ADSI
asociación de directivos de seguridad integral
30 años
NEWS flash

#530 - Noviembre 2026



Entrevista socio

Pau Pellicer

Artículo de Opinión

"Martes con ..."

Parlament de Catalunya

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
Carta del presidente

5
Artículo de opinión
- Los riesgos de una sociedad impaciente

7
Entrevista a un socio

10
Artículo
- Aprender, observar y corregir para reducir el coste del movimiento y conservar el control bajo carga
- Disturbios en Barcelona, cuando la protesta dejó de ser protesta
- Lo que su empresa enseña sin querer: cómo reducir la exposición en fuentes abiertas
- Robos a famosos y vulnerabilidades en viviendas de lujo

16
Noticias ADSI
- "Martes con..." Visita al Parlament de Catalunya
- ADSI presente en EXPOPROTECTION París
- ADSI presente en la Jornada de la Sociedad Clave sobre "La justicia ante la revolución tecnológica"
- ADSI en la Diada de la Guàrdia Urbana de Barelona
- ADSI presente en el III Congreso de seguridad en espacios públicos en Barcelona
- ADSI invitada a la 39ª Gala de los Trofeos Internacionales de Seguridad
- Miguel Merino Thomas, socio de ADSI, Premio Especial del Jurado de los Trofeos Internacionales de Seguridad de Seguritecnia
- ADSI participa en el máster universitario en seguridad pública de la UNIR
- ADSI en la jornada "Narcotráfico, blanqueo de capitales y empresa" organizada por Foment del Treball Nacional
- ADSI en el Talent Fair Event 2026 de ESERP, Business & Law School
- ADSI en el VIII Congreso ADESyD "Compartiendo (visiones de) Seguridad

28
Actualización de datos

27
Nuestros patrocinadores
- INTERNATIONAL SOS
- F24
- ARMATURA
- BARNAPORTERS
- COLLBAIX
- EULEN
- ILUNION
- TARGET

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
ALERTA y CONTROL SEGURIDAD
ARMATURA
ARMONIA SEGURIDAD
AXIS COMMUNICATIONS
Grup Barna Porters
bydemes 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

Llegamos al final de 2026, momento de valoración y buenos deseos

Esta es la última revista del 2026 que os haremos llegar, ya que en diciembre no la editamos, y por ello me gustaría hacer un breve balance del año.

Ha sido un año realmente intenso en todos los sentidos, con incidencias de seguridad relevantes; situaciones de alta afectación geopolítica; manifestaciones, protestas y alborotos como hacía años que no veíamos, con importante repercusión en establecimientos comerciales de Madrid y Barcelona, principalmente; de huelga general; de reivindicaciones socio-económicas; de elecciones generales que han aflorado la peor cara de la beligerancia de nuestra clase política, más preocupada de atacar al contrario que de exponer claramente su programa político; etc .etc.

Un año que no habrá dejado indiferente prácticamente a nadie. Un ejercicio en el que la inteligencia artificial se ha consolidado como la mejor de las herramientas de ayuda a nuestras funciones de responsabilidad en el ámbito de la seguridad, en todas y cada una de las disciplinas en que se desenvuelve el heterogéneo colectivo de integrantes de ADSI. Pero también una IA que ha sido utilizada por los delincuentes para perjudicar a nuestras entidades y procesos, aquellos que como Directores y Directivos de Seguridad estamos obligados a proteger y evitar al máximo la repercusión delictiva.

Pero ha sido, de nuevo, un año positivo para ADSI, que ha crecido en asociados, patrocinadores y amigos de nuestro proyecto asociativo. Un ejercicio en el que nuestra cuenta de resultados ha vuelto a ser también positiva, un año más. Un año en el que nuestra Cena Institucional y Entrega de Premios ADSI se ha posicionado como uno de los eventos de mayor relevancia del país.

Y todo ello, sin duda, fruto del trabajo intenso y altruista de los integrantes de la Junta Directiva de ADSI, de los 14 que la componemos, pero en especial del equipo Directivo de la misma, en el que quiero destacar a nuestra Vicepresidenta, Elvira Márquez; al Secretario, David Sanmartín y al Tesorero, Emilio Herrero. Gracias a todos, incluido también el Defensor del Socio de ADSI.

Encaramos todos este mes de diciembre como un momento para la valoración de todo lo realizado y lo pendiente; para los mejores deseos en el 2027; para planificar el próximo año; de recargar las pilas y seguir trabajando intensamente en ADSI para seguir manteniendo la posición de privilegio en la que actualmente se encuentra, en todos los sentidos, dentro del ecosistema asociativo nacional de profesionales de la seguridad privada, como siempre digo, al margen de las asociaciones empresariales, que juegan en otra liga.



Pero estas navidades y entrada de año si que todavía me toca a mí daros el mensaje tradicional que todos lanzamos en estas fechas señaladas: desearos unas muy felices fiestas y que el 2027 sea lo mas positivo posible para todos, incluida nuestra asociación y todos aquellos que, de una manera u otra, formáis parte de nuestro proyecto asociativo.

FELICES FIESTAS Y UN MAGNÍFICO 2027 PARA TODOS ¡¡¡¡



Los riesgos de una sociedad impaciente

Por Macarena Ramisa, Vocal de ADSI

Confieso que cada vez que participo en un encuentro profesional del sector me hago la misma pregunta: ¿estamos hablando de los riesgos que realmente van a afectar a nuestras organizaciones en los próximos años?

La respuesta, en muchas ocasiones, es incómoda.

Hablamos mucho de inteligencia artificial, de ciberseguridad, de nuevas tecnologías aplicadas a la protección corporativa y de sistemas cada vez más sofisticados. Sin duda son asuntos importantes. Pero tengo la sensación de que, mientras observamos fascinados el horizonte tecnológico, estamos prestando menos atención a un fenómeno mucho más cercano y visible: el cambio profundo que está experimentando nuestra sociedad.

Y ese cambio tiene consecuencias directas para la seguridad.

Después de años en esta profesión he llegado a una conclusión sencilla: buena parte de los riesgos que tendremos que gestionar en los próximos años no nacerán necesariamente de la delincuencia tradicional ni de grandes amenazas organizadas. Nacerán de una sociedad cada vez más tensionada, más impaciente y más imprevisible.

Miremos a nuestro alrededor.

La agresividad en la convivencia cotidiana aumenta. La tolerancia a la frustración disminuye. Las redes sociales amplifican cualquier conflicto hasta dimensiones insospechadas. La confrontación parece generar más atención que el diálogo. Y todo ello acaba teniendo un reflejo inevitable en las organizaciones.

Durante mucho tiempo las empresas pudieron vivir relativamente aisladas de lo que ocurría fuera de sus muros. Hoy eso es imposible.

La empresa se ha convertido en un actor social. Opina aunque no quiera. Es observada permanentemente. Puede ser cuestionada, señalada o convertida en objetivo de campañas de presión en cuestión de horas. Y lo que comienza en el mundo digital puede terminar, con demasiada facilidad, delante de una recepción, de una tienda o de un centro de trabajo.

La seguridad siempre ha consistido en anticipar riesgos. Y el riesgo hoy ya no reside únicamente en quien intenta entrar donde no debe o apropiarse de lo que no le pertenece. El riesgo también aparece cuando aumenta la conflictividad social, cuando una situación cotidiana puede escalar con rapidez o cuando nuestros empleados deben desarrollar su actividad en entornos más tensos que los de hace apenas unos años.



Barcelona es un magnífico ejemplo de esta transformación.

Lo digo desde el respeto y también desde el afecto hacia mi ciudad, una ciudad extraordinaria que ha sabido proyectarse al mundo como pocas. Pero precisamente por ser una ciudad global, Barcelona se ha convertido en un laboratorio donde observar muchos de los desafíos que marcarán el futuro de la seguridad.

Turismo masivo, grandes acontecimientos internacionales, infraestructuras críticas, intensa actividad económica, diversidad cultural, tensiones derivadas del uso del espacio público, nuevos fenómenos de delincuencia organizada y una creciente sensibilidad social frente a cualquier incidente.

Todo ocurre al mismo tiempo. Y cuando todo ocurre al mismo tiempo, gestionar seguridad deja de ser una cuestión de medios técnicos para convertirse en una cuestión de criterio.

Y precisamente ahí es donde creo que deberíamos centrar una parte importante de nuestro debate profesional.

Porque cuando una sociedad se vuelve más impaciente, más agresiva y menos tolerante a la frustración, las organizaciones también se vuelven más vulnerables.

No porque aumenten necesariamente las amenazas tradicionales, sino porque aumenta la probabilidad de que cualquier conflicto escale rápidamente.

Lo estamos viendo cada día. Clientes que reaccionan con agresividad ante una negativa. Usuarios que convierten una discrepancia en una confrontación. Empleados que desarrollan su trabajo bajo una presión creciente. Situaciones que hace unos años se resolvían con diálogo y que hoy, con demasiada frecuencia, derivan en insultos, amenazas o incluso agresiones.

No se trata de hechos aislados. Se trata de comportamientos que empiezan a repetirse con demasiada frecuencia como para ignorarlos.

La seguridad privada siempre ha trabajado para proteger a las organizaciones frente a amenazas externas identificables. Sin embargo, una parte de los riesgos que emergen hoy procede de algo mucho más difícil de controlar: el deterioro de ciertos mecanismos de convivencia que durante años dimos por descontados.

La inmediatez se ha impuesto a la reflexión.

La indignación genera más atención que la serenidad.

La discrepancia se confunde cada vez más con la confrontación.

Y las redes sociales amplifican cualquier conflicto hasta hacerlo visible para miles de personas en cuestión de minutos.

Todo ello crea un entorno más tenso, más emocional y, en muchos casos, más agresivo.

Un entorno que acaba entrando inevitablemente en las empresas, en los comercios, en los hospitales, en las infraestructuras críticas y en los espacios donde trabajan nuestros profesionales de seguridad.

Por eso creo que cometeríamos un error si centráramos toda nuestra atención en los avances tecnológicos y no dedicáramos el mismo esfuerzo a comprender la evolución de la sociedad que debemos proteger.

La tecnología seguirá siendo una herramienta imprescindible. Pero ninguna cámara detecta el deterioro de la convivencia. Ningún sistema de control de accesos reduce por sí solo la agresividad social. Y ningún algoritmo sustituirá la capacidad de interpretar los cambios que se están produciendo a nuestro alrededor.

Los riesgos del futuro no llegarán únicamente de la mano de nuevas tecnologías o de nuevas formas de delincuencia. Llegarán también de una sociedad más impaciente, más polarizada y más dispuesta a reaccionar desde la emoción que desde la razón.

Y quizá esa sea la reflexión más incómoda para quienes trabajamos en seguridad: los cambios que más van a influir en nuestro trabajo no están ocurriendo en los laboratorios tecnológicos.

Están ocurriendo en la calle.

Y cuanto antes seamos capaces de reconocerlo, mejor preparados estaremos para proteger a nuestras organizaciones y, sobre todo, a las personas que forman parte de ellas. ■



Pau Pellicer García

Director de Seguridad, Creand - Crèdit Andorrà, Banca Privada a Andorra

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

Actualmente soy el director de Seguridad de Creand Crèdit Andorrà, la principal entidad financiera de Andorra, con presencia en varios países de Europa y América, aunque la actividad y volumen principal están basados en Andorra. Desde mi departamento gestionamos la monitorización, gestión de alertas y respuesta a incidentes, así como el desarrollo de los Planes Continuidad de Negocio y la protección contra todo tipo de amenazas que puedan afectar el desarrollo de las actividades del banco y a sus personas y activos.

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

Como no podría ser de otro modo, la irrupción de la inteligencia artificial representa uno de los principales retos que tenemos por delante en estos momentos, y no tanto por la aparición de nuevas amenazas en sí, sino por la velocidad a la que estas amenazas pueden ser explotadas por los atacantes, la facilidad con la que los delincuentes pueden suplantar una voz, una imagen y la mayor parte de mecanismos de identificación y autenticación tradicionales.

¿Cuál es tu formación académica?

Soy ingeniero en Informática por la UPC, especialidad en robótica y visión artificial, pero desde que me dedico a la seguridad no he dejado de complementar mi formación con certificaciones específicas como auditor ISO27001, auditor CISA, manager CISM, gestión de riesgo CRISC, entre otras.

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

Como ingeniero informático, al principio de mi carrera profesional desarrollé distintas funciones dentro del mundo de la tecnología en diversas empresas de distintos sectores: formación académica universitaria, formación para empresas privadas, desarrollo e implantación de software para el sector de emergencias, sector del automóvil, gestión de flotas, y sector hotelero. Hasta ese momento, para mí la seguridad era simplemente una más de las actividades relacionadas con la tecnología. En 2005 me ofrecen el primer puesto específico de seguridad en una gran consultora, como responsable en un centro de datos compartido por tres entidades financieras. Aunque la orientación del puesto estaba dirigida a la ciberseguridad y protección de datos, no tardé en darme cuenta de que resultaba imposible llevar a cabo dicha protección sin implementar medidas de control de acceso, circuitos de videovigilancia, protección contra incendios y otras medidas de protección medioambiental, incluyendo la dotación de un servicio de vigilancia 24x7. Desde entonces me he mantenido en distintas posiciones vinculadas con la seguridad del sector financiero, orientando en todas ellas la seguridad como la protección integral frente a cualquier riesgo que pueda afectar al negocio y a las personas: ciberseguridad, protección de datos, seguridad ambiental, seguridad física, continuidad de negocio, riesgo laboral, formación y concienciación, etc.



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

Creo que la evolución más importante ha sido pasar de una seguridad principalmente reactiva, centrada en proteger instalaciones y sistemas frente a amenazas conocidas, a una seguridad mucho más preventiva, transversal y orientada a la gestión del riesgo. La digitalización ha multiplicado las amenazas y, sobre todo, la velocidad con la que pueden materializarse, pero también ha puesto de manifiesto que los riesgos físicos, tecnológicos y humanos están cada vez más relacionados. En mi opinión, la seguridad ha dejado de ser una función exclusivamente operativa para convertirse en un elemento estratégico, imprescindible para garantizar la continuidad de las organizaciones y la protección de las personas.

¿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 el director de Seguridad deberá asumir progresivamente un papel más estratégico dentro de las organizaciones, con una visión global de los riesgos y una participación más directa en la toma de decisiones. La inteligencia artificial, la creciente dependencia

tecnológica y la interconexión entre amenazas exigirán profesionales capaces de comprender tanto los riesgos físicos como los digitales, pero también los aspectos humanos, organizativos y regulatorios.

Si tuviera que cambiar algo, sería precisamente la excesiva fragmentación que todavía existe entre las distintas especialidades de seguridad. Creo que deberíamos avanzar hacia un perfil profesional más transversal, con mayor capacidad de interlocución con la dirección y con responsabilidades claramente definidas sobre la protección integral de la organización.

¿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?

No creo que el número de empleados o de centros de trabajo deba ser el criterio determinante, aunque evidentemente puede ser un indicador relevante. Considero mucho más importante analizar la naturaleza de la actividad, los riesgos a los que está expuesta la organización y las consecuencias que podría tener un incidente sobre las personas, el negocio o incluso la sociedad.

Una organización relativamente pequeña puede desarrollar una actividad crítica y requerir una estructura de seguridad mucho más sólida que otra de mayores dimensiones. Por ello, soy partidario de establecer obligaciones proporcionales al nivel de riesgo, evitando imponer estructuras innecesarias, pero garantizando que aquellas organizaciones cuya actividad lo justifique dispongan de una función de seguridad profesionalizada y con capacidad real de actuación.

¿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?

Aún sin conocer en detalles las dos opciones, conceptualmente no considero necesariamente negativo que existan distintas vías de acceso a una profesión, siempre que todas ellas garanticen unos conocimientos y competencias mínimos equivalentes. Lo importante no debería ser tanto la duración de los estudios como la preparación efectiva del profesional para asumir sus responsabilidades.

En mi opinión, sería conveniente definir un marco común de competencias que permitiera evaluar de manera homogénea los conocimientos adquiridos, independientemente de la vía formativa utilizada. También daría mayor importancia a la experiencia profesional y a la formación continua, porque la seguridad evoluciona a una velocidad que difícilmente puede seguir cualquier programa académico por sí solo.

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

Potenciaría especialmente la gestión integral del riesgo, la continuidad de negocio, la ciberseguridad, la protección de la información y el conocimiento de las nuevas amenazas asociadas a la inteligencia artificial. Pero también considero imprescindible reforzar aspectos que a menudo reciben menos atención, como la gestión de crisis, la comunicación, el liderazgo y la capacidad de trasladar los riesgos a la dirección en términos comprensibles para el negocio.

Creo que el director de Seguridad no necesita ser el mayor especialista técnico en todas las disciplinas, pero sí debe tener conocimientos suficientes para comprender cómo se relacionan entre ellas, coordinar a los distintos especialistas y tomar decisiones con una visión global de sus consecuencias.

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

Las ventajas de integrarse en una asociación de profesionales de la seguridad son indiscutibles. La comunicación y compartición de información sobre amenazas y posibles medidas de protección con los actores implicados resultan imprescindibles para enfrentar los retos actuales. La asociación permite conocer a esos actores en un entorno de normalidad, establecer contactos y relaciones que facilitan la gestión en un momento de crisis. Por otra parte, a través de las publicaciones y los encuentros mensuales permite conocer de primera mano las iniciativas que se están llevando a cabo en el sector y que pueden resultar muy útiles para su aplicación propia.

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

Debo reconocer que el hecho de que su presidente actual, con quien coincidí profesionalmente en el pasado y que me enseñó gran parte de lo que conozco sobre la seguridad, ha sido el factor más influyente para dar este paso. Sin embargo, después de participar en alguna de sus actividades, recibir la revista mensual y comprobar su

relevancia en el sector, creo que igualmente habría escogido a ADSI.

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

Realmente llevo poco tiempo formalmente en ADSI, y por el momento sólo podría decir cosas positivas, así que me permitirán responder a esto cuando tenga más conocimiento sobre el funcionamiento de esta prestación a lo largo del tiempo.

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

Creo que el principal obstáculo para la colaboración no es la falta de voluntad, sino la ausencia de mecanismos habituales y estructurados para compartir experiencias e información. Muchas amenazas son comunes a sectores aparentemente muy distintos, y conocer cómo las han afrontado otros profesionales puede resultar extraordinariamente útil.

Potenciaría los grupos de trabajo temáticos, los encuentros entre profesionales de distintos sectores y, especialmente, los canales de intercambio de información sobre incidentes, amenazas y buenas prácticas, siempre respetando la confidencialidad necesaria. Las asociaciones profesionales como ADSI desempeñan un papel fundamental en este ámbito, creando relaciones de confianza que permitan colaborar de forma natural cuando realmente sea necesario.

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?

Me resulta difícil destacar un único país, porque considero que existen modelos interesantes en distintos lugares y que cada uno responde a unas necesidades y a una cultura de seguridad particulares. Sí destacaría la importancia que algunos países europeos están otorgando a la resiliencia de sus organizaciones y a la cooperación entre los sectores público y privado.

Mi experiencia en el sector financiero, trabajando con actividades desarrolladas en distintos países, me ha permitido comprobar que, aunque los marcos normativos y las estructuras organizativas sean diferentes, las amenazas suelen ser muy similares. Por ello, creo que deberíamos potenciar los foros internacionales, los ejercicios conjuntos de gestión de crisis y los mecanismos de intercambio de información entre profesionales, aprovechando también las asociaciones nacionales como punto de conexión. ■

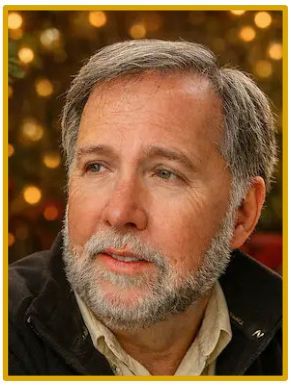
- Un hobby: Me gusta mucho el deporte, especialmente los deportes de montaña, tanto su práctica como su seguimiento, así como la tecnología en general. Esto me ha llevado a la aplicación de la tecnología en eventos deportivos, temas como el cronometraje de esquí alpino, la retransmisión por streaming de eventos, y la propia organización y difusión en las redes de eventos locales como carreras por montaña.
- Un libro: Imposible destacar un libro en concreto. Leo principalmente novela, y concretamente mucha novela histórica, tanto de las civilizaciones antiguas como sobre los conflictos del siglo XX en Europa y España.
- Una canción: Algo parecido a lo que me ocurre con los libros, soy incapaz de destacar una canción en concreto, pero puedo acotar a los temas cásicos de los años 60 y 70, como los Beatles, Creedence Crearwater Revival y por supuesto Elvis Presley.
- Un lugar para desconectar: Hay muchos, pero en este caso sí que voy a concretar uno: Me he criado en Eivissa, y es un lugar al que acudo por lo menos una vez al año y que me proporciona esa sensación de "desconectar".
- Un momento de la historia: Me habría gustado participar directamente en el nacimiento y desarrollo de la informática, especialmente durante las décadas de los años 50, 60 y 70, cuando se sentaron las bases de una revolución tecnológica que acabaría transformando prácticamente todos los ámbitos de nuestra sociedad. Como ingeniero informático, me habría resultado fascinante formar parte de aquella generación de pioneros que, con unos recursos tecnológicos muy limitados, fueron capaces de desarrollar conceptos y soluciones que siguen siendo fundamentales en la informática actual.

Aprender, observar y corregir para reducir el coste del movimiento y conservar el control bajo carga

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

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

Correr, saltar, frenar, girar, levantar una carga, golpear o descender por terreno irregular son habilidades. No aparecen de forma perfecta por repetirlas muchas veces. Necesitan aprendizaje, observación, retroalimentación y corrección. Cuando la técnica es ineficiente, el deportista gasta más energía, distribuye peor las fuerzas y pierde antes la capacidad de decidir.



ENLACE ARTÍCULO 8

OBJETIVO CENTRAL

Una técnica deficiente no causa por sí sola todas las lesiones, pero puede aumentar el coste mecánico y energético del movimiento. Revisar la técnica significa mejorar la eficiencia, ampliar el margen de seguridad y adaptar el gesto a la persona y al contexto.



Disturbios en Barcelona, cuando la protesta dejó de ser protesta

Por Joan Figuera, Vocal de Junta ADSI y Comisario (retirado) de Mossos d'Esquadra

Hace un mes, Barcelona vivió un fenómeno que no puede explicarse como una sucesión de incidentes aislados. Fue un proceso. Un proceso que comenzó con una chispa en París adquirió una dimensión simbólica en Milán, se amplificó en Barcelona, sorprendió y desbordó inicialmente la capacidad de respuesta policial, obligó a blindar el centro de la ciudad, terminó confluyendo con una huelga general y, finalmente, dejó al descubierto una raíz mucho más profunda que la propia calle: la familia, la escuela y el entorno digital.

Este artículo reconstruye aquella secuencia y analiza sus implicaciones desde la perspectiva de la seguridad pública, la inteligencia policial y la responsabilidad social. A continuación, se resume el artículo que Joan Figuera, en su condición de comisario (retirado) de la PG-ME y experto en seguridad pública y policía, publicó en la revista digital "Cuadernos de Seguridad" el pasado 15/11/2026 de este caso de reciente actualidad.

Ver: **ENLACE ARTÍCULO COMPLETO**

I. El contagio

El 24 de octubre de 2026, a las 21 horas, Barcelona vivió un claro efecto contagio. El autor identifica tres dinámicas que actúan juntas:

- **Redes sociales:** fueron detonante y herramienta logística. A diferencia de París, donde había sindicatos y movimientos estudiantiles, en Barcelona la convocatoria nació en el anonimato de canales de Telegram y chats virales. Se repitió el formato de París y Milán: convocatorias a las 15 y las 18 horas, ropa negra y rostro cubierto.
- **Televisión:** actúa como escaparate y legitima el fenómeno. Muestra además cómo se levantan barricadas, qué comercios cierran y cómo responde la policía.
- **Combustible previo:** la emulación no lo explica todo. Ya existían los altercados del 5 de octubre en una manifestación por la vivienda, con 30 agentes heridos, y la acampada de plaza de Catalunya.

Las pantallas no crean el descontento, pero determinan su momento, aceleran su propagación y condicionan sus formas.



II. La geometría París-Milán-Barcelona

El autor recupera el triángulo de modernidad del siglo XIX:

- **París** aportó la chispa y el relato de «el pueblo contra el sistema».
- **Milán** señaló el objetivo simbólico: el lujo y el escaparate, como en Vía Montenapoleone.
- **Barcelona** actuó como amplificador digital. Su paseo de Gràcia, de inspiración parisina, convive con una larga tradición de conflictividad social.

No se trata de saqueos por necesidad, sino de **«disturbios de estatus»**: se ataca el escaparate como símbolo.

Sorpresa, contención e inteligencia

En la primera semana el «Blocus» desbordó a los Mossos d'Esquadra por sorpresa. El 31 de octubre el centro fue blindado. Hubo más de 2.200 identificaciones y varias



Eje París - Milán - Barcelona

detenciones, con un gran despliegue de unidades y de los servicios de información de los cuerpos policiales. Aplicando la teoría de los vasos comunicantes, la saturación preventiva funcionó y se evitaron nuevos altercados de la misma magnitud.

Lo más relevante fue la información obtenida: los datos de filiación y de objetos intervenidos, siempre dentro del marco legal. Así, los participantes dejaron de ser anónimos. Quedan abiertas tres cuestiones:

1. La sorpresa como método.
2. El desplazamiento del conflicto.
3. París como espejo de acciones descentralizadas.

III. Del Blocus a la huelga general: la raíz del problema

El 24 de octubre se reunieron unos 600 jóvenes convocados por TikTok y Telegram, sin pancartas ni reivindicación clara. El balance oficial fue de:

- 23 comercios saqueados.
- 14 agentes heridos.
- 133 detenidos, la mayoría menores.

El 11 de noviembre, tras una manifestación pacífica por la huelga general, grupos de encapuchados intentaron saquear tiendas en paseo de Gràcia y quemaron contenedores. La consellera de Interior cifró el balance en 52 detenidos y más de 32 agentes heridos. El esquema se repite: convocatoria viral y anónima, protesta legítima como cobertura y violencia convertida en espectáculo. En ciertos grupos la violencia ya forma parte del fenómeno.

Figuera sitúa la raíz del problema en varios ámbitos:

- **Familia:** se ha pasado de educar a negociar permanentemente, con jóvenes que confunden derechos con caprichos.
- **Escuela:** el profesorado ha perdido autoridad y respaldo institucional.
- **Aulas:** la diversidad cultural sin políticas eficaces de integración se convierte en un desafío adicional.
- **Entorno digital:** redes sociales e inteligencia artificial alimentan una percepción de inmediatez sin consecuencias.

Menciona también la polémica sobre PISA 2025 en Cataluña, con una exclusión de alumnado del 23,2 % frente al máximo del 5 %, que cuestiona la representatividad de los resultados.

Conclusiones a modo de resumen:

- **Liderazgo:** el liderazgo consiste en anticiparse. La ausencia de políticas preventivas deteriora la convivencia y la confianza en las instituciones.
- **Retos:** el reto policial es la inteligencia, el social es recuperar el sentido común y el político es no instrumentalizar el conflicto.
- **Doctrina:** hay que adaptar la doctrina de orden público con inteligencia digital, anticipación, cooperación policial, proximidad con jóvenes y menores, comunicación institucional rápida y recuperación veloz de la normalidad.
- **Riesgo:** el fenómeno no ha desaparecido. La pregunta es dónde, cuándo y con qué intensidad volverá. Sin una familia fuerte, autoridad docente y límites digitales, estos episodios pueden convertirse en una «nueva normalidad».
- **Cierre:** la seguridad por sí sola no resuelve un problema educativo, cultural y social. Una sociedad que solo reacciona llega tarde, y liderar es, ante todo, anticiparse. ■



Lo que su empresa enseña sin querer: cómo reducir la exposición en fuentes abiertas

Por Julián Gutiérrez López, policía, investigador OSINT y creador de Ciberpatrulla, socio de ADSI

Antes de un fraude, una suplantación o un intento de intrusión suele haber una fase de estudio del objetivo. Hoy buena parte de ese estudio se hace con información pública. La buena noticia es que el departamento de seguridad puede hacer ese mismo trabajo antes y cerrar muchas puertas sin grandes inversiones.

OSINT son las siglas en inglés de inteligencia de fuentes abiertas: obtener información útil a partir de lo que está publicado y al alcance de cualquiera. Redes sociales, webs corporativas, registros públicos, noticias, ofertas de empleo o documentos colgados en internet.

No hace falta entrar en ningún sistema ni saltarse ninguna contraseña. Por eso esta fase no dispara alarmas ni deja rastro en la infraestructura de la empresa.

Llevo desde 2017 investigando con fuentes abiertas, y una de las primeras cosas que se aprenden es que **los datos más valiosos rara vez están escondidos. Suelen estar repartidos**. Un dato por aquí y otro por allá parecen inofensivos; juntos permiten preparar un engaño muy creíble.

Qué puede ver un atacante

Basta con ponerse en su lugar. Quien quiere colar una factura falsa o hacerse pasar por el director general necesita saber a quién dirigirse, cuándo y con qué tono.

Los perfiles profesionales suelen mostrar buena parte del organigrama: quién lleva las finanzas, quién le asiste y quién acaba de incorporarse y todavía no conoce los procedimientos.

Las fotos de una inauguración pueden enseñar cámaras, tornos y puntos de acceso. Un selfi del primer día de trabajo puede mostrar el modelo de acreditación. Una oferta de empleo puede detallar el software de control de accesos que se utiliza.

Y los documentos que la empresa cuelga en su web pueden llevar metadatos con nombres de usuario, rutas internas o versiones de programas.

La inteligencia artificial acelera el proceso

En la cena institucional de este año, el presidente de ADSI recordó una idea del profesor Lassalle: la inteligencia artificial basa su poder en el conocimiento de otros.



Aplicada a este terreno, la frase es muy precisa. La IA que utiliza un delincuente se alimenta de lo que otros han publicado; en este caso, de lo que ha publicado la empresa y su gente.

Resumir todo lo que hay en internet sobre una persona, redactar un correo que imite el estilo de un directivo o aprovechar su voz en entrevistas y vídeos corporativos ya no exige un especialista. **El atacante no necesita ser más hábil que antes: le basta con tener más material y herramientas que le ahorran trabajo**.

Medidas de prevención

La respuesta es aplicar a la propia empresa la mirada del investigador. Estas son las medidas que considero prioritarias, ordenadas por áreas:

Personas clave. Revisar qué publican los perfiles profesionales de la alta dirección y del personal de finanzas, compras y recursos humanos. Recomendar que no se anuncien viajes, agendas ni ausencias mientras ocurren, y que se separen las cuentas personales de las profesionales.

Procesos de pago. Ningún cambio de cuenta bancaria ni ninguna transferencia urgente debería ejecutarse sin confirmarlo por un segundo canal, usando un contacto que ya se tenía y nunca el que aparece en el propio mensaje.

Llamadas y videollamadas. Ante una petición inusual de un directivo, la norma debe ser colgar y devolver la llamada al número conocido. Conviene que la plantilla sepa que hacerlo no es desconfiar del jefe, sino cumplir el protocolo.

Instalaciones. Acordar con el área de comunicación una revisión de seguridad antes de publicar fotos de sedes, eventos o inauguraciones: accesos, cámaras, pantallas, acreditaciones y matrículas.

Información técnica. Redactar las ofertas de empleo sin detallar sistemas de seguridad ni software interno, y

eliminar los metadatos de los documentos antes de publicarlos.

Credenciales y dominios. Comprobar periódicamente si aparecen credenciales del dominio corporativo en filtraciones públicas y vigilar el registro de dominios parecidos al de la empresa, que suelen usarse para suplantarla.

Formación. La concienciación funciona mucho mejor cuando se hace con ejemplos de la propia exposición de la empresa que con casos genéricos.

Un matiz importante: el objetivo es la exposición de la organización, no vigilar la vida privada de los empleados. **Este trabajo debe coordinarse con el delegado de protección de datos** y plantearse como una ayuda a la plantilla para protegerse.

Ninguna empresa va a desaparecer de internet, ni debería. Necesita comunicar, contratar y vender, y para eso tiene que estar presente.

Lo que sí está en nuestra mano es decidir qué se muestra y qué no. **Alguien va a estudiar la empresa que protegemos; lo razonable es que el primero en hacerlo sea su propio departamento de seguridad**.

Si quiere comentar este artículo o valorar cómo formar a su equipo en investigación con fuentes abiertas, puede contactar conmigo por cualquiera de estas vías.

WhatsApp	+34 683 423 185
Telegram	@Ciberpatrulla (t.me/Ciberpatrulla)
LinkedIn	linkedin.com/in/0juliangl
Email	info@ciberpatrulla.com
Blog	ciberpatrulla.com/blog

Julián Gutiérrez López es policía con más de 30 años de servicio e investigador especializado en OSINT desde 2017. Ha impartido formación a Fuerzas y Cuerpos de Seguridad y a departamentos de empresa, también a través de INTERPOL. Es creador de Ciberpatrulla y autor del libro «No es magia, es OSINT».

Checklist del director de seguridad: exposición en fuentes abiertas

Una guía práctica para revisar, al menos una vez al año y tras cada cambio relevante (nombramientos, nuevas sedes, fusiones o campañas de comunicación), lo que la empresa muestra hacia fuera.

1. Preparar

• Definir qué se protege: personas clave, sedes críticas y procesos en los que se mueve dinero o se conceden accesos.

• Coordinar la revisión con el delegado de protección de datos y con el área de comunicación.

2. Revisar desde fuera

• Buscar la empresa y a sus personas clave como lo haría un tercero, sin credenciales ni información interna.

• Revisar los perfiles profesionales de dirección, finanzas, compras y recursos humanos.

• Revisar fotos publicadas de instalaciones y eventos: accesos, cámaras, acreditaciones, pantallas y matrículas.

• Revisar ofertas de empleo y notas de prensa en busca de sistemas, proveedores o software interno.

• Comprobar los metadatos de los documentos publicados en la web corporativa.

• Comprobar si hay credenciales del dominio corporativo en filtraciones públicas.

• Buscar dominios registrados que imiten el de la empresa.

3. Corregir y proteger

• Retirar o corregir lo que no debería estar publicado y forzar el cambio de las contraseñas expuestas.

• Implantar la verificación por un segundo canal para pagos urgentes y cambios de cuenta bancaria.

• Establecer el protocolo de colgar y devolver la llamada ante peticiones inusuales de directivos.

• Pactar una revisión de seguridad previa a cualquier publicación de imágenes de instalaciones.

• Formar a la plantilla con los ejemplos encontrados en la propia revisión.

4. Medir y repetir

• Documentar qué se encontró, dónde y qué medida se tomó.

• Repetir la revisión y comparar resultados para comprobar si la exposición disminuye. ■

Robos a famosos y vulnerabilidades en viviendas de lujo

Por José Miguel Ángel Olleros, CEO fundador de Angel Olleros Consultoría de Seguridad Residencial, socio de ADSI

Este artículo analiza los recientes asaltos a viviendas de personalidades públicas, los factores de riesgo asociados al diseño arquitectónico y los errores habituales en la protección residencial.



Asaltos con los moradores dentro de la vivienda

Esta modalidad delictiva, antes excepcional, está adquiriendo mayor protagonismo entre las bandas criminales que asaltan viviendas con elevada expectativa de botín. La razón fundamental es la facilidad de acceso, consumación del robo y huida. La presencia de los moradores puede favorecer la acción delictiva cuando los sistemas electrónicos están desactivados y algunas puertas o ventanas sin cerrar con llave. Además, mediante la amenaza de agresión física, los delincuentes pueden obligar a los propios moradores a entregar sus bienes de valor y abrir sus cajas fuertes.

¿Cuáles son las tipologías de viviendas más atractivas?

Determinadas viviendas unifamiliares y áticos presentan condicionantes arquitectónicos que favorecen el acceso y el aislamiento visual. Los servicios de vigilancia mediante rondas o de conserjería a tiempo parcial, no compensan, por sí solos, estas deficiencias de diseño.

¿Cuáles son las principales vulnerabilidades?

Desalineación entre el diseño arquitectónico, el paisajismo, la iluminación y las medidas de seguridad.

Diseño inadecuado de los sistemas electrónicos de protección contra la intrusión y de sus modos de activación.

Insuficiente resistencia física de puertas y ventanas.

Sobreexposición de las viviendas en redes sociales y reportajes de estudios de arquitectura e interiorismo.

Hábitos de seguridad deficientes, en ocasiones derivados de la incomodidad de las medidas de protección o de una insuficiente formación de los moradores durante la puesta en marcha del sistema. ■

Enlace al video en que el autor comenta los recientes robos a famosos en Madrid:

https://www.youtube.com/watch?v=fKZsQxCDSrQ

"Martes con..." en Barcelona, 10 de noviembre
Visita al Parlament de Catalunya

El pasado día 10 de noviembre, ADSI fue invitada a visitar el Parlament de Catalunya. La visita reunió a casi 60 asistentes y duró más de una hora. Sergi Terres, del departamento de relaciones públicas, nos explicó la historia del palacio y las etapas en las que acogió la actividad parlamentaria durante los períodos democráticos. Después, nos guió por sus instalaciones.

Visitar el Parlament de Catalunya fue una oportunidad para conocer de cerca una de las instituciones fundamentales de la vida democrática catalana. Situado en el Parc de la Ciutadella de Barcelona, el Parlament abrió sus puertas a los socios de ADSI. La visita nos permitió descubrir no solo un edificio de gran valor histórico y arquitectónico, sino también el lugar donde se debaten cuestiones que afectan al presente y al futuro de Cataluña.



Un edificio con mucha historia: el Parlament de Catalunya tiene su sede en el antiguo arsenal de la Ciutadella, un edificio construido en el siglo XVIII como parte de la fortaleza militar levantada después de la Guerra de Sucesión. Con el paso del tiempo, el inmueble tuvo diferentes usos hasta convertirse en la sede del Parlamento.

Su ubicación en el Parc de la Ciutadella y su historia hacen que la visita tenga también una dimensión cultural y patrimonial. Recorrer sus espacios permite acercarse a diferentes etapas de la historia de Barcelona y de Cataluña, desde el pasado del edificio hasta su función actual como sede de la representación política de la ciudadanía.

¿Qué es y qué funciones tiene el Parlament?

El Parlament de Catalunya es la institución que representa al pueblo de Cataluña. Está formado por 135 diputados y diputadas, elegidos democráticamente por la ciudadanía mediante elecciones.

Entre sus principales funciones destacan:

1. Debatir y aprobar las leyes que afectan a Cataluña.
2. Elegir al presidente o presidenta de la Generalitat.
3. Controlar e impulsar la acción del Gobierno de la Generalitat.
4. Debatir los principales asuntos políticos, económicos y sociales.
5. Representar la pluralidad de opiniones e intereses de la sociedad catalana.

Durante la visita, pudimos conocer cómo se organiza esta institución, cómo se desarrolla el trabajo parlamentario y qué papel tienen los diferentes grupos políticos.

Un recorrido por los espacios más emblemáticos: la visita nos permitió acceder a diferentes dependencias del Palau del Parlament y conocer algunos de sus espacios más representativos.

Uno de los lugares más significativos es el hemiciclo, donde se celebran los plenos parlamentarios y los

diputados y diputadas debaten, presentan propuestas y votan las iniciativas legislativas. En este espacio, los socios de ADSI pudimos contemplar la sala, sentarnos en los escaños de los diputados y diputadas del Parlament, así como conocer más de cerca la composición del hemiciclo y su funcionamiento.

A lo largo del recorrido, Sergi nos explicó la historia del edificio, sus características arquitectónicas y el funcionamiento de la actividad parlamentaria. De esta manera, pudimos comprender mejor cómo se toman las decisiones políticas y cómo se organiza el trabajo de los representantes públicos.

Para los socios de ADSI, esta visita también fue una forma de acercarnos a la institución y recordar que las instituciones democráticas forman parte de la vida colectiva. Conocerlas es una manera de comprender nuestros derechos, nuestras responsabilidades y el valor de la participación ciudadana.

Al finalizar la visita, todos los asistentes nos dirigimos a un local cercano, donde se sirvió un cóctel de networking en compañía de los socios, patrocinadores y amigos de ADSI que habían asistido.

Desde ADSI queremos expresar nuestro agradecimiento al Departamento de Presidencia del Parlament de Catalunya y, especialmente, a la Sra. Gemma Brugués, por su gran colaboración, y al Sr. Sergi Terres, por su amable atención durante la visita. Gracias a ambos y a su capacidad de organización, fue posible celebrar esta interesante visita. ■

Joan Figuera
Vocal de ADSI







ADSI presente en EXPOPROTECTION París

ADSI ha visitado la feria EXPOPROTECTION PARIS, el salón internacional de la seguridad, la prevención y la gestión de riesgos que se realiza bienalmente en París, que este año se ha celebrado del 3 al 5 de noviembre en el recinto ferial de Puerta de Versalles-París.

ADSI ha asistido representada por Elvira Márquez y Eduard Zamora, Vicepresidenta y Presidente de ADSI, respectivamente, atendiendo la invitación de la organización de la feria, con la que mantenemos acuerdo de colaboración, con la intención de conocer el importante evento y realizar encuentros personales con diversas de las asociaciones de profesionales de la seguridad del país vecino presentes en el mismo, además de aprovechar para saludar a los patrocinadores de ADSI que allí tenían estand.







Mantuvimos reuniones con estas asociaciones: AGORA des Directeurs de Sécurité; ACSES Association des Chargés de Sécurité des Establissements de Soins, Femmes De La Sécurité y Women4Ciber France.

En las imágenes nuestra visita a los stands de los patrocinadores de ADSI que expusieron en EXPOPROTECTION PARIS: AIRBUS, AXIS COMMUNICATIONS, BY DEMES ESPAÑA, DORLET, FERRIMAX, HIRSCH GROUP y TPLINK VIGI. Coincidimos en la visita a la feria con representantes de nuestro patrocinador LANACCESS. ■











ADSI presente en la Jornada de la Sociedad Clave sobre "La justicia ante la revolución tecnológica"

ADSI ha asistido a la Jornada celebrada en Barcelona sobre "La justicia ante la revolución tecnológica. El futuro de la prueba judicial", que organizada por nuestra entidad amiga y think tank de Detectives Privados, LA SOCIEDAD CLAVE, se ha celebrado en la espectacular Aula Magna de la Universitat Abat Oliba CEU.

Los ponentes expusieron y debatieron sobre como la inteligencia artificial manipula voces, rostros, videos y documentos que parecen realmente auténticos y sobre cómo ello puede afectar a la veracidad de las pruebas judiciales y condicionar la aportación de pruebas y su veracidad en fase de instrucción e influir en los veredictos judiciales.

Agradecemos a La Sociedad Clave su amable invitación a ADSI, que estuvo representada por los integrantes de Junta que se detallan posteriormente.

En las imágenes, vista general de Aula Magna de la UAO-CEO, la mesa de ponentes. En la fotografía de grupo, de izquierda a derecha, Enrique Vilamajó, de La Sociedad Clave; Elvira Márquez y Eduard Zamora, Vicepresidenta y Presidente de ADSI, respectivamente; Francisco Villacampa, Director de Estudios del Grado de Criminología y Seguridad de la UAO-CEO; Joan Figuera, Vocal de ADSI y David Sanmartín, Secretario de ADSI. ■







ADSI en la Diada de la Guàrdia Urbana de Barelona

ADSI ha asistido, representada por diversos integrantes de su Junta Directiva, a la ceremonia de celebración de la Festividad del patrón de la Guardia Urbana de Barcelona, celebrada este martes 17 de noviembre en el Auditorio del Centro Internacional de Convenciones de Barcelona, acto en el que se entregaron 364 reconocimientos, de los cuales 281 medallas y placas valorando acciones meritorias de agentes, instituciones y personas que han contribuido a la labor policial en la ciudad, así como 83 de homenaje a los agentes jubilados recientemente.

El evento fue presidido por el Alcalde de Barcelona, Jaume Collboni, quien destacó la reducción de los delitos en la ciudad en un 11,2%, línea descendente que se mantiene en los últimos 3 años, en los que se ha rebajado en 27.000 delitos respecto al primer semestre de 2023, éxito que atribuyó al trabajo continuado, constante y profundo que desarrolla la Guardia Urbana.

También abogó por mantener el actual modelo de cooperación entre las administraciones, los cuerpos policiales, la judicatura y la fiscalía, para levantar un muro de contención contra el delito en la ciudad.

En las imágenes foto general de la platea del auditorio y las intervenciones de Jaume Collboni, Alcalde de Barcelona; Albert Batlle, Concejal de Prevención, Seguridad, Convivencia y Régimen Interior y Pedro Velázquez, Jefe de la Guardia Urbana.

En una de ellas, de izquierda a derecha, Joan Roda, Vocal de Junta de ADSI, Pedro Velázquez, Intendente Mayor, Jefe de la Guàrdia Urbana de Barcelona, Eduard Zamora, Presidente de ADSI y Joan Vilanova, Intendente Mayor, Subjefe de la Guàrdia Urbana de Barcelona.











ADSI presente en el III Congreso de seguridad en espacios públicos en Barcelona

III CONGRESO DE SEGURIDAD EN ESPACIOS PÚBLICOS

CUADERNOS DE SEGURIDAD

ADSI ha asistido al Congreso celebrado en el salón de actos del Departament d'Interior i Seguretat Pública de la Generalitat de Catalunya, en Barcelona, organizado por Cuadernos de Seguridad y en el cual se debatió sobre la problemática de seguridad en los espacios públicos, así como de las diversas herramientas tecnológicas, sistemas, servicios e iniciativas de seguridad que ayudan a las diferentes administraciones en su objetivo de mejorar la eficiencia en la gestión de sus áreas de responsabilidad relacionadas con la seguridad y la convivencia ciudadana.

Agradecemos a Cuadernos de Seguridad su amable invitación a ADSI, que estuvo representada por los integrantes de su Junta Directiva que se detallan posteriormente.

En las imágenes, vista general del Auditorio, las intervenciones de Iván Rubio, Director de Cuadernos de Seguridad, la de Núria Parlon i Gil, Consejera de Interior y Seguridad Pública de la Generalitat de Catalunya y una de las diversas mesas redondas de la jornada. En la fotografía de grupo, de izquierda a derecha, Joan Roda, Vocal de Junta de ADSI; Iván Rubio, Director de Cuadernos de Seguridad; Eduard Zamora, Presidente de ADSI; Joan Figuera, Vocal de ADSI y Emilio Herrero, Tesorero de ADSI.







ADSI invitada a la 39ª Gala de los Trofeos Internacionales de Seguridad, concedidos por el consejo técnico asesor de seguritecnia

SEGURITECNIA

Se ha celebrado en el salón de actos del Complejo Policial de Canillas, en Madrid, la 39ª edición de la tradicional gala de entrega de los Trofeos Internacionales de la Seguridad, organizada por la revista Seguritecnia, para reconocer el talento, la innovación, la profesionalidad y el compromiso de quienes trabajan cada día para hacer de nuestra sociedad un lugar más seguro.

ADSI recibió invitación al evento del 17 de noviembre, e iba a estar representada por nuestra Vicepresidenta, Elvira Márquez, pero la generalizada suspensión de los trenes por la huelga de personal de RENFE y ADIF ese mismo día provocó la imposibilidad material de realizar el desplazamiento por tren, sin que se pudiese conseguir plaza en ningún vuelo Barcelona-Madrid, que por el caos ferroviario estaban todos al completo.

Habiendo sido materialmente inviable estar presente en la gala, como era nuestro deseo, queremos agradecer expresamente a Seguritecnia su amable invitación y por su importancia, recogemos en nuestra revista la información sobre la gala.

En las imágenes distribuidas por Seguritecnia, diversos momentos del evento, con la mesa presidencial, los premiados, autoridades e integrantes del Consejo Técnico Asesor de Seguritecnia y las intervenciones de Javier Borredá, Director de Seguritecnia y de Ana Borredá, Presidenta del Grupo Borrmart y de la Fundación Borredá.









Miguel Merino Thomas, socio de ADSI, Premio Especial del Jurado de los Trofeos Internacionales de Seguridad de Seguritecnia

El Socio de ADSI, Miguel Merino Thomas, ha sido reconocido con el Trofeo Especial del Jurado en la gala de entrega de los 39º Trofeos Internacionales de la Seguridad, concedidos por el Consejo Técnico Asesor de la revista Seguritecnia, que se ha celebrado en el complejo policial de Canillas en Madrid.

En la imagen el momento de recogida del galardón por parte de su hermano, José María Merino, junto a Piedad Álvarez de Arriba, Directora Global de Seguridad de Telefónica y Presidenta del Consejo Técnico Asesor de Seguritecnia (izquierda) y Ana Borredá, Presidenta del Grupo Borrmart y de la Fundación Borredá.



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.

ADSI participa en el máster universitario en seguridad pública de la UNIR

ADSI mantiene acuerdo de colaboración con la UNIR-UNIVERSIDAD INTERNACIONAL DE LA RIOJA y en base al mismo ha participado hoy en una de las clases del MÁSTER UNIVERSITARIO EN SEGURIDAD PÚBLICA, dependiente de su Facultad de Derecho.

La colaboración en el Máster ha sido en el marco del "SEMINARIO EN SEGURIDAD PUBLICA: DESAFÍOS Y SINGULARIDADES", donde Eduard Zamora, Presidente de ADSI, ha desarrollado la ponencia "LA SEGURIDAD PRIVADA Y SU COLABORACIÓN EN LA SEGURIDAD PÚBLICA", que se ha realizado on line para alumnos del Máster ubicados en España y diversos paises iberoamericanos.

Agradecemos al Dr. Fidel Bedia Castillo, Coordinador Académico del Máster Universitario en Seguridad Pública, de la Facultad de Derecho de la UNIR-UNIVERSIDAD INTERNACIONAL DE LA RIOJA el contar con ADSI para la formación de sus alumnos.

En la imagen la pantalla con el anuncio de la ponencia, en los momentos previos al inicio de la misma.



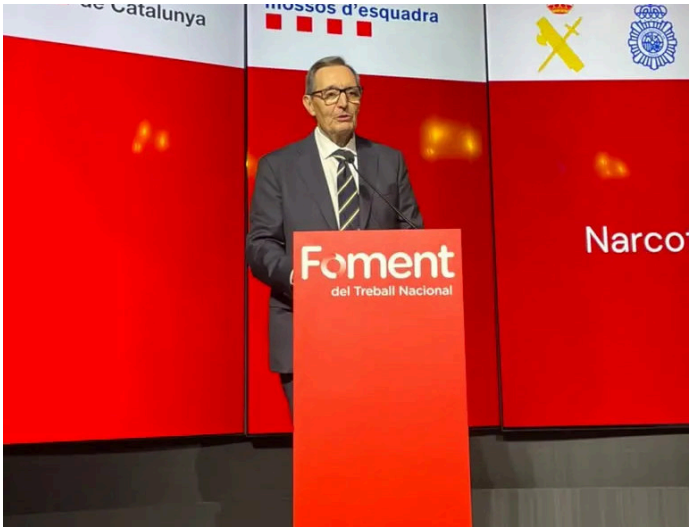
ADSI en la jornada "Narcotráfico, blanqueo de capitales y empresa" organizada por Foment del Treball Nacional

ADSI ha asistido a la jornada, que organizada por la Comisión de Seguridad y Defensa de Foment del Treball Nacional, se celebró en el auditorio de Foment y reunió a representantes institucionales, responsables de los principales cuerpos policiales, miembros de la fiscalía y del sector financiero, para abordar el impacto del narcotráfico y el blanqueo de capitales sobre la seguridad, la economía y la actividad empresarial. La jornada ha puesto sobre la mesa las consecuencias de la criminalidad organizada y los riesgos de la infiltración de capitales procedentes de actividades ilícitas en la economía legal.

ADSI forma parte de la Comisión de Seguridad y Defensa de Foment, representada por nuestro Presidente, Eduard Zamora, que asistió en representación de ADSI al desarrollo de la Jornada, cuya inauguración corrió a cargo de Vicente Codes, Presidente de la Comisión, Josep Sánchez Llibre, Presidente de Foment y Joana Ricardo, Secretaria General del Departament d'Interior i Seguretat Pública de la Generalitat de Catalunya.

En las imágenes diversos momentos de la jornada y en una de ellas, de izquierda a derecha, Eduard Zamora, Presidente de ADSI, Gerardo Cavero, Fiscal Especial Antidroga de Barcelona y Vicente Codes, Presidente de la Comisión de Seguridad y Defensa de Foment.









ADSI en el Talent Fair Event 2026 de ESERP, Business & Law School

ADSI ha participado en la edición 2026 del Talent Fair Event de ESERP Business & Law School, en su sede de Barcelona, el pasado día 19 de Noviembre, evento en el que los alumnos de grado conocen y son conocidos por las diversas empresas que buscan talento para incorporar en sus entidades.

ADSI presentó a los alumnos de doble Grado (Derecho y Criminología) que finalizan sus estudios en posesión de la TIP-Tarjeta de Identificación Profesional que les habilita como Director de Seguridad, y a los de Grado en Criminología, las salidas laborales posibles dentro de las empresas o entidades que disponen de Departamentos de Seguridad o la colaboración de los criminólogos con diversas de las funciones de seguridad en las empresas, tanto consumidoras como prestatarias de seguridad.

ADSI les ofrece también pertenecer a la asociación como adheridos, sin cuota mientras cursen sus estudios de Grado, pudiendo participar de sus numerosas e interesantes actividades y networking con los más notorios profesionales de la seguridad privada, como hace, mediante este tipo de acuerdos, con diversas universidades del país, con el objetivo de incorporar a su proyecto asociativo a los futuros profesionales de la seguridad privada.



En una de las imágenes las intervenciones de ADSI cubierta por Joan Roda, Vocal de ADSI y Elvira Márquez, Vicepresidenta de ADSI.

En otra Elvira Márquez en el aula formativa con el grupo de alumnos, donde impartió una ponencia sobre las funciones del Director de Seguridad a los alumnos interesados.

En la tercera imagen Joan Roda y Oscar Molins, vocales de ADSI y Elvira Marquez, Vicepresidenta de ADSI, presentes en el Stand de ADSI que ha tenido en esta edición 2026 del Talent Fair Event de ESERP Business & Law School.

ADSI agradece a ESERP que, en el marco de nuestro acuerdo de colaboración, nos facilitase la interlocución con sus alumnos de Grado, algunos de los cuales llegarán a ser, sin duda, parte del futuro de los Departamentos de Seguridad. ■





ADSI en el VIII Congreso ADESyD "Compartiendo (visiones de) Seguridad, de la Asociación de Diplomados Españoles en Seguridad y Defensa

ADSI ha asistido a la 8ª edición del congreso de ADESyD, celebrado el 26 de noviembre en el auditorio del Centro Cultural de los Ejércitos de Madrid, que se dividió, como es habitual, en 3 paneles: Seguridad Nacional, Seguridad Internacional y Seguridad Pública y Privada.

ADSI está hermanada con ADESyD y colabora con ella en este congreso anual aportando algunos de los ponentes del panel de Seguridad Pública y Privada, que en esta ocasión ha contado con 3 asociados a ADSI como ponentes: José Márquez, Responsable Global de Seguridad y Resiliencia en Naturgy, Pedro Sebastián, CEO de Enterprise Security Risk Managament y Tomás Gil, Consultor y Director de Seguridad.

Felicitamos a ADESyD por la brillantez de los contenidos y organización, agradeciéndoles la invitación a ADSI para acompañarlos y colaborar en el Congreso.

En las imágenes diversos momentos de la jornada, con vista del auditorio donde se celebró el Congreso y de la mesa de ponentes del Panel de Seguridad Pública y Privada, donde participaron los tres socios de ADSI. En una de ellas, de izquierda a derecha, Eduard Zamora, Presidente de ADSI; Marian Caracuel, Presidenta de ADESyD; Elvira Márquez, Vicepresidenta de ADSI y José Díaz Toribio, Vocal-Tesorero de ADESyD. En otra, de izquierda a derecha, José Márquez, Elvira Márquez, Pedro Sebastián, Tomás Gil y Eduard Zamora.









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!

Webinar

Riesgos Globales 2027



International SOS, invita a los miembros de ADSI y a los profesionales de seguridad corporativa, gestión del riesgo, continuidad de negocio, a participar en el webinar, que tendrá lugar el próximo **2 de diciembre de 2026 a las 11:00 h A.M.**

Durante la sesión, se presentarán las principales conclusiones del informe anual **Perspectivas de Riesgos 2027**, un análisis de los riesgos sanitarios, de seguridad y emergentes que pueden afectar a las organizaciones en un entorno global cada vez más complejo e interconectado. Los expertos de International SOS compartirán su visión sobre la evolución del panorama internacional de riesgos y las implicaciones para las empresas españolas con actividad internacional.

Entre los temas que se abordarán destacan:

- Las principales tendencias y amenazas globales que marcarán 2027.
- La evolución de los riesgos geopolíticos, de seguridad, sanitarios y laborales, y su impacto en las organizaciones.
- El efecto de estos riesgos en la movilidad internacional, los viajeros de negocio y los empleados desplazados.
- Casos prácticos y experiencias reales en la gestión de incidentes y situaciones de crisis.
- Recomendaciones para fortalecer la resiliencia organizativa, la capacidad de respuesta y la continuidad de negocio.
- Un espacio de preguntas y respuestas en directo con los especialistas de International SOS.

Además, todos los asistentes recibirán acceso al informe completo **Perspectivas de Riesgos 2027**, una herramienta de referencia para anticipar amenazas, apoyar la toma de decisiones y reforzar las estrategias de protección de las personas y las operaciones. ■

La asistencia es gratuita previa inscripción

Webinar
Cómo anticiparse a los riesgos y mejorar la capacidad de respuesta ante situaciones críticas



En el sector minero, la preparación y respuesta ante emergencias es clave para proteger a las personas y garantizar la continuidad operativa.

En este webinar abordaremos el **Principio 13 del GISTM**, centrado en la **preparación y respuesta ante posibles fallos en instalaciones de relaves**, y veremos cómo mejorar la comunicación y coordinación durante una situación crítica.

Descubre cómo FACT24 permite activar equipos, distribuir alertas y gestionar escalados para garantizar una respuesta rápida y coordinada cuando cada minuto cuenta.

Fecha: 1 de diciembre de 2026
Hora: 4 pm horario de España
9 am horario de CDMX
12 pm horario de Chile

REGÍSTRATE AQUÍ

¿No puedes asistir al seminario? ¡No hay problema!
Regístrate y recibirás después la grabación.

Control de accesos de alta seguridad: integración, resiliencia y confianza

La protección de instalaciones públicas y privadas exige soluciones capaces de coordinar identidades, autorizaciones y eventos, sin comprometer la continuidad operativa ni la seguridad digital.

De la puerta aislada a una arquitectura de seguridad

La protección de una instalación ya no puede abordarse como una sucesión de puertas con lectores independientes. Edificios institucionales, sedes corporativas, centros de datos, instalaciones industriales y dependencias de organismos públicos comparten un desafío: controlar quién accede, a qué espacios, en qué momento y bajo qué condiciones, manteniendo una visión coherente de toda la organización.

La complejidad aumenta cuando coinciden empleados, contratistas, visitantes y personal temporal, cada uno con atribuciones diferentes. En instalaciones utilizadas por Fuerzas y Cuerpos de Seguridad del Estado, además, pueden coexistir áreas administrativas, operativas y restringidas con exigencias de protección muy distintas. No existe, por tanto, un nivel único de seguridad válido para todos los accesos.

En este contexto, el control de accesos evoluciona desde una función local de apertura hacia una infraestructura de gestión de identidades físicas, políticas de autorización y trazabilidad. Para los responsables de seguridad, esta evolución implica adoptar una visión integral, en la que el control de accesos forma parte de la estrategia global de protección y gestión de riesgos de la organización. El objetivo no es multiplicar barreras, sino aplicar controles proporcionados al riesgo de cada zona, garantizando la seguridad sin comprometer la continuidad operativa.

Credenciales y permisos adaptados al riesgo

Una arquitectura moderna debe admitir diferentes tecnologías de identificación y mecanismos de autenticación. El ecosistema ARMATURA combina controladoras, lectores y una plataforma de gestión con opciones de credenciales encriptadas, acceso móvil mediante BLE y NFC y otras, como biometría que juegan un papel clave cuando se require de multifactor de identificación.

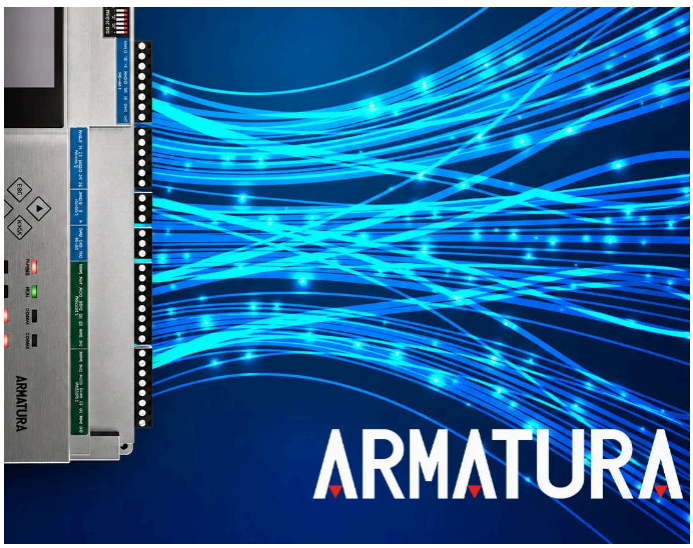
Esta diversidad permite diseñar políticas por perfiles, zonas y franjas horarias. Por ejemplo, el acceso a oficinas generales puede requerir un nivel de verificación distinto del exigido para una sala técnica, un centro de operaciones o un recinto con información sensible. También facilita gestionar altas, bajas y permisos temporales de proveedores sin alterar las autorizaciones del personal permanente.

La seguridad efectiva no depende de escoger siempre la tecnología más compleja. Depende de combinar credenciales, reglas de acceso, procedimientos de operación y supervisión conforme al riesgo real y a las obligaciones aplicables.

Interoperabilidad y gestión centralizada

El control de accesos aporta mayor valor cuando forma parte de una arquitectura coordinada con videovigilancia, detección de intrusión, gestión de visitantes y plataformas de supervisión. En lugar de crear islas tecnológicas, la integración permite correlacionar eventos y ofrecer a los equipos de seguridad una visión más completa de lo que sucede en la instalación.

ARMATURA apuesta por arquitecturas interoperables que faciliten la integración con otros proveedores de subsistemas seguridad y por el uso de interfaces y protocolos seguros como OSDP, AES256 y TLS. Su



plataforma **ARMATURA** One permite centralizar la administración de usuarios, permisos, políticas y eventos de acceso. Para ingenierías e integradores, este enfoque favorece diseños escalables, capaces de incorporar nuevas áreas o funcionalidades sin sustituir necesariamente toda la infraestructura existente. Esta flexibilidad contribuye a proteger la inversión tecnológica y facilita la evolución progresiva de las instalaciones ante nuevas necesidades operativas y de seguridad.

La integración, sin embargo, exige ingeniería: deben comprobarse la compatibilidad entre versiones, el alcance de las interfaces, la protección de las comunicaciones y el comportamiento ante fallos. Una API disponible no equivale, por sí sola, a una integración validada.

Ciberseguridad y continuidad como requisitos de diseño

La convergencia entre seguridad física y digital obliga a evaluar el sistema completo: lectores, controladoras, comunicaciones, software, credenciales, administración y mantenimiento. La integridad de las órdenes de apertura, la protección frente a manipulaciones y la disponibilidad durante incidencias son tan relevantes como la robustez mecánica de una puerta.

ARMATURA dispone de soluciones orientadas a proyectos de alta exigencia, incluidas configuraciones con certificación Grado 4 de accesos conforme a IEC/EN 60839-11-1. Esta referencia debe entenderse respecto de las configuraciones y componentes efectivamente cubiertos por la certificación, no como una propiedad automática de cualquier instalación.



En paralelo, **ARMATURA** cuenta con certificación IEC 62443-4-1:2018, relativa a los procesos de desarrollo Seguro y ciberseguros, además de disponer de certificación en el Esquema Nacional de Seguridad (ENS) que garantiza un elevado cumplimiento de la seguridad de los datos.

En sectores críticos, la resiliencia también requiere definir procedimientos de contingencia, segmentación de redes, gestión de actualizaciones, control de privilegios y respuesta ante incidentes. Para los responsables de seguridad, el verdadero reto consiste en garantizar que estas medidas se integren en una estrategia de protección coherente, capaz de anticipar riesgos, responder ante incidentes y mantener la continuidad de las operaciones. La tecnología es una pieza del modelo de seguridad, no su único componente.

Privacidad y confianza en la identidad física

La trazabilidad de accesos debe coexistir con el respeto a la privacidad y la minimización de datos. Esto cobra especial importancia cuando se estudian modalidades de autenticación avanzadas. El principio de privacidad desde el diseño invita a cuestionar qué información es realmente necesaria, dónde se almacena, quién puede acceder a ella y durante cuánto tiempo debe conservarse.

Existen aproximaciones descentralizadas a la verificación de identidad que buscan reducir la exposición de datos sensibles. En esta línea, tecnologías como BioCode, dentro del ecosistema **ARMATURA**, plantean modelos en los que el usuario mantiene un mayor control sobre su información biométrica, reduciendo la necesidad de almacenamiento centralizado de estos datos. Su posible incorporación a un proyecto debe examinarse desde la seguridad técnica, la proporcionalidad y el marco jurídico aplicable; no basta con presentar una tecnología como innovadora para considerar resuelto el cumplimiento normativo.

El futuro del control de accesos pasa por combinar protección física, ciberseguridad, interoperabilidad y gobernanza de la identidad. Para organizaciones públicas y privadas, la ventaja real reside en disponer de arquitecturas verificables, administrables y preparadas para evolucionar. Con esta visión, **ARMATURA** apuesta por soluciones que van más allá de la identificación y la apertura de puertas, aunando tecnologías avanzadas, protección de alto nivel y capacidad de integración para responder a las exigencias de seguridad actuales y futuras. ■

Barna Dron en seguridad y emergencias



Desde su creación en 2017, Barna Dron, la unidad de drones del Grup Barna Porters, se ha consolidado como servicio de apoyo aéreo a administraciones públicas y clientes privados. Sus equipos intervienen en eventos multitudinarios, dispositivos policiales, emergencias como incendios, y misiones de búsqueda y rescate.

Una unidad para la seguridad pública y privada.

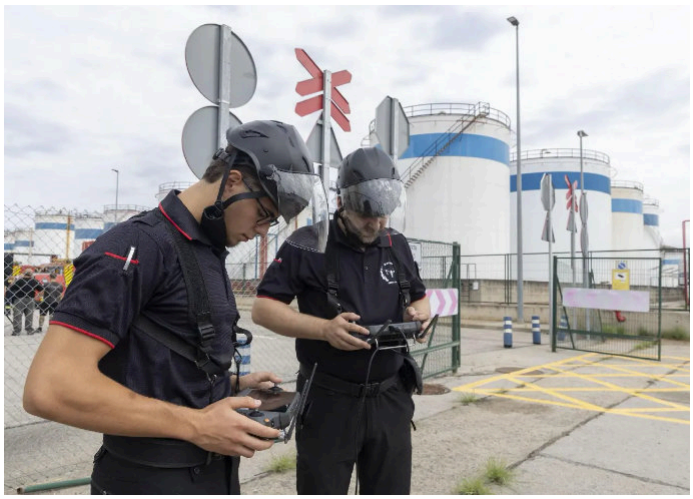
En el ámbito público, la unidad presta servicios a la Guardia Urbana de Barcelona y al Servicio de Protección Civil, Prevención, Extinción de Incendios y Salvamento de Barcelona (SPCPEIS), así como a las policías locales de Sitges, Sant Joan Despi, Vilanova i la Geltrú, Castelldefels, Granollers, Castelló d'Empúries entre otras. Del Sector Público recalcar nuestros servicios para Barcelona de Serveis Municipals, Ferrocarrils de la Generalitat de Catalunya, Jardí Botanic de Barcelona, entre otros.

En el sector privado, Barna Dron cuenta entre sus clientes con el FC Barcelona y el RCD Espanyol, grandes productoras de eventos como Live Nation, grandes inmobiliarias, plantas químicas, entre otros.

La unidad presta servicio en los conciertos en Montjuïc y en grandes citas como Monegros Desert Festival, Primavera Sound, Festas de La Mercè, Revetlla de Sant Joan, Cap d'any, Carnavales de diversas localidades, citas deportivas, emergencias, eventos multitudinarios, todo tipo de dispositivos policiales, etc.

Apoyo a agentes y vigilantes sobre el terreno.

En cada servicio, Barna Dron trabaja en coordinación con quienes actúan a pie. Los agentes de policía y los vigilantes de seguridad tienen una visión directa de su sector. Desde el aire, la unidad puede mostrar al Centro de Control qué ocurre en los alrededores, situar una incidencia respecto a los accesos y dar a los equipos en tierra una referencia clara para la intervención.







Seguridad y asistencia en grandes eventos.

En un partido de fútbol o en un festival, el puesto de mando sigue el desarrollo del evento desde la apertura de puertas hasta la salida del público. Para el control de masas, las cámaras visuales muestran si avanzan las colas, dónde se cruzan los flujos de asistentes y si una aglomeración empieza a bloquear un paso. Al caer la noche, la cámara térmica ayuda a observar la presencia y el movimiento de personas en los sectores menos iluminados.

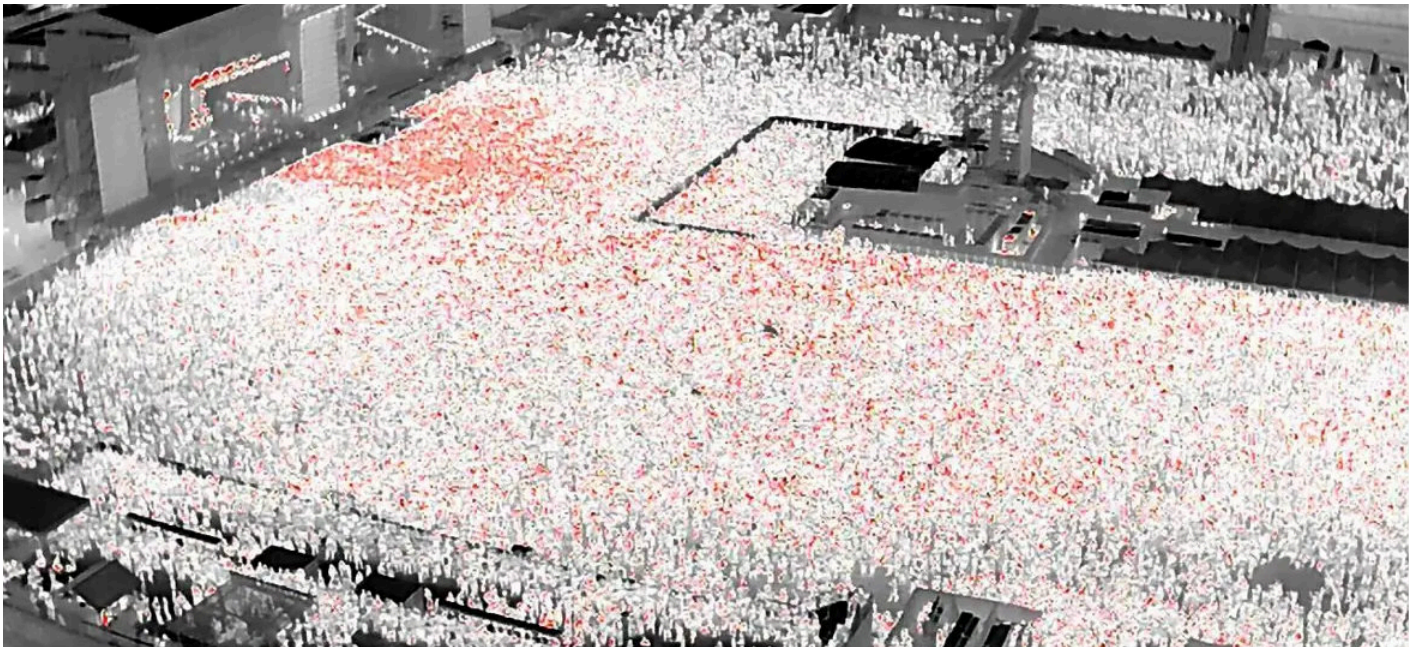
Cuando surge un altercado o emergencia médica se utiliza el zoom de la cámara visual para examinar la zona y localizar el punto de la incidencia. Se comunica a los agentes, vigilantes y sanitarios una referencia que puedan reconocer desde el suelo, como una puerta numerada o un lateral del escenario. Mientras el personal interviene, la vista general permite a Sala seguir la intervención desde el aire.

Manifestaciones y dispositivos complejos.

La unidad se ha empleado con éxito en el dispositivo de huelga general y en manifestaciones de alta complejidad, incluidas situaciones con disturbios. La imagen aérea permite observar cómo se distribuye la concentración, qué sucede en los sectores próximos y dónde requieren apoyo los agentes desplegados. Con poca luz, la térmica ayuda a mantener la referencia sobre agrupaciones y desplazamientos, y la imagen visible aporta contexto sobre lo que está ocurriendo.

Visión térmica en incendios y rescates.

En un incendio, la cámara térmica ayuda a localizar focos de calor y a observar su evolución. Durante las labores de extinción y revisión, la unidad puede mostrar a los equipos de emergencia dónde se mantiene un punto





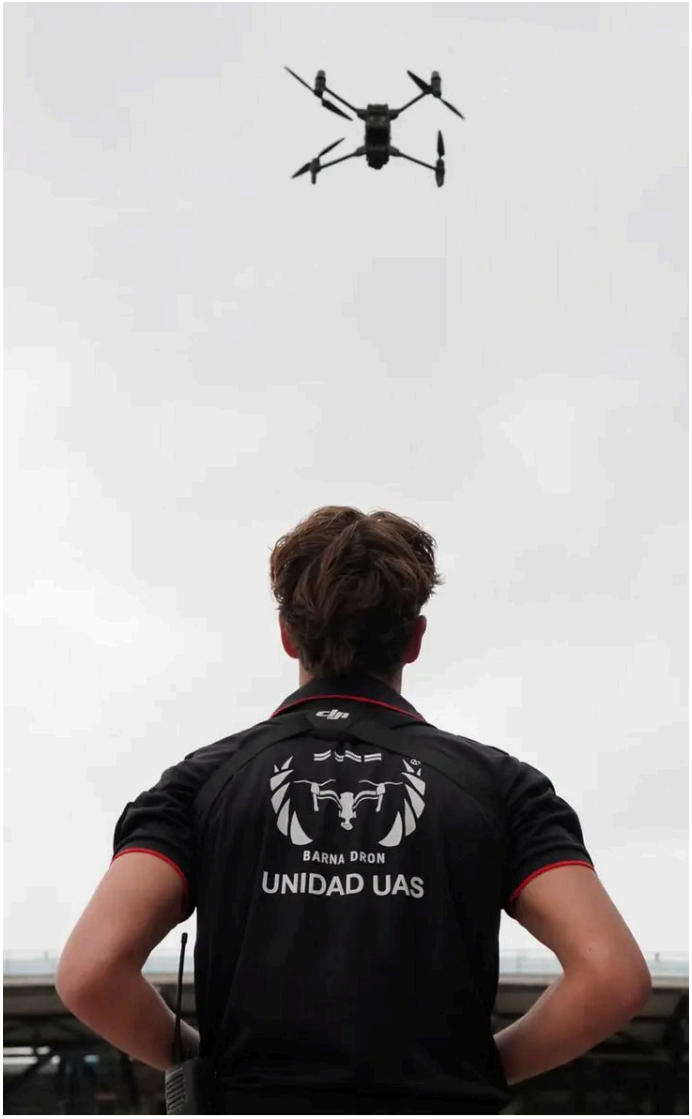
caliente y situarlo respecto al terreno o a la estructura. La imagen visible aporta referencias del entorno para que los mandos puedan tomar las mejores decisiones.

En búsquedas y rescates, el dron permite revisar desde el aire zonas extensas, con poca iluminación o de difícil acceso. La cámara térmica ayuda a localizar contrastes que pueden corresponder a una persona.

Para nuestros clientes conseguimos lo que otros no pueden, llegamos a donde otros no llegan y lo hacemos siempre.

La trayectoria de Barna Dron empresa aérea del Grup Barna Porters, muestra cómo una misma unidad puede integrarse en operativos muy distintos. En un concierto, aporta una vista de los flujos de público. En una manifestación, ayuda a Sala a seguir la evolución del conjunto. En una emergencia, acerca al mando información de sectores que cuesta observar desde el suelo. En todos esos servicios, el valor de la imagen aérea está en que llega a quienes deben decidir o intervenir mientras la situación sigue en marcha.

Tras más de 5.000 vuelos, Barna Dron se ha ganado la confianza de quienes trabajan en la seguridad pública y privada. La unidad cuenta con más de 14 pilotos altamente calificados, diferentes unidades móviles y centros de mando avanzado propios. Disponemos de base de UAS para entrenamiento de nuestros pilotos. Ofrecemos un servicio de emergencia operativo las 24 horas del día, 365 días del año. En caso de ser requeridos, nuestro equipo está operativo en el lugar solicitado en un plazo de entre 30 minutos y 1 hora. ■



COLLBAIX refuerza la seguridad de la nueva Joyería Rabat Zaida en Tarragona con su sistema certificado Securbaix BL

La compañía, especializada en soluciones de acceso y alta seguridad para establecimientos comerciales de lujo a nivel internacional, ha participado en el proyecto de renovación y ampliación de la emblemática boutique RABAT Zaida de Tarragona, incorporando en sus fachadas puertas de seguridad SECURBAIX BL, certificadas con clasificación RC4 según la norma europea EN 1627:2021.

COLLBAIX ha llevado a cabo el proyecto de cerramientos de seguridad de la nueva joyería RABAT Zaida, situada en el número 35 de la Rambla Nova de Tarragona, una de las principales arterias comerciales de la ciudad.

La intervención forma parte de la ambiciosa renovación y ampliación del establecimiento, que prácticamente duplica su superficie comercial, pasando de aproximadamente 200 a 400 metros cuadrados, mediante la incorporación de varios locales anexos situados en la calle Sant Agustí.

Este proyecto supone una transformación integral de la boutique, que apuesta por un concepto arquitectónico más amplio, moderno y exclusivo, en consonancia con la imagen de los establecimientos RABAT en otras ciudades españolas.

En este contexto, COLLBAIX ha aportado su experiencia en el desarrollo e instalación de soluciones de alta seguridad, integrando en las fachadas del establecimiento su sistema **SECURBAIX BL**, especialmente diseñado para proteger espacios comerciales que requieren elevados niveles de resistencia frente a intentos de intrusión.



Securbaix BL: máxima protección con seguridad certificada rc4

Las fachadas de la nueva joyería incorporan puertas enrollables de alta seguridad SECURBAIX BL, desarrolladas por COLLBAIX y certificadas con clasificación de resistencia **RC4 según la norma europea antiefracción EN 1627:2021**.

Esta certificación acredita que el sistema ha superado los ensayos de resistencia correspondientes a su clase, ofreciendo una elevada protección frente a intentos de acceso forzado.

SECURBAIX BL combina una estructura robusta de aluminio extrusionado de doble pared con sistemas de bloqueo de alta seguridad, proporcionando resistencia, fiabilidad y facilidad de utilización.

Su diseño permite integrar elementos de protección avanzada en proyectos arquitectónicos de alto nivel sin renunciar a la estética, un aspecto especialmente importante en boutiques de lujo, joyerías y establecimientos situados en enclaves comerciales emblemáticos.

La instalación en RABAT Tarragona demuestra cómo la tecnología de seguridad puede incorporarse al diseño de una fachada comercial, ofreciendo protección y respetando al mismo tiempo la identidad arquitectónica de la marca.

La seguridad, un elemento estratégico en joyerías y comercios de lujo

La seguridad constituye uno de los principales desafíos para los establecimientos dedicados a la alta joyería, la relojería de prestigio y el comercio de productos de elevado valor.

Estos espacios requieren soluciones capaces de proteger mercancías, instalaciones y activos empresariales frente

a posibles robos, actos vandálicos e intentos de intrusión, especialmente durante las horas de cierre.

En el sector del lujo, la seguridad no puede considerarse un elemento independiente de la arquitectura. Debe formar parte del proyecto desde sus primeras fases, combinando resistencia certificada, funcionalidad, discreción e integración estética.

La incorporación de sistemas antiefracción certificados permite elevar los niveles de protección física de los establecimientos y reforzar otras medidas de seguridad, como los sistemas de alarma, videovigilancia y control de accesos.

Asimismo, contribuye a generar confianza entre clientes, empleados y operadores comerciales, ayudando a garantizar la continuidad de la actividad y la protección del patrimonio.

En este sentido, las puertas de seguridad representan una primera barrera física fundamental dentro de una estrategia de protección integral.

COLLBAIX: especialización en seguridad para el retail de lujo a nivel internacional

COLLBAIX está especializada en el diseño, fabricación e instalación de puertas enrollables, accesos automáticos de cristal y sistemas de alta seguridad para proyectos comerciales, arquitectónicos e institucionales.

La compañía desarrolla soluciones específicas para establecimientos de alta exigencia, como joyerías, boutiques de lujo, relojerías, entidades bancarias, museos, galerías de arte y otros espacios que requieren protección avanzada.

Su especialización combina ingeniería, innovación tecnológica, fabricación a medida y conocimiento de las normativas europeas de seguridad.

Gracias a su experiencia y a una red de distribuidores y colaboradores especializados, **COLLBAIX desarrolla su actividad tanto en el mercado nacional como internacional**, ofreciendo soluciones adaptadas a las necesidades de cada proyecto y a las exigencias de grandes marcas y operadores del sector retail.

La compañía dispone de una gama de productos con diferentes clasificaciones de resistencia antiefracción, incluyendo soluciones certificadas desde RC3 hasta RC6, así como sistemas de protección balística para aplicaciones específicas.

Esta capacidad técnica permite abordar proyectos de distinta complejidad, en los que la seguridad, la calidad de los materiales, la fiabilidad y la integración arquitectónica resultan determinantes.

Un proyecto que une arquitectura, lujo y protección

La renovación de RABAT Zaida representa una nueva etapa para una joyería histórica de Tarragona, con una trayectoria que se remonta a 1965.

Con esta intervención, COLLBAIX reafirma su posicionamiento como especialista en soluciones de alta seguridad para establecimientos comerciales premium, aportando tecnología certificada y experiencia a proyectos arquitectónicos de referencia.

La instalación de SECURBAIX BL en la nueva boutique RABAT Tarragona refleja el compromiso de COLLBAIX con la innovación, la seguridad y la excelencia, consolidando su especialización en la protección de espacios comerciales de lujo a nivel internacional. ■



De la academia al operativo: la colaboración entre empresas y centros de formación

Por David Reina Cherino, Gestor en EULEN Seguridad y docente acreditado en Seguridad Privada

El sector de la seguridad privada atraviesa un momento de transformación profunda. A la creciente sofisticación tecnológica de los servicios y la mayor exigencia normativa se suma uno de los principales retos operativos para cualquier director de seguridad o responsable de operaciones: la captación, cualificación y fidelización de vigilantes de seguridad habilitados.

Hoy en día, contar con profesionales debidamente acreditados no basta si no existe una alineación real entre lo que se enseña en las aulas y lo que demandan los entornos operativos actuales como grandes superficies comerciales, complejos corporativos, centros hospitalarios o infraestructuras críticas. En este contexto, la colaboración estrecha entre las empresas de seguridad y las academias de formación homologadas se consolida como un modelo de éxito imprescindible para elevar los estándares del sector.

Más allá de la habilitación tradicional: Certificados de Profesionalidad y Grado Medio

En EULEN Seguridad llevamos tiempo trabajando codo con codo con centros de formación homologados en el desarrollo de los Certificados de Profesionalidad de Vigilancia, Seguridad Privada y Protección de Personas, aportando visión de campo y facilitando una pasarela directa hacia el empleo estable.





Sin embargo, el compromiso con la profesionalización del sector exige dar un paso más. Por ello, este mismo mes de noviembre marcamos un nuevo hito acogiendo por primera vez en nuestros operativos a alumnos del ciclo formativo de Grado Medio en Seguridad. Esta incorporación supone un avance cualitativo clave para atraer talento joven y construir cantera con una base técnica, jurídica y operativa mucho más amplia y estructurada desde el inicio de su carrera.

Cerrando la brecha entre la teoría y la realidad del Servicio

Tradicionalmente, la formación para la obtención de la Tarjeta de Identidad Profesional (TIP) y la operativa diaria de las empresas han caminado en paralelo. Sin embargo, cuando los profesionales que gestionan grandes cuentas y servicios operativos participan activamente en el ecosistema formativo, se genera un círculo virtuoso con beneficios inmediatos:

- **Formación orientada a la operativa real:** Más allá de superar las pruebas oficiales, los futuros vigilantes comprenden desde el aula cómo aplicar el marco jurídico-penal en situaciones reales (control de accesos, actuación ante hurtos, tratamiento de menores o coordinación con las Fuerzas y Cuerpos de Seguridad), reduciendo la curva de aprendizaje al incorporarse a su primer destino.
- **Anticipación a las necesidades del cliente:** Permite detectar de forma temprana perfiles con competencias específicas –trato al cliente, gestión de conflictos en entornos de alta afluencia o manejo de sistemas tecnológicos– antes incluso de que finalicen su proceso de habilitación.

• **Reducción de la rotación y mayor compromiso:** Cuando el alumno percibe un vínculo directo entre su centro de formación y una compañía líder con proyectos estables, su implicación durante el curso aumenta y su aterrizaje en el servicio resulta mucho más sólido.

Un impacto directo en la calidad percibida por el cliente

Desde la perspectiva de la gestión de cuentas y servicios integrales, este modelo de colaboración trasciende el ámbito de los recursos humanos para convertirse en una herramienta estratégica de calidad. Para el director de seguridad de la empresa cliente, supone la tranquilidad de incorporar profesionales que no solo cumplen con los requisitos legales, sino que entienden la cultura preventiva, los protocolos de actuación y la importancia de representar correctamente la imagen de la instalación.

En EULEN Seguridad, apostamos por tender puentes constantes entre el entorno formativo y la realidad operativa de nuestros clientes. Impulsar esta sinergia entre academias, docentes con experiencia de campo y gestión operativa no solo dignifica la profesión del vigilante de seguridad, sino que garantiza servicios más eficientes, estables y preparados para los desafíos actuales de la seguridad integral. ■





ILUNION Seguridad lanza ILUNION Tech Security, su nueva marca especializada en seguridad tecnológica



Pepa Alonso, Directora de ILUNION Tech Security

La compañía, anteriormente Ingloba Seguridad, se integra bajo el paraguas de ILUNION Seguridad y responde a los nuevos retos del sector con una propuesta híbrida, innovadora y centrada en las personas.

ILUNION Seguridad, tercera empresa del sector de la seguridad privada en España, da un nuevo paso en su estrategia de crecimiento y especialización con el lanzamiento de **ILUNION Tech Security**, la nueva denominación de la compañía que hasta ahora operaba como **Ingloba Seguridad** y que pasa a integrarse bajo esta marca en la propuesta global de seguridad de ILUNION Facility Services.

Este cambio supone la evolución natural del proceso iniciado tras la adquisición de Ingloba Seguridad por parte de ILUNION, una operación estratégica que reforzó la posición de la compañía en el sector de la seguridad privada y permitió ampliar sus capacidades tecnológicas, especialmente en el ámbito de los sistemas de seguridad, la vigilancia avanzada y la protección de infraestructuras críticas.

Con **ILUNION Tech Security**, ILUNION Seguridad consolida una propuesta diferencial basada en un modelo de **seguridad híbrida**, en el que la experiencia de los profesionales y el valor de la tecnología trabajan de forma complementaria para ofrecer soluciones más inteligentes, preventivas y adaptadas a las necesidades actuales de empresas, administraciones públicas y organizaciones.

"El nacimiento de ILUNION Tech Security representa mucho más que un cambio de nombre. Es la evolución de un proyecto que une la experiencia humana de ILUNION Seguridad con el conocimiento tecnológico de Ingloba para dar respuesta a los nuevos retos del sector. Nuestro propósito sigue siendo el mismo: proteger lo que realmente importa, incorporando nuevas capacidades para ofrecer una seguridad más avanzada, cercana y eficaz", señala la directora nacional de ILUNION Seguridad, Pepa Alonso de Castañeda.

Una marca para responder a los nuevos retos de la seguridad

Durante los últimos años, el sector de la seguridad ha experimentado una profunda transformación. Los riesgos son cada vez más complejos, los entornos más conectados y las necesidades de protección requieren respuestas más ágiles, precisas y tecnológicas.

Por esa razón, nace **ILUNION Tech Security**, para reforzar el posicionamiento de ILUNION Seguridad en el ámbito de los **sistemas de seguridad inteligente**, mediante soluciones capaces de prevenir, anticipar y proteger de manera más eficiente.

La nueva marca combina la trayectoria de ILUNION Seguridad, basada en la confianza, la orientación al cliente y el compromiso con las personas, con la especialización técnica de Ingloba en integración tecnológica, sistemas avanzados de seguridad y servicios dirigidos a administraciones públicas, empresas e infraestructuras críticas.

Tecnología al servicio de las personas

ILUNION Tech Security desarrollará soluciones de seguridad tecnológica bajo el paraguas de ILUNION Seguridad, con una propuesta centrada en la prevención, la monitorización y la integración de sistemas.

Su actividad permitirá reforzar servicios vinculados a la videovigilancia, la protección de instalaciones, el control de accesos, la gestión remota, la seguridad electrónica y otras soluciones tecnológicas avanzadas, siempre con el

objetivo de ofrecer una protección más eficiente y adaptada a cada cliente.

"En esta nueva etapa queremos reforzar nuestra capacidad para acompañar a los clientes con soluciones tecnológicas cada vez más integradas, eficientes y adaptadas a sus necesidades. ILUNION Tech Security nos permite sumar conocimiento técnico, innovación y experiencia en sistemas de seguridad, PCI y consultoría para ofrecer una respuesta más completa ante entornos cada vez más exigentes", afirma el gerente nacional de Sistemas de Seguridad, PCI y Consultoría, Juan José García.

En línea con la estrategia de ILUNION, la nueva marca mantiene intacta la esencia del proyecto: situar la tecnología al servicio de las personas y avanzar hacia un modelo de seguridad más innovador, inclusivo y centrado en las necesidades reales de los clientes.

Una evolución con vocación de liderazgo

La creación de ILUNION Tech Security refuerza la apuesta de ILUNION Facility Services por el crecimiento, la especialización y la innovación en sus líneas de actividad. Además, permite consolidar una oferta más completa dentro de ILUNION Seguridad, que presta soluciones orientadas a proteger personas, instalaciones, activos y entornos corporativos mediante un modelo que combina experiencia profesional, innovación tecnológica y compromiso social.

La anterior Ingloba Seguridad aporta a esta nueva etapa una sólida experiencia técnica, una reconocida capacidad de integración tecnológica y un profundo conocimiento del sector, tanto a nivel nacional como internacional. Todo ello se suma a la trayectoria de ILUNION Seguridad, que avanza en su objetivo de ser un referente en la prestación de servicios de seguridad privada, en línea con el propósito de construir un mundo mejor con todos incluidos.

Con el lanzamiento de **ILUNION Tech Security**, la compañía consolida una nueva etapa en la que innovación, tecnología y talento se unen para seguir construyendo la seguridad del futuro. ■

ILUNION
Tech Security

Seguridad 2027: integrar capacidades, construir confianza

Llevamos 30 años protegiendo aeropuertos, puertos, infraestructuras críticas, edificios públicos y espacios de alto valor patrimonial, y de esa experiencia hemos sacado una convicción en Target Tecnología: la seguridad no se mide por la tecnología que se instala, sino por la confianza que genera cuando de verdad hace falta.

El cierre de 2026, con la cena institucional y la entrega de premios ADSI, es un buen momento para compartir lo aprendido y mirar a 2027. Las amenazas se diversifican, los riesgos digitales crecen y la frontera entre seguridad física y ciberseguridad es cada vez más difusa. Es un escenario exigente, pero también lleno de oportunidades para quienes estén dispuestos a revisar cómo se concibe, se diseña, se implanta y se gestiona la seguridad.

30 años de experiencia: lo que hemos aprendido

Tres décadas trabajando en entornos donde un fallo no es una opción nos han enseñado que los sistemas rara vez fallan por falta de tecnología. Fallan por falta de integración, de adaptación a la realidad del cliente o de continuidad en el tiempo.

Integrar, conocer al cliente y acompañarlo a largo plazo, junto con el papel de las personas, son el hilo de esta reflexión de cara a 2027.

Integrar para proteger mejor

Todavía hay organizaciones con excelentes sistemas de seguridad que funcionan cada uno por su cuenta, y eso limita todo lo que podrían aportar.

La videovigilancia y la analítica inteligente, el control de accesos, la detección, las plataformas de gestión y la ciberseguridad funcionan mejor dentro de una única arquitectura, que incluya también a las personas, los procedimientos y los protocolos de actuación.

Integrar no es conectar dispositivos. Es dar sentido operativo a la información que generan, relacionar acontecimientos y ofrecer al profesional una visión completa para decidir bien. Por eso la interoperabilidad es un criterio estratégico desde el diseño del proyecto: mejora la eficiencia, evita duplicidades y protege tanto los sistemas como la información que manejan.

La inteligencia artificial multiplica estas posibilidades en la detección de anomalías, la priorización de alertas o el análisis de información. Su valor llega cuando siempre hay una persona que supervisa y unos criterios claros de fiabilidad.

Del suministro tecnológico al compromiso con el cliente

Cada organización tiene sus propios riesgos y necesidades. Lo que funciona en un aeropuerto puede no servir en una instalación industrial, un edificio corporativo o un espacio de pública concurrencia.

Por eso, nuestra experiencia nos lleva a empezar siempre por el cliente y no por el catálogo: escuchar, analizar vulnerabilidades, entender sus procedimientos y dimensionar la solución adecuada. Eso exige experiencia, especialización y criterio profesional.





El valor diferencial de una empresa de seguridad está en el asesoramiento, la ingeniería, la integración y el acompañamiento a largo plazo; es decir, en ser un socio de confianza y no solo un proveedor.

No se trata de poner más tecnología, sino la tecnología adecuada y conseguir que responda cuando se la necesita.

Las personas, protagonistas de la transformación

Ningún avance tecnológico compensa las carencias de formación o de conocimiento operativo. Un sector de tanta importancia como la Seguridad exige actualizar las competencias de operadores, vigilantes, técnicos, ingenieros y directores de seguridad.

La formación va más allá del manejo de los equipos: enseña a interpretar la información, gestionar incidencias y decidir en situaciones críticas. Para ello ganan protagonismo los ejercicios prácticos, la simulación de escenarios y la revisión periódica de los procedimientos.

El sector también necesita atraer y retener talento, ofrecer carrera profesional y reconocer la responsabilidad de quienes trabajan en seguridad.

La seguridad no termina con la instalación

Con frecuencia la atención se concentra en el diseño, la compra y la puesta en marcha. Pero la eficacia de un sistema se demuestra a lo largo de los años, y así lo hemos comprobado desde Target Tecnología, en tres décadas de proyectos.

Es por ello que consideramos que el servicio de postventa ocupa un lugar central: el mantenimiento predictivo se anticipa a las incidencias, analizando el comportamiento de los equipos. el preventivo reduce la probabilidad de fallos y el correctivo recupera la funcionalidad tras una avería.

A ello se suman la monitorización del estado de los sistemas, las actualizaciones tecnológicas y de ciberseguridad, la asistencia técnica especializada, la formación continua de los usuarios y la revisión periódica de las soluciones, porque los riesgos evolucionan y las empresas también deben hacerlo.

Garantizar la disponibilidad, minimizar las interrupciones y proteger la inversión exige planificación y compromiso.



La continuidad del servicio forma parte de la calidad desde el momento en que se concibe un proyecto.

Un futuro que construimos entre todos

Ninguna empresa, tecnología o institución puede responder sola a los desafíos actuales. La colaboración entre la seguridad pública y la privada, respetando cada ámbito competencial, sigue creciendo a través de la coordinación, el intercambio de información y la confianza mutua.

En ese camino, asociaciones como ADSI son fundamentales: gracias a la aportación de sus socios, presidentes y juntas directivas, representan el valor del asociacionismo como espacio de encuentro, representación profesional, interlocución institucional, formación y difusión de buenas prácticas.

De cara a 2027, en Target Tecnología queremos seguir avanzando, con la experiencia de 30 años, hacia una seguridad más integrada, especializada y colaborativa, que convierta la innovación en capacidades operativas reales.

El progreso del sector se mide no solo por la sofisticación de sus sistemas, sino por la confianza que genera, la preparación de sus profesionales y la protección efectiva que proporciona.

Porque el verdadero avance de la seguridad se mide por lo que somos capaces de proteger: las personas, que son lo más importante. ■





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:

aesYc & Observatorio SEGURIDAD INTEGRAL CENTROS HOSPITALARIOS

ADSI asociación de directivos de seguridad integral

udima UNIVERSIDAD A DISTANCIA DE MADRID

DIRECCIÓN Y GESTIÓN DE LA SEGURIDAD EN ENTORNOS HOSPITALARIOS

Formación universitaria especializada para directivos, gerentes y responsables de seguridad, orientada a la gestión estratégica del riesgo, la protección integral y la resiliencia hospitalaria.

Condiciones económicas exclusivas para **socios** y **Patrocinadores** de ADSI

15% Descuento

LIDERANDO LA SEGURIDAD Y LA RESILIENCIA EN LOS ENTORNOS SANITARIOS

La Alianza Española de Seguridad y Crisis (aesYc), en colaboración con el Observatorio de Seguridad Integral en Centros Hospitalarios (OSICH), impulsa este programa universitario especializado para fortalecer la cultura de seguridad, la gestión estratégica del riesgo y la capacidad de respuesta de las organizaciones sanitarias, contribuyendo a garantizar la continuidad asistencial.

CARACTERÍSTICAS DEL PROGRAMA

Modalidad: Formación online síncrona (presencial virtual), con interacción directa entre alumnos y docentes.

Duración: Más de 80 horas lectivas, complementadas con clases magistrales y horas de estudio y trabajo individual.
Créditos universitarios: 20 créditos universitarios.

Destinatarios: Directivos, gerentes, responsables de seguridad y profesionales del sector sanitario.

Metodología:
Enfoque estratégico, integral y multidisciplinar.
Análisis de casos reales y experiencias profesionales.
Tres webinarios con especialistas del sector.
Dos conferencias magistrales.

Evaluación:
Ejercicios de evaluación tipo test.
Trabajo de fin de curso.

Titulación:
Diploma acreditativo de aesYc y OSICH.
Diploma universitario.
Inicio del programa: **15 de enero de 2027**.

Precio del programa: 1.580 €.

Descuentos y condiciones especiales:
- 15 % de descuento para miembros de las organizaciones
- patrocinadoras y sus referenciados, mediante pago único.
- 10 % de descuento por matrícula anticipada antes del 20 de
- diciembre de 2026, mediante pago único.
- 5 % de descuento por matrícula anticipada antes del 20 de
- diciembre de 2026, mediante pago fraccionado.
- 50 % de descuento para personas en situación de desempleo,
- limitado a dos plazas asignadas por orden de solicitud.

Los descuentos no son acumulables entre sí. Posibilidad de bonificación a través de FUNDAE.

PROGRAMA ACADÉMICO

Módulo I. Marco legal, normativo y cultura de seguridad en entornos hospitalarios.
Legislación aplicable, normativa internacional, prevención de riesgos laborales, bioseguridad y cultura de seguridad.

Módulo II. Seguridad del paciente y del profesional sanitario.
Protección de pacientes y profesionales, prevención de la violencia ocupacional, seguridad perimetral y control de accesos.

Módulo III. Seguridad física, emergencias y planes de autoprotección.
Planes de seguridad integral, gestión de emergencias, evacuación de pacientes, autoprotección y coordinación operativa.

Módulo IV. Ciberseguridad, continuidad de negocio y sistemas de gestión.
Gestión del riesgo tecnológico, protección de datos sensibles, ciberseguridad y continuidad de la actividad asistencial.

Módulo V. Dirección de seguridad y habilidades directivas.
Dirección estratégica, gestión de proyectos, liderazgo, comunicación en situaciones de crisis, inteligencia artificial e innovación tecnológica.

Actividades formativas complementarias:
- Tres webinarios sectoriales con profesionales especializados.
- Dos conferencias magistrales.
- Ejercicios de evaluación y trabajo de fin de curso.

Objetivos del programa:
- Fortalecer la cultura de seguridad hospitalaria.
- Optimizar la prevención y la gestión integral de riesgos.
- Mejorar la protección de pacientes, profesionales e
- instalaciones.
- Potenciar las competencias directivas y la toma de decisiones.
- Reforzar la capacidad de respuesta ante situaciones de crisis.
- Impulsar la resiliencia organizativa y la continuidad asistencial.

INTERESADOS CONTACTAR CON: coordinacion@aesyc.com



- 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

LISA Institute

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

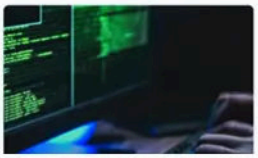
Programa formativo en ciberseguridad de Policía Nacional y Universidad de Salamanca

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



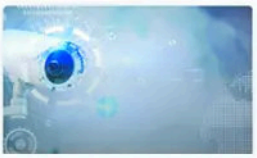
Curso de Seguridad en Infraestructuras Críticas (DSICE)



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 Seguritecnia
Nº 522 Nov/Dic 2026
Enlace

AES
ASOCIACIÓN ESPAÑOLA EMPRESAS DE SEGURIDAD

La Guía de Seguridad en Eventos de Masas y los documentos de anexos a la misma ha sido elaborada por el Area de Seguridad Electrónica de AES-Asociación Española de Empresas de Seguridad y el Observatorio SEET de AES FUNDACIÓN.

Guia de Seguridad en Eventos de Masas



Enlace

Anexos de la Guía de Seguridad en Eventos de Masas



Enlace



Vulnerabilidades, retos y soluciones para la seguridad y protección de las infraestructuras críticas en España desde la perspectiva de NIS2 y CER.

Enlace



Innovación Tecnológica e Inteligencia en Seguridad Integral e Integrada. Un nuevo modelo de cooperación público-privada para la protección y resiliencia de las infraestructuras críticas y esenciales

Enlace

CCN-CERT centro criptológico nacional
CCN centro criptológico nacional

Hoja de ruta de la transición a criptografía postcuántica en España.

Enlace

Medios de protección y armamento



Autor: Antonio Gómez Montolío

Este libro desarrolla la Unidad Formativa Medios de protección y armamento (UF2675), integrada en los Módulos Formativos MF0080_2 Vigilancia y protección en Seguridad Privada y MF0081_2 Protección de personas. Estos módulos están asociados a las Unidades de Competencia UC0080_2 y UC0081_2, pertenecientes a la Cualificación Profesional de referencia SEA029_2 Vigilancia y seguridad privada (RD 295/2004). Asimismo, se encuentra incluida en los Certificados Profesionales SEAD0112 Vigilancia, seguridad privada y protección de personas y SEAD0212 Vigilancia, seguridad privada y protección de explosivos, ambos regulados por el Real Decreto 548/2014, de 27 de junio.

Ofrece una completa visión de diversos aspectos de gran importancia para la seguridad: desde sistemas electrónicos, barreras físicas y protección contra incendios, hasta el control de accesos. Asimismo, incluye la descripción del armamento habitual para la vigilancia armada y aborda los diferentes aspectos de la preparación física. Todo ello redactado con un tono formal y accesible, acompañado de numerosas imágenes e ilustraciones que facilitan la comprensión de la materia.

SOBRE EL AUTOR

El autor, Antonio Gómez Montolío, es director de seguridad habilitado por el Ministerio de Interior, titulado como director de seguridad por la Universidad Internacional de Catalunya, diplomado en Curso Superior de Seguridad Integral en la Empresa por la UPC, técnico especialista en Electrónica Industrial y licenciado en ADE Tech por la URL de la Salle. Ha dirigido diversas empresas de seguridad y participado en múltiples proyectos, tanto civiles como militares, en distintos países. Ha recibido diversos premios y reconocimientos nacionales e internacionales. Asimismo, es socio fundador de ADSI (Asociación de Directivos de Seguridad Integral), socio de ADISPO (Asociación de Directores de Seguridad Privada Online), socio de AEINSE (Asociación Española de Ingenieros de Seguridad). Además, es autor de otros libros de formación publicados por esta misma editorial.



ADSI

30 anos

CONECTANDO E IMPULSANDO