ADSI
asociación de directivos de seguridad integral
30 año
NEWS flash
#528 - Octubre 2026



Entrevista socia

Paola Laguna Palacios

Artículo de Opinión

Noticias ADSI

Junta Directiva

Presidente
Eduard Zamora

Vicepresidenta
Elvira Márquez

Secretario
David Sanmartín

Tesorero
Emilio Herrero

Vocales
Lourdes Castellsaguer
Francesc Chía
Joan Figuera
Isabel García
Oscar Molins
Míriam Pérez
Macarena Ramisa
Joan Roda
Jordi Silvestre
Oriol Verdura

Defensor del Socio
Miguel E. Arredonda

En este número ...

3
Patrocinadores ADSI

4
Nota de condolencias

5
Carta del presidente

6
Artículo de opinión
- El Espejismo del Cumplimiento NIS2, CER y las Normas ISO en el Sector Privado y la Administración Pública

8
Entrevista a una socia

12
Artículo
- Trabajar movilidad y estabilidad con sentido
- El conocimiento como nuevo activo estratégico: de proteger la información a proteger la ventaja tecnológica

13
Noticias ADSI
- ADSI en el acto inaugural del curso académico 2026-2027 del Institut de Seguretat Pública de Catalunya
- ADSI en la celebración del 45º aniversario del Capítulo 143-España de Asis Internacional
- ADSI en la celebración de la Patrona de la Guardia Civil en la Comandancia de Barcelona
- ADSI en la celebración del Dia Català de la Seguretat Privada
- ADSI presente en la conferencia regional de España 2026 de TAPA EMEA
- ADSI presente en la jornada del Foro "Profesiones de futuro" de su patrocinador Sabadell Profesional
- ADSI presente en la jornada de la asociación EFITEC
- Narcotráfico, blanqueo de capitales y empresa
- ExpoProtection 2026
- ExpoSecurity 2026
- TECNOSEC dronexpo
- Tu arma, tu responsabilidad

26
Actualización de datos

27
Nuestros patrocinadores
- ARMONIA
- CLECE
- COLLBAIX
- CSL
- DORLET
- HIRSCH
- LANACCESS
- RKL

44
Formación

53
Revistas y enlaces de interés

54
Lectura recomendada

La opinión manifestada por los autores de los artículos publicados a título personal que se publican en este medio informativo no necesariamente se corresponde con la de ADSI como Asociación.

Esta comunicación se le envía a partir de los datos de contacto que nos ha facilitado. Si desea cambiar su dirección de correo electrónico dirija su petición por correo postal a "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, o mediante e-mail a vicepresidente@adsi.pro

Si o no desea recibir nuestros mensajes informativos utilice los mismos medios, haciendo constar como asunto "DAR DE BAJA". Su petición será efectiva en un máximo de diez días hábiles.


accesor
Soluciones en control de accesos y seguridad


AIRBUS


SEGURIDAD
ALERTA y CONTROL
SEGURIDAD


ARMATURA


ARMONIA
SEGURIDAD


AXIS
COMMUNICATIONS


Grup
Barna
Porters


by demes
GROUP


chillida


Clece
SEGURIDAD


COLLBAIX
access solutions


CoreWeave


CSL


DORLET


Ecommunicator
SMART SAFETY


EULEN
SEGURIDAD


EuroSegur
PUERTAS DE SEGURIDAD


F24


FERRIMAX
ADVANCEDSECURITYSOLUTIONS


PUERTAS CORTAFUEGOS
PUERTAS
GISMERO
PUERTAS ACÚSTICAS


GONBER
SEGURIDAD
DGP4452


HIRSCH


ILUNION
Seguridad


IMAN
SEGURIDAD


INDRA
GROUP


INTERNATIONAL
SOS


Iron
Lock
Sistemas


LANACCESS
Discover the power of video.


mkv
medialab


PETROSECUR
SECURITY & DEFENSE


PROSEGUR
SECURITY


PYCSECA
seguridad


RKL
integral


Sabadell
Professional


SABICO
group


SCATI


TARGET
TECNOLOGIA


Trablisa
SERVICIOS DE SEGURIDAD


VIGI
by tp-link

Afectados por el accidente ferroviario en Urda (Toledo)

En estos momentos de desolación, la JUNTA DIRECTIVA de ADSI expresamos nuestras más sinceras condolencias a las familias de los fallecidos y nuestra profunda solidaridad y cercanía, tanto a ellas como a todos los afectados, por el terrible accidente ferroviario ocurrido en Urda (Toledo) que ha asolado a toda España. Nos unimos a todos ellos en su dolor y transmitimos nuestros ánimos más sinceros, como seguro hace toda la sociedad del país.

Gracias a todos los efectivos de las Fuerzas y Cuerpos de Seguridad, la UME, Bomberos, Protección Civil, Cruz Roja, y un largo etcétera, por la labor encomiable que habéis realizado.



Descontento y desconfianza

Hemos vivido en estos días dos graves circunstancias, aunque bien diferenciadas entre ellas por la tipología y consecuencias, pero evidencian un notable malestar de nuestra sociedad.

El gravísimo accidente ferroviario de Urda (Los Yébenes-Toledo) del 28 de octubre, que sumado al del pasado 18 de enero en Adamuz (Córdoba) conmociona a todos, y en especial a los usuarios de la Alta Velocidad y acrecienta la desconfianza en la seguridad de este servicio esencial de comunicación de nuestro país.

España ha apostado por incrementar sobremanera los quilómetros de Alta Velocidad y la intensidad de uso de sus vías (que todavía permitirían mayor número de servicios, según los expertos), pero parecería que no ha realizado las inversiones precisas en mantenimiento y seguridad, tanto en vías, sistemas técnicos o procedimientos.

La mayoría de nuestras empresas no nos toleraría incidentes de este tipo y exigiría responsabilidades si no hubiésemos sido capaces de proponerles un adecuado y robusto plan de mantenimiento y dotación de elementos, sistemas y procedimientos de seguridad. Otra cosa sería que, propuestos se denegasen o dilatasen en el tiempo, con lo que la responsabilidad recaería en los directivos del nivel decisorio que asumieron el riesgo con su decisión.

Entre nuestras propuestas, seguramente se encontraría la de no confiar tan sólo al factor humano, y todavía menos unipersonal, decisiones que puedan causar resultados como los vividos en el último accidente. Uno de nuestros lemas básico, como Directores y Directivos de Seguridad, es el de dotar de sistemas tecnológicos redundantes o que, de fallar estos, requerir duplicidad de personas expertas para tomar decisiones críticas.

Esperemos que las mejoras que todos exigen ahora, con la desgracia consumada, se implanten lo antes posible y no haya que esperar nuevos accidentes para que la mejora de la seguridad, en todos sus campos, sea un elemento esencial en la gestión de esta actividad de alto riesgo.

La segunda situación a la que me refería es la de los graves saqueos vandálicos provocados por quienes han seguido las convocatorias de Blocus, mimetizando lo ocurrido antes en Francia, Italia y Alemania, que en la primera convocatoria del fin de semana del 24 y 25 de octubre en España, especialmente en Barcelona y Bilbao, cogió desprevenidos a quienes deberían haber hecho una mejor evaluación del riesgo que implicaban, especialmente ante la gravedad de lo vivido en los países antes mencionados en fechas tan recientes.



De nuevo remarco que cualquiera de nuestras empresas nos exigiría responsabilidad por el grave error de cálculo en la evaluación de riesgos y medidas preventivas a aplicar.

Que se podía haber hecho mucho mejor entonces se evidencia en los resultados de este mismo fin de semana, cuando las detenciones preventivas, las advertencias mediáticas de tolerancia cero e imputación a los tutores de los menores, además del amplio despliegue policial han motivado un resultado bien diferente, casi sin incidentes, pese a la mayor relevancia de las convocatorias de Blocus.

Tras esa primera actuación de evitar daños a establecimientos comerciales y mobiliario público, como objetivo de inmediatez, se debería analizar por expertos el motivo por el cual tantos jóvenes, la gran mayoría muy menores de edad, se suman a esas llamadas y, lo que es peor, en ellas actúan como vándalos y delincuentes de la peor calaña.

Formación, información y concienciación de esos menores y sobre sus familias merecerían mayor atención para minimizar estas situaciones tan alejadas del derecho de manifestación y de promover y reivindicar iniciativas de mejora de todo aquello que preocupa a la ciudadanía.

Se hacen precisos estudios técnicos para conocer problemáticas y proponer soluciones a ese descontento latente de los menores y su incapacidad para valorar correctamente las consecuencias de actuaciones como las que nos ocupan.

Unos adecuados planes de trabajo en esas líneas, junto a la adecuada formación-información-concienciación que minimice esas conductas antisociales vandálicas fuera de logar, habrán de acompañarse de cambios legislativos para exigir responsabilidades por sus actos a los propios menores y/o a sus tutores legales, como una medida disuasoria relevante para evitar estos vandalismos totalmente fuera de lugar en nuestra sociedad.

No hablo de controlar mentes, sino de analizar causas, conocer inquietudes y frustraciones e implantar correctos planes de actuación sobre esas problemáticas, en especial cuando vemos que, en muchos casos hablamos de personas en edad casi infantil que vandalizan gravemente nuestras ciudades. ■

El Espejismo del Cumplimiento NIS2, CER y las Normas ISO en el Sector Privado y la Administración Pública

Por Jordi Silvestre, Vocal de ADSI

En los parlamentos durante la entrega de premios de ADSI, me pareció estar viviendo en el día de la marmota con los comentarios sobre el reglamento que debería acompañar a la Ley de Seguridad Privada 5/2024. Desde hace unas cuantas reincidencias sobre el tema en determinados foros del sector, se incorporan a los comentarios del reglamento algo sobre la "NIS2".

Desde entonces, y solo en este mes de octubre, se ha marcado en negro para la ciberseguridad por las batallas hibridas, la IA, y la vulnerabilidad en WordPress (PHP) que ha expuesto a millones de servidores en el mundo. El cambio climático también anotó siniestros por estas tierras, donde todavía estamos digiriendo la última DANA en la costa Mediterránea. En el ámbito social de nuestro entorno más próximo, es manifiesta la escalada en violencia de las acciones reivindicativas con ejemplos en Francia, Barcelona o Madrid.

Y la curiosidad del novato en estos temas me llevó a repasar unas notas de trabajo, que empiezan con una directiva europea sobre Infraestructuras Criticas de 2008, que llegó a nuestro ordenamiento jurídico en 2011. También encontré que, en julio de 2016, la UE aprobó la directiva NIS1, que se traspuso en el 2018 y 2021 con el RD 12/2018 para llegar el reglamento técnico con el RD 43/2021.

Con la persistencia de la UE, se actualizó la directiva sobre infraestructuras con la Directiva CER (Resiliencia Entidades Criticas) de 2022, esta nueva norma amplía la protección más allá de la seguridad física tradicional, obligando a los Estados miembros a blindar la resiliencia operativa global de las infraestructuras frente a sabotajes, crisis climáticas o emergencias sanitarias. Además, se aprobó en octubre de 2024 la Directiva NIS2 (Protección de Información y Redes) con la promesa de un continente ciber-resiliente. Ambas Directivas esperando su trasposición a nuestro ordenamiento jurídico con el plazo ampliamente superado.

Esta avalancha regulatoria, la escalada en riesgos (conocidos o emergentes), y los limites presupuestarios, lleva la realidad operativa en Seguridad de las Compañías a apoyarse en las certificaciones y estándares internacionales como UNE-EN ISO/IEC 27001 (Seguridad de la Información) y la ISO 22301 (Continuidad de Negocio) junto al esquema nacional de seguridad (ENS).

Con NIS2 la responsabilidad salta del Departamento de Seguridad a la sala de Juntas corporativa y a los despachos de las instituciones del Estado (ministerios, autonomías, ayuntamientos, etc.). La convergencia entre la Seguridad Física y Lógica nos llevan a una visión holística de la seguridad, ya que un ransomware puede afectar una cámara de CCTV, una línea de producción o la sede digital de cualquier ayuntamiento. La unificación de CSO y CISO mejora claramente la capacidad de respuesta ante incidentes críticos. La supervisión del riesgo de terceros también es una fortaleza ya que refuerza la seguridad de la cadena de suministro, afectando tanto a público como a privado.



Las grandes compañías y entidades de la Administración cumplirán con NIS2 y CER, pero será interesante comprobar el músculo de las Administraciones locales y PYMES, para el cumplimiento, sobre como para la notificación de incidentes y aplicación de los planes que se desencadenan. Las organizaciones que operan en varios países de UE, ya sufren las asimetrías en la aplicación. Como ejemplo la rigurosidad sancionadora alemana, o la falta de trasposición española, a la que hay que sumar las probables divergencias interpretativas entre las instituciones.

Cuando llego a esta parte de mis apuntes, me asalta la duda si se trata de construir ecosistemas más seguros o se está alimentado una maquinaria burocrática experta en auditorias y sanciones. Con tanta burocracia, auditoria y checklist toma relevancia el evitar la falsa sensación de seguridad por tener una certificación de conformidad sobre la gestión, pero no se garantiza la invulnerabilidad frente amenazas o ataques ni la mejor respuesta para el control del daño y la recuperación de la normalidad.

Sobre todo, parece un reto para el director de seguridad, y el departamento que lidera, el contentar al regulador y facilitar la misión de su organización con este marco regulado de mínimos y con recursos finitos.

Después de un vistazo rápido a cuatro notas, el debate sobre un reglamento de seguridad privada ha incorporado tantas variables que, incluso, hace antigua la Ley que acompañaría.

El liderazgo de la Seguridad en estos tiempos va más allá de reunir sellos de certificación, cumplir con la legislación o auto felicitarse. El éxito estará en cambiar la cultura de la Seguridad del ciudadano, las organizaciones o el Estado, para que la resiliencia operativa y física sea real. ■



Hazte socio de ADSI

¿Quieres ser Socio de ADSI – Asociación de Directivos de Seguridad Integral?

Para iniciar el proceso de alta como Asociado, envíe un email a vicepresidente@adsi.pro, indicando nombre y apellidos, una dirección de correo y un teléfono de contacto.

En cuanto recibamos su solicitud le enviaremos el formulario de Solicitud de Admisión.

¿Quién puede ser socio de ADSI?

- Quien esté en posesión de la titulación profesional de Seguridad Privada reconocida por el Ministerio del Interior (T.I.P. de Director de Seguridad, Jefe de Seguridad, Detective Privado o Acreditación de Profesor de Seguridad Privada).
- Todo Directivo de Seguridad que posea, a criterio de la Junta Directiva de la Asociación, una reconocida y meritoria trayectoria dentro del sector.

Paola Laguna Palacios

Corporate Security Specialist, PROSEGUR

¿En qué campos de la seguridad se centra tu día a día y que función desempeñas?

En la actualidad, desarrollo mi actividad profesional en España dentro del ámbito de la seguridad corporativa, colaborando en el departamento de seguridad de una reconocida marca española del sector de la automoción. Mi labor se centra en colaborar con la planificación y gestión de la seguridad de eventos, así como en la realización de investigaciones y análisis OSINT orientados a la identificación temprana de riesgos y la prevención de amenazas. Esta experiencia me ha permitido desarrollar una visión más amplia de la seguridad desde una perspectiva internacional, integrando las realidades y enfoques de México y España.

¿Principales retos o proyectos relacionados con la seguridad en tu empresa?

Hoy en día la seguridad se enfrenta al desafío de operar en un escenario cada vez más cambiante, donde las amenazas evolucionan con rapidez, impulsadas en gran medida por la transformación tecnológica, lo que exige una adaptación constante de las estrategias de seguridad.

En este contexto, el objetivo es mantener la capacidad de anticipación que permita identificar vulnerabilidades emergentes, evaluar su impacto y adaptar las medidas de protección de manera ágil y eficaz. Más que responder a los desafíos cuando ya se han materializado, el enfoque debe estar orientado a la prevención, la gestión proactiva del riesgo y la mejora continua de los procesos de seguridad.

¿Cuál es tu formación académica?

Soy Licenciada en Geografía egresada de la Universidad Nacional Autónoma de México (UNAM) y poseo un Máster en Dirección de Seguridad Privada por la Universidad de Barcelona. Complementé mi formación con estudios especializados en análisis de inteligencia e inteligencia geoespacial en la Escuela de Inteligencia para la Seguridad Nacional de México, entre otras instituciones, lo que sumado a mi experiencia profesional me permite aportar una visión estratégica para la gestión de riesgos y la seguridad en entornos complejos.

¿Cómo accediste al mundo de la Seguridad y en qué empresas / responsabilidades has ido avanzando desde entonces?



Mi ingreso al mundo de la seguridad se dio en el ámbito de la administración pública, cuando me incorporé al proyecto de Fusión de Inteligencia del Centro Nacional de Inteligencia (CNI) en México. Formé parte de un equipo interdisciplinario de analistas de inteligencia, donde mi principal aportación consistió en integrar la geografía y el análisis geoespacial como herramientas tecnológicas para fortalecer los procesos de inteligencia, la toma de decisiones y el desarrollo de operaciones dirigidas al combate del narcotráfico y el crimen organizado.

Posteriormente, me incorporé a la Fiscalía General de la República, asumiendo responsabilidades en inteligencia estratégica aplicada a la seguridad y la investigación del crimen organizado, mediante la elaboración de análisis e informes, así como la coordinación de operativos terrestres y misiones con sistemas RPAS (Sistema de Aeronave Pilotada de Forma Remota).

Mi transición al sector privado se dio en Aguila Ammunition, donde desarrollé la creación del Centro de Control y Comando, responsable del monitoreo de activos, transporte y sistemas de videovigilancia, así como de la coordinación de los servicios de protección ejecutiva y la respuesta ante incidentes. Posteriormente, fui promovida a Gerente de Seguridad Patrimonial, liderando equipos de seguridad, la protección de activos críticos, la relación con autoridades y la implementación de estrategias orientadas a la reducción de riesgos y pérdidas.

Actualmente, desarrollo mi carrera profesional en Barcelona en el ámbito de la seguridad corporativa, colaborando en la planificación y gestión de la seguridad de eventos de alto nivel, la elaboración de análisis de riesgos y el desarrollo de investigaciones OSINT para una destacada marca española del sector de la automoción. Mi labor está orientada a la identificación de riesgos y la

protección de activos y personas en un entorno corporativo internacional.

¿Cómo crees que ha evolucionado la Seguridad desde tus inicios hasta ahora?

Creo que la seguridad ha evolucionado de forma muy significativa, pasando de un enfoque principalmente físico y reactivo a un modelo mucho más estratégico, tecnológico y preventivo. Cuando inicié mi carrera, gran parte de los esfuerzos se centraban en amenazas tradicionales relacionadas con la seguridad física y el crimen organizado; sin embargo, la transformación digital ha incorporado nuevos riesgos asociados al ámbito tecnológico, la gestión de la información, la ciberseguridad y la exposición en entornos digitales.

Además, la irrupción de tecnologías como la inteligencia artificial está transformando la manera en que identificamos, analizamos y anticipamos amenazas, al tiempo que plantea nuevos desafíos para las organizaciones. Esta evolución ha obligado a los profesionales de la seguridad a adaptarse constantemente, incorporar nuevas herramientas y desarrollar una visión más integral que permita anticipar riesgos en un entorno cada vez más global, interconectado y tecnológicamente complejo.

¿Cómo ves la profesión de director de seguridad en el medio/largo plazo, qué cambiarías de la misma y como crees que evolucionará?

Considero que la profesión de Director de Seguridad evolucionará hacia un modelo más estratégico, tecnológico y orientado a la anticipación. Para hacer frente a nuevas amenazas, será necesario incorporar herramientas digitales y tecnologías avanzadas, además de mantener una actualización constante de conocimientos. En mi opinión, la toma de decisiones no deberá estar excesivamente centralizada, sino que deberá apoyarse en equipos multidisciplinares de especialistas que aporten distintas capacidades y permitan responder de forma ágil y eficaz a escenarios más complejos y cambiantes.

¿Exigirías Departamento de Seguridad a las empresas en función del nº de empleados, nº de centros de trabajo, nº de ocupantes, de sus riesgos específicos, etc., o consideras que debe ser de libre creación en todo caso?

Desde mi punto de vista, la exigencia de disponer de un Departamento de Seguridad no debería establecerse únicamente en función del número de empleados o de centros de trabajo, sino principalmente atendiendo al nivel de criticidad de la actividad, el contexto operativo, el tipo de industria y los riesgos específicos de cada organización. Especialmente, debería valorarse si se trata de una instalación estratégica o de un sector esencial. En definitiva, el criterio debería ser la necesidad real de protección y el impacto que un incidente podría tener sobre las personas, la actividad empresarial, los servicios esenciales o los bienes, adaptando las exigencias de seguridad en proporción al nivel de riesgo.

¿Te parece correcto disponer de dos vías formativas tan diferenciadas para obtener la habilitación como Director de Seguridad (curso de habilitación TIP de un año, o grado universitario de 4 años) y que cambiarías?

Considero que es positivo que existan diferentes vías de acceso a la habilitación, ya que ello permite incorporar perfiles con trayectorias y experiencias diversas que enriquecen la profesión. No obstante, creo que el debate no debería centrarse únicamente en la duración de la formación, sino en garantizar que todos los profesionales alcancen un nivel homogéneo de competencias, conocimientos y capacidades para asumir responsabilidades y tomar decisiones.

En mi opinión, tanto la formación académica universitaria como los programas específicos de habilitación aportan valor, aunque desde enfoques distintos. Por ello, más que establecer una preferencia por una u otra vía, avanzaría hacia un modelo que combine una sólida base teórica con una fase práctica que permita trasladar los conocimientos al entorno real de la seguridad.

En síntesis, apostaría por un modelo equilibrado que combine formación inicial de calidad, experiencia práctica acreditada y actualización continua, poniendo el foco en las competencias reales más que en la duración de la vía formativa elegida.

¿En la formación para ejercer como director de Seguridad, que materias o aspectos deberían potenciarse, que no se traten en profundidad ahora?

Sería conveniente potenciar contenidos relacionados con la transformación digital, la ciberseguridad y, especialmente, la aplicación de la inteligencia artificial como herramienta de apoyo para el análisis predictivo y la detección y análisis de riesgos y amenazas.

Dicha transformación ha generado un entorno en el que

los riesgos físicos y tecnológicos están cada vez más interconectados, por lo que el Director de Seguridad debe comprender cómo integrar ambas dimensiones dentro de una estrategia de seguridad global.

Asimismo, considero que debería reforzarse la formación práctica en gestión de crisis, continuidad de negocio, así como el liderazgo en equipos de trabajo multidisciplinares. En muchas ocasiones, el éxito de una estrategia de seguridad no depende únicamente de los conocimientos técnicos, sino de la capacidad para coordinar recursos, tomar decisiones bajo presión y gestionar escenarios complejos.

¿Ventajas de integrarse en una asociación de profesionales de la seguridad?

Integrarse en una asociación aporta un importante valor añadido tanto a nivel de desarrollo profesional como de actualización continua. Permite acceder a una red de expertos (networking) con los que se puede compartir experiencias, buenas prácticas y conocimientos sobre el sector, favoreciendo el intercambio de información y la generación de contactos profesionales.

Adicionalmente suelen promover actividades formativas, jornadas técnicas y foros especializados que ayudan a mantenerse al día en aspectos normativos, tecnológicos y operativos. Desde mi punto de vista, en un entorno tan dinámico como el de la seguridad, formar parte de una asociación profesional facilita el aprendizaje continuo, amplía la visión estratégica y favorece el crecimiento profesional a largo plazo.

¿Qué te ha llevado a afiliarte a ADSI en concreto?

Durante el Máster de Seguridad Privada tuve la oportunidad de conocer ADSI a través de una de las ponencias impartidas por su presidente, lo que me permitió descubrir de primera mano la labor que desarrolla la asociación y su contribución al sector de la seguridad. Recién llegada de México, me pareció una excelente oportunidad para comprender mejor la realidad de la seguridad en España, intercambiar experiencias con otros profesionales y ampliar mi red de contactos en el sector.

Además, considero que formar parte de una asociación como ADSI favorece el intercambio de buenas prácticas y la creación de sinergias entre profesionales con diferentes perfiles, nacionalidades y trayectorias, aspectos que aportan un gran valor tanto a nivel profesional como personal.

¿Qué debe mejorar ADSI en relación con la prestación a sus asociados?

En mi opinión, potenciaría la creación de sinergias y alianzas estratégicas con otras asociaciones profesionales, no solo en España, sino también a nivel internacional. La seguridad es un ámbito cada vez más globalizado, donde los riesgos, las tendencias y los desafíos trascienden fronteras, por lo que la colaboración entre organizaciones de distintos países resulta fundamental para intercambiar experiencias.

En este sentido, sería interesante promover acuerdos de colaboración con asociaciones homólogas de Europa y otras regiones como América Latina para desarrollar jornadas técnicas conjuntas y programas de intercambio profesional, estas alianzas podrían fortalecer la capacidad de las asociaciones para impulsar iniciativas comunes, establecer una interlocución con universidades, instituciones, organismos internacionales y administraciones públicas. Esta visión colaborativa permitiría ampliar oportunidades para los asociados y contribuir al desarrollo y reconocimiento de la profesión a una escala mucho mayor.

¿Cómo podría incrementarse la colaboración entre directores de seguridad de ámbitos/sectores/empresas diferentes de nuestro país?

La colaboración podría impulsarse a través del desarrollo de proyectos conjuntos entre empresas, asociaciones, universidades e instituciones, lo que contribuiría a crear una red de más sólida y transversal, favoreciendo el intercambio de conocimientos, la innovación y el fortalecimiento de la profesión en el país.

Sería fundamental fomentar la participación activa en casos prácticos reales, compartiendo experiencias, analizando incidentes, estudiando situaciones complejas y poniendo en común las soluciones adoptadas. Este enfoque permitiría aprender de situaciones concretas, identificar buenas prácticas y mejorar la capacidad de respuesta ante amenazas comunes, siempre respetando la confidencialidad de la información sensible.

En un mundo cada vez más globalizado y por tu experiencia, ¿destacarías algún país en la gestión de la seguridad y cómo mejorarías el intercambio de experiencias y conocimiento entre países?

No considero que exista un único país que pueda tomarse como referencia absoluta en materia de seguridad, ya que cada entorno presenta problemáticas, amenazas,

prioridades y marcos normativos diferentes. Más que destacar un modelo concreto de gestión, sería importante identificar las estrategias y prácticas que han demostrado ser eficaces en distintos contextos y evaluar su posible adaptación a cada realidad.

Por ello, creo que impulsar una mayor cooperación internacional entre profesionales e instituciones del sector, favorecería el intercambio de experiencias y casos de éxito. Este enfoque permite conocer soluciones innovadoras, anticiparse a riesgos emergentes, contribuyendo a una gestión de la seguridad más eficaz y alineada con los desafíos globales actuales. ■

- Un hobby: Uno de mis hobbies es apoyar a instituciones dedicadas al rescate y la protección animal, ya que me gusta promover su cuidado y bienestar. También me apasiona la botánica y la jardinería, especialmente la colección de cactáceas y crasuláceas. Disfruto estudiarlas, conocer sus características y nombres científicos, así como comprender las adaptaciones que han desarrollado para sobrevivir en distintos entornos.
- Un libro: Lecciones para volar, de Lilyan de la Vega, trata sobre el crecimiento personal, el amor propio y la importancia del autoconocimiento. A través de la relación con su abuela, la protagonista aprende valiosas lecciones sobre la vida, la confianza y la libertad. La obra enseña que para superar los miedos y las inseguridades es necesario aceptarse, reconocer nuestras fortalezas y dejar atrás lo que nos limita. Además, destaca la sabiduría de las personas mayores, la sororidad y el apoyo entre mujeres.
- Una canción: Fix You de ColdPlay, una canción muy especial para mí, transmite esperanza y resiliencia, anima a levantarse y a no rendirse ante la adversidad, me refleja la importancia de tener a la familia a tu lado para sostenerte, mi frase favorita es "Lights will guide you home", las luces te guiarán de regreso a casa.
- Un lugar para desconectar: Los acantilados de Irlanda (Cliffs of Moher). Es uno de esos sitios a los que me encantaría regresar para desconectar un poco de todo, disfrutar de la naturaleza y apreciar las vistas del océano Atlántico. Los paisajes son espectaculares, me parece un lugar increíble para pasear, respirar aire puro, olvidarte por un rato de la rutina y recargar energía.
- Un momento de la historia: Me habría interesado vivir la década de 1970, una época marcada por profundas transformaciones sociales y por el impulso de los movimientos en favor de los derechos de las mujeres. Me resulta especialmente inspirador cómo muchas lograron abrirse camino en ámbitos como la ciencia, la investigación, la academia, la tecnología y la política, contribuyendo al progreso de la sociedad y sentando las bases para las generaciones futuras.

ADSI 30 años
asociación de directivos de seguridad integral

Moverse más no siempre es moverse mejor. Movilidad y estabilidad deben responder a una necesidad real.

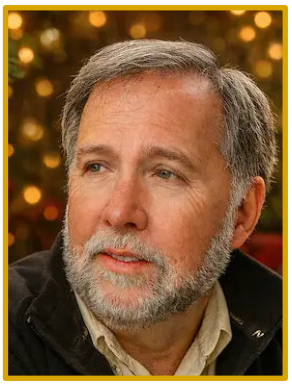
Por Francesc Sanahuja, Coordinador SECOT- Técnico en seguridad CEPREVEN y socio de ADSI

Adjuntamos la séptima parte de la serie de artículos sobre prevención y seguridad en los deportes de naturaleza que se publicarán sucesivamente en la revista ADSI.

Durante años, la prevención se ha asociado con frecuencia a estirar más. Pero ganar amplitud articular sin saber qué falta, dónde falta y para qué se necesita puede aportar poco. La movilidad útil no consiste en alcanzar el mayor rango posible, sino en disponer del movimiento necesario para la tarea deportiva.

Movilidad y estabilidad no son conceptos opuestos. Una permite moverse; la otra permite gobernar ese movimiento. El deportista necesita rango suficiente en tobillo, cadera, hombro o columna, pero también fuerza y control para utilizarlo cuando aumenta la carga, la velocidad o la fatiga.





Por eso tampoco debemos confundir estabilidad con rigidez. Mantener una plancha o realizar ejercicios sobre una superficie inestable puede tener sentido, pero solo si forma parte de una progresión que termina transfiriéndose al gesto real: correr, escalar, saltar, girar, lanzar o descender por terreno irregular.

La prevención debe empezar por una pregunta sencilla: ¿qué movimiento necesita realmente esta persona y puede controlarlo? A partir de aquí, pocas tareas bien elegidas y revisadas periódicamente resultan más útiles que una larga colección de estiramientos o ejercicios genéricos.

IDEA CENTRAL

movilidad útil
=
rango suficiente + fuerza dentro del rango + control de la tarea.

ENLACE ARTÍCULO 7

El conocimiento como nuevo activo estratégico: de proteger la información a proteger la ventaja tecnológica

Por Pedro Sebastián, CEO, Founder & Owner ESRM Consulting Global S.L

Proteger el Conocimiento (I) – La Amenaza

En un entorno marcado por la innovación, la transformación tecnológica y la creciente competencia estratégica, proteger la información ya no es suficiente. El verdadero desafío consiste en **proteger el conocimiento que permite a las organizaciones innovar, competir y mantener su ventaja tecnológica**.

Este artículo analiza la evolución de las amenazas contra el patrimonio tecnológico empresarial, abordando cuestiones como el espionaje tecnológico e industrial, la protección del know-how, los algoritmos, la propiedad intelectual, los procesos industriales y el talento como depositario del conocimiento crítico.

Asimismo, plantea la necesidad de identificar las **«Crown Jewels» tecnológicas** de cada organización y avanzar hacia una **Estrategia Corporativa de Protección del Conocimiento y la Tecnología (ECPT)**, integrando seguridad corporativa,inteligencia, contrainteligencia y gestión de riesgos.



Una reflexión dirigida especialmente a la Alta Dirección y a los profesionales de la seguridad sobre un nuevo paradigma: pasar de proteger información a proteger conocimiento para preservar la ventaja tecnológica y competitiva.

Artículo completo disponible para su lectura y descarga a través de **este enlace**.



ADSI en el acto inaugural del curso académico 2026-2027 del Institut de Seguretat Pública de Catalunya

El acto se celebró el 9 de octubre en las instalaciones del ISPC en Mollet del Vallès y ADSI asistió a dicha inauguración representada por su nuestro Presidente, Eduard Zamora.

Tras unas palabras iniciales de su Directora, Marta Roca, se impartió la magistral lección inaugural, "La cultura de la seguridad", por parte de José María Lassalle, profesor universitario, jurista, ensayista y experto en transformación digital.

Seguidamente se entregaron las distinciones honoríficas 2026 y clausuró el acto la Consellera d'Interior i Seguretat Pública de la Generalitat de Catalunya, Nuria Parlón.

Agradecemos al Departament d'Interior i Seguretat Pública la amable invitación a @ADSI.

En las imágenes, diversos de los momentos del acto.





ADSI en la celebración del 45º aniversario del Capítulo 143-España de Asis Internacional

El acto se celebró el 30 de septiembre en Madrid y ADSI asistió a dicha inauguración representada por su nuestro Presidente, Eduard Zamora.

Tras unas palabras iniciales de Elena Salas, Presidenta del capítulo 143-España de ASIS INTERNATIONAL, conocimos de la mano de algunos de sus expresidentes, la historia de esta asociación amiga de ADSI y en diversas mesas redondas los estándares ASIS y sus certificaciones profesionales.

Agradecemos a la Junta Directiva de ASIS INTERNATIONAL Capítulo 143 la amable invitación a ADSI para acompañarles en tan entrañable celebración.

En las imágenes, diversos de los momentos del acto y en la foto de grupo, los representantes de las asociaciones amigas de ASIS INTERNATIONAL que asistieron al acto. ■







ADSI en la celebración de la Patrona de la Guardia Civil en la Comandancia de Barcelona

El acto se celebró el 12 de octubre en el acuartelamiento de Sant Andreu de la Barca (Barcelona) y asistieron invitados por la Directora General de la Guardia Civil y el General de Brigada Pedro Pizarro, Jefe de la 7ª Zona Cataluña, Elvira Márquez, Vicepresidenta de ADSI, y Eduard Zamora, Presidente de ADSI.

El acto, que se inició con la habitual misa y posterior entrega de condecoraciones, para finalmente servirse un cóctel de networking y fue presidido por el Delegado del Gobierno en Catalunya, Carlos Prieto.



Agradecemos a la Zona de Catalunya y la Comandancia de Barcelona la amable invitación a ADSI.

En las imágenes, diversos de los momentos del acto y en una de ellas, de izquierda a derecha, Elvira Márquez, el General de Brigada Pedro Pizarro y Eduard Zamora.





ADSI en la celebración del Dia Català de la Seguretat Privada

ADSI ha asistido a la celebración del DIA CATALÀ DE LA SEGURETAT PRIVADA, organizado por la GENERALITAT DE CATALUNYA, celebrado el 15 de octubre en el Auditorio de Cornellà de Llobregat y que fue presidido por la Consellera d'Interior i Seguretat Pública, Núria Parlón.

En el acto se otorgó MENCION HONORÍFICA a dos de los integrantes de la Junta Directiva de ADSI: Jordi Silvestre, Vocal de ADSI, y Eduard Zamora, Presidente de ADSI, que en una de las imágenes se encuentran junto a la Consellera Parlón y la Secretaria General del Departament, Joana Ricardo.

ADSI agradece a la Conselleria d'Interior i Seguretat Pública de la Generalitat de Catalunya la invitación al acto y las condecoraciones otorgadas.

En las imágenes, diversos de los momentos del acto.









ADSI presente en la conferencia regional de España 2026 de TAPA EMEA

En base a los acuerdos de colaboración entre ADSI y TAPA EMEA, hemos asistido a la conferencia regional de España de nuestra asociación amiga, habiéndola ayudado previamente a materializar parte de la logística de su evento.

ADSI estuvo representada institucionalmente por nuestro Presidente, Eduard Zamora, en el evento celebrado en Madrid el pasado 21 de octubre, en el que se inscribieron más de 140 profesionales de la seguridad, para conocer de primera mano las diversas ponencias que se impartieron sobre protección del transporte por carretera, materia en la que TAPA es la asociación líder mundial.

La jornada fue inaugurada por el General de Brigada Antonio Cortés, responsable de la Jefatura de Armas, Explosivos y Seguridad, de la que depende el SEPROSE, órgano especializado de relación de Guardia Civil con el sector de la Seguridad Privada, seguida de la intervención de Filipe de Almeida, Embajador de APA EMEA para España y Portugal y Corporate Security & Business Resilience Manager de Rangel Logistics Solutions en Portugal.

Agradecemos a Filipe de Almeida y TAPA EMEA su amable invitación y atenciones. Esperamos seguir colaborando con ellos en todo lo preciso, en beneficio del sector.

En las imágenes, el momento de inauguración por parte del General Cortés, la intervención de Filipe de Almeida y una de las mesas de trabajo. En la foto de grupo, de izquierda a derecha, Daniel García Caellas, socio de ADSI, Director de Seguridad de DESIGUAL e integrante del grupo de trabajo de TAPA organizador del evento; el General Cortés; Filipe de Almeida y Eduard Zamora. ■









ADSI presente en la jornada del Foro "Profesiones de futuro" de su patrocinador Sabadell Profesional

ADSI ha asistido a una nueva jornada del Foro Profesiones de Futuro" de su patrocinador SABADELL PROFESSIONAL, el segmento de colectivos profesionales de BANCO SABADELL.

La jornada se celebró en la sede corporativa del Banco Sabadell en la calle Serrano de Madrid y en ella se debatió sobe el "Relevo generacional: el futuro de las profesiones".

ADSI acompaña a sus patrocinadores en los eventos que organizan y en esta ocasión estuvo representada institucionalmente por nuestro Presidente, Eduard Zamora.

Agradecemos #SABADELL PROFESSIONAL la invitación a la interesante jornada y el apoyo al proyecto asociativo de ADSI, del que son patrocinadores.

En una de las imágenes, de izquierda a derecha, Ignacio Lerroux González, Director Comercial de Sabadell Professional; Charo Fernández Alvarez, Directora nacional segmento de Sabadell Professional; Eduard Zamora y Alfons Rodríguez Morillo, Director Sabadell Professional em la Territorial Cataluña. En otra de ellas, de izquierda a derecha, Eduard Zamora, Charo Fernández y Montserrat Burriel Porcar, Directora de Segmento Institucional de la Territorial de Cataluña en Banco Sabadell. En las otras la mesa redonda de debate de la jornada y la intervención de Charo Fernández ante el auditorio.









ADSI presente en la jornada de la Asociación EFITEC

ADSI ha asistido a la jornada anual de EFITEC, Asociación de Profesionales de la Seguridad Bancaria que se ha celebrado los días 26 y 27 de octubre en el Euroforum de El Escorial. Ën esta ocasión coincidiendo con el 30 aniversario de la creación de la Asociación EFITEC, en su momento creada como FORO EFITEC.

En la misma, como es habitual, se debatió de la problemática habitual de seguridad de las entidades financieras, incluyendo en esta ocasión también materias relacionadas con los delitos de odio, criptografía post-cuántica, inteligencia, etc.

Otro de los aspectos brillantes de la jornada fueron los momentos de networking que se facilitaron a los profesionales y autoridades asistentes.

ADSI acostumbra a acompañar a las asociaciones hermanadas en sus actos institucionales, en esta ocasión representada por su Presidente, Eduard Zamora.

Agradecemos a EFITEC su amable invitación a la jornada y la felicitamos por la brillantez de sus contenidos y organización.

En una de las imágenes, el momento de presentación de la inauguración y en otra, de izquierda a derecha Humberto Hortelano, Secretario de EFITEC; Eduard Zamora, Presidente de ADSI; José Carlos Vázquez, Vicepresidente de EFITEC y Valentín Yebra, Presidente de EFITEC. ■





Foment del Treball Nacional

Narcotráfico, blanqueo de capitales y empresa

El cultivo y tráfico de Marihuana: una amenaza para la seguridad y la economía

20 NOVIEMBRE 2026

9:30 — **BIENVENIDA INSTITUCIONAL**

Sr. Vicente Codes, Presidente de la Comisión de Seguridad y Defensa de Foment del Treball Nacional
Sr. Josep Sánchez Llibre, Presidente de Foment del Treball Nacional
Hble. Sra. Núria Parlon, Consellera d'Interior i Seguretat Pública
Excmo. Sr. D. José Crespín, Delegado del Gobierno en Cataluña

10:00 — **MESA 1:** El nuevo narcotráfico: organizaciones criminales, territorio y respuesta policial

Ilmo. Sr. D. David Sánchez, Comisario Jefe de la Brigada Provincial de Policía Judicial de la Policía Nacional en Barcelona
Sr. D. Patrick Montes, Comandante Jefe de la Unidad de Policía Judicial de la Zona de la Guardia Civil de Cataluña
Sr. D. Josep Naharro, Intendente Jefe de la Comisaría General de Investigación Criminal de Mossos d'Esquadra

MODERA: Sr. Pere Garcia, Vicepresidente de la Fundació per la Seguretat Pública y Secretario General de FEPOL

10:45 — **MESA 2:** Narcotráfico en España y Cataluña: respuesta penal y retos de salud pública

Ilmo. Sr. D. Gerardo Cavero, fiscal especial antidroga de Barcelona
Ilmo. Sr. D. Ricardo Sanz-Gadea, Delegado en Barcelona de la Fiscalía Especial contra la Corrupción y Crimen Organizado
Sr. Emilio Zegrí, abogado penalista especialista en seguridad ciudadana y miembro de la Ponencia Jurídica de Foment
Dr. Joan Colom, ex-subdirector general de drogodependencias de la Generalitat de Catalunya

11:30 — **COFFEE BREAK**

11:45 — **MESA 3:** Impacto económico, fraude y el blanqueo de capitales

Sr. José Ignacio Lence, global head de financial crime Compliance de Banco Santander
Sr. Joan Torres, subdirector general y director de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo de Banco Sabadell
Sr. Victor Porcel, Head Massive Inspections de EDistribución
Sr. Óscar Enrique Morales , Gerente de Seguridad Operativa del Departamento de Seguridad e Inteligencia de CaixaBank

MODERA: Sr. Salvador Sedó, director de Seguridad y Defensa de Foment del Treball Nacional

12:30 — **PONENCIA:** Visión internacional ante una problemática global

Sr. John Fernández, ex agente especial y ex jefe de la unidad anti-narcoterrorismo de la DEA y asesor-enlace para asuntos policiales de la unidad de prevención de delitos financieros de UBS

13:00 — **CLAUSURA**

Hble. Sr. Ramon Espadaler, Conseller de Justícia i Qualitat Democràtica

Con el apoyo de:

Generalitat de Catalunya · mossos d'esquadra

Con la colaboración de:

CaixaBank · endesa · Sabadell · Santander · Fundació per a la Seguretat Pública

INSCRIPCIÓN

ExpoProtection 2026



En su 30.ª edición, EXPOPROTECTION, el salón internacional de la prevención y el control de riesgos, cita a los profesionales en Paris. En un contexto de policrisis, el evento reunirá a profesionales del sector bajo un eje estratégico: **"Descompartimentar la gestión de riesgos frente a la convergencia de las amenazas y las tecnologías"**, en la que será una plataforma europea de intercambio, influencia y soluciones al servicio de la resiliencia sostenible de las organizaciones.

EXPOPROTECTION se articulada en torno a 2 universos de referencia

La feria se organiza en dos universos de referencia, que permite a los actores de la prevención, expertos y decisores, acceder a una visión de 360° de la cadena de valor del riesgo de manera fluida y exhaustiva:

El Universo Riesgos Profesionales e Industriales: reúne los sectores Salud y Seguridad en el Trabajo, Prevención y Calidad de Vida, Condiciones de Trabajo, Salud y Seguridad en el Trabajo, Protección, Intervenciones y Socorro, y Riesgos Climáticos e Industriales.

El Universo Riesgos de Actos Malintencionados e Incendio: agrupa los sectores Seguridad y Protección, e Incendio.

En un contexto de rápidas transformaciones, la edición 2026 refleja una prevención en la que los desafíos de la seguridad física, los incendios y la salud en el trabajo se cruzan con la intensificación de los riesgos cibernéticos, climáticos y operativos. Esta dinámica está impulsada por la inteligencia artificial, la robótica y los sistemas conectados, que refuerzan la capacidad de anticipación, al mismo tiempo que plantean nuevos retos en materia de regulación.

Acerca de EXPOPROTECTION

Fundado en la década de 1960, **Expoprotection** celebra en 2026 su 30.ª edición. Esta cita bienal de la prevención y el control de riesgos reúne a cerca de 660 expositores y alrededor de 15.000 visitantes.

El salón ofrece una visión de 360° del mercado de la prevención de riesgos, ya sean profesionales, industriales, climáticos o vinculados a actos malintencionados.

En el evento se presentan las últimas innovaciones del sector, facilita reunirse con expertos de alto nivel y contactar con proveedores de soluciones eficaces para proteger a las personas y a las organizaciones frente al conjunto de amenazas a las que están expuestas.

Enlace e inscripciones gratuitas: ■

EXPO PROTECTION

ExpoSecurity 2026







La Feria de Altas Tecnologías de la Seguridad e Inteligencia, Drones y Antidrones, TECNOSEC DRONExpo celebra su V edición los próximos 5 y 6 de noviembre en el Madrid Arena.



TECNOSEC es un ecosistema de nuevos desarrollos de seguridad, inteligencia, ciberseguridad y emergencias, que tendrá lugar junto con DRONExpo , un espacio centrado en tecnología de drones, sistemas antidrón y aplicaciones para seguridad.

Acudirán organismos públicos, Fuerzas y Cuerpos de Seguridad nacionales, autonómicos y locales, y empresas de infraestructuras críticas estarán presentes junto con los protagonistas de la industria.

TECNOSEC DRONExpo será una ocasión para presentar novedades del sector,

Encontrar oportunidades de colaboración entre empresas y con las administraciones, además de promover proyectos y negocios.

Esta V edición de la feria se consolida como un escaparate de la industria nacional con participación internacional, mostrando la cohesión de los actores del sector ante los retos y novedades de la seguridad global y los drones.

REGISTRO GRATUITO



TU ARMA, TU RESPONSABILIDAD

CUSTODIA, TRANSPORTE Y USO SEGURO EN LA CAZA

GUARDIA CIVIL

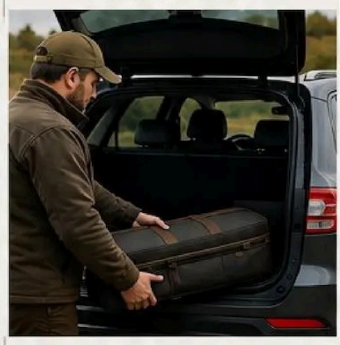
BUENAS PRÁCTICAS EN TODO MOMENTO

1. EN CASA



- Custodia tus armas adoptando las medidas de seguridad exigibles según su categoría.
- Las armas y la munición deben mantenerse inaccesibles para personas no autorizadas.
- Comprueba que llevas la documentación necesaria.

2. TRANSPORTE



- Transporta el arma siempre descargada y en funda o maletín.
- Transpórtala descargada, debidamente acondicionada y manteniéndola siempre bajo tu control.
- La munición debe transportarse de forma separada.

3. DURANTE EL TRAYECTO



- Tu arma debe permanecer bajo tu control.
- No la dejes desatendida en el vehículo.
- Ante cualquier parada, asegúrate de que nadie pueda acceder a ella.

4. EN LA JORNADA DE CAZA



- Manipula y porta el arma con la máxima precaución y conforme a las normas de seguridad.
- No la apoyes en ningún sitio ni la dejes fuera de tu control.
- Respeta siempre la normativa de caza y las normas de seguridad.

LO QUE NUNCA DEBES HACER

NO DEJES TU ARMA DESATENDIDA EN EL COCHE



Es una oportunidad para el robo o el acceso de personas no autorizadas.

NO LA LLEVES CARGADA DURANTE EL TRANSPORTE



Debe transportarse siempre descargada.

NO LA DEJES VISIBLE DESDE EL EXTERIOR



Evita que tu arma pueda ser vista desde fuera del vehículo.

NO PERMITAS EL ACCESO A PERSONAS NO AUTORIZADAS



Guárdala de forma que impida el acceso a menores y a terceros.

DOCUMENTACIÓN NECESARIA

Lleva siempre contigo:

- ✓ Licencia de armas en vigor.
- ✓ Guía de pertenencia del arma.
- ✓ Licencia y demás documentación necesaria para la actividad cinegética (según normativa autonómica).





SI PIERDES, TE SUSTRAEN O ROBAN TU ARMA,

COMUNÍCALO AL

062

NO LO DEJES PARA MÁS TARDE.

RECUERDA

- Tu arma no es un objeto más.
- Eres responsable de su seguridad siempre y en todo lugar.
- Un descuido puede tener graves consecuencias para ti y para los demás.

CUSTODIA RESPONSABLE, CAZA SEGURA

POR TI, POR LOS DEMÁS, POR EL FUTURO DE LA CAZA

MÁXIMA PRECAUCIÓN SIEMPRE

Actualización de datos de socios y amigos de ADSI

Estimado/a Socio/a, Amigo/a,

En su momento, nos aportasteis vuestros datos profesionales y personales, pero en muchas ocasiones estos han cambiado y nos dificulta el contacto con vosotros cuando nos es preciso.

Por ello, te agradeceríamos que:

Nos escribas un **correo** a:

- Elvira Márquez vicepresidente@adsi.pro
- Eduard Zamora presidente@adsi.pro



Si eres socio de ADSI

Indicando:

Nombre y apellidos
Empresa y cargo
Domicilio profesional
E-mail profesional
Teléfono de contacto

Domicilio particular
E-mail particular
Teléfono de contacto

Si eres amigo de ADSI

¿Deseas recibir nuestras comunicaciones? Facilítanos tus datos, remarcando que no eres socio.

Gracias por vuestra colaboración!

La seguridad también se nota en los detalles

Por Rubén García, Chief Operations Officer

Cómo convertir un servicio imprescindible en una fuente de confianza para las personas y las organizaciones.

La seguridad de una organización se mide, ante todo, por su capacidad para prevenir riesgos, proteger a las personas y los activos y responder adecuadamente cuando se produce una incidencia. Es una responsabilidad que exige rigor, preparación y una operativa bien coordinada.

Pero hay otra dimensión que también merece atención: cómo se presta ese servicio y qué transmite a quienes interactúan con él cada día.

Pensemos en la entrada de una sede corporativa, la recepción de un edificio o el acceso a unas instalaciones. Antes de llegar a su destino, un empleado, un visitante o un cliente ya ha tenido un primer contacto con la organización. La forma de recibirle, la discreción del personal, la claridad de las indicaciones y la gestión de una situación imprevista contribuyen a generar una impresión de orden, profesionalidad y confianza.

La seguridad no deja de ser seguridad por prestar atención a estos aspectos. Al contrario: cuando la protección y el cuidado conviven en un mismo servicio, la experiencia mejora sin perder de vista lo esencial.

De cubrir un puesto a diseñar un servicio

Durante mucho tiempo, la contratación de seguridad se ha planteado principalmente en términos de cobertura, horarios, procedimientos y cumplimiento de los requisitos establecidos. Todos ellos son elementos imprescindibles. Sin embargo, una gestión verdaderamente cuidada requiere mirar también el contexto en el que se presta el servicio.

No necesita lo mismo un entorno industrial que una sede corporativa, un espacio de atención al público o unas instalaciones con un elevado tránsito de visitantes. Los riesgos, los protocolos y las prioridades cambian; también lo hacen las expectativas sobre el trato, la comunicación y la coordinación con el resto de los equipos.

Por eso, el punto de partida debería ser comprender las necesidades de cada organización y traducirlas en una operativa coherente: perfiles adecuados, instrucciones claras, coordinación con los interlocutores del cliente, supervisión cercana y capacidad para anticiparse a los problemas.



La diferencia no está necesariamente en hacer más, sino en que cada elemento responda a un propósito y funcione de forma consistente. Que el servicio esté bien pensado, que las personas sepan qué se espera de ellas y que el cliente tenga la tranquilidad de contar con un equipo que conoce su entorno y actúa con criterio.

La calidad se construye cada día

Un servicio no se define, sobre todo, en la operativa diaria.

En cómo se incorpora una nueva persona al equipo; en la transmisión de las instrucciones; en la coordinación entre turnos; en la respuesta ante una incidencia; y en la rapidez con la que se resuelve una dificultad antes de que termine afectando al cliente.

Para que todo ello no dependa exclusivamente de la iniciativa individual, hacen falta método, seguimiento y responsables accesibles. La supervisión debe servir para detectar oportunidades de mejora, acompañar a los equipos y asegurar que los estándares acordados se mantienen en el tiempo.

Este trabajo, muchas veces invisible para quien visita las instalaciones, es el que permite que el servicio resulte natural y fiable. El cliente no debería tener que estar pendiente de cada detalle para asegurarse de que todo funciona. Debería poder confiar en que existe una estructura detrás, capaz de gestionar el día a día y actuar cuando hace falta.

Cuidar a las personas que cuidan

Ningún protocolo funciona por sí solo. Detrás de cada servicio hay profesionales que toman decisiones,

interpretan situaciones, atienden a otras personas y representan a la organización en la que trabajan.

Por eso, la preparación técnica es imprescindible, pero también lo son el acompañamiento, la comunicación y el reconocimiento del trabajo bien hecho. Cuando los profesionales conocen su función, cuentan con el apoyo necesario y tienen referentes claros a los que acudir, disponen de mejores condiciones para desarrollar su labor con seguridad, responsabilidad y atención.

En ARMONÍA llamamos colaboradores a las personas que hacen posible nuestros servicios y, proyecto luciérnaga, al protocolo que nos permite acompañar y sacar lo mejor de cada uno. Este concepto refleja una convicción: cuidar a quienes están en primera línea forma parte de cuidar el servicio. No es una cuestión accesoria ni separada de la operativa, sino una forma de trabajar que busca que cada profesional se sienta acompañado, preparado y parte de un equipo.

La dimensión humana no sustituye a la exigencia técnica. La complementa. Y en un servicio que implica contacto directo con personas, esa combinación importa.

Una forma distinta de entender la seguridad

Para ARMONÍA, prestar un servicio de seguridad significa asumir una responsabilidad que va más allá de la presencia física en unas instalaciones. Significa comprender el entorno del cliente, trabajar conforme a sus necesidades, cuidar la coordinación y mantener una atención constante sobre aquello que permite que el servicio funcione como debe.

La protección de personas, instalaciones y activos sigue siendo la prioridad. Pero la manera de alcanzarla también importa: con profesionalidad, discreción, cercanía cuando corresponde y una gestión que aporte confianza al cliente.

Cuando la seguridad está bien diseñada y bien gestionada, no necesita llamar la atención para demostrar su valor. Se percibe en el orden, en la capacidad de respuesta, en la tranquilidad de saber que hay un equipo preparado y en la confianza que genera el servicio día tras día.

Porque la seguridad no solo debe estar preparada para responder cuando ocurre algo. También debe contribuir, cada día, a que las personas estén protegidas y las organizaciones puedan desarrollar su actividad con tranquilidad. ■



Tecnología al servicio de la reinserción: monitorización penitenciaria 24/7 para la Generalitat de Catalunya

Caso de éxito

La transformación digital está redefiniendo sectores tan diversos como la industria, la sanidad o las infraestructuras críticas. Sin embargo, existe un ámbito donde la tecnología aporta un valor social especialmente relevante: la gestión y seguimiento de personas sometidas a medidas penales.

En **CLECE SEGURIDAD** gestionamos el servicio **de monitoreo, seguimiento y vigilancia remota de personas sometidas a medidas penales para la Generalitat de Catalunya**, un proyecto que combina tecnología avanzada, atención permanente y una elevada capacidad operativa para garantizar el cumplimiento de las medidas judiciales y favorecer los procesos de reinserción social.

Un servicio operativo 24 horas al día, 365 días al año

La clave de este servicio reside en una monitorización continúa basada en tecnologías de geolocalización, control de presencia y verificación remota.

Toda la gestión operativa se realiza desde nuestra **Central Receptora** desde donde se supervisan las incidencias, se generan informes y se mantiene una comunicación constante con las instituciones penitenciarias.

Además, cuando se producen nuevas incorporaciones al sistema o incidencias técnicas en los dispositivos de control, nuestros técnicos se desplazan de forma inmediata para asegurar la continuidad del servicio.

Tres tecnologías para diferentes necesidades de monitorización

Cada persona sometida a medidas penales requiere un nivel de control adaptado a su situación específica. Por ello, el servicio integra tres sistemas tecnológicos diferentes.

1. Control de permanencia mediante Radiofrecuencia (RF)

Diseñado para verificar el cumplimiento de medidas de arresto domiciliario o permanencia en una ubicación determinada.

El sistema incorpora un **brazalete electrónico RF** con múltiples mecanismos de protección frente a manipulaciones.

La información es transmitida mediante un receptor domiciliario con doble vía de comunicación, utilizando tanto línea fija como red celular, garantizando una elevada disponibilidad del servicio.



2. Rastreo y geolocalización mediante GPS

Para aquellos casos que requieren seguimiento de movilidad, se emplea un avanzado sistema GPS de dos piezas.

El sistema se complementa con un brazalete RF de alta resistencia, diseñado para entornos exigentes, resistente al agua y dotado de tecnologías anti-manipulación que permiten detectar cualquier intento de alteración del dispositivo.

3. Monitorización de consumo de alcohol y control de toque de queda

Determinadas medidas judiciales requieren verificar el cumplimiento de restricciones relacionadas con el consumo de alcohol.

Para ello se utiliza un sistema basado en sensores electroquímicos de alta precisión capaces de realizar pruebas de alcohol en aliento.

Tecnología con impacto social

Más allá de la innovación tecnológica, este tipo de proyectos tienen un importante componente humano y social.

La implantación de este servicio ha permitido consolidar un modelo de supervisión remota basado en la disponibilidad permanente, la trazabilidad de los eventos y la rápida capacidad de respuesta ante cualquier incidencia.

Entre los principales resultados obtenidos destacan:

- **Monitorización continua 24x7x365** de las personas sometidas a medidas penales, garantizando la supervisión ininterrumpida desde la Central Receptora de Alarmas.
- **Respuesta rápida ante incidencias técnicas y operativas**, gracias a la coordinación entre el centro de control y los técnicos especializados desplegados en Cataluña.
- **Mayor fiabilidad en el cumplimiento de las medidas judiciales**, mediante tecnologías avanzadas de geolocalización, control de presencia y detección de manipulaciones.
- **Trazabilidad completa de eventos y alertas**, permitiendo disponer de registros verificables para las instituciones penitenciarias.
- **Optimización de recursos penitenciarios**, facilitando modelos de seguimiento remoto que complementan la gestión tradicional de los centros penitenciarios.
- **Mayor seguridad operativa**, gracias a sistemas capaces de detectar intentos de manipulación, incumplimientos de permanencia, desplazamientos no autorizados o consumos de alcohol incompatibles con las medidas impuestas.
- **Contribución a los procesos de reinserción social**, permitiendo el seguimiento de personas en regímenes de semilibertad o medidas alternativas manteniendo los niveles de control requeridos.

La tecnología, cuando se aplica con rigor y responsabilidad, se convierte en una herramienta clave para construir modelos más eficientes, sostenibles y orientados a las personas.

Seguimos apostando por soluciones tecnológicas que combinan innovación, seguridad y servicio público, demostrando que la digitalización puede generar un impacto positivo real en la sociedad.



Los disturbios de Barcelona reabren el debate sobre la seguridad real de los escaparates

Los incidentes del 24 de octubre evidencian la necesidad de compatibilizar transparencia comercial, integración arquitectónica y resistencia frente a intentos de intrusión.

Barcelona vivió el sábado 24 de octubre de 2026 una jornada de graves altercados en el entorno de la plaza de Catalunya y varias calles comerciales del centro. El balance conocido tras los incidentes incluye 23 establecimientos vandalizados o saqueados, escaparates destrozados, incendios y múltiples daños en el mobiliario urbano. Más allá de las pérdidas materiales inmediatas, lo sucedido plantea una pregunta de fondo para el sector del comercio y la arquitectura comercial: ¿están suficientemente protegidos los puntos de acceso y los escaparates cuando se producen ataques violentos y simultáneos?

Las escenas de cristales rotos, cierres forzados y tiendas que se vieron obligadas a bajar sus persianas ilustran una realidad conocida por los profesionales de la seguridad física: una fachada atractiva y transparente no siempre es una fachada resistente. El vidrio, incluso cuando incorpora prestaciones de seguridad, puede resultar vulnerable ante agresiones reiteradas y contundentes si el conjunto del cerramiento no ha sido concebido específicamente para resistir una intrusión.

El límite de los cerramientos tradicionales

En numerosos ejes comerciales conviven locales protegidos únicamente por grandes superficies acristaladas con otros que mantienen cierres metálicos de diseño tradicional: persianas de varilla, rejas o puertas de hierro y acero galvanizado cuya estética remite al comercio barcelonés de hace décadas. Estos sistemas pueden ofrecer visibilidad y continuidad visual con el entorno urbano, pero su aspecto robusto no constituye, por sí solo, una garantía de resistencia frente a ataques coordinados.

Cuando varias personas actúan simultáneamente sobre un cierre, los puntos débiles pueden encontrarse en las guías, los anclajes, las uniones o el propio material. Por eso, no basta con evaluar la lama o la apariencia del producto: la seguridad debe analizarse como un sistema completo, considerando puerta, guías, fijaciones, cierres e instalación. Algo similar ocurre con los escaparates acristalados: el término «vidrio de seguridad» engloba prestaciones muy diferentes y no equivale automáticamente a un cerramiento antiefracción.

En áreas con condicionantes estéticos o patrimoniales, el reto es todavía mayor. La preservación de la imagen urbana y la posibilidad de mostrar el interior del establecimiento son objetivos legítimos; sin embargo, conviene que los criterios de integración arquitectónica puedan dialogar con soluciones contemporáneas de protección, evitando que la transparencia implique renunciar a una barrera física eficaz.

Protección y visibilidad pueden ir de la mano

En este escenario, el fabricante especializado **COLLBAIX** apuesta por puertas enrollables de seguridad elaboradas con perfiles de aluminio extrusionado. La compañía dispone de configuraciones opacas y de modelos con





visión, concebidos para permitir que el escaparate continúe siendo visible y mantenga su función comercial cuando el establecimiento está cerrado.

Estas puertas pueden plantearse, según las características del proyecto y sus requisitos técnicos, por delante o por detrás del acristalamiento. La incorporación de una barrera enrollable resistente añade una capa de protección al acceso, dificulta los intentos de entrada y contribuye a proteger tanto el equipamiento del local como las mercancías expuestas o almacenadas. Para el comerciante supone, además, la posibilidad de reforzar la seguridad sin convertir necesariamente su fachada en un frente completamente ciego.

Seguridad certificada para entornos de mayor exposición

En establecimientos donde el valor de los bienes o el nivel de exposición exigen una protección superior, **COLLBAIX** también ofrece puertas enrollables antiefracción ensayadas y clasificadas conforme a la **norma europea EN 1627**. Esta norma establece clases de resistencia —RC— y permite distinguir las prestaciones verificadas de un sistema frente a las afirmaciones genéricas de seguridad. La gama de la firma incluye soluciones con y sin visión, con variantes certificadas, entre otras, en clases RC3 y RC4, según modelo y configuración.

Esta diferencia resulta especialmente relevante para el retail de lujo, la joyería, la relojería y las boutiques de firmas internacionales que se concentran en enclaves como el Paseo de Gràcia. Marcas y establecimientos de segmentos como los representados por Chanel, Cartier, Louis Vuitton, TAGHeuer o Rolex, por mencionar algunas, comparten una exigencia: conservar una presentación comercial cuidada y, al mismo tiempo, estudiar medidas de protección proporcionadas al riesgo y al valor de sus productos. La mención de estas firmas es ilustrativa del sector y no implica que utilicen sistemas de **COLLBAIX**.

Los incidentes de Barcelona recuerdan que la seguridad del comercio no debería evaluarse únicamente después de un robo o de un episodio de vandalismo. La prevención comienza en el diseño de la fachada y en la elección de cerramientos cuya resistencia pueda justificarse técnicamente.

Compatibilizar estética, visión del producto y seguridad real no es una contradicción: es uno de los principales desafíos —y oportunidades— de la arquitectura comercial actual. ■





Conectividad IoT multioperador: cuando la tecnología también ayuda a simplificar la operación

La conectividad móvil se ha convertido en un componente esencial de muchas soluciones de seguridad. Centrales de alarma, sistemas de videovigilancia, teleasistencia, control de accesos y otros dispositivos conectados dependen cada vez más de las redes móviles para mantener una comunicación continua con sus plataformas de supervisión.

Sin embargo, a medida que aumenta el número de dispositivos conectados, también lo hace la complejidad de su gestión. Y no siempre es el coste de la conectividad el factor más relevante.

Una segunda visita porque la cobertura del operador seleccionado no es adecuada, una incidencia que obliga a consultar diferentes plataformas o la necesidad de sustituir una SIM para probar otra red pueden tener un impacto operativo muy superior al propio coste mensual del servicio.

Por eso, la gestión de la conectividad IoT está evolucionando hacia un modelo donde adquieren mayor importancia **el acceso a diferentes redes, el diagnóstico remoto y la integración con las herramientas que ya utiliza la organización.**

Una SIM, diferentes redes disponibles

Uno de los elementos que facilita este cambio es la utilización de SIMs IoT multioperador.

En una SIM tradicional, la conectividad está vinculada a la cobertura de un determinado operador. Esto puede ser suficiente en muchas instalaciones, pero introduce una variable difícil de prever: cuál será la calidad de cobertura disponible exactamente en el lugar donde se instalará el dispositivo.

Las SIMs multioperador permiten utilizar diferentes redes móviles disponibles. En la solución de CSL Iberia, además, **no se establece una prioridad fija entre operadores**, de manera que la conectividad no queda condicionada a intentar utilizar sistemáticamente una determinada red antes que las demás.

Esta capacidad aporta resiliencia, pero también simplifica el despliegue. El instalador no necesita disponer de diferentes tarjetas para comprobar qué operador funciona mejor en cada ubicación y se reduce la posibilidad de que un problema de cobertura termine requiriendo una nueva visita para sustituir físicamente la SIM.

Cuando hablamos de cientos o miles de dispositivos, reducir este tipo de intervenciones puede tener un impacto significativo sobre el coste de mantenimiento y soporte.

La conectividad no termina en la SIM

La conectividad IoT necesita además herramientas que permitan entender qué está sucediendo cuando aparece una incidencia.

La **CSL IoT Plataforma** centraliza la gestión de las SIMs y permite consultar información relacionada con su funcionamiento: estado, consumo, operador utilizado, tecnología de acceso, APN, dirección IP o información sobre las últimas sesiones de conexión.

Esta visibilidad resulta especialmente útil durante el diagnóstico. Antes de considerar un desplazamiento, el técnico puede comprobar el comportamiento de la conexión y realizar determinadas acciones de forma remota. Esto facilita determinar si el problema está relacionado con la comunicación móvil o se encuentra en otro punto de la instalación.

La plataforma permite también realizar operaciones habituales sobre las SIMs, consultar históricos y disponer de una visión centralizada del parque de dispositivos.

El objetivo no es únicamente gestionar las comunicaciones, sino reducir el tiempo necesario para hacerlo.

Integrar la conectividad en las herramientas que ya utiliza el sector

Existe un paso adicional: llevar esa información hasta las aplicaciones desde las que trabajan diariamente los usuarios.

El ejemplo más evidente es una Central Receptora de Alarmas. Ante una incidencia de comunicación, el operador de la CRA trabaja habitualmente desde su

software de recepción y gestión de alarmas. Tener que acceder a una plataforma independiente únicamente para comprobar el estado de una SIM añade pasos precisamente cuando interesa disponer de información con rapidez.

Por este motivo, la **CSL IoT Plataforma está integrada con Manitou y SBN**, soluciones utilizadas en el sector de la seguridad. Estas integraciones permiten acercar determinadas funciones de diagnóstico al entorno habitual del operador, pudiendo consultar el estado de la comunicación y realizar acciones como un reinicio sin iniciar un proceso independiente en otra aplicación.

Es un buen ejemplo de una tendencia que probablemente veremos cada vez con mayor frecuencia: **la conectividad como una funcionalidad integrada dentro de las aplicaciones de negocio**, en lugar de funcionar como un servicio aislado.

El mismo planteamiento puede aplicarse a los procesos administrativos. La CSL IoT Plataforma también está integrada con **Beta10**, software de gestión y facturación. De esta forma, la información relacionada con las comunicaciones puede acercarse al proceso administrativo y reducir la necesidad de mantener datos y procedimientos independientes en diferentes sistemas.

No se trata de añadir más tecnología al trabajo diario, sino precisamente de eliminar pasos que no aportan valor.

El coste de la conectividad va más allá de la tarifa

Cuando se comparan servicios de comunicaciones IoT es habitual comenzar por variables como el precio de la SIM o el volumen de datos incluido. Son criterios importantes, pero ofrecen únicamente una parte de la imagen.

En un parque amplio de dispositivos, el coste operativo incluye también el tiempo dedicado a instalar, diagnosticar, administrar y mantener esas comunicaciones.

Un desplazamiento técnico evitado puede representar mucho más que varios meses de conectividad. Lo mismo ocurre con el tiempo que un equipo de soporte dedica a localizar una incidencia o con las tareas administrativas necesarias para mantener información sincronizada entre distintos sistemas.

Las SIMs multioperador ayudan a simplificar los despliegues y reducen la dependencia de una única red. Las plataformas de gestión aportan visibilidad y capacidad de actuación remota. Y las integraciones permiten que esa información esté disponible dentro de las aplicaciones que ya forman parte de la operativa diaria.

Por separado, cada mejora puede parecer pequeña. Aplicadas conjuntamente sobre cientos o miles de dispositivos, su impacto puede ser considerable.

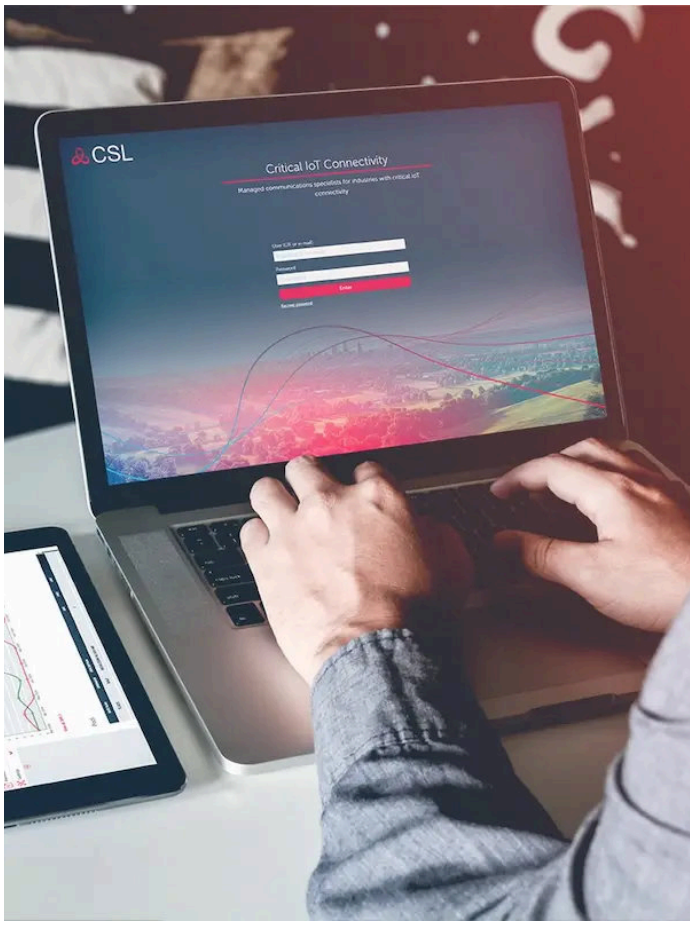
Una conectividad cada vez más integrada

La evolución del IoT está haciendo que la conectividad deje de percibirse únicamente como la capacidad de transmitir datos entre un dispositivo y una plataforma.

En sectores como el de la seguridad, donde muchas comunicaciones tienen además un carácter crítico, la disponibilidad de diferentes redes, la capacidad de diagnóstico y la rapidez con la que puede identificarse una incidencia adquieren especial relevancia.

En CSL Iberia estamos siguiendo este camino: combinar conectividad IoT multioperador, herramientas de gestión y diagnóstico e integración con aplicaciones del sector como Manitou, SBN y Beta10.

El objetivo final es sencillo: **que la conectividad proporcione más información, más capacidad de actuación y, al mismo tiempo, requiere cada vez menos intervención**. ■



La seguridad física ya no puede gestionarse por separado

ODISEE, la nueva plataforma abierta 100% web de DORLET, apuesta por la interoperabilidad, la unificación operativa y la libertad tecnológica para transformar la operación de seguridad.

El reto de gestionar una seguridad cada vez más compleja

La seguridad física de las organizaciones ha experimentado una profunda transformación en los últimos años. Los sistemas de control de accesos, videovigilancia, intrusión y detección de incendios han evolucionado significativamente, incorporando nuevas capacidades que permiten proteger instalaciones cada vez más complejas. Sin embargo, esta evolución también ha generado un nuevo desafío: la fragmentación tecnológica.

En muchas organizaciones, especialmente en grandes instalaciones e infraestructuras críticas, conviven soluciones de distintos fabricantes y tecnologías implantadas en diferentes momentos que funcionan de manera independiente.

Para los responsables de seguridad, esta situación plantea dificultades que van más allá de la tecnología: información distribuida entre distintas plataformas, múltiples interfaces de supervisión, procedimientos de actuación independientes y una visión parcial de lo que sucede en las instalaciones.

El reto no es solo detectar las amenazas, sino integrar los sistemas de seguridad para facilitar al operador información contextualizada, coordinar las actuaciones y agilizar la toma de decisiones ante incidencias.

<< El futuro de la seguridad física no consiste en incorporar más sistemas, u obligar a que todos sean de un mismo fabricante, sino en conseguir que todos trabajen juntos, unificando la operativa. **>>**

Una nueva forma de entender la seguridad física

Con esta visión naceODISEE, el nuevo Open Physical Security Software desarrollado por DORLET; una plataforma abierta y 100 % web concebida para unificar, optimizar y proteger la gestión del ecosistema de seguridad física de las organizaciones.

Su filosofía parte de una premisa: la tecnología debe adaptarse a las necesidades de cada organización, y no condicionar su estrategia de seguridad.

ODISEE propone un enfoque basado en la apertura y la interoperabilidad, que permite integrar distintas tecnologías en un entorno común de supervisión y



operación. Esta capacidad resulta especialmente relevante para organizaciones que cuentan con instalaciones distribuidas geográficamente o sistemas incorporados en distintas fases de crecimiento. En lugar de sustituir las tecnologías existentes, ODISEE aprovecha las inversiones realizadas y facilita la incorporación progresiva de nuevas soluciones.

El objetivo va más allá de desarrollar una plataforma. Es crear un ecosistema abierto en el que DORLET facilite a terceros las herramientas necesarias para ampliarlo con integraciones y funcionalidades propias, validadas por DORLET.

Una visión unificada de todo el ecosistema

ODISEE permite reunir información procedente de diferentes sistemas, como control de accesos, videovigilancia, intrusión o detección de incendios, y presentarla en un entorno de operación común.

A través de herramientas de supervisión, sinópticos y visualización de información, los operadores pueden relacionar dispositivos, eventos y ubicaciones para comprender mejor cada situación. Esta perspectiva resulta especialmente importante en instalaciones donde un mismo incidente puede afectar a diferentes subsistemas.

Por ejemplo, una alarma de intrusión puede requerir la consulta de cámaras cercanas, la comprobación del estado de determinados accesos y la ejecución de acciones de seguridad específicas. El objetivo no es mostrar más datos, sino facilitar el acceso a la información relevante en el momento adecuado.

Detectar, analizar y actuar

La gestión de incidentes constituye uno de los ámbitos donde la integración tecnológica puede aportar mayor valor.

Detectar una alarma es solo el comienzo. A partir de ese momento, resulta necesario verificar qué ha sucedido, evaluar su alcance, determinar las actuaciones correspondientes y dejar constancia de las decisiones adoptadas. ODISEE incorpora herramientas de gestión de incidentes y procedimientos de actuación que permiten estructurar este proceso.



Mediante workflows configurables, las organizaciones pueden definir las comprobaciones y acciones que deben realizarse ante determinados eventos, facilitando una respuesta más homogénea y alineada con sus protocolos de seguridad.

Imaginemos una incidencia en una instalación crítica:

1. Un dispositivo genera una alarma y el operador recibe la notificación. Desde el entorno de supervisión puede localizar el elemento afectado, consultar la información disponible y acceder a las imágenes de vídeo relacionadas.

2. A continuación, el procedimiento asociado puede guiar las verificaciones necesarias y las actuaciones que correspondan, incorporando las observaciones y decisiones del operador.

3. Finalmente, la gestión queda documentada para su posterior consulta y análisis.

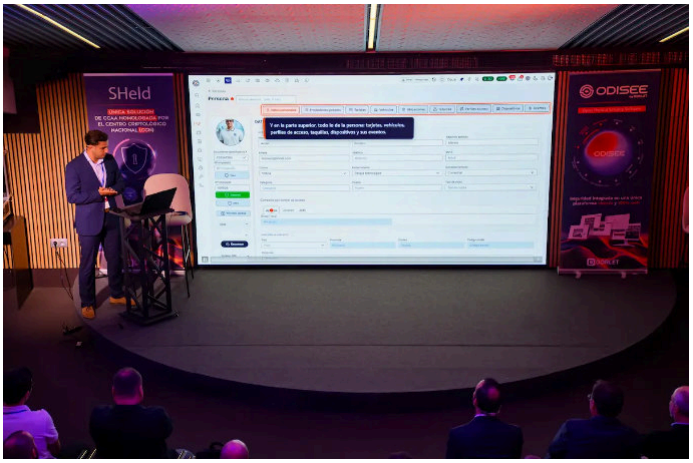
Este modelo contribuye a reducir la dependencia de actuaciones improvisadas, facilita la coordinación operativa y favorece la trazabilidad de los incidentes.

<< El valor de esta plataforma no está únicamente en detectar lo que ocurre, sino en ayudar a gestionar qué hacer a continuación, de manera mucho más eficiente. **>>**

Información útil para una seguridad más eficiente

Cada acceso, alarma, evento o actuación produce datos que pueden aportar conocimiento sobre el funcionamiento de las instalaciones y la actividad de la organización. ODISEE incorpora herramientas de visualización y análisis que permiten configurar dashboards, consultar indicadores y generar informes a partir de la información disponible. Estas capacidades facilitan que los responsables de seguridad puedan analizar la actividad de sus instalaciones, identificar tendencias y disponer de información estructurada para apoyar sus decisiones.

La plataforma también contempla la interacción con los datos mediante lenguaje natural, aplicando tecnologías IA, con el objetivo de simplificar determinadas consultas y hacer más accesible la información a cualquier gestor, sin necesidad de un conocimiento previo del uso del software.



Interoperabilidad, ciberseguridad y continuidad

Las plataformas de seguridad forman parte del entorno digital de las organizaciones y, por tanto, deben considerar aspectos como la protección de la información, la disponibilidad de los sistemas y la continuidad operativa. Esta realidad adquiere especial relevancia en sectores estratégicos e infraestructuras críticas, donde una interrupción puede tener consecuencias importantes para la actividad.

Marcos regulatorios europeos como NIS2 y la Directiva CER refuerzan la importancia de adoptar enfoques de gestión del riesgo, ciberseguridad y resiliencia, de acuerdo con las obligaciones aplicables a cada organización.

En este escenario, las plataformas de seguridad física deben evolucionar hacia arquitecturas que contemplen la ciberseguridad desde su concepción y faciliten una gestión controlada y trazable de las operaciones. Además, debe ir acompañada de criterios rigurosos de integración y mantenimiento, de forma que la incorporación de nuevos sistemas no comprometa la seguridad del conjunto.

ODISEE en la práctica: seguridad integrada en una instalación de alta exigencia

Un ejemplo de aplicación real de ODISEE es su implantación en una importante instalación cultural, donde la protección del patrimonio, la presencia continua de visitantes y la necesidad de mantener una vigilancia permanente plantean importantes desafíos operativos:

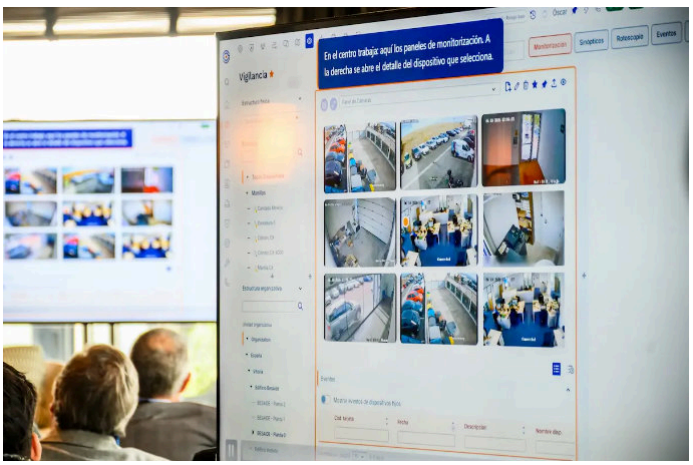
• El cierre de una sala puede agrupar diferentes actuaciones, como cerrar puertas, apagar luces, accionar cortinas y activar sensores, evitando que el operador tenga que ejecutar cada operación de forma independiente.

• Cuando un dispositivo genera un aviso, ODISEE puede mostrar automáticamente las cámaras asociadas y facilitar al vigilante las acciones a realizar según los workflows definidos por la dirección de seguridad.

• Activación de rondas de vigilancia de las cámaras, supervisando los sensores de intrusión sobre los planos de la instalación y gestionar las alarmas correspondientes de forma agrupada. Además, su naturaleza web facilita la consulta y gestión de alarmas sin depender exclusivamente de un puesto fijo. El vigilante traslada el puesto de control a su Tablet de trabajo.

Este proyecto demuestra cómo la integración de diferentes tecnologías puede traducirse enuna operación más sencilla, una respuesta mejor coordinada y una mayor trazabilidad de las actuaciones.

En un entorno donde los desafíos de seguridad son cada vez más complejos, el futuro pasa por plataformas abiertas, interoperables y capaces de evolucionar junto a las necesidades de cada organización.Con ODISEE, DORLET reafirma su apuesta por una seguridad física más integrada, eficiente y preparada para los retos del futuro.





Proteger un aparcamiento de camiones reduciendo la obra civil

Caso de éxito

Región de Zaragoza. Un hub de transporte de mercancías por carretera necesitaba hacer frente a las intrusiones y los robos de mercancía en su aparcamiento de camiones. Hirsch ha desplegado una detección perimetral por capas, desde la valla hasta el acceso de vehículos. La valla y el acceso se protegieron sin zanjas ni obra civil, y todas las alarmas llegan a una única plataforma de hipervisión.

El reto: un aparcamiento lleno de mercancía en espera

Para una empresa de transporte por carretera, el aparcamiento no es una zona secundaria. Es el lugar donde los camiones cargados esperan antes de salir a ruta. Cada remolque aparcado es mercancía de valor al alcance de quien consiga entrar.

Eso es lo que ocurría en este lugar de la región de Zaragoza. El aparcamiento tenía que hacer frente a intrusiones y robos de mercancía. La vigilancia humana estaba presente, pero un perímetro de varios cientos de metros es difícil de cubrir solo con rondas. Hacía falta saber, en el mismo momento, que alguien intentaba entrar y por dónde.

Esta sede imponía además dos condiciones prácticas:

• **La actividad no podía parar**. Los camiones tienen que seguir entrando y saliendo durante la instalación.

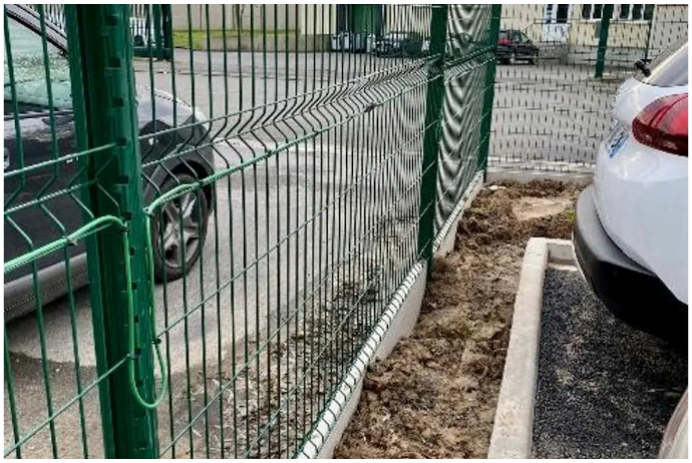
• **Reducción en el impacto en obra civil.** Abrir zanjas en un aparcamiento es caro, lento y molesto para la operativa.

La solución: tres capas de detección y una sola pantalla

Hirsch propuso una detección perimetral por capas. Cada capa cubre un punto débil distinto, y todas informan al mismo lugar.

1. La valla se convierte en detector: G-FENCE 2400

Se instalaron en torno a 400 metros de cable G-FENCE 2400 directamente sobre la valla existente. El cable integra sensores que detectan los golpes típicos de un corte, una escalada o un intento de arrancar la valla. El sistema se divide en zonas, así que la alarma indica en qué tramo se produce el intento. No es sensible a la lluvia



Cable G-Fence 2400



Cable G-Fence

ni al viento (filtra hasta 80km/h), lo que limita las falsas alarmas en un entorno exterior.

2. Una segunda línea de infrarrojos: MAXIRIS

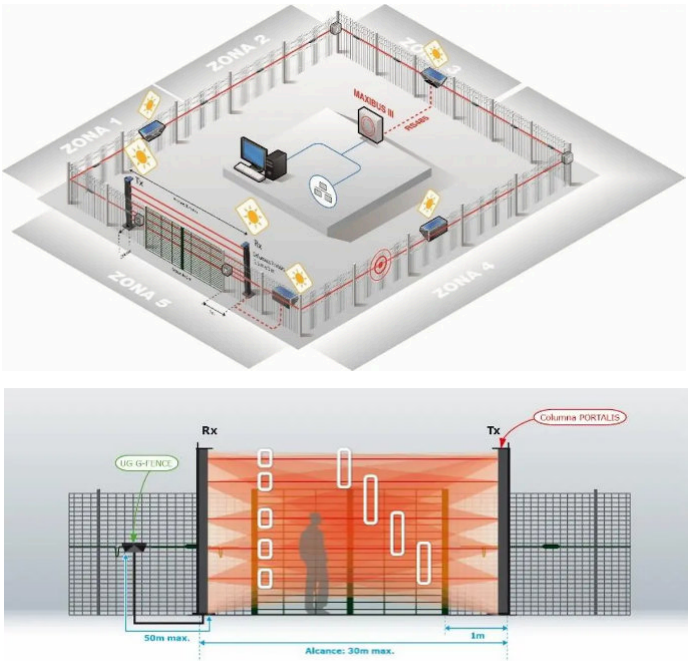
El perímetro se completó con 14 columnas de infrarrojos activos MAXIRIS. Cada par de columnas crea un muro de haces invisibles. Varios modos de detección funcionan a la vez: por ejemplo, la alarma puede exigir el corte simultáneo de dos o más haces. Así se filtra el tamaño de lo que cruza y se reducen las falsas alarmas, sobre todo las causadas por animales, por ejemplo gatos, pájaros, hojas volando etc.

3. El acceso de vehículos, sin cables: PORTALIS

La entrada de camiones es uno de los puntos más delicados. Tiene que quedar libre para la operativa, pero no puede ser un hueco en la protección. PORTALIS es una barrera de infrarrojos pensada para los accesos de vehículos. Cada columna lleva su propio panel solar y su batería: no hace falta cable de alimentación ni obra civil. Sus alarmas se comunican directamente a la unidad de control G-FENCE más cercana, sin receptor de radio. El



Barrera Portalis



Funcionamiento de Portalis

acceso queda así integrado en la misma línea de detección que la valla.

4. Todas las alarmas en un mismo lugar: AppVision

Todas las alarmas llegan a AppVision, la plataforma de hipervisión que el cliente utiliza como software de gestión de alarmas. El operador ve en una sola pantalla qué detector ha saltado y en qué zona. No tiene que consultar varios sistemas. Puede reaccionar de inmediato y enviar al equipo de vigilancia al punto exacto.

¿Por qué encaja en este tipo de lugares?

Un aparcamiento logístico necesita una protección que se instale rápido, sin parar la actividad, y que dé información útil al vigilante. Esta combinación responde a esas tres necesidades.

- **Sin zanjas en la valla ni en el acceso**. G-FENCE se fija a la valla existente y PORTALIS funciona con energía solar. La instalación no interrumpe el paso de camiones.

- **Una alarma que dice dónde**. La zonificación indica el tramo o la columna en alarma con mucha precisión. En tramos de hasta 100 m, las columnas crean zonas virtuales que orientan el zoom de las cámaras PTZ.

- **Menos falsas alarmas**. Los filtros de cada detector descartan la lluvia, el viento o el paso de animales. El vigilante solo se desplaza cuando hay un motivo o alarma real.

- **Apoyo a las personas, no sustitución**. La tecnología detecta y localiza; el equipo de vigilancia decide y actúa. Deja de buscar y empieza a responder. Se gana tiempo en la reacción.

- **Preparado para crecer**. Si el aparcamiento se amplía, se añaden tramos de cable o columnas y se conectan a la misma plataforma.

Ficha del proyecto

Sector: Transporte de mercancías por carretera

Ubicación: Región de Zaragoza, España

Problema: Intrusiones y robos de mercancía en el aparcamiento de camiones

Detección en valla: 400 m de cable G-FENCE 2400

Barreras de infrarrojos: 14 columnas MAXIRIS

Acceso de vehículos: PORTALIS, autónomo con panel solar, conectado a G-FENCE

Gestión de alarmas: Plataforma de hipervisión AppVision

Puesta en servicio: 2026

Sobre Hirsch

Hirsch es un líder mundial en seguridad física de alto nivel de garantía: control de acceso de alta seguridad, protección perimetral, videointeligencia y plataformas de software unificadas. Con más de 45 años de experiencia, Hirsch diseña soluciones fiables, interoperables y escalables, adaptadas a entornos críticos y regulados. Visite www.hirschsecure.com *Seguridad unificada. Posibilidades ilimitadas.*

Contacto

¿Gestiona un aparcamiento de camiones o un emplazamiento logístico con un reto similar? Nuestro equipo estará encantado de estudiarlo con usted. Contacte con:

Rud Badey

Export Sales Manager, South Europe & North Africa
r.badey@hirschsecure.fr | +34 674 89 28 33.

Videovigilancia inteligente para la gestión de residuos

Por Luiggi Pechini, Senior Account Manager de Lanaccess. Ingeniero de telecomunicaciones

Caso de éxito

Una empresa española de clasificación de residuos con casi 50 instalaciones ha implantado la infraestructura de videovigilancia de Lanaccess, incluida la analítica de vídeo LAVA, para fortalecer la seguridad y detectar incidentes en tiempo real.

Tres riesgos en la planta

La compañía recoge, clasifica y trata residuos industriales y urbanos. Cada instalación se dedica a una labor distinta, como el compostaje, la clasificación de envases ligeros o la incineración. Por ejemplo, en una planta de compostaje de 8.000 m², el cliente necesitaba controlar tres riesgos:

- **Atascos en las cintas transportadoras:** cada atasco ralentiza la producción y aumenta la probabilidad de accidente laboral que, en este entorno, puede ser fatal.
- **Operarios sin equipo de protección individual (EPI):** el cliente quería detectar a quienes circulan por la instalación sin él.
- **Incendios:** el aumento de baterías de litio en los contenedores genéricos eleva este riesgo en los fosos de residuos, que por su naturaleza ya concentran gases propensos a inflamarse.

Analítica de vídeo

Para hacer frente a estos riesgos, la empresa implementó cuatro analíticas LAVA:

- **LAVA Flow:** el sistema detecta cuándo el material se atasca en la cinta transportadora. Como Lanaccess desarrolla su propio software, su departamento de I+D+i pudo entrenar un modelo de analítica específico para este caso de uso, diseñado a medida para las plantas del cliente.
- **LAVA Clothing:** comprueba que el personal lleva el EPI.
- **LAVA Fire:** identifica la presencia de humo o fuego en su fase más temprana.
- **LAVA Behaviour:** detecta personas o vehículos en zonas prohibidas y máquinas que deben estar supervisadas y quedan desatendidas.

Cada detección genera una alerta inmediata que el cliente recibe en Lanaccess Suite, el VMS de Lanaccess, y en su aplicación móvil.



Integración con SCADA y señalización luminosa

Lanaccess integró la analítica con dos sistemas de la planta: el sistema SCADA de las máquinas procesadoras, que detiene la máquina de inmediato cuando LAVA Flow detecta un atasco, y un sistema lumínico que alerta de la presencia de vehículos y personas a la vez en áreas mixtas.

Cámaras aisladas de la red corporativa

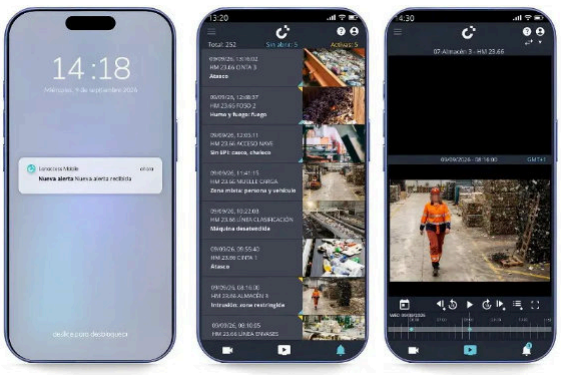
Las cámaras se conectan al chasis mural de Lanaccess, un videograbador con switch PoE con la analítica integrada. El switch PoE actúa de barrera en los dos sentidos: desde una cámara no se puede acceder a la red corporativa y, desde la red, nadie accede a las grabaciones sin permisos.

Resultados

De media, en cada centro donde está instalada la solución, en el mes de prueba:

- El tiempo de parada se ha reducido un 4,5 %: los atascos siguen produciéndose, pero provocan una disrupción mínima.
- LAVA Clothing detecta una media de cuatro personas al mes sin el EPI adecuado.
- LAVA Fire detectó humo en una ocasión antes de que se convirtiera en incendio.

Más información: www.lanaccess.com.



Alertas de analítica en la aplicación móvil Lanaccess Mobile

El Hospital General Universitario Gregorio Marañón digitaliza su Plan de Catástrofes con VES

Caso de éxito

Sobre RKL Integral y VES

RKL Integral desarrolla VES, una plataforma SaaS para la gestión de emergencias, procedimientos operativos, planes de autoprotección, continuidad de negocio y notificaciones ante incidentes críticos. VES ayuda a las organizaciones a coordinar la respuesta, reducir errores y disponer de trazabilidad completa de cada actuación.

Activar a más de 400 profesionales en cuestión de minutos y saber, en tiempo real, quién está disponible para actuar

Cliente: Hospital General Universitario Gregorio Marañón (Hospital General y Hospital Materno Infantil)

Ámbito: Plan de Catástrofes sanitarias y Código Rosa (Hospital Materno Infantil)

Solución: VES, plataforma de gestión de emergencias de RKL Integral

Alcance: Niveles de activación según gravedad, notificación por fases a los grupos de acción, seguimiento de respuestas y cadenas de suplencia

Uso: Activaciones reales y simulacros

El reto: activar a cientos de personas cuando cada minuto cuenta

Un plan de respuesta hospitalaria frente a catástrofes sanitarias sólo es útil si puede ponerse en marcha con rapidez y con certeza. Cuando un hospital recibe un número de víctimas que supera su capacidad ordinaria, la primera necesidad es avisar a las personas adecuadas, en el orden adecuado, y saber cuanto antes con quién se puede contar.

En un hospital de la dimensión del Gregorio Marañón, eso supone coordinar a más de 400 personas de numerosos grupos de acción (desde órganos y personal directivo hasta equipos de coordinación y operativos), en dos centros (el Hospital General y el Hospital Materno Infantil), a cualquier hora del día y con un nivel de respuesta proporcional a la gravedad del incidente. Hacerlo de forma manual, con listados y llamadas una a una, consume un tiempo crítico y deja poca visibilidad sobre quién ha recibido el aviso, quién ha respondido y qué puestos clave siguen sin cubrir.

La solución: el plan de catástrofes, convertido en un procedimiento digital con VES

El Hospital ha digitalizado su plan de catástrofes sanitarias sobre VES, la plataforma de gestión de emergencias y procedimientos operativos desarrollada por RKL Integral. El plan ya no depende de documentos y listas de teléfonos: está modelado en la plataforma, con sus niveles, sus grupos de acción y sus reglas de comunicación, listo para activarse tanto en una situación real como en un simulacro.

Los elementos principales del proyecto son:

- **Niveles de actuación según la gravedad**. El plan contempla distintos niveles de activación. Cada nivel determina qué grupos de acción se movilizan, de forma que la respuesta es proporcional al incidente.
- **Activación por el Gerente o por el Jefe de Hospital**. El responsable del comité permanente de catástrofes lanza el plan de respuesta desde VES en el momento en que se comunica un incidente con múltiples víctimas o se activa un simulacro.



Figura 1. Fases de una activación del plan en VES. (Figura actualizada)

• **Un aspecto muy importante es que el diseño de la activación del plan es flexible, pudiéndose activar simultáneamente distintos niveles y está configurada de forma diferente según la incidencia se en turno de mañana de día laborable, muchos más recursos presenciales disponibles o en horario de guardia, cuando es necesario movilizar recursos activables.**

• **Notificación por fases**. La notificación no es un único aviso, sino un proceso en varias fases: VES avisa de forma secuencial a los distintos grupos de acción implicados en cada fase del procedimiento, por vía telefónica y por otros canales configurados. En las comunicaciones participan órganos y personal directivo, de coordinación y operativo. En total, una activación puede movilizar a más de 400 contactos, con avisos que en ocasiones se completan en menos de 2 minutos.

• **Seguimiento de respuestas en tiempo real**. Cada contacto responde a la notificación indicando su disponibilidad. El sistema registra esa respuesta y su tiempo, lo que permite saber quién puede participar en el plan y en qué plazo.

• **Cadenas de suplencia para perfiles clave**. Para los puestos críticos se ha definido un titular y hasta cinco suplentes. VES llama de forma secuencial y escalonada a cada nivel hasta localizar a una persona disponible para actuar.

Cómo funciona una activación

Cuando se produce un incidente, el Gerente/Jefe de Hospital, como presidente del Comité Permanente de Catástrofes, selecciona en VES el plan y el nivel de actuación correspondiente. A partir de ese momento, la plataforma inicia la notificación por fases: va avisando de forma secuencial a los grupos de acción implicados en cada fase del procedimiento, de modo que cada grupo recibe el aviso en el momento que le corresponde, sin necesidad de marcar números ni consultar listados.

Mientras los avisos se envían, el panel de seguimiento se va actualizando con las respuestas: quién ha confirmado, quién no está disponible y quién todavía no ha contestado. En los perfiles clave, si el titular no responde o no puede acudir, el sistema pasa automáticamente al siguiente suplente, y así sucesivamente, hasta cubrir el puesto. El responsable del comité de catástrofes dedica su atención a decidir, no a localizar personas.

Todo queda registrado en el histórico de la activación: quién lanzó el plan, a quién se avisó, cuándo respondió cada persona y en qué sentido. Esa trazabilidad es la misma tanto en una emergencia real como en un simulacro, lo que permite revisar después cada ejercicio y mejorar el plan con datos.

Qué aporta al Hospital

• **Rapidez en la activación**. Cientos de avisos lanzados desde un único punto, en minutos, en lugar de una cadena de llamadas manuales.

• **Comunicación ordenada**. Cada grupo de acción recibe el aviso en la fase del procedimiento que le corresponde.

• **Visibilidad real de la capacidad de respuesta**. El Hospital sabe con quién cuenta y en qué plazo, no solo a quién ha avisado.

• **Cobertura de los puestos críticos**. Las cadenas de suplencia reducen el riesgo de que un perfil clave quede sin cubrir porque una persona no esté localizable.

• **Menos dependencia de procesos manuales**. El plan se ejecuta según las reglas definidas, con menos margen para olvidos o errores en un momento de máxima presión.



Esquema ilustrativo del funcionamiento configurado en VES

Figura 2. Funcionamiento de la cadena de suplencias para perfiles clave del plan.

- La digitalización del sistema de activación del Plan de Respuesta Hospitalaria frente a Catástrofes externas se detectó como una necesidad operativa desde los primeros simulacros. Desde el año 2025 en que el sistema de activación está plenamente operativo la activación del Plan se realiza de forma completa en menos de diez minutos y fundamentalmente permite la activación secuencial y predeterminada de todos los recursos asistenciales y unidades de apoyo. También ha permitido estructurar mejor el Plan de Respuesta y considero que es un avance fundamental para la gestión de la respuesta.

  Ignacio Sánchez-Arcilla . Responsable del Plan de respuesta frente a Catástrofes Externas y Emergencias en salud Pública.

- **Simulacros con evidencias**. Los ejercicios se realizan con la misma herramienta que una activación real y dejan un registro que sirve para el análisis posterior y la mejora continua del plan.

Un proyecto que crece: el Código Rosa

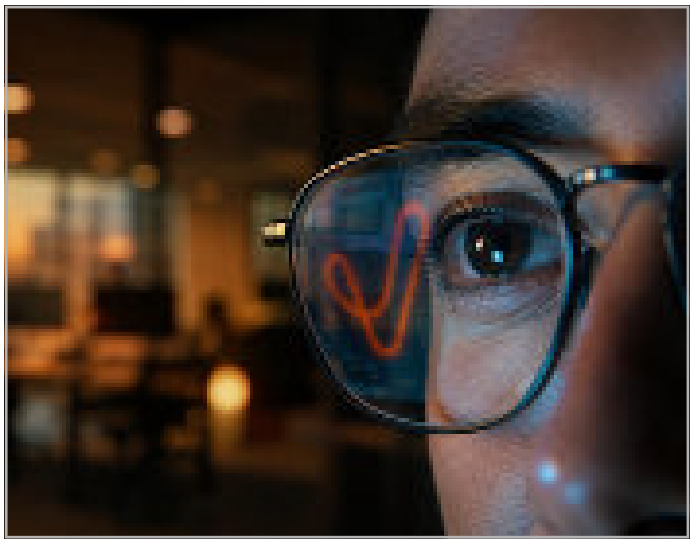
Además del Plan de Catástrofes, el Hospital ha digitalizado en VES el Código Rosa, el protocolo de actuación del Hospital Materno Infantil ante la desaparición de menores. Es un ejemplo de cómo el proyecto ha ido creciendo: sobre la misma plataforma se incorporan nuevos protocolos críticos, cada uno con sus propios grupos de actuación, reglas de comunicación y registro de lo ocurrido.

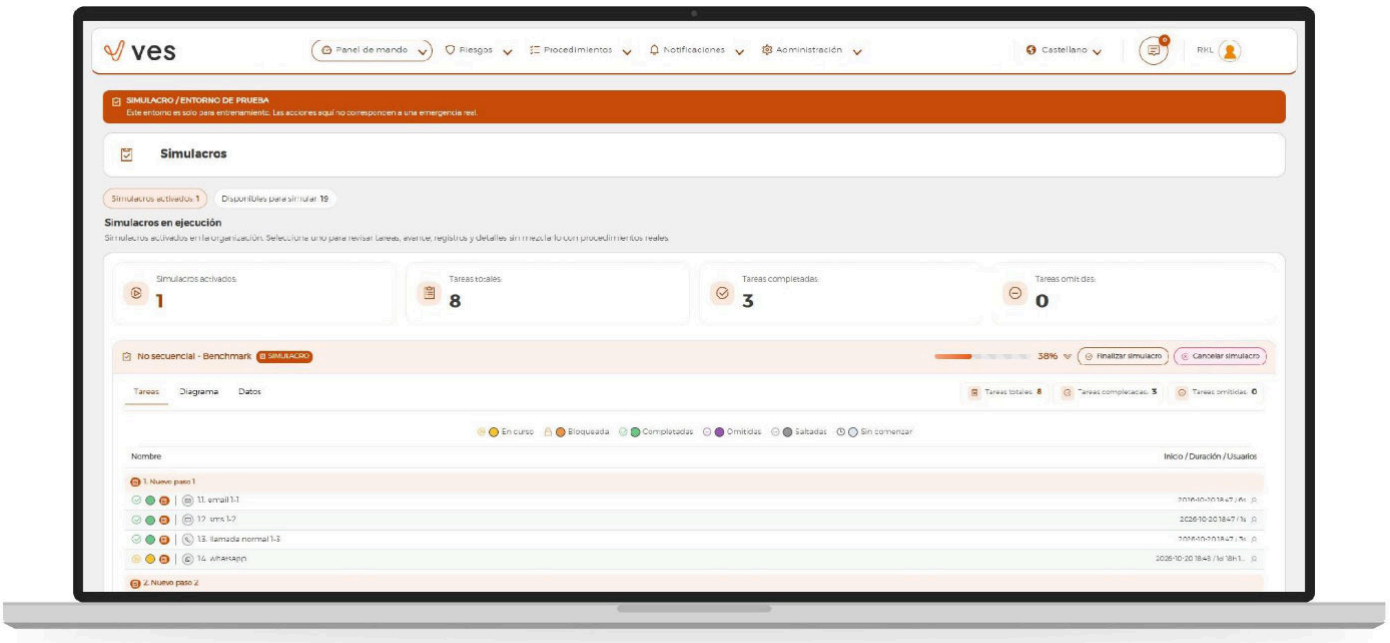
Un modelo aplicable más allá del ámbito sanitario

El caso del Gregorio Marañón responde a un problema que comparten muchas organizaciones con responsabilidades de seguridad y continuidad: puertos, industria, administraciones públicas, centros de control o grandes instalaciones. Todas necesitan movilizar a las personas adecuadas en poco tiempo, confirmar su disponibilidad y dejar constancia de lo que ha ocurrido.

VES permite trasladar planes de autoprotección, procedimientos de emergencia y planes de continuidad a flujos digitales: listas de tareas por rol, notificaciones multicanal, seguimiento en tiempo real, simulacros y exportación de evidencias. El objetivo es que el plan que está escrito sea el plan que realmente se ejecuta.

Más información: www.rklves.com
José Mari Sanz Yarritu
josemari@rklintegral.com
646.321.812.





Vista de simulacros de VES con un ejercicio en curso: tareas por fase, avance y tiempos (captura de un entorno de demostración).



Dentro del marco de colaboraciones, **ADSIy IMMUNE Technology Institutea través de su área de conocimiento en ciberseguridad aplicada a entornos de vigilancia, combinando seguridad física y digital, ha desarrollado este programa formativo, que tiene como objetivo fundamental capacitar a los profesionales de la seguridad en la identificación, prevención y respuesta ante amenazas híbridas, así como en el cumplimiento normativo y la operación segura de sistemas como CCTV, controles de acceso, biometría o drones.**

IMMUNETechnology Institutenos ofrece: Promover un acceso preferente de las formaciones a los **Socios y Patrocinadores de ADSI**, con un descuento del 20%.

DESCARGA PROGRAMA COMPLETO

PARA MÁS INFORMACIÓN

Borja de Alarcón
Business Director

borja.alarcon@immune.institute

Resumen de los datos más relevantes de la convocatoria

Modalidad: Híbrida (online con prácticas y simulaciones).

Duración: 48 horas lectivas + 8 horas de simulacro (total estimado: 56 horas).

Nivel: Intermedio.

Dirigido a: Vigilantes de seguridad privada con funciones en CCTV, control de accesos, alarmas, drones y sistemas biométricos.

Requisitos: Certificado de Profesionalidad y tarjeta TIP en vigor.

Metodología:

- Enfoque práctico (20% teoría, 60% práctica, 20% simulacros).
- Casos reales, simulaciones de incidentes y material operativo (checklists, guías, etc.).

Evaluación:

- Prueba teórico-práctica (mínimo 70% para aprobar).
- Simulacro de incidente híbrido con evaluación por competencias.

Titulación:

- Diploma acreditativo alineado con el SEPE.
- Opcional: acreditación con sello de la AEPD.

DESCARGA DOCUMENTO RESÚMEN

Contenidos principales:

- Fundamentos de ciberseguridad y marco legal.
- Protección de datos en videovigilancia y control de accesos.
- Amenazas híbridas (físicas + cibernéticas).
- Sistemas biométricos y control de accesos seguros.
- Operación segura de CCTV, alarmas y drones.
- Detección de indicadores de compromiso (IoC).
- Prevención de ingeniería social y desinformación.
- Notificación de incidentes de seguridad.
- Ciberhigiene operativa y concienciación continua.

Objetivos del programa:

- Reducir riesgos de brechas por errores humanos.
- Garantizar el cumplimiento normativo.
- Mejorar la respuesta ante incidentes híbridos.
- Posicionar a las empresas de seguridad como socios estratégicos en resiliencia digital.

Certificación y renovación:

- Certificado válido por un año.
- Posibilidad de renovación mediante examen y simulacro.

Formación continua opcional:

Plataforma online con alertas de amenazas, contenidos formativos y ejercicios periódicos.

Condiciones especiales de matriculación para socios, adheridos y patrocinadores de ADSI en cursos de la UNIR-Universidad Internacional de La Rioja

unir LA UNIVERSIDAD EN INTERNET

ADSI asociación de directivos de seguridad integral 30 años



UNIR te ofrece más de 400 titulaciones con descuentos y ventajas exclusivas gracias al Convenio de Colaboración con tu organización. Además, tienes condiciones especiales en las siguientes titulaciones destacadas:

GRADOS

DESCUENTO 45% PRIMER AÑO (20% en años sucesivos)

- Grado en Derecho
- Grado en Criminología
- Grado en Ciencias de la Seguridad
- Grado en Ciencias Políticas y Gestión Pública
- Grado en Relaciones Internacionales

Participa en **seminarios y cursos gratuitos** y **reconoce hasta 18 ECTS adicionales.**

DESCUENTO 40% PRIMER AÑO (10% en años sucesivos)

- Grado en Psicología

MÁSTERES OFICIALES

DESCUENTO 40%

- Máster Universitario en Ciberdelincuencia
- Máster Universitario en Delincuencia Juvenil e Intervención con Menores
- Máster Universitario en Estudios Avanzados en Terrorismo: Análisis y Estrategias
- Máster Universitario en Estudios de Seguridad Internacional
- Máster Universitario en Investigación Criminal
- Máster Universitario en Seguridad Pública
- Máster Universitario en Victimología y Criminología Aplicada
- Máster Universitario en Análisis y Prevención de la Corrupción

Docencia 100% online | Clases en directo | Mentor personal | Infórmate en: colectivos@unir.net

Delta13-UDIMA

Cátedra en Tecnología aplicada a la seguridad

CURSO DE DIRECTOR DE SEGURIDAD



OFERTA ASOCIADOS:

70€ AL MES

Aprende las habilidades esenciales para convertirte en un líder en seguridad. ¡No te lo pierdas!
Curso Homologado por el Ministerio del Interior y acreditado por la Universidad a Distancia de Madrid (UDIMA)

ADSI asociación de directivos de seguridad integral 30 años

INSTITUTO DELTA13 | udima La universidad online más cercana

CÁTEDRA EN TECNOLOGÍA APLICADA A LA SEGURIDAD

INSTITUTO DELTA13

UNIVERSITAT DE BARCELONA | Facultat de Dret

ADSI
Asociación de Directivos de Seguridad Integral

CONOCIMIENTO • NETWORKING • PROFESIÓN

MÁSTER EN DIRECCIÓN DE SEGURIDAD PRIVADA

FORMACIÓN UNIVERSITARIA DE REFERENCIA

El conocimiento, la experiencia y la visión estratégica para liderar la seguridad de hoy y de mañana.



TITULACIÓN UB
Prestigio académico y reconocimiento universitario.

PROFESORADO EXPERTO
Profesionales en activo y referentes del sector.

MODALIDAD ONLINE Y PRESENCIAL
Flexibilidad para tu desarrollo profesional.

PERSPECTIVA INTERNACIONAL
Casos, tendencias y retos globales.

SI ERES ASOCIADO O PATROCINADOR DE ADSI

DISPONES DE GRANDES VENTAJAS EN TU MATRÍCULA

ADSI
Asociación de Directivos de Seguridad Integral

- Condiciones especiales de matrícula para asociados.
- Beneficios exclusivos para patrocinadores de ADSI.
- Consulta todos los detalles a través de nuestros canales de contacto.



UNA FORMACIÓN COMPLETA Y ACTUAL

DIRIGIDA A PROFESIONALES DE LA SEGURIDAD

- Dirección y gestión de la seguridad
- Marco normativo y compliance
- Seguridad corporativa y riesgos
- Seguridad en sectores estratégicos
- Visión internacional y adaptación local

MÁS INFORMACIÓN E INSCRIPCIÓN

Escanea el QR o accede a:
https://web.ub.edu/ca/web/estudis/w/masterpropi-202511680

+34 93 403 96 17
postgrausegur@ub.edu
postgrausegur@gmail.com

Tu próximo paso empieza aquí

Si eres asociado o Patrocinador de ADSI dispones de un 15% de descuento en el importe del curso.

Formación certificada por IMQ Business school

IA ESTRATÉGICA DESDE EL CONSEJO

Del criterio a la ventaja competitiva, el único executive programa certificado de gobierno de la IA diseñado por y para consejeros.

La inteligencia artificial está modificando cómo se vende, cómo se atiende al cliente, cómo se calcula el riesgo, como se controla el fraude y cómo se explica una decisión ante reguladores y accionistas.

La cuestión no es si el Consejero debe aprender a programar, es si puede ejercer con rigor su función de supervisión cuando una parte creciente de la compañía decide, recomienda y automatiza mediante modelos que no siempre son visibles para el órgano de administración.

EL PRIMER PROGRAMA QUE CONVIERTE LA IA EN MATERIA DE CONSEJO

Un consejero necesita poder formular exigencias verificables, no basta con "entender la IA". Qué casos de uso existen, qué datos los alimentan, quién responde por sus decisiones, qué riesgos se han clasificado, qué controles son proporcionales, qué métricas se reportan y qué evidencia quedará en acta. Criterio estratégico: Distinguir valor real de ruido de mercado. Aprobar, pausar o exigir cambios a una iniciativa de IA con argumentos estratégicos, regulatorios y económicos. Diligencia documentada: AI Act en vigor, AESIA activa.

La formación certificada es un instrumento de trazabilidad y defensa, no un reconocimiento honorífico. Gobierno operativo: Un sistema operativo de Consejo para la IA: charter, inventario, scoring, KPIs/KRIs y hoja de ruta. Herramientas que se usan desde la siguiente reunión.

Para mayor información en el siguiente link:

CIBERSEGURIDAD ESTRATÉGICA

Hay dos clases de Consejeros en 2026: los que ya supervisan el riesgo digital con criterio propio y los que aún confían en que el problema lo resolverá el departamento técnico.

La distancia entre ambos se mide en sanciones evitadas, brechas contenidas y reputación preservada. La transformación digital ha redefinido el mapa de riesgos del Órgano de Administración.

La ciberseguridad ha dejado de ser un asunto operativo del CIO para convertirse en una palanca estratégica que impacta directamente en la continuidad del negocio, la valoración corporativa, el cumplimiento regulatorio y la responsabilidad personal de cada Consejero.

En enero de 2026, el World Economic Forum lo formuló sin matices: la ciberseguridad ha pasado del departamento de IT a la sala del Consejo. El 94 % de los líderes mundiales identifica la Inteligencia Artificial como el principal motor de cambio del riesgo digital, y el 87 % sitúa las vulnerabilidades asociadas a IA como el riesgo de mayor crecimiento de 2025.

ESTE PROGRAMA OFRECE a

Consejeros, Consejeros Delegados, Secretarios del Consejo y miembros de Comités las claves para comprender, supervisar y decidir con criterio en materia de ciberseguridad, gestión de crisis e Inteligencia Artificial. Un itinerario construido sobre casos reales con nombre propio, herramientas inmediatamente aplicables y un claustro que vive el problema cada día. El programa contribuye al cumplimiento de DORA, NIS2 y el Reglamento Europeo de IA, y culmina con la certificación oficial de IMQ Ibérica Business School.

Para mayor información en el siguiente link:

Programa ejecutivo

«Transformación cuántica, la nueva ventaja competitiva para la empresa»

Orientado a explorar las aplicaciones empresariales de las tecnologías cuánticas y sus implicaciones, también en el ámbito de la ciberseguridad.

- Inicio: 5 de noviembre de 2026
- Duración: 10 horas, los jueves de 17:30 a 20:00 h
- Precio: 400 €
- Bonificación FUNDAE: hasta 130 € bonificables para empresas, según los requisitos aplicables.
- **SOCIOS Y PATROCINADORES DE ADSI pueden beneficiarse de un 10 % de descuento adicional.**

En el momento de realizar la inscripción, deben indicar que pertenecen a ADSI, asociación colaboradora de ASCICAT.

No es necesario ningún código promocional.

👉 Consultar el programa y las inscripciones

Como lectura complementaria, Eurecat también nos comparte este artículo científicodel NIST sobre criptografía poscuántica y el futuro de la ciberseguridad.





- Si cumples el nivel de titulación académica requerida Obtendrás el titulo de Posgrado por la Universidad de Vic (30ECTS)
- En caso de no contar con una titulación requerida, obtendrás el Certificado de Aprovechamiento del Curso de Dirección de Seguridad Integral (400H) expedido por Universidad de Vic.

ised ADSI 30 años asociación de directivos de seguridad integral

UCAV www.ucavila.es

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

MÁS INFORMACIÓN

ADSI 30 años asociación de directivos de seguridad integral





MÁSTER UNIVERSITARIO
EN PROMOCIÓN PROFESIONAL PARA LA GESTIÓN DE CRISIS
EN SEGURIDAD Y DEFENSA

UNIVERSIDAD CATÓLICA DE ÁVILA

DIRECTOR: Dr. Alberto Barea Vera
CODIRECTOR: Coronel José Luis Calvo Albero

Becas de Excelencia para analistas de riesgos

En el siguiente enlace se detalla el **Proceso de selección de Becas de Excelencia de LISA Institute** para aspirar a una **Beca de 50%** de importe del curso para estos Másteres universitarios:

- **Máster Profesional de Analista de Inteligencia**
- **Máster Profesional de Analista Criminal y Criminología Aplicada**
- **Máster Profesional de Analista Internacional y Geopolítico**
- **Máster Profesional de Analista Estratégico y Prospectivo**
- **Máster Profesional en Ciberseguridad, Ciberinteligencia y Ciberdefensa**

¿Cómo participar?

FORMULARIO

Características de los másteres

- **100% online**, prácticos, interactivos e inmersivos.
- Duración: **9 meses** con avance **flexible**.
- **Doble titulación universitaria** emitida por LISA Institute y la Universidad a Distancia de Madrid (UDIMA), con 60 créditos ECTS.
- **Requisitos**: NO hace falta titulación universitaria previa.
- **100% de profesores son profesionales en activo** en empresas e instituciones públicas.
- **Prácticas reales** en unidades de análisis mentorizadas por profesionales en activo.
- Bolsa de Trabajo

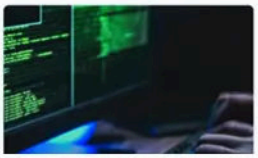
Programa formativo en ciberseguridad de Policía Nacional y Universidad de Salamanca

INFORMACIÓN



FORMACIÓN ESPECIALIZADA

con la colaboración y el respaldo del
Instituto Universitario Gutiérrez Mellado-UNED



Curso de Ciberseguridad y preparación del Director de Seguridad – CISO



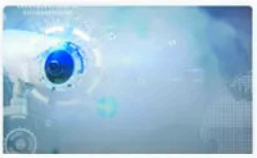
Curso de Seguridad en Infraestructuras Críticas (DSICE)



Curso de Continuidad de Negocio, herramienta para la sostenibilidad de la empresa



Curso de Gestión del Riesgo: Sistemática y Metodología



Curso de Técnico en Sistemas de Seguridad

20% descuento para asociados ADSI

DESCARGAR INFORMACIÓN

Más información - formacion@getseguridad.com - 915 001 724

Cursos bonificables para empresas. Desde GET realizan la consulta del crédito disponible, así como la tramitación de la bonificación en caso de realizar algún curso

Curso de Especialista en Seguridad en Infraestructuras Críticas y Estratégicas

Enlace

Curso Superior de Dirección y Gestión de Seguridad Integral

Enlace

Master de Formación Permanente en Cibersecurity Management

Enlace

Grado en Prevención y Seguridad Integral (100% a distancia)

Enlace

Grado de Criminología y Dirección de Seguridad

Enlace



Revista Red Seguridad
Nº 114 3er Trim 2026
Enlace



Revista Seguritecnia
Nº 521 Sep/Oct 2026
Enlace

Guía de Desarrollo e Implementación de Proyectos de Instalación de Sistemas Electrónicos de Seguridad.

Publicada en AES FUNDACIÓN, esta guía ha sido elaborada por el Area de Ingeniería, Instalación y Mantenimiento de AES, el documento aborda el ciclo completo de un proyecto de seguridad electrónica, desde el análisis y la evaluación de riesgos hasta el diseño, la implementación, la operación y la mejora continua de los sistemas, incorporando aspectos clave como la integración tecnológica, la ciberseguridad y el cumplimiento normativo.

Enlace



Ebook gratuito
"La seguridad como ventaja competitiva"

Esta publicación de Cuadernos de Seguridad-Editorial Peldaño, analiza cómo la inversión en seguridad puede ser un elemento diferenciador para mejorar la competitividad y fortalecer el negocio de una empresa.

Enlace



MINISTERIO DEL INTERIOR
SECRETARÍA DE ESTADO DE SEGURIDAD
DIRECCIÓN GENERAL DE COORDINACIÓN Y ESTUDIOS

Balance Trimestral de Criminalidad.

Enlace

aproser 1977 - 2027 50 AÑOS por tu seguridad

APROSER: Estudio sociológico de la seguridad privada.

Enlace

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Menor engañado para hacer falsas inversiones en criptomonedas.

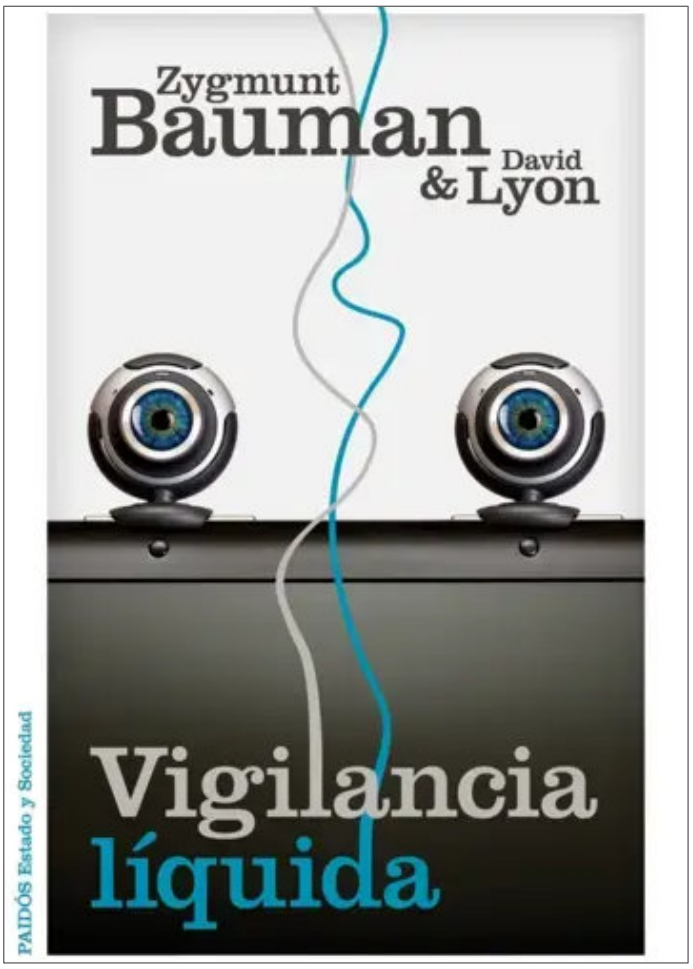
Enlace



"Guía de buenas prácticas frente al modelo de IA ofensiva".

Enlace

Vigilancia Líquida



Autor: David Lyon Zygmunt Bauman

Hoy en día, los detalles más insignificantes de nuestras vidas son registrados y examinados como nunca antes, y a menudo quienes son vigilados cooperan voluntariamente con los vigilantes. Desde Londres y Nueva York hasta Nueva Delhi, Shanghái y Río de Janeiro, la presencia de cámaras de vídeo en los lugares públicos ya es algo habitual y aceptado por la población. En la actualidad, los viajes aéreos implican el paso por escáneres humanos y controles biométricos que se han multiplicado a raíz del 11-S. Diariamente Google y los proveedores de tarjetas de crédito apuntan el detalle de nuestros hábitos, preocupaciones y preferencias, y con ellos van elaborando estrategias de marketing personalizadas con nuestra activa y, en algunos casos, entusiasta cooperación.

En este libro el análisis de la vigilancia de David Lyon confluye con el mundo líquido moderno que Zygmunt Bauman ha descrito con su característica agudeza. ¿Nos encontramos ante un futuro lúgubre de vigilancia continua o existen aún espacios de libertad y esperanza? ¿Cómo podemos ser conscientes de nuestras responsabilidades para con nuestros semejantes, perdidos como estamos con frecuencia en discusiones sobre datos y categorizaciones? Nos encontramos ante temas del poder, la tecnología y la moral, este libro constituye un análisis brillante de lo que implica ser observado -y estar observando- en la actualidad.

SOBRE EL AUTOR

Nació en Poznan, Polonia, en 1925 y falleció en la ciudad inglesa de Leeds en 2017.

Tras la invasión nazi, su familia se refugió en la zona soviética y Bauman se alistó en el ejército polaco, que liberaría su país junto a las tropas soviéticas. Fue miembro del Partido Comunista hasta la represión antisemita de 1968; la consiguiente purga le obligó a abandonar su puesto como profesor de filosofía y sociología en la Universidad de Varsovia. Después enseñó sociología en Israel, Estados Unidos y Canadá, y fue profesor emérito en la Universidad de Leeds (Reino Unido).

En su abundante producción destacan libros fundamentales de la sociología contemporánea como Modernidad y holocausto o Modernidad líquida, o el volumen de conversaciones Vivir en tiempos turbulentos, donde nos brinda un acceso privilegiado a su pensamiento y a diversos aspectos clave de su vida. Zygmunt Bauman mereció el Premio Príncipe de Asturias de Comunicación y Humanidades 2010, el Premio Amalfi de Sociología y Ciencias Sociales (1992) y el Theodor W. Adorno (1998).



ADSI

30 anos

CONECTANDO E IMPULSANDO