer nuevos modelos de seguridad, analizar la captación del talento en seguridad y la protección integral de las infraestructuras críticas, entre otros temas.

Más de 200 profesionales acudieron el pasado 29 de octubre al VII Congreso de Seguridad Privada en Euskadi, organizado por Cuadernos de Seguridad, con la colaboración del Gobierno Vasco, la Ertzaintza y la Asociación Vasca de Profesionales de Seguridad (SAE).

Iván Rubio, director de Cuadernos de Seguridad, destacó que una edición más Bilbao volvía a convertirse en el «punto de encuentro de quienes compartimos la vocación de proteger, prevenir y contribuir a una sociedad más segura». Un encuentro que «permitirá analizar los nuevos desafíos que afronta la seguridad privada, impulsados por la transformación tecnológica y la creciente cooperación con la seguridad pública», añadió.

El congreso, que se celebró en el Bizkaia Aretoa de Bilbao, fue inaugurado por Ricardo Ituarte, viceconsejero de Seguridad del Gobierno Vasco, quien destacó la importancia de reforzar la colaboración público-privada como "eje central de la seguridad de nuestro modelo de negocio. Un rasgo distintivo más de la marca Euskadi. Caminando juntos, compartiendo información, estrategias y objetivos, la seguridad se fortalece como servicio esencial a la ciudadanía".

La ponencia inaugural corrió a cargo de Ramsés Gallego, ISACA Hall of Fame & Chief Technologist, Cybersecurity, DXC Technology, quien bajo la temática "Ciberseguridad 2048: Días del Futuro Pasado", comenzó señalando que "el futuro depende de lo que hagamos hoy", ya que "existen amenazas persistentes y muy avanzadas; lo importante cuán persistentes somos nosotros a la hora de proteger y defender".

En un viaje a la ciberseguridad de 2048, es ahora el momento de hacerse preguntas y aprender a protegerse ante un mundo cambiante. "Hablamos de ciberresiliencia, de anticiparnos a las amenazas, resistir, aprender y reaccionar", apuntó.

Vista general del VII Congreso de Seguridad Privada en Euskadi.

Iván Rubio, en un momento del acto de apertura del Congreso.

"Estamos en un cambio de era", donde la identidad, los datos y aplicaciones están intrínsecamente relacionados, y donde existe una correlación entre el mundo ciber y físico, apuntó.

INFRAESTRUCTURAS CRÍTICAS EN EUSKADI

«Un enfoque colaborativo para la protección integral de las Infraestructuras de Euskadi», fue la ponencia impartida por Asier Erkoreka, director de Coordinación de Seguridad del departamento de Seguridad del Gobierno Vasco, quien analizó el Plan de Protección de las Infraestructuras Sensibles de Euskadi (PISE), y que definió como un «modelo colaborativo, flexible, ...».

«Un servicio es catalogado como sensible cuando su operación es necesaria para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones de Euskadi y sus Administraciones Públicas», señaló Erkoreka, tras lo cual enumeró los servicios involucrados en el PISE, categorizados en 12 sectores, entre ellos: Energía, agua, sanidad, gobierno y administración pública, finanzas, etc.

Durante su intervención aportó datos concretos, destacando la existencia de más de 50 operadores adscritos al PISE, más de 80 operadores identificados, más de 60 infraestructuras protegidas,... y más de 20 mil millones de facturación entre todos los operadores.

Señaló que PISE nace con el objetivo de proporcionar nuevas formas de seguridad y dar respuestas a las nuevas amenazas y viene a corroborar "nuestro compromiso con la seguridad compartida.

Ricardo Ituarte, viceconsejero de Seguridad del Gobierno Vasco, inauguró el VII Congreso de Seguridad Privada en Euskadi

"La Captación del Talento en Seguridad", fue la temática de la mesa de debate que contó con las intervenciones de Karmelo Martínez, Comisario Jefe de Formación y Perfeccionamiento de la Ertzaintza; Eduardo Cobas, secretario general de APROSER, y Francisco López, responsable de Security en Euskal Trenbide Sarea (ETS)- Red Ferroviaria Vasca, y fue moderada por Iván

Ramsés Gallego, ISACA Hall of Fame & Chief Technologist, Cybersecurity, DXC Technology

Rubio, director de Cuadernos de Seguridad.

Ante la falta de talento en el sector de la seguridad, los ponentes apuntaron como punto de partida la necesidad implacable el "dignificar el sector". Eduardo Cobas explicó tres elementos clave a la hora de mantener el talento en el sector: mejorar las condiciones laborales y la conciliación familar, y promover la valoración profesional de la seguridad.

Francisco López coincidió con Cobas, pero de nuevo insistió en la necesidad de "dignificar al sector, reforzar y potenciar su formación". Mientras, Karmelo Martínez, destacó la necesidad de adaptar los contenidos curriculares a las nuevas tecnologías, ya que "las competencias actuales han variado".

Durante el debate se puso sobre la mesa el Grado Medio de FP en Seguridad, que ya se encuentra implantado en 8 comunidades autónomas, y donde 650 personas están cursando una formación de 2.000 horas. "Es una manera de atraer a jóvenes al mundo de la seguridad, con competencias adquiridas. Estamos ante una oportunidad histórica".

Francisco López, apostó por contar con un talento más especializado y "esas horas de formación son hoy en día fundamentales. Es un puente hacia las FF y CC de Seguridad y el sector privado". Karmelo Martínez fue más allá al apuntar la necesidad de establecer "Plan de Carrera en materia de seguridad".

"Estamos a tiempo de tener talento dotado de formación en tecnologías, que es la base del futuro", señaló López, quien además apuntó: "Basta de zanganear en la seguridad privada; estamos a tiempo de corregir este declive."

Jorge Salgueiro, presidente de AECRA, y Javier Zorrila, director general de SEGURMA, compartieron panel de intervención bajo el tema "La nueva seguridad en la protección de bienes".

"La seguridad es una integración de muchos mundos: digital y físico", apuntó Salgueiro, quien además subrayó el papel de la inteligencia humana y la inteligencia artificial para anticipar riesgos y delitos, destacando también la creciente fusión entre seguridad y defensa.

Javier Zorrilla ofreció una visión empresarial y tecnológica del mercado de alarmas para hogares y negocios, un sector que considera expansivo pero que carece de innovación disruptiva.

Asier Erkoreka, director de Coordinación de Seguridad del departamento de Seguridad del Gobierno Vasco

Karmelo Martínez, Comisario Jefe de Formación y Perfeccionamiento de la Ertzaintza; Eduardo Cobas, secretario general de APROSER; Francisco López, responsable de Security en Euskal Trenbide Sarea-Red Ferroviaria Vasca; e Iván Rubio, director de Cuadernos de Seguridad como moderador.

Jorge Salgueiro, presidente de AECRA, y Javier Zorrilla, director general de SEGURMA.

Zorrilla explicó que "el cliente busca calidad, precio competitivo y tecnologías avanzadas" y propuso un enfoque más centrado en el servicio al cliente y la transparencia, sugiriendo optimizar la prevención, "la supervisión diaria de equipos y el uso de tecnología para minimizar falsas alarmas y mejorar la gestión de incidentes".

A continuación, Ismael López, Product Manager Video de Casmar, intervinó con la ponencia «Protección inteligente: aportación de la IA a la seguridad pública». Tas hacer un recorrido por la historia de la IA, hasta llegar a la actualidad con la IA Generativa como agente transformador, el ponente se centró en la IA aplicada a los sistemas de seguridad, explicando que los sistemas de CCTV convencionales «son simples y reactivos, y la IA los transforma en inteligentes y proactivos». Además, destacó que la IA "nos ayudará en los grandes retos que vendrán en la Seguridad Pública". En concreto, en su aplicación a las ciudades, en la gestión de tráfico -control de parking y pasos a nivel, detección automática de incidentes; detección de incidencias y emergencias y la supervisión de espacios públicos, eventos e infraestructuras críticas.

Durante su intervención hizo hincapié en la importancia de la colaboración público-privada en el uso de la IA, por ejemplo con la implantación de cámaras privadas integradas en sistemas municipales. Destacó que la IA «debería convertirse en una palanca para abrir nuevos caminos para permitirnos colaborar de forma más estrecha con las FF y CC de Seguridad».

«El modelo de gestión de seguridad: Osakidetza», fue el título de

Ismael López, product manager Video de CASMAR.

Juan José Quiñones director de Seguridad de Osakidetza

Marcos Fenollar, sales director Iberia de SUPREMA.

Walter Varela, country manager Spain IoT Blue.

la ponencia impartida por Juanjo José Quiñones, director de Seguridad de Osakidetza, quien apuntó cifras concretas del Servicio Vasco de Salud creado en 1983 que cuenta actualmente con una red de 460 infraestructuras con diferentes perfiles (Hospitales, ambulatorios, centros de salud, consultorios, etc.), así como una plantilla de más 35.000 profesionales. El ponente hizo hincapié que en 2023 el Consejo de Administración de Osakidetza decidió «incluir en su Plan Estratégico la vigilancia y la seguridad como una de las líneas estratégicas».

El Plan Director de Seguridad tenía como objetivo preparar una hoja de ruta que permita a Osakidetza establecer las líneas maestras sobre las que construir un nuevo Modelo de Gestión de la Seguridad, enfocado a mejorar la percepción de la seguridad por parte del personal propio y usuarios/as; minimizar los riesgos e incidencias; o modernizarse con mejoras tecnológicas, entre otras cosas. La estrategia puesta en marcha, según explicó Quiñones, estaba enfocada a «Promover la cultura de Seguridad, establecer un contrato corporativo de servicios de vigilancia, plan integral de formación y colaborar con el Modelo de Formación en Seguridad de FP».

En este sentido, Quiñones destacó que la «buena seguridad comienza con una buena comunicación interna y externa, entre todos».

Marcos Fenollar, sales director Iberia de SUPREMA, abordó "Normativa europea RED: ciberseguridad y cumplimiento en tecnologías de control de acceso". Comenzó explicando la certificación CE RED -Directiva 2014/53/UE actualizada con el Acto Delegado 2022/30,: "Norma europea que regula los dispositivos inalámbricos. La actualización introduce requisitos de ciberseguridad obligatorios: Teléfonos móviles, Dispositivos IOT, Control de accesos..., obligatoria desde el pasado 1 de agosto de 2025", mientras añadió que "todos los nuevos productos inalámbricos deben cumplir

Mesa de debate en la que participaron Ane Miren, directora de Modernización del Ayuntamiento de Bilbao; Agustín Moyano, responsable de Seguridad Corporativa de EJIE, que fue moderada por Jon Zuazo, presidente de SAE.

Amaia Arregi, concejala de Seguridad del Ayuntamiento de Bilbao, clausuró el VII Congreso de Seguridad Privada en Euskadi.

con estos requisitos para poder llevar el marcado CE".

Además, detalló los cuatro pilares de seguridad que añade esta certificación: protección de la transmisión de datos, prevención de la suplantación de dispositivos (spoofing), protección y firma del firmware, y medidas contra la manipulación física.

La empresa SUPREMA ha sido pionera en certificar sus equipos de infraestructura crítica bajo esta normativa, asegurando así una mayor protección del usuario final frente a ciberataques y facilitando el cumplimiento de marcos legales como NIS 2 y el Esquema Nacional de Seguridad. .

Por su parte, Walter Varela, country manager Spain IoT Blue, analizó la "Interoperabilidad de sistemas y gobernanza". Varela argumentó que, si bien la tecnología para la digitalización abunda en silos (como el IoT o sistemas de seguridad física), existe una falta de comunicación y coordinación entre ellos, generando "ruido" y retrasando la respuesta ante incidentes.

Enfatizó sobre la necesidad de pasar de las alarmas aisladas a la inteligencia conectada para evitar que las incidencias se conviertan en crisis, integrando los activos, las personas y los procesos.

Para finalizar destacó como beneficios de la interoperabilidad la reducción al tiempo de respuesta, optimización de recursos o mejora de la conciencia situacional de la emergencia.

Para finalizar el encuentro tuvo lugar una mesa de debate sobre "CISO y Director de Seguridad en la NIS2", que contó con las intervenciones de Ane Miren, directora de Modernización del Ayuntamiento de Bilbao, y Agustín Moyano, responsable de Seguridad Corporativa en EJIE (Sociedad Informática del Gobierno Vasco), y fue moderada por Jon Zuazo, presidente de SAE (Segurtasun Adituen Euskal Elkartea), donde abordaron la relación entre el CISO, el director de Seguridad y la nueva normativa NIS 2 en el entorno de la seguridad corporativa y pública. Los ponentes debatieron temas cruciales como la responsabilidad ante un ciberataque —cuestionando quién debe firmar los incidentes— y la gestión de la cadena de suministro bajo el nuevo marco legal. En este sentido, Agustín Moyano apuntó que "el proveedor debe tener la acreditación del Esquema Nacional de Seguridad (ENS)".

Subrayaron que la seguridad no es delegable y debe ser una responsabilidad compartida que involucre a todos los departamentos, enfatizando la necesidad de equilibrar la inversión versus riesgo y realizar simulacros de comunicación. A este respecto, Ane Miren, destacó la importancia a los procesos de comunicación y apostó por llevar a cabo "simulacros de comunicación". En relación a aspectos de inversión, Moyano explicó que es importante el equilibrio con la inversión en aquellos elementos críticos.

Finalmente, se hizo mención al apagón ocurrido el pasado mes de abril como una lección aprendida clave, que evidenció la urgencia de adoptar medidas de comunicación robustas, como la telefonía satelital, ante fallos generalizados de infraestructura.

El VII Congreso de Seguridad Privada en Euskadi fue clausurado por Amaia Arregi, concejala de Seguridad del Ayuntamiento de Bilbao, quien puso en valor la implicación de todo el Consistorio en la seguridad, en especial, el papel de la Policía Municipal en pro de la seguridad ciudadana, al tiempo que apostó por una seguridad compartida, ya que “juntos avanzaremos para mejorar la seguridad”. ✱

DISTINCIONES CUADERNOS DE SEGURIDAD

En el marco del VII Congreso de Seguridad Privada en Euskadi se procedió a la entrega de las Distinciones de CUADERNOS DE SEGURIDAD en reconocimiento a la labor de distintos profesionales y entidades en pro del sector.

Distinción otorgada a la trayectoria profesional y su contribución al desarrollo del sector. Asier Larramendi, director de Seguridad de Laboral Kutxa, recoge el galardón de manos de Iván Rubio, director de Cuadernos de Seguridad.

Distinción otorgada a la trayectoria profesional y su contribución a fortalecer los canales de colaboración con el sector. Francisco Llaneza, Comisario Jefe de la Unidad de Seguridad Privada de la Ertzaintza, recoge el premio de manos de Gemma G. Juanes, directora de Programas de Cuadernos de Seguridad.

Distinción especial a la Concejalía de Seguridad del Ayuntamiento de Bilbao, por el desarrollo de políticas para garantizar la seguridad en los espacios públicos de Bilbao. Amaia Arregi, concejala de Seguridad del Ayuntamiento de Bilbao, recoge el galardón de manos de Iván Rubio, director de Cuadernos de Seguridad.

Vista general del público en el acto de entrega de las distinciones.

ERTZAINTZA

DENUNCIA ONLINE

DESDE DONDE QUIERAS

CON UN CLICK

euskadi.eus


EUSKADI
Bien
veni
dos


VII Congreso de
Seguridad Privada
EUSKADI
VII Segurtasun
Pribatuko Batzarra
ISACA


CUADERNOS


VII Congreso de
Seguridad Privada
iotblue


peck


VII Congreso de
iotblue


VII Congreso de
Seguridad Privada
EUSKADI


VII Congreso de
Seguridad Privada
casmar
ISACA
DORLET
pecket


VII Congreso de
Seguridad Privada
EUSKADI


VII Congreso de
Seguridad Privada


ISACA


VII Congreso de
Seguridad Privada


ISACA
pecket
DELTA


VII Congreso de
Seguridad Privada
casmar
DELTA
segurma
Altrona Spain
DORLET
iotblue
suprema
trebide


VII Congreso de
Seguridad Privada
EUSKADI
casmar
iotblue
trebide
DORLET
suprema

ANNALAURA GATTO. MARKETING MANAGER DE VIBRAM

«La industria demanda más innovación en el calzado de seguridad, y nosotros respondemos a esa demanda»

A lo largo de los años, Vibram se ha convertido en un nombre imprescindible en el sector del calzado de seguridad, especialmente ahora que los trabajadores se centran cada vez más en el rendimiento y la protección.

En la Feria A+A, celebrada del 4 al 7 de noviembre en Düsseldorf, Alemania, la empresa anunció una importante innovación que revoluciona el sector.

—En A+A, Vibram ha hecho una importante innovación para el sector del calzado de seguridad. ¿Qué puede contar al respecto?

—La industria demanda más innovación en el calzado de seguridad, y nosotros respondemos a esa demanda.

En A+A presentamos un compuesto innovador capaz de establecer nuevos estándares en materia de agarre. A lo largo de los años, hemos introducido con orgullo nuevos estándares de agarre en la industria del calzado, especialmente en el mundo de los deportes al aire libre.

El compuesto Vibram MegaGrip se ha convertido en un referente indiscutible en materia de agarre y en un aliado esencial, tanto para los amantes de la montaña como para los atletas profesionales.

En el mundo del calzado de seguridad, el agarre no es solo una característica técnica, sino una respuesta concreta a una necesidad diaria de seguridad.

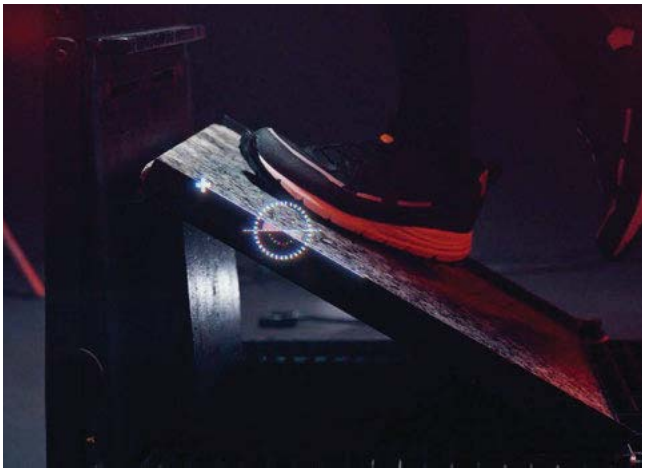
Cada día, los trabajadores de sectores como la industria pesada, la construcción, la logística o el mantenimiento se enfrentan a superficies peligrosas (húmedas, resbaladizas, irregulares) que ponen en riesgo su estabilidad, sus movimientos y su seguridad.

Basándose en los conocimientos técnicos de MegaGrip, nuestros departamentos de I+D han desarrollado una versión del compuesto específicamente adaptada a los trabajadores al aire libre. Esta nueva fórmula satisface las exigencias de agarre de los entornos más difíciles, al tiempo que mantiene un excelente equilibrio entre agarre y durabilidad, todo ello en pleno cumplimiento de las normas de seguridad europeas.

—¿Este compuesto se ha desarrollado en colaboración con marcas específicas o socios industriales?

—Este compuesto es el resultado de años de investigación y desarrollo internos, y ahora está disponible para todas las marcas que buscan ofrecer el mejor equilibrio posible entre agarre y durabilidad, especialmente en entornos de trabajo al aire libre húmedos, irregulares y difíciles.

Partimos de una necesidad clara identificada en el campo, especialmente en sectores como la construcción, el petróleo y el gas, y para los trabajadores que operan en terrenos montañosos o accidentados.



Estos profesionales pedían más: mejor agarre, rendimiento más constante y calzado más seguro que se adaptara realmente a condiciones del terreno impredecibles y, a menudo, extremas.

Nuestro objetivo era desarrollar un compuesto que permitiera a los trabajadores sentirse seguros y confiados en cada paso, independientemente de la superficie, ya fuera húmeda, helada, fangosa, rocosa o inestable.

En definitiva, se trata de generar confianza: confianza en las suelas Vibram que protegen, sostienen y resisten el paso del tiempo.

—¿Ha sido la única innovación que Vibram presentó en A+A este año?

—Sin duda, ha sido nuestra innovación más importante para el sector del trabajo y la seguridad, y esperamos que despierte un gran interés entre los profesionales del sector. Sin embargo, no es la única novedad que presentamos en A+A este año.

Además del nuevo compuesto, también presentamos una solución totalmente nueva centrada en otro reto clave del calzado de seguridad: la tracción. Para el público en general, la tracción y el agarre son esencialmente lo mismo, ya que ambos proporcionan una sensación de seguridad en cualquier terreno. Pero desde nuestra perspectiva, son dos aspectos complementarios: el agarre se aplica a superficies duras, mientras que la tracción se refiere a terrenos blandos o irregulares.

«Vibram lidera el camino: tecnología innovadora de agarre para el trabajo y la seguridad en la Feria A+A»

En entornos de trabajo de alta complejidad, como bosques, canteras, obras con pendientes pronunciadas, minas, entornos militares o tácticos, los operarios se enfrentan a superficies irregulares, inclinadas, resbaladizas o impredecibles.

En estos contextos, además de la tracción que proporciona la suela, la tracción activa en los laterales del calzado, es decir, en las paredes laterales, también puede ser de vital importancia.

Por eso hemos desarrollado Sidewall Traction, una banda de goma basada en la tecnología Vibram Traction Lug. Se trata de un sistema específico de tacos laterales diseñado para la pared lateral del calzado, con el objetivo de proporcionar mayor protección, seguridad y funcionalidad en las zonas laterales más expuestas a impactos y esfuerzos, especialmente en entornos operativos particularmente exigentes.

Un agarre revolucionario y una tracción de última generación al servicio de los trabajadores: estas dos tecnologías suponen un claro avance en nuestra misión de apoyar a los trabajadores con un calzado que refleja la complejidad de los movimientos del mundo real y las exigencias del lugar de trabajo. ✱

TECNOLOGÍA AL SERVICIO DE LA PROTECCIÓN DE LAS SEGUNDAS VIVIENDAS

JOSÉ IGNACIO JIMÉNEZ DEL CASTILLO, DIRECTOR DE RELACIONES INSTITUCIONALES DE SECURITAS DIRECT

Cada vez más personas prefieren viajar en septiembre. Hay varias razones para ello: el clima es más agradable, los precios suelen ser más accesibles y la oferta turística sigue siendo excelente. Esta tendencia ha provocado que, a partir de octubre, muchas segundas residencias – que en verano estaban llenas de veraneantes – comiencen a quedarse vacías.

Y es que, con la vuelta a la rutina, una de las principales preocupaciones es la seguridad de estas viviendas. Según la última edición del Observatorio de Securitas Direct, las segundas residencias tienen más probabilidad de sufrir una intrusión que las viviendas habituales. Este riesgo aumenta considerablemente en el caso de las propiedades que se encuentran en zonas rurales o costeras que permanecen vacías la mayor parte del año. En particular, los chalets o villas son los inmuebles más vulnerables, enfrentando el doble de robos que los apartamentos.

La mayoría de los propietarios son conscientes de esta problemática. De hecho, más de la mitad de las personas encuestadas por el estudio de Securitas Direct considera que el riesgo de intrusiones ha aumentado. Como resultado, el 83% de los españoles con segundas residencias reconoce la necesidad de proteger estas viviendas durante todo el año. A tenor de ello, este nivel de riesgo se traduce en un aumento en la adopción de medidas de protección.

Los sistemas de seguridad conectados a una Central Receptora de Alarmas (CRA) se han consolidado como una de las soluciones más eficaces. Esos sistemas han experimentado un crecimiento de 4,3 puntos porcentuales en segundas residencias en tan solo un año, según indica esta última edición del Observatorio de Securitas Direct, y ofrecen una respuesta profesional e inmediata ante cualquier intento de intrusión.

CERRADURAS INTELIGENTES

Al mismo tiempo, en los últimos años, la integración de nuevas tecnologías en el ámbito de la seguridad ha avanzado de forma significativa. Un ejemplo de ello es el uso de cerraduras inteligentes, una medida que permite un control remoto del acceso, lo que añade una capa de seguridad y comodidad.

De hecho, tal y como señala el estudio, un 12% de los propietarios con segundas residencias ya ha instalado una cerradura inteligente en sus hogares. Por ejemplo, en el caso de la alarma con cerradura inteligente de Securitas Direct, cuenta con un cilindro antirrobo a prueba de bumping, con defensa ante ganzúa, taladro y extracción, añadiendo así una capa extra de seguridad al punto más vulnerable de cualquier vivienda, la puerta. ✱

Hyfire

Orama group

LÍDERES EN TECNOLOGÍA DE DETECCIÓN CONTRA INCENDIOS

20+ años de experiencia en soluciones vía radio

2+ millones de dispositivos instalados

30+ áreas geográficas atendidas en todo el mundo

Tecnología Certificada EN54-25

www.hyfirewireless.com

LA MARCA HYFIRE ATERRIZA EN ESPAÑA

La disponibilidad de los productos Hyfire marca el inicio de una nueva etapa, con la clara misión de liderar el mercado ibérico hacia el futuro de la tecnología vía radio promoviendo soluciones innovadoras y sostenibles.

Advantronic, empresa española que forma parte del grupo internacional Orama, da un paso decisivo y anuncia la disponibilidad de la marca Hyfire en España. Una novedad que representa una auténtica evolución estratégica, la unión entre la solidez de una empresa consolidada en el mercado ibérico y la fuerza de Orama, grupo internacional líder en la protección contra incendios. Orama, sinónimo de innovación en Europa y en el mundo, trae a la península ibérica una oferta que combina fiabilidad, rapidez de instalación y sostenibilidad. La experiencia de Advantronic se integrará así con la visión global del grupo, dando vida a una marca capaz de interpretar las necesidades locales con el impulso innovador de un líder internacional.

FUTURO DE LA TECNOLOGÍA VÍA RADIO

La disponibilidad de los productos Hyfire marca el inicio de una nueva etapa, con la clara misión de liderar el mercado ibérico hacia el futuro de la tecnología vía radio promoviendo soluciones innovadoras y sostenibles, capaces de responder a los retos de un sector en rápida evolución.

La nueva marca estará presente en la feria SICUR en febrero de 2026 en Madrid, un escenario ideal para presentar al mercado el potencial de las tecnologías vía radio aplicadas a la seguridad contra incendios, destacando sus ventajas concretas: reducción de los tiempos de instalación, disminución de costes, flexibilidad en edificios complejos y los más altos estándares de seguridad.

«La tecnología vía radio es mucho más que una tendencia, es el futuro del sector contra incendios - afirma

José Luis Azcona,
Delegado Comercial de Advantronic

José Luis Azcona, Delegado Comercial de Advantronic-, permite reducir tiempos y costes de instalación, ofrece máxima flexibilidad con estándares de seguridad altísimos. Hyfire nace para poner todo esto al alcance de los profesionales del mercado ibérico».

COMPROMISO DE LA EMPRESA CON PARTNERS, INSTALADORES Y PROYECTITAS

Como anticipo de este lanzamiento, tuvo lugar un momento especial dedicado a los partners. Los días 23 y 24 de octubre se celebró en Madrid un evento exclusivo reservado a los miembros del programa Wireless Partnership, pensado para crear una red cualificada de profesionales capaces de acelerar la difusión de las tecnologías vía radio en el mercado ibérico. Un paso concreto en el territorio, que confirma el compromiso de la empresa con partners, instaladores y proyectistas.

Advantronic se une a Argus, Hyfire y Ramtech dentro de Orama, guiados por una visión común y por valores que guían cada decisión estratégica: pensar en digital, mantenerse cerca de los clientes, actuar con transparencia, asumir responsabilidades y tener el coraje de marcar la diferencia. Estos son los principios que orientan el desarrollo del grupo y que se reflejan de manera concreta en las soluciones que ofrece al mercado.

Con Hyfire, estas soluciones encuentran un punto de referencia dedicado, preparado para apoyar al sector con el salto tecnológico que el mercado requiere, poniendo en valor la colaboración entre producciones locales e internacionales.

«Con Hyfire damos un salto de calidad. Unimos la experiencia de Advantronic con la fuerza internacional de Orama - comenta Andrés Martínez, Director Gerente de Advantronic-. Esto significa tener lo mejor de ambos mundos, con un enfoque local y un impulso innovador global». ✱

Andrés Martínez,
Director Gerente de Advantronic

BLUEEVO: UN SISTEMA DE CIERRE ELECTRÓNICO INNOVADOR PARA EL CONTROL DE ACCESO

blueEvo incorpora la tecnología Mifare Desfire EV3 (con certificación EAL5+).

JUAN JURADO. DELEGADO COMERCIAL WINKHAUS – DIRECTOR DE SEGURIDAD

El pasado mes de junio Winkhaus fue galardonado con el Red Dot Award, en la categoría “Product Design”, por el nuevo sistema de cierre electrónico blueEvo. Este sistema de cierre accionado por llave se caracteriza por un lenguaje de diseño unificado.

El producto ha sido concebido para diferentes campos de aplicación, como plantas industriales, edificios de oficinas, organismos públicos e instituciones educativas, así como numerosas infraestructuras críticas y es un componente indispensable para dar cumplimiento a la normativa NIS2.

blueEvo incorpora la tecnología Mifare Desfire EV3 (con certificación EAL5+), la comunicación con las llaves electrónicas se realiza de acuerdo con el procedimiento de intercambio seguro en modo completo, que incluye autenticación en 3 vías.

Mediante el uso de elementos seguros (Mifare SAM AV3 con certificación EAL6+) como parte integral de los componentes de puerta, se lleva a cabo el almacenamiento

NUEVA Serie U

Mejore la seguridad básica con precisión impulsada por IA

No se conforme con una seguridad obsoleta que no detecta amenazas. La serie i-PRO U ofrece detección basada en IA, información en tiempo real y tiempos de respuesta optimizados. Con flexibilidad para la nube y ciberseguridad líder en la industria, redefine la seguridad básica.

- AI-VMD para una detección de amenazas superior
- Opciones de domo, box y bullet de 2MP, 5MP y 4K
- Grabación de audio para una mejor conciencia de la situación
- Modelos de lentes fijas y varifocales flexibles disponibles.
- VSaaS listo para conectarse directamente a la nube para una implementación sencilla
- Ciberseguridad FIPS 140-3 Nivel 3 para protección de datos

Nuestras soluciones tecnológicas amplían los sentidos humanos con innovaciones que informan y mitigan los riesgos, incluso en los entornos más desafiantes.

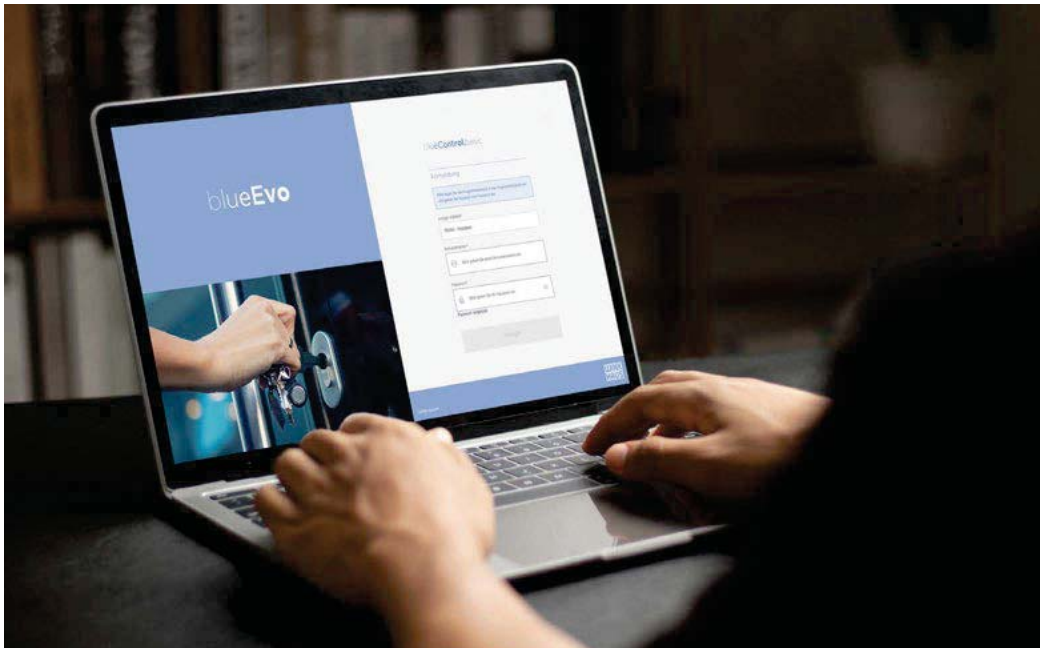
Somos su socio de confianza.

Scan to learn more

Descubra más
info.es@i-pro.com
www.i-pro.com

Anteriormente Panasonic Security

i-PRO



seguro de claves criptográficas, así como la autenticación de los componentes y el cifrado de los datos. No hay datos en la nube y toda la información se custodia en bases de datos alojadas en servidores del cliente.

A través de la intefaz API del software de administración blueControl, se pueden integrar sistemas ya existentes y automatizar los flujos de trabajo y la gestión del personal.

Dado que los componentes offline no requieren ningún cableado para las puertas, el cambio a esta moderna tecnología es muy sencillo.

El cilindro electrónico es autónomo, funciona autoalimentado por baterías internas o externas con hasta 10 años de autonomía y se fabrica a medida, de manera que siempre queda enrasado en la cerradura y no puede ser vandalizado desde el exterior.

Los medios de identificación pasivos (llave electrónica, tag, tarjeta, pulsera) tienen un transpondedor Mifare Desfire EV3 de 8K (13,56) Mhz con un ID único.

Además, los cilindros se pueden complementar con manillas electrónicas, candados y lectores de proximidad. La amplia gama de componentes en combinación con el software flexible (offline, red virtual y online) ofrece la solución adecuada para cada aplicación, ya sea cilindros con requisitos de protección a la intemperie, zonas húmedas o incluso para áreas potencialmente explosivas.

Para cumplir con el RGPD, ofrecemos diferentes funciones en el software. Los datos personales y eventos de cierre se almacenan solamente en el software de administración y no en los medios de identificación ni en los componentes de puerta.✱

PACOM
VIGIL CORE™

PACOM: LA EVOLUCION DE UNA MARCA Y PRODUCTO CONSOLIDADO

Seguridad y Gestión Empresarial en una única Plataforma Saas / Ompremise

PACOM VIGIL CORE es una solución única y escalable en seguridad y gestión empresarial, basada en la nube o local, que combina control de acceso y alarmas de intrusión, video verificación y monitoreo centralizado de alarmas, todo en un solo sistema. Esta rentable solución SaaS puede monitorear datos desde un solo sitio hasta miles, ofreciendo escalabilidad e integración con terceros.

Con un sistema flexible diseñado para el éxito a largo plazo, puede mejorar la seguridad, optimizar las operaciones, ahorrar costos y lograr un retorno de la inversión más rápido. Todas referencias de nuestra nueva gama de producto disponen de las certificaciones pertinentes según normas europeas EN 50131 en cuanto a grados 3 y Grado 4, incluyendo sus comunicaciones ✱

GCC ISO 27001 CERTIFIED

GCC ISO 27017 CERTIFIED

GCC ISO 27018 CERTIFIED

PACOM REVOLUCIONA LA SEGURIDAD EMPRESARIAL CON VIGIL CORE

Cumple con las normas EN en cuanto a Grado 4 específicamente para infraestructuras críticas

PACOM, líder global en soluciones de control de acceso y seguridad integrada, presenta VIGIL CORE, su innovadora plataforma en la nube de última generación que redefine el concepto de seguridad y gestión empresarial. Diseñada para ofrecer máxima eficiencia, escalabilidad y rentabilidad, VIGIL CORE va mucho más allá de la seguridad tradicional: impulsa la inteligencia operativa y optimiza la gestión del negocio desde una única plataforma centralizada.

UNA PLATAFORMA INTELIGENTE QUE EVOLUCIONA CON TU NEGOCIO

VIGIL CORE combina control de acceso, alarmas de intrusión, videoverificación, gestión de edificios y monitorización centralizada en una interfaz intuitiva y potente. Gracias a su integración con el Internet de las Cosas (IoT), la plataforma transforma datos y señales en inteligencia empresarial accionable, ayudando a las organizaciones a tomar decisiones más rápidas, reducir costos y aumentar su eficiencia operativa.

Su arquitectura SaaS escalable garantiza una solución preparada para el futuro: VIGIL CORE crece al ritmo de tu empresa, eliminando la necesidad de costosas infraestructuras locales y ofreciendo retornos de inversión más rápidos.

MÁS VALOR PARA DISTRIBUIDORES Y PARTNERS

Para la comunidad de distribuidores de valor añadido (VAR), VIGIL CORE representa una oportunidad única para ampliar su oferta, generar ingresos recurrentes y fortalecer la relación con sus clientes.

Su implementación en la nube elimina la complejidad de los servidores locales, reduce los tiempos de instalación y minimiza la necesidad de formación técnica, permitiendo a los partners centrarse en lo que realmente importa: hacer crecer su negocio.

MÁS QUE SEGURIDAD: CONTROL TOTAL DEL ECOSISTEMA EMPRESARIAL

VIGIL CORE ofrece un control integral del entorno físico y digital. Su panel de control

personalizable permite supervisar, gestionar y actuar en tiempo real desde cualquier dispositivo con conexión a internet —ya sea PC o smartphone—, brindando total libertad y flexibilidad.

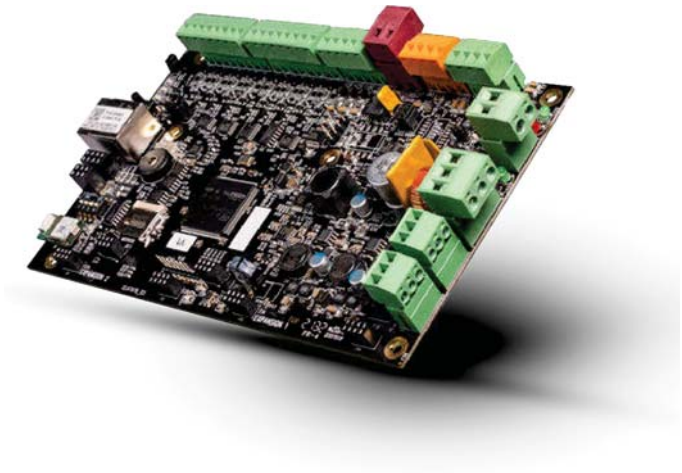
Los usuarios pueden acceder a video en directo o grabado, gestionar permisos, asignar credenciales, crear reglas automatizadas, exportar videos y controlar dispositivos desde cualquier lugar, en cualquier momento.

Además, su diseño flexible permite elegir entre una implementación totalmente en la nube, local o híbrida, adaptándose a las necesidades de cada organización.

«VIGIL CORE va mucho más allá de la seguridad tradicional: impulsa la inteligencia operativa y optimiza la gestión del negocio desde una única plataforma centralizada»

IDEAL PARA MÚLTIPLES SECTORES

Gracias a su versatilidad, VIGIL CORE es perfecta para entornos exigentes como banca y finanzas, logística y almacenamiento, retail, telecomunicaciones, infraestructura crítica y campus corporativos.



Su ruta de migración sencilla ofrece a los usuarios actuales de PACOM una transición fluida y sostenible hacia esta nueva generación de tecnología.

"VIGIL CORE es el resultado de meses de investigación, desarrollo y escucha activa a nuestros partners y clientes. Estamos entusiasmados de lanzar una solución que redefine lo que la seguridad puede lograr, impulsando la eficiencia y el valor en todos los niveles". ✱

LA INTEGRACIÓN INTELIGENTE COMO CLAVE PARA UNA SEGURIDAD MÁS EFICIENTE

En un contexto de creciente complejidad tecnológica y escasez de profesionales cualificados, las organizaciones necesitan soluciones que simplifiquen la operación y garanticen el cumplimiento de sus políticas de seguridad.

Advancis Software, con más de 30 años de experiencia y presencia en 87 países, desarrolla plataformas de integración que ayudan a más de 2.700 centros de control a gestionar sus operaciones de forma más eficiente y segura.

WinGuard (PSIM) integra todos los sistemas de seguridad y gestión de edificios en una sola interfaz, independientemente del fabricante. Su arquitectura modular permite proyectos escalables, adaptados a las necesidades y presupuesto de cada cliente. Además, incorpora procedimientos operativos guiados, que ayudan a los operadores a actuar con rapidez, reducir errores y mejorar la trazabilidad.

Con AIM (PIAM), la gestión de identidades y accesos se centraliza y automatiza, garantizando coherencia, cumplimiento normativo y control total sobre quién accede, dónde y cuándo.

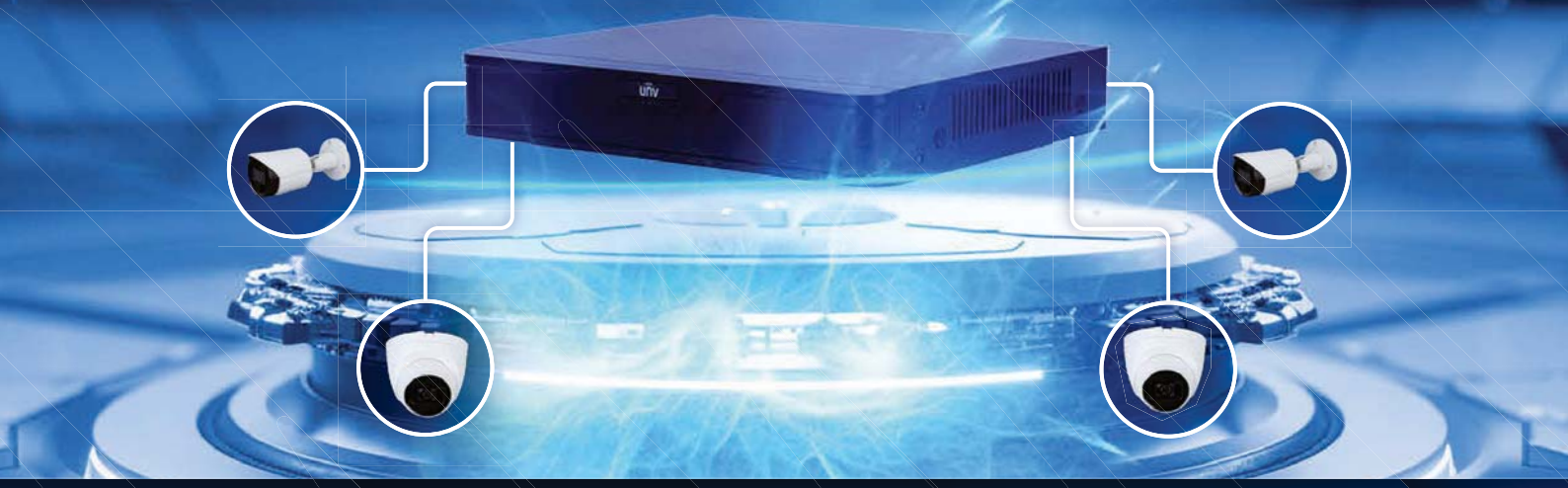
Advancis trabaja junto a integradores y partners, ofreciendo formación, asistencia y soporte continuo para asegurar implementaciones sin configuraciones complejas y adaptadas a cada entorno. Este acompañamiento permite a los integradores ofrecer soluciones de alto valor y máxima fiabilidad a sus clientes finales.

Advancis participará en SICUR 2026, donde mostrará cómo la integración inteligente y la gestión unificada transforman la seguridad en eficiencia operativa y valor sostenible.
Más información: sales@advancis.net ✱

INNOVACIÓN Y FIABILIDAD QUE REVOLUCIONAN LA SEGURIDAD

SOFTWARE VMS EZStation

CON HASTA 512CH Y P2P GRATUITO



EZCloud

Gestión en nube
y **P2P** gratuito

UNV Link

La App móvil más intuitiva
y actualizada del mercado

EZStation

512 canales gratuitos

El grabador más sencillo
de instalar y configurar

Las mejores condiciones
financieras

VISIOTECH

Calle Alberto Sánchez 31
28052 Madrid (España)
www.visiotechsecurity.com

Telf.: (+34) 911 836 285
comercial@visiotechsecurity.com

CIBERSEGURIDAD EN INFRAESTRUCTURAS FORESTALES INTELIGENTES

La seguridad forestal del siglo XXI es integral: física, digital y humana.

RICARDO BARRASA, MIEMBRO DE LA JUNTA DIRECTIVA DE ISACA MADRID

Todavía humean los rescoldos de los incendios en la España vaciada. En muchas zonas, la combinación de altas temperaturas, terrenos escarpados, acumulación de maleza han generado fuegos que se retroalimentaban, incontrolables que hacían inútil el esfuerzo de los operativos.

Ante estas circunstancias, y sin olvidarlas, tenemos que poner foco en la prevención; hemos oído a los técnicos agrarios la necesidad de mantener el campo, los bosques, ... limpios de vegetación, llamando la atención a la pérdida de las actividades agrícolas y ganaderas históricas, y en pleno siglo XXI debemos también poner la tecnología al servicio de la prevención de incendios.

La realidad es que hay varias iniciativas piloto para la realización de "bosques inteligentes" mediante la instalación de sensores de humo, temperatura, cambios bruscos de humedad, dispuestos estratégicamente para detectar conatos de incendios, complementados con cámaras y torres de vigilancia que aportan alertas tempranas. No olvidemos la dependencia crítica de conectividad y energía entre los dispositivos y los centros operativos.

Estamos ante un despliegue de tecnología importante, en un entorno no controlado físicamente, por lo que la superficie de ataque cibernético es muy amplia.

BUENAS PRÁCTICAS DE CIBERSEGURIDAD EN EL ÁMBITO FORESTAL

Las amenazas se concentran en tres frentes: manipulación de datos e imágenes, ataques a las comunicaciones, e intrusión en los sistemas de mando. Su combinación podría retrasar la detección, generar evacuaciones innecesarias o aumentar el coste económico y ambiental de los incendios.

Ante estos riesgos hay que implementar, sin dilación, unas buenas prácticas de ciberseguridad en el ámbito forestal mediante el diseño seguro de sistemas IoT: autenticación fuerte, segmentación de red, además de una monitorización continua, centros de operaciones de seguridad (SOC) adaptados al entorno de emergencias, con capacidad de correlación de eventos en tiempo real

y protocolos específicos para servicios forestales. Tener entornos ciber-resilientes con redundancia mediante copias de respaldo de datos críticos, canales de comunicación alternativos (satélite + radio) y en línea con los marcos ISO 27001, NIS2 o ENS.

No olvidemos que no basta con implementar, hay que hacer pruebas de pentesting y simulacros conjuntos (bomberos + especialistas en ciberseguridad) para parametrizar adecuadamente los dispositivos y redes.

La protección de infraestructuras forestales inteligentes exige no solo conocimiento tecnológico, sino también una gestión rigurosa del riesgo. ISACA mediante sus certificaciones internacionales proporciona profesionales CISA (Certified Information Systems Auditor) que aportan la capacidad de auditar y evaluar controles en sistemas IoT y plataformas en la nube: desde la integridad de los datos recogidos por sensores hasta la trazabilidad de las alertas enviadas a los centros de coordinación. Su rol garantiza que las soluciones desplegadas cumplen políticas, normativas y buenas prácticas internacionales, reduciendo vulnerabilidades.

Por su parte, los profesionales CISM (Certified Information Security Manager) asumen una visión más estratégica: diseñan programas de gestión de seguridad adaptados a entornos críticos, definen planes de respuesta ante incidentes y asegura la alineación con la continuidad operativa de brigadas y cuerpos de emergencia. La combinación de ambos perfiles crea un puente entre la auditoría técnica y la gestión ejecutiva, imprescindible para que la ciberseguridad se convierta en un aliado frente al fuego. Mientras que el CISA garantiza la confianza técnica y la trazabilidad de los sistemas, el CISM asegura que la seguridad esté integrada en la estrategia y la gestión operativa. Juntos aportan una defensa integral.

IA Y MACHINE LEARNING, PREDICCIÓN DE INCENDIOS

En el futuro próximo, la inteligencia artificial y machine learning se utilizarán para predicción de incendios, pero estos también tienen sus riesgos tecnológicos como la manipulación de modelos de IA, envenenamiento de datos, ... que siempre necesitarán de profesionales cualificados para su implementación y realización de auditorías tecnológicas y de cumplimiento.

La digitalización de la defensa forestal es una oportunidad, pero también un riesgo. Los incendios son un fenómeno natural y humano que ahora se puede combatir con tecnología avanzada, y esta debe estar blindada cibernéticamente. La seguridad forestal del siglo XXI es integral: física, digital y humana.✱

EUROPA ANTE SU ENCRUCIJADA DE SOBERANÍA DIGITAL: DE LAS PALABRAS A LAS CAPACIDADES

La soberanía digital debe convertirse en criterio troncal de innovación, regulación y gasto público.

PIERRE-YVES HENTZEN, PRESIDENTE Y CEO DE STORMSHIELD

Europa depende en exceso de proveedores tecnológicos externos, con un 80% del gasto cloud en manos de EE.UU. Esta brecha amenaza su autonomía, innovación y seguridad. El Observatorio de Soberanía Digital evidencia que el debate es ya político. Ahora, el desafío es pasar de las palabras a la acción.

OBSERVATORIO DE SOBERANÍA DIGITAL

La interconectividad digital ha traído eficiencia y escala, pero también una dependencia que ya es estratégica. Según Cigref, el 80%, es decir, 265.000 millones de euros, del gasto europeo en software y servicios profesionales en la nube, fluye hacia empresas estadounidenses. Esto no es solo un desequilibrio comercial, sino una pérdida de control sobre herramientas críticas para la autonomía estratégica, la continuidad económica y la seguridad nacional.

El lanzamiento de un Observatorio de Soberanía Digital revela que el tema ha escalado al centro de la agenda política. Es hora de pasar de las declaraciones a la ejecución.

La soberanía digital consiste en que un Estado o bloque sea dueño de sus infraestructuras, sus datos y su capacidad de elección tecnológica, garantizando el cumplimiento regulatorio. Renunciar a perseguirla equivale a delegar márgenes de maniobra en actores foráneos, con impactos en innovación local, exposición a injerencias y riesgos de espionaje.

Europa, hoy, depende en exceso de tecnologías y cadenas de suministro externas y el resultado es fragilidad: interrupciones en servicios críticos, subidas de costes de hasta un 4.000% en ciertos componentes en los últimos años y vulnerabilidad ante normativas extraterritoriales, como el Cloud Act, que puede alcanzar datos corporativos europeos sensibles, ya sea militares, industriales, comerciales o políticos.

CAPACIDAD EUROPEA PARA ESTABLECER OBJETIVOS

Para afrontar los retos de la soberanía digital, Europa ha emprendido una estrategia estructurada basada en

varias líneas de acción complementarias.

Desde el punto de vista regulatorio, marcos como el GDPR, Cyber Resilience Act y EUCC (Esquema Europeo de Certificación de Ciberseguridad) están sentando las bases de una economía digital soberana conforme a estándares europeos.

El objetivo es establecer reglas claras que protejan a las personas y proporcionen un marco a los agentes económicos. A ello se suma la cooperación intraeuropea en intercambio de información, normas comunes y respuesta a incidentes. Además, la I+D recibe una inyección relevante: el programa Horizon Europe 2025 moviliza más de 7.300 millones de euros con 1.600 millones para acelerar una IA alineada con valores europeos. En paralelo, la UE promueve soluciones de ciberseguridad "made in Europe".

Pero la brecha entre discurso y práctica persiste. Un barómetro de Ipsos y Yousign indica que el 78% de decisores reconoce la importancia de soluciones locales, aunque solo el 32% las prioriza en inversión. ¿Debe, por tanto, introducirse una preferencia explícita por tecnologías europeas en la contratación pública? ¿Cabe explorar cuotas o criterios reforzados para impulsar el ecosistema? No se trata de proteccionismo ciego, sino de interiorizar riesgos geopolíticos y de continuidad de negocio que hoy el precio no refleja.

EUROPA, ANTE UN CAMBIO CULTURAL

Europa necesita además un cambio cultural: asumir que la soberanía digital no es un proyecto técnico, sino una política industrial transversal. Eso implica decisiones informadas que integren seguridad, origen, interoperabilidad y resiliencia en su justa jerarquía, con métricas y auditorías verificables. El objetivo no es cerrar puertas, sino diversificar dependencias, elevar estándares y crear capacidad propia en cifrado, infraestructuras certificadas y gobernanza de datos.

DIGITALIZACIÓN

La soberanía digital debe convertirse en criterio troncal de innovación, regulación y gasto público. Frente a tensiones geopolíticas crecientes y amenazas híbridas, Europa solo será competitiva si ancla su digitalización en capacidades propias, reglas exigentes y mercados que premien —no penalicen— la seguridad y la autonomía. ✱

ALARMA Y CONTROL

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

BOSCH
Innovación para tu vida

BOSCH

C/ Hermanos García Noblejas, 19
28037 Madrid
es.securitysystems@bosch.com
www.boschsecurity.es

IRONLOCK
C/ Tomás Redondo, nº2
28033 Madrid
Teléfono: 902 112 777
www.ironlocksistemas.com

CERTIFICACIONES

SALTO
Pol. Lanbarren, Arkotz Kalea, 9,
Arragua, 20180
Oiartzun, Gipuzkoa
Tel.: 943 344 550
www.saltosystems.com/es-es/

IMQ IBÉRICA S.L.
C/ Velázquez 126 5º A.
28006 Madrid
Tel. 91 401 22 25
www.imqiberica.com
info@imqiberica.com

RadioBit Sistemas, S.L.
C/ Relleu, 4, Edif. Romeral 2,
Escalera 3, Local 3
(03502 Benidorm)
Tel.: (+34) 96 585 64 57
info@vigilant.es
https://vigilant.es/

CONTROL DE ACCESOS ACTIVO

ZKTeco Europe
Carretera de Fuencarral 44.
Edificio 1 Planta 2.
28108 Alcobendas. Madrid. Spain
Tel.: 91 653 28 91
Fax: 91 659 32 00

iberia@zkteco.eu

DETECCIÓN DE EXPLOSIVOS

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

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

DICTATOR ESPAÑOLA
DICTATOR ESPAÑOLA
C/ Montcada, 8.
Pol. Ind. Camp de les pereres.
08130 Santa Perpetua de la Mogoda
Barcelona
www.dictator.es
dictator@dictator.es

PROTECCIÓN CONTRA INTRUSIÓN. ACTIVA

EASY-DETECT
Passeig dels Ferrocarrils Catalans 143
08940 Cornellá de Llobregat
(BARCELONA)
Teléfono: +34 935 172 933

www.easy-detect.com
info@easy-detect.com

ROBOTNIK AUTOMATION

Ronda Auguste y Louis Lumiere, 8
46980 Parque Tecnológico – Paterna

Tel. 961 475 400

TELECOMUNICACIONES

DAHUA IBERIA, S.L.

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

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

DALLMEIER ELECTRONIC ESPAÑA
C/ Princesa 25 – 6.1 (Edificio Hexágono)
Tel.: 91 590 22 87
28008 • Madrid
dallmeierspain@dallmeier.com
www.dallmeier.com

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

HIKVISION SPAIN

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

QNAP

Calle de Anabel Segura, 10. 3ª planta,
Edificio Fiteni, 28108 Alcobendas,
Madrid

Tel: +34 91 184 64 15
www.qnap.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

Fermax
Avenida Tres Cruces, 133
46017 Valencia (España)
Tel: (+34) 96 317 80 00
fermax@fermax.com
www.fermax.com

TP-LINK ESPAÑA, S.L.

C/ Quintanavides, 17, 3ºE – 28050
Madrid
Tel.: 91 200 07 27

www.tp-link.com/es/

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

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

AKUVOX

10th Flr, No.56 Guanri Road, Software
Park II, Xiamen, Fujian (China) 361009
Tel: +34 603701273
www.akuvox.com
sales@akuvox.com

VISIOTECH

C. de Alberto Sánchez, 31,
Vicálvaro, 28052 Madrid
comercial@visiotechsecurity.com
Tel.: 911 836 285
www.visiotechsecurity.com/es

ASOCIACIONES

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

VIGILANCIA POR TELEVISIÓN

i-PRO Co., Ltd.,
Laarderhoogtweg 25,
Amsterdam-Zuidoost
1101 EB Amsterdam, the Netherlands
Tel.: +39 3401344982

https://i-pro.com/
i-PRO EMEA info.eu@i-pro.com

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

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

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

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

INTEGRACIÓN DE SISTEMAS

SECURITAS DIRECT
C/ Priégola 2. 28224,
Pozuelo de Alarcón

www.securitasdirect.es

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

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

GENETEC
Calle Velazquez 157 - Business Center Ibercenter,
Madrid 28002 – Spain
Tel: (+34) 91 52 45 771
www.genetec.com/es

TRANSPORTE Y GESTIÓN DE EFECTIVO

FEDERACIÓN ESPAÑOLA DE SEGURIDAD
C/ Vizcaya, 4. Local
28045 Madrid
Tel.: 915 542 115
fes@fes.es
C/C: comunicacion@fes.es

CIBERSEGURIDAD

VIGILANCIA Y CONTROL

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

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

INETUM ELECTRONIC SECURIT

C/ María de Portugal 9-11;
28050 Madrid

inetum.world/es

ILUNION

C. de Albacete, 2,
Cdad. Lineal,
28027 Madrid

www.ilunion.com/es/servicios/empresa-seguridad-vigilancia

DRONES

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

KAPRES TECHNOLOGY
Dirección: Calle de Emilio Muñoz, 3, 2º Derecha
Teléfono: +34 919 351 031

info@kapres.es
kapres.es

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

WOLFAVIONIC

C/ Pollensa, 6
28290 Las Rozas (Madrid)

www.wolfavionic.com

Peldaño

Nuestro mejor regalo eres tú.

Gracias por formar parte del camino
y por confiar en nosotros para impulsar
tu negocio.

Peldaño te desea unas felices fiestas
y un feliz 2026.

NAN ARQUITECTURA · mab HOSTELERO · GD · AUTOC · CONTACT CENTER HUB · TECNOHOTEL

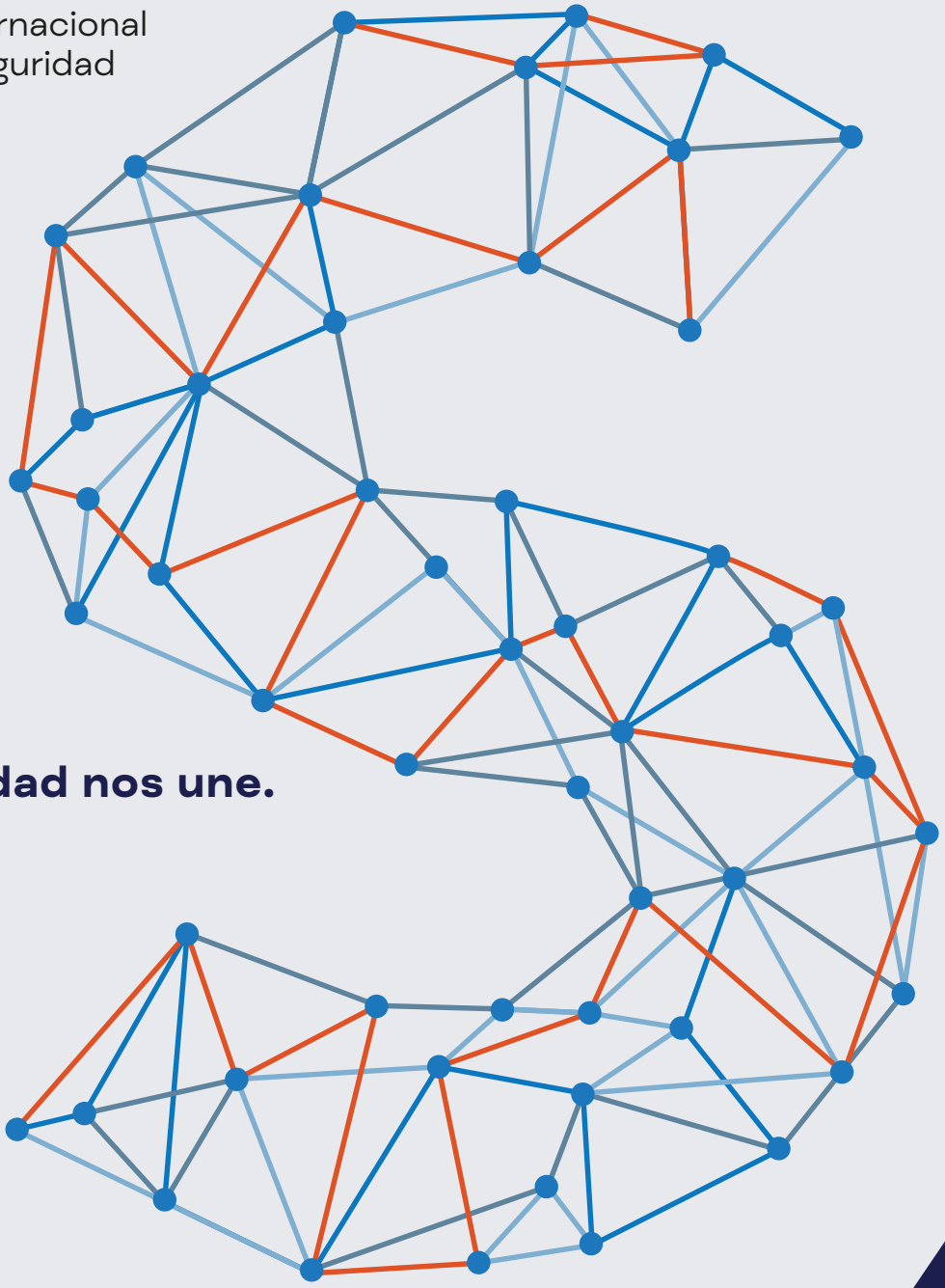
diffusionSPORT · Restauración News · campingsalon · Camping Profesional · CUADERNOS DE SEGURIDAD

Comunicamos. Conectamos. Impulsamos.

sicur

Salón Internacional
de la Seguridad

QUIERO
PARTICIPAR



La seguridad nos une.

24-27 Feb **2026**

ifema.es

IFEMA
MADRID