



Entrevista socio

Carlos Juanes

*Calendario
de eventos
ADSI*

"Martes con ..."

Google Málaga
Abertis Autopistas España
Banco Santander

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

En este número ...

3

PATROCINADORES ADSI

4

CONDOLENCIAS POR LA DANA

5

CARTA DEL PRESIDENTE

7

AGENDA DE EVENTOS

8

ARTÍCULO DE OPINIÓN

Protección personal de ejecutivos y personas

11

ENTREVISTA A UN SOCIO

14

ARTÍCULO DE OPINIÓN

La protección de datos y la seguridad corporativa

16

ARTÍCULO DE OPINIÓN

Por qué occidente no cree en la guerra

19

NOTICIAS ADSI

"Martes con..." Google Málaga

"Martes con..." Abertis Autopistas España

"Martes con..." Banco Santander

4ª Reunión del Foro Integral de Cultura de Seguridad Nacional

ADSI en la Diada de Guardia Urbana BCN

ADSI en el 25 Aniversario de la ACEDE

ADSI en la 10ª Edición del Día de la Seguridad Privada del Departament d'Interior i Seguretat Pública - Generalitat de Catalunya

ADSI en el acto de Graduación del Grado en Seguridad del ISPC y la UB- Universitat de Barcelona

ADSI organiza con TAPA la Jornada de Seguridad en la Cadena de Suministros

Security Forum 2025, con el foco puesto en la Seguridad 360

Actualización de datos

33

NUESTROS PATROCINADORES

RIBA-VIDAL

COLLBAIX

ILOQ

FERRIMAX

43

FORMACIÓN

46

REVISTAS Y ENLACES DE INTERÉS

47

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 Vía 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.



 <p>accesor Soluciones en control de accesos y seguridad</p>	 <p>AXIS COMMUNICATIONS</p>	 <p>Grup Barna Porters</p>	 <p>demes GROUP</p>
 <p>chillida</p>	 <p>COLBAIX access solutions</p>	 <p>Ecommunicator SMART SAFETY</p>	 <p>EULEN SEGURIDAD</p>
 <p>F24</p>	 <p>FERRIMAX ADVANCED SECURITY SOLUTIONS</p>	 <p>FREEMATICA Business technologies</p>	 <p>PUERTAS CORTAFUEGOS PUERTAS GISMERO PUERTAS ACÚSTICAS</p>
 <p>Honeywell THE POWER OF CONNECTED</p>	 <p>iLOQ Life made limitless.</p>	 <p>ILUNION Seguridad</p>	 <p>IMAN SEGURIDAD</p>
 <p>indra</p>	 <p>INTERNATIONAL SOS</p>	 <p>Iron Lock Sistemas</p>	 <p>LANACCESS Discover the power of video.</p>
 <p>metropolis UNA MARCA DE GROUPE ARMONIA</p>	 <p>ONSECUR Expertos en Alta Seguridad</p>	 <p>PETROSECUR SECURITY & DEFENSE</p>	 <p>PHOENIX VIGILANCIA Y SEGURIDAD S.A.</p>
 <p>PROSEGUR SECURITY</p>	 <p>PYCSECA seguridad</p>	 <p>RIBA-VIDAL ABOGADOS</p>	 <p>Sabadell Professional</p>
 <p>SABICO group</p>	 <p>SCATI</p>	 <p>SORHEA</p>	 <p>TARGET TECNOLOGIA</p>
 <p>Trablisa SERVICIOS DE SEGURIDAD</p>			





En estos momentos de desolación en las zonas afectadas, la JUNTA DIRECTIVA de ADSI traslada su más sincera condolencia a las familias de los fallecidos y nuestra profunda solidaridad y cercanía, tanto a ellas como a todos los afectados, por esta terrible y catastrófica DANA que ha asolado tantas poblaciones y lugares de nuestro país de forma especialmente intensa en la Comunidad Valenciana, Andalucía Oriental, Murcia y Este de Castilla la Mancha.

Nos unimos a todos ellos en su dolor y transmitimos nuestros ánimos más sinceros, como seguro hace toda la sociedad del país.

Gracias a todos los efectivos de los Cuerpos de Seguridad Pública, la UME, Bomberos, Protección Civil, Cruz Roja, Seguridad Privada y un largo etcétera, por la labor encomiable que estáis realizando, tan importante en estos momentos tan traumáticos para las zonas afectadas.



Lecciones de una catástrofe: “el uno por el otro..... las víctimas perjudicadas”

Habiendo esperado unos días para no opinar “en caliente” sobre las actuaciones de todas las instancias con responsabilidad en la prevención y minimización de impactos derivados de la catástrofe provocada por la dana en levante la pasada semana, no he cambiado mucho mi opinión pese a dicha espera. Una opinión influenciada por estos aspectos:

- No conozco en la profundidad suficiente todo el complejo ordenamiento aplicable en estas situaciones y las limitaciones de unas administraciones entretanto otras no autoricen-soliciten-declaren ciertas situaciones legales de emergencia.
- Focalizada a la prevención y protección, en primer lugar, de las personas, en este caso las víctimas (las personas siempre lo primero y por encima de todo tipo de intereses económicos o guerras políticas partidistas.
- Influenciada por mi desviación profesional, de más de 40 años dedicado a la seguridad, que me lleva a pensar siempre en modo prevención y protección de los intereses para los que trabajamos: la sociedad en general si tenemos responsabilidad profesional en la administración, o la entidad privada para la que desarrollamos nuestra tarea como Directivos/Directores de Seguridad, cuando hablamos de nuestra función específica a cargo de un Departamento de Seguridad.

Situaciones extremas como la que vivimos estos días no sólo sacan lo peor del ser humano (los vándalos que saquean impunemente establecimientos sin que se trate en absoluto de productos de primera necesidad, como vemos estos días), sino también lo mejor de las personas (solidaridad extrema de la sociedad en general), pero me centraré en algo que ocupa la mayoría de comentarios respecto a las administraciones, a todas las implicadas: la dilación en activar las alertas iniciales, el motivo por el

cual no se decreta el nivel 3 de emergencia nacional, que permita la intervención coordinada de todos los medios a disposición del país.

Leemos en todo tipo de medios de comunicación afirmaciones y declaraciones contradictorias, según las ideologías de estos: que si corresponde a la Comunidad Autónoma, que si pudiera declararla el Gobierno Central, que si de facto ya estaría declarada con la intervención de la UME-Unidad Militar de Emergencia, etc., etc.

En definitiva.... “El uno por el otro, la casa sin barrer” y las víctimas perjudicadas.

No puedo dejar al margen a los Directivos con responsabilidad en seguridad y protección (seguridad corporativa, seguridad laboral, continuidad de negocio y comunicación interna, todos ellos afectados por estas dudas:

- ¿Qué medios de información utilizan para conocer la llegada de situaciones de emergencia de este tipo?
- ¿Cómo se coordinan internamente para mejorar efectividad de las acciones preventivas y reactivas precisas?
- ¿Se han aplicado las mismas de manera correcta en esta ocasión?
- ¿Cómo se han hecho llegar a sus plantillas las instrucciones precisas?
- Etc., etc.



Excesivas dudas sobre las actuaciones de todos los implicados, públicos y privados, en esta gravísima y extraordinaria incidencia, pero tiempo habrá para tratarlos en detalle y mejorar los procedimientos preventivos, decisorios y comunicativos necesarios, pues seguro se entrará en próximos y múltiples debates en profundidad sobre todo ello.

Lástima que, una vez más, se deban producir grandes tragedias para mejorar en algo que debería tener mayor calado en todos los estamentos públicos y privados.

Ahora tan sólo desear que todos ellos se centren en lograr la mejor coordinación y efectividad en la atención a las víctimas, el motivo principal que debería regir, por encima de cualquier otra circunstancia, sus actuaciones y, en paralelo o tras ello, según las circunstancias de cada lugar y situación, en recuperar las actividades productivas y de servicios que puedan paliar, con inmediatez, las consecuencias y contribuyan al inicio de la reconstrucción y mínima usabilidad de las zonas devastadas.

Acabo con mis habituales referencias al refranero y las frases célebres aplicables en este caso a todos y cada uno de los actores antes mencionados:

- “La unión hace la fuerza”
- “El trabajo en equipo es el secreto que hace que las personas comunes logren resultados extraordinarios” – lfeanyi Onuoha
- “La fuerza del equipo reside en cada miembro. La fuerza de cada miembro es el equipo” – Phil Jackson.
- “Yo hago lo que usted no puede, y usted hace lo que yo no puedo. Juntos podemos hacer grandes cosas” – Madre Teresa de Calcuta
- “El trabajo en equipo divide el trabajo y multiplica los resultados” – Desconocido
- “Ninguna persona puede ganar un partido por sí mismo” – Pelé.
- “Es increíble lo que puede lograr si no te importa quién se lleva el crédito” – Harry Truman. ■



Aunque recibiréis información de cada evento con antelación a su desarrollo para formalizar las inscripciones, os detallamos los eventos que organiza ADSI en exclusiva, los que coorganiza con otra entidad y los organizados por terceros en los que ADSI tiene una participación activa de algún integrante de Junta o socio. Anotadlos en vuestra agenda.

Eventos organizados en exclusiva por ADSI

◆ "Martes con..." en MADRID

– 19 noviembre: *Cruz Roja (Centro de Formación y Emergencias de Madrid-El Plantío)*

◆ "Martes con..." en BARCELONA

– 26 noviembre: *Corporación Catalana de Medios Audiovisuales – 3 CAT*

Organizados por terceros en los que ADSI tiene una participación activa

◆ 26 a 28 marzo 2025: **II SEDEXPO**, *Feira Galicia - Silleda*

◆ 4 y 5 junio 2025: **11º Security Forum**, *Atarazanas Reales - Barcelona*



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.



Protección personal de ejecutivos y personas

Por **Joan Roda**, vocal de ADSI

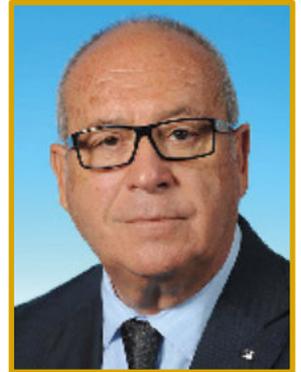
La protección personal de ejecutivos y personas influyentes es un tema de creciente relevancia en un mundo donde la seguridad se ha convertido en una preocupación primordial. La necesidad de proteger a estas personas va más allá de la simple vigilancia; implica un enfoque integral que abarca desde la evaluación de riesgos hasta la implementación de medidas de seguridad efectivas. Este texto explora las distintas facetas de la protección personal, los métodos y técnicas utilizados, así como la importancia de la capacitación en este ámbito.

Bases de actuación siempre hay que actuar evaluando los riesgos haciendo un estudio previo a la actuación con análisis de inteligencia para prevenir posibles ataques externos nunca se tiene que esperar a la reacción que siempre suele ser desfavorable hay que tener cápsulas de reconocimiento para detectar peligros emergentes y analizar y cambiar el recorrido para evitar la sorpresa hay que tener en cuenta que cuando se produce un ataque el atacante siempre tiene la ventaja de la sorpresa dejando a la cédula en desventaja por no estar preparados para la reacción todos estos eventos suelen acabar en un desastre nunca hemos de esperar a la respuesta de reacción siempre hay que anticiparse.



Contexto y Necesidad de Protección

En un entorno global cada vez más complejo, los ejecutivos y personas influyentes están expuestos a diversas amenazas, que pueden ir desde el acoso hasta intentos de secuestro. Las razones detrás de estas amenazas pueden variar: desde rivalidades empresariales hasta conflictos personales. El impacto de un ataque o una situación de riesgo puede ser devastador, no solo para la persona afectada, sino también para las empresas y organizaciones que representan. Por ello, la protección personal se ha vuelto una prioridad para muchas corporaciones y organizaciones.



Tipos de Amenazas

Las amenazas pueden clasificarse en varias categorías:

1. Amenazas Físicas: Incluyen agresiones, secuestros y ataques violentos. Estas situaciones son las más evidentes y requieren una respuesta inmediata.
2. Amenazas Cibernéticas: Los ejecutivos pueden ser blanco de ataques cibernéticos que busquen robar información sensible o causar daño a la reputación de la empresa.
3. Amenazas Sociales: Situaciones de acoso o violencia relacionada con la fama o la influencia de una persona, que pueden surgir en entornos públicos o privados.

Evaluación de Riesgos

Antes de implementar cualquier medida de protección, es esencial realizar una evaluación de riesgos. Esto



implica identificar las amenazas específicas a las que se enfrenta la persona, así como los entornos y situaciones en los que se encuentra más vulnerable. La evaluación debe considerar:

- **Perfil de la Persona:** La historia, la reputación y el nivel de influencia de la persona en su ámbito.
- **Entorno de Trabajo:** La naturaleza de la industria, la ubicación de las oficinas y el contexto social y político de la región.
- **Actividades y Movimientos:** La agenda diaria, eventos públicos y reuniones que puedan representar un riesgo.

Medidas de Protección

Las medidas de protección personal pueden ser tanto preventivas como reactivas. Entre las más comunes se encuentran:

1. **Protección Física:** Esto incluye la asignación de agentes de seguridad, la instalación de sistemas de videovigilancia y el uso de vehículos blindados. Los agentes de seguridad suelen ser entrenados para identificar y neutralizar amenazas antes de que se materialicen.
2. **Planificación de Rutas:** Para minimizar riesgos, es crucial planificar cuidadosamente los desplazamientos.



Esto puede incluir el uso de rutas alternativas y el conocimiento de áreas seguras y peligrosas.

3. **Protocolos de Emergencia:** Las personas protegidas deben conocer los procedimientos a seguir en caso de un incidente. Esto puede incluir desde la evacuación de un lugar hasta cómo comunicarse con las autoridades.
4. **Formación y Capacitación:** Es fundamental que los ejecutivos y sus equipos reciban capacitación sobre cómo actuar en situaciones de crisis. Esto incluye habilidades en evasión, negociación y autoprotección.

Protección Cibernética

Dada la creciente interconexión digital, la protección cibernética es igualmente esencial. Esto implica:

- **Seguridad Informática:** Implementar firewalls, software antivirus y sistemas de encriptación para proteger la información sensible.
- **Concienciación sobre Ciberseguridad:** Capacitar a los ejecutivos para que reconozcan las amenazas cibernéticas, como el phishing y el malware, y cómo evitar caer en estas trampas.
- **Gestión de la Reputación Online:** Monitorear la presencia en redes sociales y gestionar la información pública para mitigar posibles ataques a la reputación.





Importancia de la Confidencialidad

La confidencialidad es un aspecto crucial en la protección personal. Los detalles sobre la seguridad de un ejecutivo no deben ser divulgados, ya que esto podría comprometer su seguridad. Las empresas deben establecer políticas claras sobre quién tiene acceso a esta información y cómo se maneja.

Ciberseguridad y Redes Sociales

Las redes sociales, aunque son herramientas poderosas para la comunicación y el marketing, también representan un riesgo significativo. Publicar información sobre movimientos, viajes o eventos puede proporcionar a los delincuentes pistas sobre la ubicación y vulnerabilidad de un ejecutivo. Por ello, es esencial establecer directrices claras sobre el uso de redes sociales.

Cultura de Seguridad

Para que las medidas de protección sean efectivas, es necesario cultivar una cultura de seguridad dentro de la organización. Esto implica no solo implementar políticas, sino también fomentar la concienciación y la responsabilidad entre todos los empleados. Todos deben entender su papel en la seguridad general de la empresa y de los ejecutivos.

Tecnologías Emergentes

El avance tecnológico ha traído consigo nuevas herramientas para mejorar la protección personal. Dispositivos como aplicaciones de seguridad, sistemas de rastreo y tecnologías de reconocimiento facial están revolucionando la forma en que se aborda la protección. Sin embargo, también es fundamental considerar los aspectos éticos y de privacidad asociados con el uso de estas tecnologías.

Colaboración con Autoridades

Una estrategia efectiva de protección personal debe incluir la colaboración con las autoridades locales y organismos de seguridad. Establecer relaciones con la policía y otros cuerpos de seguridad puede ser crucial para obtener asistencia en situaciones de riesgo y para recibir actualizaciones sobre amenazas potenciales en la zona.

Conclusión

La protección personal de ejecutivos y personas influyentes es un desafío multifacético que requiere un enfoque proactivo y adaptativo. Las amenazas son diversas y evolucionan constantemente, por lo que es vital que las organizaciones mantengan una vigilancia constante y estén dispuestas a ajustar sus estrategias de seguridad según sea necesario. La inversión en medidas de protección, capacitación y tecnología no solo salvaguarda a las personas, sino que también protege la integridad y la reputación de las organizaciones que representan. En un mundo donde la seguridad es cada vez más incierta, la preparación y la prevención son clave para asegurar un entorno seguro para quienes lideran y toman decisiones en nuestras sociedades. ■



Carlos Juanes

Director de Seguridad de IRONLOCK Sistemas

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

Mi actividad como Director de Seguridad se desarrolla a través de IRONLOCK SISTEMAS, donde desarrollo mi trabajo y desde donde presto mis servicios como Director de Seguridad en Nationale Nederlanden y otras entidades financieras que tienen el servicio externalizado. En las mismas desarrollo mi trabajo como responsable de los sistemas de seguridad y cumplimiento normativo de dichos sistemas.

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

Fundamentalmente, la eficiencia en el servicio a nuestros clientes, mejorando los sistemas en los que prestamos servicios y trabajando como socios estratégicos para dar soporte y asesoría profesional permanente para tener actualizados todos los sistemas y cumplir con las normativas que se van implementando en el sistema jurídico español.

¿Cuál es tu formación académica?

Soy Licenciado en Derecho y Director de Seguridad por la Universidad Autónoma de Madrid, además de Cursos superiores de Seguridad en Infraestructuras Críticas por el Instituto Universitario Gutiérrez Mellado de las Fuerzas Armadas, aparte de otros muchos Cursos relacionados con el mundo de la Seguridad.

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

Después de trabajar en una Ingeniería de Defensa dependiente de la Empresa Nacional Santa Barbara,

accedí al sector de la Seguridad con una empresa de detección de armas y explosivos con equipos de rayos-X y posteriormente en empresas de seguridad de sistemas hasta llegar a la actual Ironlock Sistemas.



Desde el 2001 comencé a prestar mis servicios como Director de Seguridad de ING BANK, donde he estado más de diez años en distintas épocas y posteriormente en otras entidades financieras como Unión de Bancos Suizos, Money Exchange, A&G Banca Privada y Nationale Nederlanden donde llevo más de diez años prestando mis servicios de Director de Seguridad externalizados desde IRONLOCK Sistemas.

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

Durante las últimas décadas ha cambiado considerablemente con los avances en Tecnología que han mejorado notablemente los estándares de seguridad que se ha ido implantando en las organizaciones.

También la Normativa legal ha cambiado y se tienen que cumplir Directivas europeas y nuevas normas en Infraestructuras críticas por poner un ejemplo, que han mejorado decisivamente la gestión y los medios de implantar la seguridad en las organizaciones.

Las campañas de profesionalización de los Directores de Seguridad que tiene que formarse como gestor pero con una formación continua en un mundo digital en evolución.



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

Cada día más la gestión de los Directores de Seguridad están interrelacionadas con los CISO de las organizaciones pues la ciberseguridad en todas los elementos de los sistemas que se utilizan y deben estar más asegurados a su vez para proteger a la organización.

La profesionalización es cada día más urgente y para ello es necesario que la formación reglada sea cada día más completa y con mayores exigencias., donde la formación no solo debe centrarse en las nuevas tecnologías, sino también en la gestión de equipos, estrategias de seguridad, planificación de medios y capacidad de gestión ante las nuevas amenazas cambiantes, con Cursos reglados y especializados en distintas áreas.

¿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?

Exigiría Departamento de Seguridad a aquellas empresas que por su actividad u organización así lo requieran, independientemente de permitir que constituyesen Departamento de Seguridad aquellas otras que no lo exija la Ley.

Es evidente que aquellas empresas que no tengan la obligación de disponer de un departamento de seguridad deben evaluar los riesgos que ello comporta y por tanto tener en cuenta la conveniencia de implantarlo.

¿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?

Como antes comentaba, la formación es fundamental y

debe ser reglada y especializada, por lo que se debe exigir un Grado Universitario para el desempeño de la profesión. Los Cursos de Director de Seguridad se han quedado muy cortos en cuanto a formación y algunos obsoletos o con grandes lagunas en dicha formación pues es necesario profundizar para tener un conocimiento global de las nuevas amenazas con nuevas tecnologías y con la IA, así como un conocimiento profundo de las Normativas aplicables a cada caso concreto.

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

Cada día los cambios tecnológicos y su rápida evolución condicionan la amplia formación necesaria para un Director de Seguridad y el conocimiento estricto de la Normativa legal incluida la de las Directivas europeas en este ámbito.

Por ello es necesario una formación exhaustiva para las Directores de Seguridad.

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

Integrarse en ADSI, como asociación profesional, ha supuesto para mi, una formación y aprendizaje permanente, además de una gran oportunidad de intercambiar conocimientos y experiencias con compañeros de muy diferentes ámbitos de la seguridad.

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

No cabe duda que las actividades de ADSI son las más completas que hay el sector, con múltiples actividades con empresas logísticas, banca, empresas energéticas, institucionales, etc. que suponen una experiencia difícil de encontrar en otras asociaciones profesionales.

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



En todo caso depende de las diferentes organizaciones donde se celebran los eventos formativos, en relación con la cantidad de asistentes ,pues ADSI no puede determinar el número de asistentes sino que son las organizaciones quienes lo determinan.

Quizá podría llevar a cabo acuerdos de colaboración con Universidades para obtener precios más ajustados para sus afiliados profesionales.

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

La colaboración de los distintos departamentos de seguridad de empresas tan diversas puede incrementarse a través de su colaboración en eventos de formación e intercambio de información más completa entre los propios profesionales del sector. Se producen en otros ámbitos encuentros sectoriales dentro del mundo de la seguridad y quizá desde ADSI se podría conseguir que aún más se produjesen encuentros y formación desde esos distintos ámbitos profesionales

de actuación.

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?

Hace años, hablábamos de otros países y organizaciones de dichas naciones como parte fundamental de la especialización en la formación de los Directivos de Seguridad si bien ahora podemos asegurar que disponemos de centros de formación con grandes profesionales especializados en todo tipo de organizaciones y grandes eventos internacionales que son ejemplo para profesionales de todo el mundo.

Quiero dar las Gracias a ADSI por su permanente contribución , esfuerzo y colaboración para que ese conocimiento sea compartido con otros profesionales del sector. ■

🚴 Un hobby: Es difícil entender que le llame hobby a servir, pero me gusta dedicar mi tiempo libre a servir, especialmente a/y entre los jóvenes. Porque sirviendo recibes ciento por uno.

📖 Un libro: “Se hace tarde y anochece “ de Robert Sarah. Una forma de entender las relaciones entre los pueblos de distintas culturas y religiones y el respeto a la forma de vida de occidente frente a las

migraciones desordenadas.

🎵 Una canción: Huracán, de Hakuna. Canción que comporta todo un estilo de vida.

🏠 Un lugar para desconectar: Las montañas de Puellezo en Cantabria.

🕒 Un momento de la historia: La época de la Resurrección de Jesucristo, que cambio nuestra vida e historia para siempre.



La protección de datos y la seguridad corporativa

Por **José Ignacio Olmos**, Jefe control operativo de seguridad en Renfe Operadora

Cualquiera de los trabajadores que pertenecemos al sector de la seguridad privada conocemos la importancia de la protección de datos de carácter personal. Esta importancia viene dada no sólo por ser una prolongación del derecho fundamental a la intimidad (incluso por extensión jurisprudencial como un derecho fundamental autónomo más) que debemos proteger, sino también por las importantes sanciones que puede conllevar un incumplimiento de la normativa vigente al respecto.

Dentro de la seguridad privada las dos cuestiones que más afectan en esta materia son, posiblemente los controles de acceso y la videovigilancia. Me centraré, en esta ocasión, en la problemática que suscita esta última dentro de los departamentos de seguridad.

Al margen de las cuestiones meramente formales como pueda ser el cumplimiento con el trámite de colocar los carteles correspondientes, etc., hay algunas que interfieren notablemente, y no para bien, en el funcionamiento de los departamentos de seguridad corporativa.

En particular, cumplir con el derecho de acceso es una carga para las corporaciones, sobre todo para aquellas que disponen de innumerables instalaciones con una gran dispersión geográfica y, fundamentalmente, con afluencias masivas de personas, porque estos departamentos deben destinar muchos recursos humanos y materiales a atender tanto estas peticiones del derecho de acceso de los ciudadanos, como las de las Fuerzas y Cuerpos de Seguridad (FCS) y Jueces y Tribunales.

Ya de por sí, se debe hacer un filtrado, puesto que parte de las solicitudes de imágenes no constituyen un derecho de acceso ("me han rozado el coche en el parking y quiero saber qué coche ha sido", por ejemplo). Y en cuanto a las FCS y al poder jurisdiccional, ¿hasta dónde llega mi deber de colaboración?; perfectamente una corporación podría decir: "ahí tiene usted una silla y los equipos, si quiere venga y extraiga las imágenes". Esta tampoco es la solución ideal en el marco de las relaciones con organismos públicos, pero es cierto que conllevan costes que soportan nuestras compañías, y, particularmente,

nuestros limitado presupuestos del departamento de seguridad (o a veces tecnología).

Para el derecho de acceso aún es posible facilitarlo, conforme la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, mediante escrito certificado en el que, con la mayor precisión posible y sin afectar a derechos de terceros, se especifiquen los datos que han sido objeto de tratamiento (artículo 5.2). Esta posibilidad es interesante desde el punto de vista de seguridad, pues al no aportar literalmente las imágenes, el solicitante no tiene acceso a ciertas informaciones sensibles. Pensemos en las Infraestructuras Críticas y la confidencialidad que conllevan; ¿debo entregarle las imágenes del recorrido del reponedor de la máquina de coca cola de una zona de mi central nuclear si este me lo solicita?.

Esta Instrucción, debido a su obsolescencia, es previsible que pierda su vigencia en no mucho tiempo. Es más, bajo mi punto de vista, es excesivo que la Instrucción obligue a una descripción con "la mayor precisión posible", ya que el titular quiere saber qué datos de carácter personal se tienen y su fuente, con lo que, en consonancia con la información ya aportada en los carteles debería ser suficiente saber que se dispone de su imagen captada por cámaras de videovigilancia; a mayores, el detalle podría llegar a fecha y ubicación; por ejemplo, se dispone de la imagen de un viajero que accede a la estación de tren de xxxx a las 16:02 el día xxxx y baja al andén 2, subiéndose a un tren a las 16:04. Todo lo demás, entiendo que es irrelevante para el derecho de acceso.

En los casos de peticiones policiales o judiciales evidentemente se aportarán las imágenes si se dispone de ellas. Estas peticiones de datos, fuera de la videovigilancia, son muchas veces excesivas (por ejemplo, listado de todos los pasajeros que han viajado entre 2 ciudades en un determinado medio de transporte



durante los últimos 3 meses), con lo que es necesario acotar la petición para hacerla viable.

En el caso de tener que aportar las imágenes para un derecho de acceso, sobre todo en lugares de afluencia masiva, se debería difuminar el resto de personas, lo cual supondría trabajo y coste extra.

Y, volviendo a la descripción escrita de las imágenes, ¿qué ocurre si el ciudadano decide solicitarlo con la idea de aportar imágenes en un proceso judicial? A mi juicio, sin ser experto en la materia, no es esa la finalidad del derecho de acceso, por lo que la vía correcta para obtener una prueba sería vía Cuerpos de Seguridad o vía juzgados, pero muchos usuarios, debido a la lentitud de la justicia, optan por esta vía para que se reserven las imágenes y no se eliminen; aquí, una descripción escrita podría suponer una vulneración del derecho a la tutela judicial efectiva del artículo 24 de la Constitución. Recordemos que, aunque existe un plazo máximo de conservación para las imágenes de un mes, los sistemas de almacenamiento pueden tener menor capacidad; para las imágenes de cámaras de seguridad, la única prescripción legal es la del artículo 120.1 a) del Reglamento de seguridad privada, que impone a las entidades de crédito la obligación de conservar un mínimo de 15 días las imágenes, lo que se podría extender por analogía al resto de usuarios.

Vayamos a la realidad con ejemplos sangrantes, como la de un usuario de un determinado medio de transporte que solicita las imágenes de las cámaras de a bordo de dicho medio. Para poder extraerlas hay que retirar de la circulación el vehículo en cuestión con el perjuicio que supone para todos los ciudadanos usuarios de un servicio público. Se llegó a hablar desde el departamento de seguridad con el usuario, que confesó que el motivo de ver las imágenes era saber dónde se había extraviado el tupper con la comida del día...pero si el ciudadano lo solicita, se debe atender la petición; ¿ustedes creen que se debe de dejar a los usuarios sin un medio de transporte público para que alguien sepa dónde extravió un cacharro con comida? No es de recibo...

Más allá de todo lo comentado, debemos atender la petición de una persona y para ello le solicitamos su identificación y fotografía reciente, tal y como señala la norma. De tal manera que enviando una copia de un DNI mediante un correo electrónico, al supuesto peticionario le damos toda la información de días y horas a las que viene a nuestra instalación la persona a la que pertenece el documento de identidad, pero ¿qué ocurriría si la

persona que envía el documento no es el titular, sino una persona que suplanta su identidad? ¿Cuántas posibilidades hay de que un hombre condenado por violencia de género tenga una copia del documento de su mujer?; yo creo que bastantes, con lo que estamos facilitando toda la información de la persona a su posible agresor; esto es una clara deficiencia del sistema, pues no hay forma de comprobar si quien solicita es el titular del documento, tan fácil como eso.

Y hablando de la conservación de las imágenes, el plazo previsto de 30 días es difícilmente justificable en su ampliación, lo cual puede suponer casos de indefensión para las empresas. Por ejemplo, si una persona presenta una denuncia por daños en su abrigo de pieles o lesiones en su persona por mal funcionamiento de unas escaleras mecánicas el día siguiente a finalizar el plazo previsto de un mes, ya no dispondremos de imágenes que, con un simple visionado nos mostraría que el carísimo abrigo de pieles no lo portaba ese día la persona o que la caída que provocó sus lesiones no fue fruto de un mal funcionamiento, sino de las prisas por acceder a un tren y el tropiezo con su propia maleta.

En relación al derecho de acceso, en esa labor de "pentester" que debemos realizar los directores de seguridad en la elaboración de nuestro análisis de riesgos, se me ocurren algunas cosas interesantes. Por ejemplo, pongamos que existe en una determinada región del país una plataforma de asociaciones proindependentistas; pongamos que esa plataforma promueve una concentración de miles de personas que consistirá, entre otras cosas, en entrar y salir a un recinto (una estación de transporte, un centro comercial...). Pongamos también que, inmediatamente después, esas miles de personas aleccionadas para una finalidad, solicitan a la empresa que gestiona la instalación donde han accedido su derecho de acceso, recibiendo la compañía miles de solicitudes simultáneamente. Resultado, el colapso del sistema y la imposibilidad de cumplir en el plazo establecido de un mes con la respuesta al derecho de acceso. Sería una especie de ataque de Denegación de Servicio desde el mundo físico.

En resumen, es fundamental garantizar los derechos de los ciudadanos pero el coste e inconvenientes que se genera para las empresas debería hacer que la regulación tuviese en cuenta también estas circunstancias, pues como se dice en el mundo jurídico, ningún derecho es absoluto, y la imposición forzosa de obligaciones no suele ser una buena filosofía. ■



Por qué occidente no cree en la guerra

Por **Jesús Alberto García Riesco**, Col. ET, Político, Analista y Conferenciante.
Artículo de opinión publicado en el DIARIO EL RADAR, de fecha 31 octubre 2024

Occidente carece de la capacidad para enfrentarse a la amenaza del Sur Global en una guerra convencional porque no dispone de los efectivos ni de los medios necesarios. Su población —escasa y envejecida— no sabe ni quiere luchar y su industria es incapaz de producir el material bélico que demandaría el conflicto.

La causa profunda es que el hombre moderno es nihilista, por lo que no considera a la sociedad como una comunidad regida por un propósito común, sino como un compuesto de individuos aislados que sólo buscan su propia gratificación.

Capacidades de las autocracias

La interdependencia entre Rusia, China, Irán y Corea del Norte está aumentando. Las autocracias disponen de sociedades, cohesionadas por la coerción, que aportan efectivos dispuestos a morir y una industria de guerra con mano de obra activada 24 horas diarias.

China está superando a Estados Unidos en la capacidad de combate y en la producción de defensa. Dado el problema demográfico que tendrá en el futuro, es probable que intente invadir Taiwán esta década con el millón de soldados disponibles, lo que contrasta con la capacidad estadounidense; Keating señala que si Estados Unidos tuviese que defender la isla «sólo podría reclutar la mitad de los 100.000 soldados necesarios» [[1]].

Rusia libra una guerra de desgaste contra Ucrania —un país que ha asombrado al mundo por su resiliencia social— y ha mostrado su capacidad para poner a la



población en pie de guerra; Todd dice que, al comienzo de la invasión de Ucrania, «Rusia y Bielorrusia, con sólo el 3,3 % del PIB de Occidente, producían más armas que todo el mundo libre, lo que cuestiona las nociones dominantes del neoliberalismo» [[2]]. Rusia está produciendo actualmente —a un costo menor— más proyectiles de artillería que Estados Unidos y Europa juntos; Kasapoğlu precisa que el Kremlin «puede estar fabricando cerca de 4,5 millones al año» [[3]].



Hasta marzo del presente año, Corea del Norte —una dictadura empobrecida con una población de sólo 25 millones de habitantes— envió más de un millón de proyectiles a Rusia, mientras, en el mismo período, la Unión Europea —un gigante económico poblado con casi 500 millones— sólo logró remitir a Ucrania la mitad.

Carencias de Occidente

Problema de efectivos y de moral de combate

Los ejércitos occidentales no están preparados para librar guerras de desgaste como la de Ucrania —en donde los dos contendientes tienen la moral de combate eslava— porque sus sociedades no saben ni quieren luchar.

Las fuerzas de la OTAN sufren de un problema crónico de reclutamiento y retención de efectivos, por lo que «la Alianza», señala Kahn, «necesitaría entre 35 y 50 brigadas adicionales para responder a un ataque ruso» [[4]].

Tal logro es difícil porque los ejércitos combaten en el frente, pero los conflictos los ganan las sociedades en la retaguardia. Los ciudadanos del mundo libre no quieren combatir porque, en realidad, no pueden hacerlo; «son demasiado acomodaticios y consumistas», precisa Fukuyama, «para exponerse a la muerte» [[5]]. Los jóvenes estadounidenses, por ejemplo, están poco capacitados para la guerra y no se sienten comprometidos con la defensa del país; Esper precisa



que, en 2022, «sólo el 23 % eran aptos para el servicio militar por motivos físicos, de los cuales el 10 % no tenía el nivel académico, y sólo el 9 % de la juventud mostró algún interés en unirse a las fuerzas armadas» [[6]].

Los ejércitos europeos están en peor situación, por lo que Rehka enfatiza que «si no hacemos nada ante la falta de efectivos, no seremos capaces de disuadir a ningún enemigo potencial» [[7]].

La industria de defensa no responde a las necesidades

Occidente tiene una industria de defensa construida para tiempos de paz. Los simulacros de guerra han mostrado que el Reino Unido agotaría su arsenal en poco más de una semana y Alemania se quedaría sin municiones en pocos días; Rasmussen precisa que «aunque el poder económico e industrial de los países de la Alianza eclipsan al de Rusia y sus aliados, nos estamos dejando superar en la producción de guerra» [[8]].

Los países de la OTAN producen armamento caro que solo puede ser adquirido en pequeñas cantidades lo que lleva a un problema de escalabilidad cuya consecuencia principal es la grave desconexión entre sus compromisos públicos y su capacidad para cumplirlos; «Rheinmetall», dice Kasapoğlu, «no podrá producir 1,1 millones de proyectiles de artillería de 155 mm al año hasta 2027» [[9]].

Causas de las carencias

La razón principal es que la democracia liberal no cree en la guerra debido al nihilismo y al posmodernismo.

El nihilismo

Surge como resultado de la desconfianza en la tradición, lo que lleva a no creer en nada y a renunciar a interpretaciones previamente aceptadas sobre la existencia humana y la moral; sin embargo, «la muerte de



Dios por Nietzsche», señala Afriyie, «implicaba para Dostoiévski que todo era permisible, lo que llevaba a la anarquía» [[10]].

Las nuevas fuentes de verdad que surgieron con la modernidad modelaron el mundo, pero —al dismantelar los juicios de valor ligados a la tradición— han dejado inerte a la sociedad; «el nihilismo», señala Brown, «elimina el fundamento sobre el que se asientan los valores, incluida la verdad misma» [[11]].

Para el nihilismo los seres humanos no están motivados sólo por la racionalidad, sino por los instintos y el inconsciente; todo es relativo y permisible sin verdad objetiva; Fukuyama señala que «el capitalismo y la democracia liberal son la respuesta consumada al problema del nihilismo y de la muerte de Dios» [[12]].

El nihilismo ha permeado el pensamiento occidental desde la Ilustración y se ha vuelto esencial en la cultura actual. Después de las dos guerras mundiales, los valores más elevados, ligados a la historia, perdieron su vitalidad y el existencialismo se convirtió en una ideología generalizada.

El posmodernismo: la teoría de la paz democrática

El posmodernismo, como culto predominante al individualismo y a la falta de compromiso social, extendió aún más el significado del nihilismo: todo era permisible en una contracultura que aceleró la descomposición social, sin ofrecer tras la destrucción ninguna solución viable.

Toma impulso en Occidente después de la Guerra Fría y se apoya en la «teoría de la paz democrática», la cual sostiene que las democracias son menos propensas a la violencia que las autocracias y «no luchan entre sí», señala Rumber, «por tres razones: no quieren la guerra la esencia de la cultura democrática es la negociación de la violencia y los ciudadanos resuelven sus intereses por vías pacíficas» [[13]].

En la misma línea, Mousseau señala que «el mundo se encuentra en el final de una trayectoria hacia la paz y la prosperidad permanentes» [[14]] y Goldstein sostiene que «el declive de la guerra llega por la expansión de las economías de mercado y los acuerdos internacionales que la impiden» [[15]]. También está extendida la idea de que la tecnología militar imposibilita la guerra; Bloch dice que «en el futuro, la letalidad de las armas nos impedirá luchar» [[16]].

En suma, ya no es necesario mantener las fuerzas armadas tradicionales para mantener la seguridad,



porque existen las condiciones y las instituciones para centrarse en la interdependencia y en los derechos humanos.

Consecuencias

Debilidad occidental

El individualismo liberal ha abandonado los lazos comunitarios para dedicarse a satisfacer el sinfín de pequeñas necesidades individuales, lo que ha aflojado los hilos que sujetaban la cohesión social y ha debilitado a Occidente; «a falta de la tradición», dice Bell, «las instituciones que sostenían la sociedad capitalista han ido cayendo» [[17]].

En consecuencia, la generación occidental posterior a la Guerra Fría creció en la creencia de que la paz era un derecho adquirido y no era necesario preocuparse por la seguridad, por lo que la ciudadanía actual es incapaz de cumplir con el deber cívico más fundamental: defender a su país. La decadencia del Estado nación —comunidad de tradiciones y sentimientos de la población— impide a Occidente enfrentarse a una guerra convencional porque la posmodernidad ha dado la espalda al drama íntimo del alma humana en la confusión del combate.

Esta incapacidad lleva a plantear soluciones escapistas basadas en el predominio de la tecnología y la digitalización; Carter dice que el Reino Unido podría algún día «tener un ejército de 120.000 efectivos, de los cuales 30.000 podrían ser robots» [[18]], aspecto en el que profundiza Walker: «Con drones e inteligencia artificial, el ejército británico duplicará la capacidad de combate en tres años y la triplicará para el final de la década» [[19]].

Fuerza del comunitarismo en el Sur Global

Al contrario, la mayoría de los países del Sur Global consideran la seguridad en términos de integridad



territorial y sus sociedades mantienen los «viejos valores» estatocéntricos que les permiten desarrollar una disuasión más efectiva. Este modelo está desplazando la política impuesta por Occidente tras la Guerra Fría.

Conclusiones

El modelo actual de defensa no funciona, lo que constituye un riesgo crítico para la seguridad de Occidente. El posmodernismo ha de dar paso a un nuevo «contrato social» en donde la teoría de la paz democrática sea sustituida por una doctrina más realista y transparente que se atreva a informar verazmente a la ciudadanía de los peligros que afectan a la seguridad de todos, sopesando los riesgos y los costos tanto de la acción como de la inacción. Nos va en ello la democracia.

Notas:

- [[1]] KEATING, Joshua. "The world is running out of soldiers", Vox, Jun 18, 2024. <https://www.vox.com/world-politics/355547/soldiers-shortage-demographics-population-conscription>
- [[2]] TODD, Emmanuel. La derrota de Occidente, Ediciones Akal, mayo 2024.
- [[3]] KASAPOĞLU, Can. "NATO Is Not Ready for War", Hudson Institute, Jun 28 2024. <https://www.hudson.org/security-alliances/nato-not-ready-war-assessing-military-balance-between-alliance-russia-can-kasapoglu>
- [[4]] KAHN, Michael "Eastern Europe's armies struggle to enlist young people with war not far away". Reuters, August 9 2024. <https://www.reuters.com/world/europe/eastern-europes-armies-struggle-enlist-young-people-with-war-not-far-away-2024-08-09/>
- [[5]] FUKUYAMA, Francis. El fin de la historia y el último hombre. Barcelona, Planeta 1992.
- [[6]] ESPER, Mark. "Long, slow decline of the US military's all-volunteer force puts America in danger", Fox News, September 19 2022. <https://www.foxnews.com/opinion/long-slow-decline-us-military-all-volunteer-force-puts-america-danger>
- [[7]] Citado en KAHN, Michael. Op. Cit.
- [[8]] Citado en KUPER, Stephen. "Red Alert! Concerns grow over Europe's dramatic military weakness", Defence Connect, 12 December 2023. <https://www.defenceconnect.com.au/geopolitics-and-policy/13298-red-alert-concerns-grow-over-europe-s-dramatic-military-weakness>
- [[9]] KASAPOĞLU, Can. Op. Cit.
- [[10]] AFRIYIE Anobel. "A History of Nihilism as a Reflection on Western Values since the 19th Century", Youngstown State University, August 2024. https://etd.ohiolink.edu/acprod/odb_etd/ws/send_file/send?accession=ysu1722445491346713&disposition=inline
- [[11]] BROWN, Wendy. Nihilistic Times Thinking with Max Weber, Belknap Press, 2023.
- [[12]] FUKUYAMA, Francis. Op. Cit.
- [[13]] RUMMEL, R.J.. Power Kills Democracy as a Method of Nonviolence, Routledge, 2002.
- [[14]] MOUSSEAU, Michael. "The End of War. How a Robust Marketplace and Liberal Hegemony Are Leading to Perpetual World Peace", International Security July 2019, https://www.researchgate.net/publication/334754260_The_End_of_War_How_a_Robust_Marketplace_and_Liberal_Hegemony_Are_Leading_to_Perpetual_World_Peace/link/5f1ee90b299bf1720d682265/download
- [[15]] GOLDSTEIN, Joshua. "The decline of armed conflict worldwide", International Journal on World Peace, June 2013. <https://www.jstor.org/stable/24543783>
- [[16]] Citado en FAZAL, Tanisha y POAST, Paul. "War Is Not Over. What the Optimists Get Wrong About Conflict", Foreign Affairs, November/December 2019. <https://www.foreignaffairs.com/world/war-not-over>
- [[17]] BELL, Daniel. Las contradicciones culturales del capitalismo, Alianza Editorial, Madrid 1975.
- [[18]] KEATING, Josua. Op. Cit.
- [[19]] Citado en SABBAGH, Dan. "Army chief says UK must double its lethality or be prepared for war in 2027", The Guardian, Tue 23 Jul 2024. <https://www.theguardian.com/uk-news/article/2024/jul/23/british-defence-chief-vows-to-triple-fighting-power-but-shies-away-from-conscription>



"Martes con..." en Málaga, 1 de octubre

Google GSEC Málaga

El pasado 1 de octubre, ADSI celebró en Málaga un "Martes con ..." muy diferente de los que tenemos por costumbre realizar. Por un lado, por la ubicación, fuera de las ciudades habituales como son Barcelona y Madrid, y por supuesto, por el anfitrión que nos acogió. Una vez más tuvimos el enorme placer de visitar una instalación de Google, la más nueva y revolucionaria que ha instalado en España; el GSEC (Google Safety Engineering Center) de Málaga, que es uno de los 4 centros de estas características que la empresa tiene en Europa.

Otra de las novedades de este acto fue el horario de mañana, a diferencia del habitual horario de tarde. **Ello permitió el desplazamiento de asistentes provenientes no sólo de Málaga (y por proximidad de Andalucía en general), sino que conseguimos reunir a socios y simpatizantes de lugares tan lejanos como Asturias, Madrid y Barcelona.**

Nuestro presidente, Eduard Zamora, dio comienzo la jornada presentando a los ponentes Juan de Parra y Pancho Perdomo, que en representación de Google nos deleitaron con unas ponencias sumamente interesantes.

En primer lugar Juan de Parra, Cloud Space Program Manager en el GSEC de Málaga, nos explicó el porqué Google es un referente mundial en Ciberseguridad, qué les hace serlo, qué equipos tienen dedicados a este ámbito y compartió algunos detalles significativos de la historia de Google en ciberseguridad, como la generación

de un estándar llamado Zero Trust, que surgió del concepto de no confiar en nadie y que se ha convertido en una metodología ampliamente utilizada por innumerables empresas.

Nos contó sobre la historia del centro, y de por qué Google se ha acabado implantando de manera tan potente en Málaga. Todo nació con la creación de una pequeña empresa llamada VirusTotal, fundada en 2002 por Bernardo Quintero con 4 socios más en la ciudad costasoleña. Esta empresa, dedicada a recopilar información sobre virus y malware, a modo de gran base de datos de ciberseguridad, fue creciendo y ganando reputación, hasta el punto de llamar la atención de Google, que la incorporó a su Corporación en 2012. Desde ese momento, Google pasó a tener presencia en la ciudad, primero en las oficinas originales de VirusTotal (un chalet conocido como el "chalet de la ciberseguridad"), luego en las dependencias de la Universidad de Málaga, hasta trasladarse a finales del 2023 a la ubicación actual, un edificio que antiguamente había sido del Gobierno Militar y que Google reformó íntegramente (respetando la fachada y la estructura) para poder albergar a sus equipos de ingenieros (unos 70 en la actualidad). El edificio consta de 2.500 m2, de los que 1.500 m2 son para eventos, visitas, congresos, etc. De hecho, nuestra sesión se desarrolló en el auditorio habilitado para este tipo de actos, con capacidad para un centenar de asistentes. Ello es así porque uno de los principales objetivos del GSEC es el de dar a conocer y





compartir todo lo que allí se hace, con el objetivo de concienciar de la importancia de la ciberseguridad en la sociedad.

A continuación, Pancho Perdomo, Customer Success Manager en GSEC Málaga, nos expuso algunas de las herramientas que Google está desarrollando para gestionar tanto su ciberseguridad, como también la de sus clientes, ya que al fin y al cabo son herramientas que Google comercializa en su mayoría (aunque hay algunas que son plenamente gratuitas). Fue muy interesante ver cómo esas herramientas pueden ayudar a equipos de ingenieros a detectar ciberamenazas de una forma muy rápida. Uno de los datos más impactantes que nos dio Pancho fue el tiempo que se tarda en detectar una nueva amenaza, ya sea en forma de virus o de malware, desde que "sale" al mercado. En estos momentos se tarda 10 días (en media) en tenerla detectada y controlada para que no siga infectando. Puede parecer mucho tiempo, pero si lo comparamos con los más de 400 días que se tardaba hace tan sólo 6 años, nos podemos dar cuenta de la velocidad a la que evoluciona este mundo. Gran parte de esta velocidad se debe a la aplicación de Inteligencia

Artificial (IA). Google es uno de los pioneros en este campo de investigación y está aplicándola en todos sus productos. Pancho nos demostró cómo la IA ayuda en concreto a detectar código malicioso, sobretodo en los casos en los que los programadores lo hayan "ofuscado" para hacer la tarea casi imposible para un humano. La IA, en cuestión de segundos, ya tiene el diagnóstico hecho y puesto a disposición del ingeniero para que éste tome las decisiones adecuadas.

Pasamos al turno de preguntas donde permitieron a los asistentes profundizar un poco más, en cuestiones más técnicas, o en curiosidades del centro y de Google en general.

Para finalizar Google nos obsequió con un magnífico Coffee Break en el patio del edificio, momento en que aprovechamos todos los asistentes para poder charlar con los ponentes y disfrutar del magnífico clima con el que nos recibió la ciudad de Málaga.

Agradecer a todo el equipo de Google su magnífica acogida y en particular a Lorena Nieto, Industry Manager de Google que fue el hilo conductor para poder organizar esta jornada tan diferente a las que estamos acostumbrados y en la que, gracias a nuestros anfitriones, pudimos cargar nuestra mochila de conocimientos con un buen puñado de lecciones y vivencias.

Gracias a todos los Socios y Patrocinadores que nos pudieron acompañar, sin todos ellos nada de esto sería posible. ■

***Oriol Verdura
Vocal de ADSI***



"Martes con..." en Barcelona, 8 de octubre

Ciberseguridad en Abertis Autopistas España

El pasado día 8 de octubre tuvimos la ocasión de asistir a la convocatoria del "Martes con." sobre la CIBERSEGURIDAD, esta vez desde el Auditorio de Abertis AUTOPISTAS ESPAÑA de la Avenida Pedralbes de Barcelona. El edificio que es el Centro Corporativo de Abertis es un ejemplo de estética, representatividad, buen funcionamiento y control.

Las conferencias giraron alrededor del siguiente título: "Prospectiva en Seguridad Tecnológica. Nuevos retos de la seguridad", siempre desde el punto de vista de la Ciberseguridad. **Los cuatro conferencias** contaron con la participación de expertos en esta materia que lo abordaron desde orígenes y puntos de vista diferentes. **Los ponentes fueron José Valiente Pérez (Director del CCI-Centro de Ciberseguridad Industrial), Enrique Ávila Gómez (Director de Centro de Análisis y Prospección de la Guardia Civil), Ángel Pérez Beumala (CISO Autopistas) y Martín Vigo (Consultor de Ciberseguridad, conferenciante, podcasts i divulgación).**

Inicialmente la presentación de los ponentes y la introducción de la temática fue llevada a cabo por **Eduard Zamora, presidente de ADSI**, que tras agradecer la participación tanto de ponentes como de asistentes dio paso en primer lugar a José Valiente que trató la Ciberseguridad en los servicios esenciales automatizados. Continúo Enrique Ávila, que trató los riesgos emergentes en la prospectiva tecnológica. Siguió Ángel Pérez, dialogando sobre la convergencia reguladora, CER, NIS2, RIA, etc., y por última Martín Vigo intervino sobre el futuro de la privacidad

digital, es decir, la seguridad "on line".

La primera ponencia se inició explicando las características del Centro de Ciberseguridad Industrial, el cual engloba expertos, programas, escuela de formación y eventos y publicaciones específicas de Ciberseguridad. El ponente planteó un escenario de Ciberseguridad mediante amenazas críticas en un centro de producción. En el ejemplo explico los diferentes ataques que se podían producir y las consecuencias. En las diferentes amenazas se incluyó ataques a sistemas SCADA, RANSOMWARE, manipulación de procesos, accesos no autorizados, etc. Se describió las diferentes tipologías de escenarios, relacionando las de alto impacto, alta frecuencia, alta dependencia y criticidad temporal.

En la siguiente ponencia se describieron los riesgos emergentes en materia de prospectiva tecnológica. Se describió un escenario tecnológico desde la perspectiva de la territorialidad, la complejidad y la progresiva tecnologización social. Se planteó el cibercrimen como un nuevo y inesperado territorio, con una dificultad de aplicación de la soberanía, un marco legal súper complejo y la génesis del ciberespacio. Se relacionó la necesidad del uso de la IA con la ciberseguridad, investigaciones en la nube y un plan de protección de la cadena logística, es decir, algoritmos de toma de decisiones. Y si no fuera suficientemente complejo, apareció un concepto relacionado con la desinformación, "la antología" un problema más de duda o ignorancia que de desinformación.



Se comentaron sistemas de vigilancia, como patrones de detección, análisis de imágenes, medicina exponencial, ADN artificial, etc.

El siguiente ponente nos describió el marco normativo: NIS2 (Seguridad de Sistemas y Redes), CER (Resiliencia de Entidades Críticas), DORA (Resiliencia operativa Digital sector financiero) y RIA(Reglamento de la IA). Se desarrollo la estrategia de la soberanía de la UE basada en la resiliencia de todos los servicios y productos conectados. En esta de desarrollo que se debe trabajar conjuntamente, se debe responder colectivamente a una amenaza, garantizar un internet global y abierto y un despliegue de instrumentos principales, como la resiliencia, soberanía tecnológica y liderazgo, capacidad para prevenir, disuadir y responder y cooperación para avanzar en un ciberespacio globalizado y abierto. Se expresaron las características principales del marco legal y las conclusiones generales se describieron como una hiperregulación y un aumento de obligaciones y de sanciones. Como complemento se planteo si tenemos capacidad de adaptación y suficiente talento para asimilar toda la información o desinformación que tenemos en la actualidad y en futuro.

Para cerrar la sesión, el ultimo ponente explico como la privacidad es invadida diariamente a través del robo de datos personales, explicando que las aplicaciones almacenan nuestra actividad online y el abuso que se genera con la recolección de datos a gran escala, y que después son vendidos. Con estas actuaciones y con la tendencia de estas prácticas en aumento, el ponente

plantea que es crucial tomar medidas proactivas para reducir nuestra huella digital. Toda esta información se recoge de las redes sociales, búsquedas en internet de forma genérica, de formularios rellenos que dejan huella en el historial de internet. El ponente dejo claro que se tiene que evitar compartir información personal, se ha limpiar los historiales y la huella digital y se deben proteger los dispositivos electrónicos,

Una vez finalizado las cuatro ponencias, se inició el turno de preguntas, las cuales desembarcaron respuestas directas hacia los presentes des de los ponentes y un dialogo entre ellos, que aunque los puntos de vista pudieron ser diferentes, la conclusiones finales coincidieron en su finalidad.

A continuación, se dio por finalizado el acto y tras los agradecimientos pasamos a compartir en la antesala del auditorio un cóctel-networking en el que pudimos aprovechar para saludar y compartir experiencias entre todos los asistentes, socios y amigos de ADSI.

Dar las gracias a todos los ponentes por su dedicación y entrega con ADSI, a Abertis por facilitar sus instalaciones y a los asistentes al acto. ■

Francesc Chía
Vocal de ADSI



"Martes con..." en Madrid, 15 de Octubre

Banco Santander - Boadilla del Monte

El pasado día 15 de Octubre, ADSI celebró con éxito su "Martes con.." en el Centro Corporativo de Formación y Desarrollo "El Solaruco" de la Ciudad Financiera del Grupo Banco Santander, bajo el Título "Santander Seguridad & Inteligencia. Desde la acción local hasta el análisis global".

Tras el saludo inicial de bienvenida por parte del Presidente de ADSI, Eduard Zamora, dio comienzo la jornada.

Las ponencias se llevaron a cabo por:

D. Jose Antonio Lozano González. Director Departamento de Seguridad de Santander España, Open Bank y Euro Automatic Cash.

D. Rafael Sánchez-Puerta Ortiz. Responsable Departamento de Inteligencia y Amenaza Interna del Grupo Santander.

D. Juan Luis López Martínez-Arroyo. Delegado Nacional de Seguridad Bancaria de Banco Santander España.

El Área de Seguridad e Inteligencia se organiza en tres departamentos:

El de **Seguridad Física**, a cargo de la seguridad de personas, datos e instalaciones; el de **Seguridad Bancaria y Coordinación**, responsable de la seguridad de la red de oficinas y de la coordinación con los departamentos de seguridad de todos los países en los que está el Grupo Santander, así como con Fuerzas y Cuerpos de Seguridad; y un tercer departamento, de **Inteligencia y Amenaza Interna**, que elabora inteligencia y lleva a cabo procesos de vetting.

Las características que diferencian el modelo de inteligencia son que están recogidos en un documento normativo del Grupo Santander y que, por tanto, ha sido aprobado y publicado como parte del gobierno interno.



Este documento contempla la creación de capacidades de inteligencia propias y establece un sistema de inteligencia integrada para el Grupo, en el que la función de seguridad e inteligencia no trabaja aislada. Han probado que la inteligencia contribuye de un modo muy relevante a proporcionar seguridad, facilitando información contrastada y la toma de decisiones mejor informadas.

El horizonte de amenazas que, potencialmente, pueden tener impacto en las entidades financieras se extiende desde las amenazas externas y las crisis globales hasta las amenazas internas. En inteligencia, además de la amenaza interna, consideran especialmente relevantes la inestabilidad geopolítica, el terrorismo, las amenazas híbridas, las campañas de desinformación, las amenazas tecnológicas y los ciberataques, el crimen organizado, el cambio climático, el activismo violento y las actividades de inteligencia de actores hostiles.

Para garantizar la seguridad de las personas y edificios, tienen implantados planes de protección adecuados en todos los edificios singulares, instalaciones críticas y en todos los eventos institucionales. Las zonas destinadas a Centro de Proceso de Datos (CPD) y otras que puedan considerarse como áreas restringidas cuentan con protocolos específicos de control de accesos y vigilancia.

Respecto al Análisis prospectivo e inteligencia para contribuir a una mejor gestión de la seguridad, con criterios de anticipación y prevención, se establecen procesos de análisis que permiten el estudio de situaciones actuales, la previsión de la evolución de los acontecimientos y la definición de criterios que aseguren un nivel adecuado de protección de clientes, empleados, instalaciones e información.

Respecto a la Coordinación con la Corporación, la función de Seguridad e Inteligencia está coordinada de forma adecuada entre sus responsables en la Corporación y en el ámbito local para la mejor gestión de la seguridad, distribución de buenas prácticas y aportación de valor.

La Función de Seguridad e Inteligencia se asegura de que todos los empleados en viajes internacionales y/o los expatriados reciban formación e información sobre los riesgos para su seguridad y salud así como las medidas de protección y prevención necesarias en sus

desplazamientos. Para ello la Función de Seguridad e Inteligencia es responsable del programa global de protección de viajeros con el que prestará protección y asesoramiento al viajero y/o expatriado, antes, durante y después de un viaje.

Una vez finalizadas las ponencias, **tuvimos el honor de visitar toda la Ciudad del Grupo Santander mediante un recorrido en un autocar privado**, también conocida como la Ciudad Financiera, es el lugar en el que se desarrollan los servicios centrales del banco y uno de los campus empresariales más grandes de todo el mundo:

- Ocupa una superficie de 250 hectáreas, con edificios y oficinas amplias, modernas, rodeados de naturaleza, y en las que trabajan más de 6.000 personas.
- El innovador complejo combina arquitectura y



naturaleza, cuenta con 43,5 hectáreas de zonas ajardinadas con más de 10.000 árboles y 300.000 arbustos, un espacio forestal de más de 70 hectáreas en El Bosque con 14.000 árboles y 60.000 arbustos, y 64 hectáreas en el campo de golf, con más de 1.200 olivos, de los cuales 400 superan los 500 años y 13 son olivos milenarios. Entre ellos, sobresalen los 77 ejemplares denominados "árabes" y los 257 ejemplares (163 en El Bosque y 94 en la CGS) provenientes de Calabria, cuya altura de más de trece metros hace de ellos modelos excepcionales.

La sede operativa de Santander, en constante transformación, representa mucho más que los servicios centrales de un banco global líder. El espacio, concebido para las personas, fue diseñado por el estudio de Kevin Roche y John Dinkeloo. Hoy es un lugar para el talento comprometido, diverso, global y multidisciplinar, donde se encuentran la arquitectura, la naturaleza y el paisajismo, el arte, la sostenibilidad y el progreso.

Desde su inauguración, más de 63.000 personas han tenido allí su puesto de trabajo, entre empleados, personal para colaboración temporal, contratados, becarios y personal de empresas de servicio en CGS. En la actualidad, casi 7.000 personas trabajan, colaboran, aprenden e innovan en ella con el cliente siempre en el centro.

Pudimos visitar el Global Command Center de Seguridad,

desde donde se visualizan las alarmas y cámaras de las más de 500 sucursales del Banco Santander, conformado por 14 pantallas y 21 puestos que permiten una visualización centralizada de alarmas, cámaras de vigilancia, información interna y visualización de las diferentes sucursales. Este centro de seguridad física permite centralizar información, detectar irregularidades y prestar la ayuda necesaria a las más de 500 sucursales instantáneamente.

Por último visitamos también el Patrimonio artístico que cuenta con una sala de exposiciones con 194 obras pertenecientes a la Colección Banco Santander y otras temporales; así como con esculturas en espacios exteriores de 8 autores internacionales como Richard Serra, Kimmo Schoroderus, Richard Deacon, Dan Graham, Cristina Iglesias o Juan Muñoz.

Como colofón final, pudimos degustar de un cocktail-networking en compañía de todos los asistentes que nos pudieron acompañar. Gracias a todos ellos!!

Agradecer a cada uno de los ponentes la profesionalidad y la entrega prestada con ADSI para poder llevar a cabo esta lujosa jornada. ■

Elvira Márquez
Vicepresidenta de ADSI



4ª Reunión del Foro Integral de Cultura de Seguridad Nacional

El Foro Integral de Cultura de Seguridad Nacional se crea para desarrollar actividades e iniciativas dirigidas a incrementar la conciencia sobre la trascendencia de la seguridad nacional.



Se ha celebrado la cuarta reunión del **Foro Integral de Cultura de Seguridad Nacional** en el Complejo de la Moncloa, bajo la presidencia de la directora del Departamento de Seguridad Nacional.

Durante esta reunión, se presentó un balance de actividades llevadas a cabo en 2024 para fomentar una **mayor concienciación sobre la importancia de la Seguridad Nacional** y la corresponsabilidad de toda la sociedad en su salvaguarda.

Tuvieron particular protagonismo los líderes y colideres de los **cinco grupos de trabajo** creados en el marco de este Foro, que han estado trabajando durante estos últimos meses sobre distintos ámbitos de la Seguridad Nacional. Todos estos grupos están liderados por organizaciones de la **sociedad civil y del sector privado**, y coliderados por distintos organismos de la administración pública.

Entre otras iniciativas, destaca la publicación de un **Diccionario formativo: términos y propuestas para la interculturalidad, la inclusión y contra el racismo, la xenofobia y la intolerancia** en el marco del grupo liderado por la Confederación Española de Asociaciones de Padres y Madres de Alumnado (CEAPA) y coliderado por el Observatorio Español del Racismo y la Xenofobia (OBERAXE) de la Secretaría de Estado de Migraciones, en el que también han participado el Ministerio de Educación, Formación Profesional y Deportes, así como el Movimiento contra la Intolerancia.

Asimismo, el grupo liderado por Unión Profesional,

coliderado por el Ministerio de Trabajo y Economía Social, y en el que participa la Confederación Española de Organizaciones Empresariales (CEOE), presentó el informe **«Profesiones colegiadas y sector empresarial en pro de la seguridad nacional»**.

Fomentar una cultura de seguridad nacional entre todas las instituciones

Por otro lado, los demás grupos también presentaron sus avances. El grupo liderado por la Conferencia de Rectores de las Universidades Españolas (CRUE) informó sobre la celebración del **día internacional de la Convivencia en Paz** celebrado en la Universidad de Burgos el pasado 16 de mayo de 2024 y anunció los planes de conmemoración de este día para 2025.

Asimismo, presentaron los avances del estudio que están realizando sobre la **evaluación del desarrollo humano sostenible en el Sistema Universitario Español** y el impacto social de las políticas universitarias.

Respecto al grupo liderado por la Federación Española de Municipios y Provincias (FEMP), presentó los avances logrados en sus tres objetivos generales: **fomentar una cultura de seguridad integral en los municipios**; promover la seguridad y bienestar de los ciudadanos en espacios públicos y laborales; y desarrollar herramientas y recursos para la autoprotección y gestión de riesgos en los gobiernos locales. Asimismo, informó sobre la **reciente publicación** de un «Manual de Buenas Prácticas en Salud y Bienestar Policial» que proporciona un marco estratégico integral.



Finalmente, el Consejo de la Juventud de España (CJE), que representa a los jóvenes en este Foro, presentó su plan de trabajo para los próximos meses, cuyo objetivo es **promover la seguridad humana** en la educación no formal.

Al finalizar esta sesión, se alentó a todos los miembros a continuar con la **promoción de una mayor concienciación sobre la importancia de la seguridad nacional**, así como a seguir desarrollando actividades conjuntas en el marco de este espacio de colaboración público-privado.

El Foro Integral de Cultura de Seguridad Nacional

Este Foro es un órgano colegiado de carácter **multidisciplinar y paritario**, que se compone de igual número de representantes de la Administración Pública;

y de la sociedad y sector privado: organizaciones de la sociedad civil, del ámbito académico, de asociaciones y de entidades sin ánimo de lucro.

Además, el Foro puede contar con la **participación de personas expertas independientes**, de otras organizaciones de la administración, la sociedad civil y el sector público, así como de la ciudadanía.

El **Foro Integral de Cultura de Seguridad Nacional** se crea para desarrollar actividades e iniciativas dirigidas a incrementar la conciencia sobre la trascendencia de la seguridad nacional, así como la corresponsabilidad de todos en su salvaguarda. ■

ADSI en la Diada de Guardia Urbana BCN

La Guardia Urbana de Barcelona ha celebrado su Diada Anua, en esta ocasión el 16 de octubre en el Auditorio del CCIB-Centro Convenciones Internacional de Barcelona.

Agradecemos al Concejal de Prevención, Seguridad, Convivencia y Régimen Interno, ALBERT BATLLE BASTARDAS, a la Gerente de Prevención y Seguridad, Prevención y Convivencia, MAITE CATALÀ PUJOL y al Intendente Mayor, Jefe de la Guardia Urbana de Barcelona, PEDRO VELÁZQUEZ MORENO, su invitación y los estrechos lazos de relación y colaboración que mantienen con ADSI.

Diversos asociados de ADSI fueron reconocidos en este importante y concurrido evento del Ayuntamiento de Barcelona, que celebra anualmente el reconocimiento al cuerpo policial y, a su vez, a los integrantes del sector de la seguridad privada que han sido merecedores de algún tipo de mención por su valiosa aportación al funcionamiento de la Guardia Urbana de Barcelona.

En la imagen, intervención del alcalde de Barcelona, JAUME COLLBONI y del Jefe de la Guardia Urbana, el Intendente Mayor PEDRO VELÁZQUEZ. ■



ADSI en el 25 Aniversario de la ACEDE

ADSI mantiene convenio de colaboración con ACEDE-Asociación Catalana de Ejecutivos, Directivos y Empresarios, en base al cual ha asistido como invitada a la celebración del 25 aniversario de su fundación, que se celebró en la Casa Milà de Barcelona.

Una nutrida representación de empresarios, asociados y amigos de ACEDE, junto a una notoria representación de autoridades, vivió personalmente esta entrañable celebración.

Desde ADSI felicitamos a ACEDE en esta especial efeméride y agradecemos a su presidente, Paco Camarasa, su gentil invitación.

En la imagen, de izquierda a derecha, Joan Vilar, Presidente Honorífico de ACEDE, Paco Camarasa, Presidente de ACEDE y nuestro Presidente, Eduard Zamora. ■



ADSI en la 10ª Edición del Día de la Seguridad Privada del Departament d'Interior i Seguretat Pública - Generalitat de Catalunya

ADSI ha asistido, invitada por la Consellera d'Interior i Seguretat Pública, l'Hble. Sra. Núria Parlon Gil, que presidió el evento, a la celebración del 10º Día de la Seguridad Privada, organizado por dicho Departamento de la Generalitat de Catalunya.

El acto se celebró el 4 de octubre en un repleto Teatro Romea de Barcelona.

En las imágenes, la mesa presidencial y las autoridades con los reconocidos en el evento, por sus méritos en el sector de la seguridad. ■



ADSI en el acto de Graduación del Grado en Seguridad del ISPC y la UB-Universitat de Barcelona

ADSI ha estado presente en el acto de graduación de la 7ª promoción del Grado en Seguridad organizado por el Institut de Seguretat Pública de Catalunya (ISPC) y la UB-Universitat de Barcelona, celebrado en el paraninfo de dicha Universidad.

ADSI da total apoyo a las nuevas generaciones de futuros gestores de la Seguridad Privada especialmente, para lo que ha creado una figura especial de **Afiliado ADSI**, que les permite, mientras cursen sus estudios, participar de sus múltiples actividades e introducirse en el sector de la mano de los expertos y consolidados profesionales del mismo. También reconoció en los Premios ADSI de la pasada semana al mejor expediente académico, que recayó en uno de los graduados de hoy, Enric Crespi Julian.

Agradecemos a l'Hble. Sra Núria Parlon Gil que hiciese mención expresa de tales circunstancias de ADSI en favor de las nuevas generaciones de profesionales de la seguridad en su discurso dedicado a los nuevos graduados.

En la imagen de pie, de izquierda a derecha, la Consellera d'Interior i Seguretat Pública, l'Hble. Sra. Núria Parlon Gil, Joan Guàrdia Olmos, Rector Magnífico de la UB, Eduard Zamora Peral, presidente de ADSI y Marta Roca Fina,



ADSI coorganiza con TAPA la Jornada de Seguridad en la Cadena de Suministros

Exitosa celebración de la Jornada en el Auditorio de la Asociación pro-huérfanos de Guardia Civil de c/ Príncipe de Vergara en Madrid, el 9 de octubre.

El evento en el que ADSI ha colaborado estrechamente en la organización por los lazos de relación con su asociación amiga, TAPA emea - Transportet Asset Protection Association, liderada en España y Portugal por FILIPE DE ALMEIDA, ha contado con la participación de los asociados de ADSI, Daniel García Caellas, Director de Seguridad de Desigual y Alejandro Fernández Palacios, Director de Seguridad de DHL Express Spain.

Agradecemos al SEPROSE-Servicio de Protección y Seguridad de Guardia Civil, y en especial al General de Brigada, Antonio Cortés Ruiz, de quien depende la unidad y que inauguró la Jornada, el Teniente Coronel Antonio Suárez Yáñez y la Capitán Mariluz Pérez González, su enorme colaboración para posibilitar la organización del evento.

En la imagen de la mesa, de izquierda a derecha, Filipe de Almeida (Responsable de TAPA en España y Portugal), Carmen Nickstat (Directora de Handling de Naeko Logistics), Daniel García Caellas y Alejandro Fernández Palacios. En imagen de pie, de izquierda a derecha, Daniel García Caellas, Eduard Zamora y Filipe de Almeida. ■



Security Forum 2025, con el foco puesto en la Seguridad 360

security forum

El punto de encuentro de los profesionales de la seguridad, [Security Forum](#) ya tiene fechas: **4 y 5 de junio de 2025**, en [Las Drassanes Reials](#). El mayor evento de seguridad B2B en Barcelona, impulsado por Peldaño Media Group y organizado por Cuadernos de Seguridad, y que contará con la colaboración especial del Ayuntamiento de Barcelona, vuelve una edición más para explorar el presente y futuro de la (ciber) seguridad.

En su duodécima edición, y bajo la temática "Seguridad 360", Security Forum vuelve para convertirse en un espacio para conectar en una [experiencia única de networking](#) en la que la seguridad privada, seguridad pública, seguridad física y ciberseguridad se unen para impulsar y potenciar una industria cada vez más resiliente.

Security Forum 2025: tendencias e innovación tecnológica

Con la experiencia de 11 ediciones, Security Forum, convertido en el **evento de referencia para marcas y profesionales**, volverá a convertirse en el escenario donde conocer las principales **tendencias e innovación tecnológica en el sector de la seguridad global**.

En esta edición, el **área de exposición** volverá a convertirse en el **escaparate de compañías punteras a nivel tecnológico y de innovación**. Los visitantes podrán encontrar **soluciones tech** aplicadas al ámbito de la **videovigilancia, integración de sistemas, seguridad física, control de accesos, protección contra incendios, ciberseguridad, protección contra robo e intrusión...**

Y de manera paralela una edición más tendrá lugar el **Congreso Security Forum 2025**, el día 4 de junio, donde los mayores **expertos en seguridad, tecnología y ciberseguridad**, compartirán todo su conocimiento y experiencia. ■



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? Facilitanos tus datos, remarcando que no eres socio.

Gracias por vuestra colaboración!



Estimados miembros de ADSI

Nos dirigimos a todos ustedes con motivo de nuestra incorporación a la Asociación con el carácter de patrocinadores.

Habíamos colaborado como conferenciantes y asistentes en jornadas de ADSI con anterioridad y ha sido la intensidad y calidad del trabajo desarrollado por la asociación, así como el clima cordial y humano en el que se desenvuelven las actividades lo que nos ha decidido a involucrarnos de manera más directa e intensa en la misma. Nuestro objetivo es contribuir desde la vertiente jurídica a potenciar el área de seguridad en los entornos empresariales y reforzar la figura del director de seguridad dentro y fuera del organigrama funcional de las compañías.

Quienes somos

RIBA-VIDAL Abogados nace en 1991 con vocación de asistencia legal a empresarios, consejeros y directivos en el ámbito de los negocios.

Pioneros en la utilización de criterios de inteligencia



jurídica, inicialmente en el proceso judicial y en la planificación jurídica estratégica, estos metodos desembocaron en la creación hace mas de 20 años de un área de trabajo específica de seguridad e inteligencia.

A día de hoy nadie discute que el área de seguridad e inteligencia es un pilar básico en la supervivencia de las empresas, junto a la ciberseguridad y el cumplimiento normativo("compliance"), materias todas estas que deberían estar coordinadas por la dirección de seguridad, y con un respaldo legal de especialistas en el materia.

Nuestro equipo está compuesto por más de 25 abogados, gran parte de los cuales ha desarrollado íntegramente su carrera profesional en el despacho, pero siempre ligados a la docencia y a la formación.

Nuestros servicios en materia de seguridad e Inteligencia

Asesoramiento jurídico a las áreas de inteligencia y seguridad.

- Asesoramiento jurídico en el diseño y la implantación de los departamentos de seguridad e inteligencia en las compañías.
- Asesoría permanente de cumplimiento normativo y desarrollo de protocolos de actuación y alerta temprana de riesgos.
- Defensa de los responsables de seguridad ante incidencias de ámbito civil, penal o administrativo.
- Asesoramiento personalizado a los profesionales de la seguridad en todas las materias jurídicas que les afectan.

Gobierno corporativo y compliance

Asesoramiento jurídico en la implantación de sistemas eficaces de gobierno corporativo, prevención de riesgos penales, control de cumplimiento normativo y gestión de riesgos.

- Buen gobierno corporativo y prevención de riesgos penales (Corporate Compliance) y cumplimiento en materia de defensa de la competencia.
- Asesoramiento en la preparación de certificación en la UNE 19601 de sistema de gestión de compliance penal e ISO 37001 de anticorrupción.
- Informe de auditoría e Investigación – Forensic.
- Asesoramiento canal de denuncias y corporate defense: asistencia jurídica.
- Formación a órganos de administración, directivos y órganos de prevención penal.
- Asesoramiento jurídico en Prevención del Blanqueo de Capitales y Financiación del Terrorismo (PBC-FT).
- Sostenibilidad y criterios ESG.
- Estado de Información no financiera.

Privacidad y ciberseguridad

Asesoramiento integral y personalizado en materia de protección de datos.

- Asesoramiento jurídico en la ISO 27001 de seguridad información y la ISO 27701 de privacidad.
- Defensa jurídica.
- Auditoria de Protección de Datos.
- Formación.
- Ciberdefensa.

- Gestión de crisis ante un ciber incidente y ataques de "raiding corporativo".

- Respuesta a incidentes y análisis forense.

Otros servicios

Mercantil, administrativo, penal, procesal, laboral, fiscal, tributario, arbitraje.

Agradecimientos

Desde Riba Vidal Abogados nos ponemos al servicio de los miembros de ADSI con el propósito de acompañar a los profesionales de la seguridad en el objetivo de potenciar y reforzar el desempeño de una labor que se ha convertido ya, en eje central de la actividad empresarial y ciudadana.

Y agradecer a la Dirección de ADSI por su acogida y por permitirnos formar parte de esta prestigiosa organización.

Nuestra web www.ribavidalabogados.com. ■





COLLBAIX refuerza la seguridad del Aeropuerto de Indianápolis con sus puertas antibalas



Las puertas modelo DIAMOND, instaladas en las instalaciones de un destacado operador logístico internacional en el Aeropuerto de Indianápolis, destacan por su capacidad para proteger áreas críticas gracias a un diseño certificado y probado contra múltiples amenazas. Desarrolladas según normativas de resistencia balística como EN 1522 (Europa), UL 752 y NIJ 0108.01 (EE. UU.), estas puertas garantizan protección frente a ataques directos, estableciendo un elevado estándar de seguridad que cumple con los requisitos de infraestructuras críticas.

La necesidad de resiliencia en infraestructuras críticas y el papel de COLLBAIX

El Aeropuerto de Indianápolis, como infraestructura crítica de alta afluencia y relevancia estratégica, requiere soluciones de seguridad de alto rendimiento para proteger la integridad de las personas, los bienes y garantizar la continuidad de las operaciones. Áreas de carga y puntos de acceso restringido deben estar protegidos contra diversas amenazas externas. La seguridad en este tipo de instalaciones demanda

proveedores que no solo cumplan con estándares técnicos internacionales, sino que también ofrezcan soluciones certificadas para entornos de alto riesgo.

Diseño adaptativo y versatilidad en la instalación

Además de su robustez, el modelo DIAMOND ha sido diseñado para integrarse eficazmente en sistemas de seguridad complejos. Su estructura permite un rendimiento óptimo en aislamiento y resistencia sin comprometer la funcionalidad operativa. Adaptables a entornos de alta actividad, estas puertas se incorporan sin dificultad en sistemas de seguridad existentes, facilitando una implementación ágil en infraestructuras críticas como aeropuertos y terminales logísticas.

Gracias a su diseño modular, la puerta DIAMOND puede configurarse para necesidades específicas, adaptándose a diferentes espacios y niveles de seguridad dentro de una instalación. Desde accesos externos hasta zonas de carga o puntos de tránsito crítico, este modelo aporta una capa adicional de protección física que refuerza los





sistemas de seguridad existentes, cumpliendo con los estándares internacionales.

Valor añadido: integración en la infraestructura de seguridad y monitoreo

La puerta DIAMOND no solo actúa como barrera física, sino que también se integra estratégicamente en la infraestructura de seguridad del aeropuerto. Su capacidad de conectarse con sistemas de monitoreo y control permite a los operadores disponer de una solución completamente integrada, proporcionando supervisión en tiempo real, esencial para respuestas rápidas ante eventos inesperados.

Al conectarse a los sistemas de seguridad, los responsables pueden controlar y monitorear el estado y funcionamiento de las puertas desde un único panel de control, optimizando la reacción ante intentos de

intrusión. Esta conectividad permite al aeropuerto mantener una visión completa y actualizada de sus niveles de seguridad, favoreciendo respuestas ágiles y eficientes ante cualquier incidencia.

El futuro de la seguridad en infraestructuras críticas: innovación constante ante la evolución de amenazas

El panorama de seguridad en infraestructuras críticas está en constante cambio; los métodos de ataque evolucionan rápidamente debido a avances tecnológicos y al ingenio de quienes buscan vulnerar los sistemas de protección. Para COLLBAIX, mantenerse a la vanguardia implica más que desarrollar puertas robustas; requiere una actualización continua y rigurosa de sus soluciones, sometiéndolas a ensayos de resistencia y adaptándolas a las últimas normativas internacionales de protección contra intrusiones y ataques balísticos.

Actualización continua y cumplimiento de normativas globales

Los modelos de seguridad de COLLBAIX, como la puerta DIAMOND, son el resultado de un exhaustivo trabajo de adaptación y mejora para cumplir con los estándares de las principales normativas de seguridad. En un contexto globalizado, donde las infraestructuras críticas deben cumplir con requisitos de seguridad en Europa y América, COLLBAIX ha logrado que sus productos cumplan con normativas estrictas de ambas regiones. Este enfoque garantiza que las puertas DIAMOND cuenten con certificaciones europeas (EN 1522) y americanas (UL 752



y NIJ 0108.01), cada una con protocolos y exigencias específicas en resistencia balística y protección contra intrusión.

Ensayos de resistencia: la clave para adaptarse a nuevas amenazas

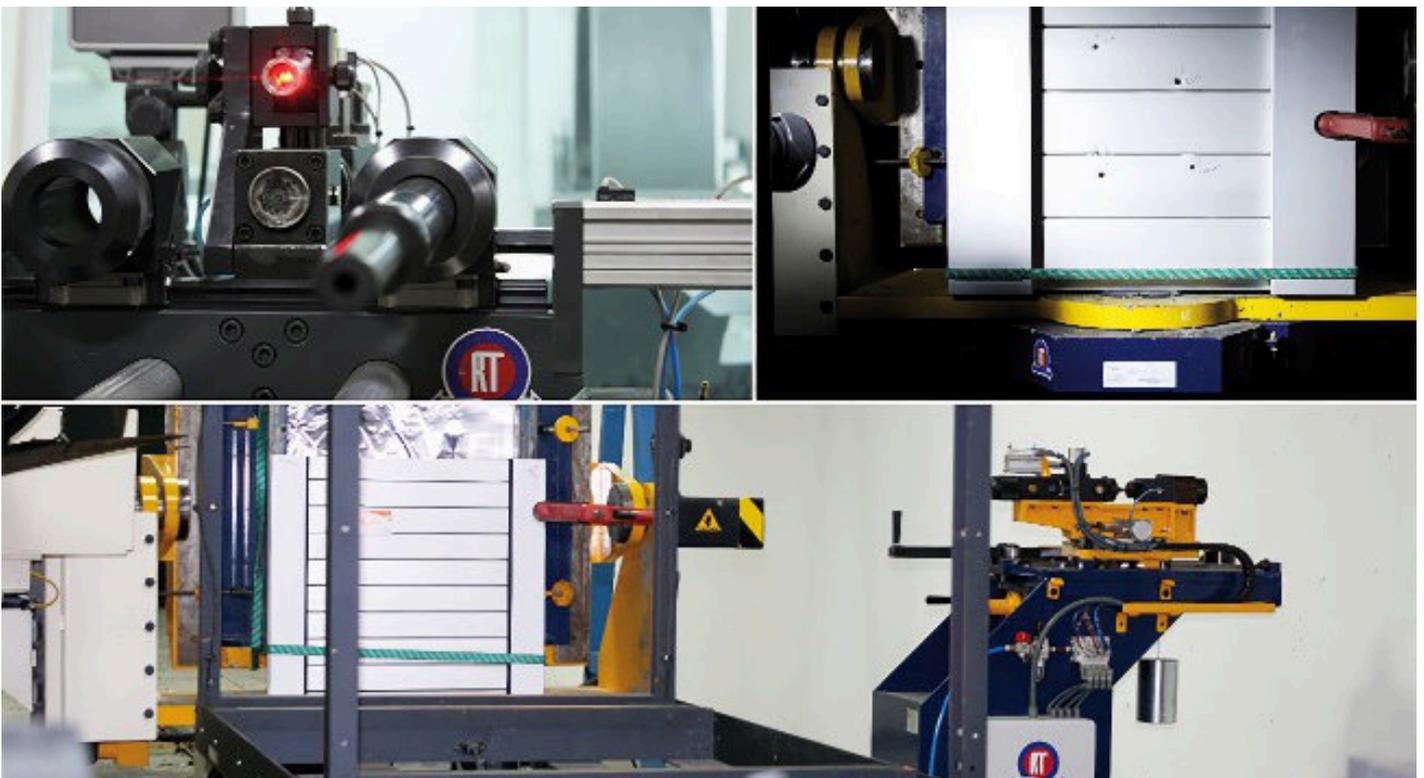
La innovación en COLLBAIX incluye una estrategia de ensayos periódicos que garantizan que sus puertas respondan a las últimas amenazas. Estos ensayos de resistencia evalúan el rendimiento de las puertas DIAMOND frente a intentos de intrusión y ataques balísticos cada vez más sofisticados, simulando escenarios reales de riesgo. Esto permite que las soluciones de COLLBAIX no solo cumplan con las normativas actuales, sino que se anticipen a posibles cambios en los requisitos de seguridad, manteniéndose un paso adelante frente a las amenazas emergentes.

Complejidad en el desarrollo: tecnología que responde a retos globales

Cumplir con normativas internacionales en seguridad

física representa un reto de diseño y producción que COLLBAIX ha asumido con rigor. Cada mercado y normativa implica desafíos técnicos únicos: en Europa, los estándares se enfocan en la resistencia estructural bajo condiciones extremas; en Estados Unidos, se valoran aspectos adicionales como la durabilidad frente a impactos repetidos y la respuesta balística en distintos escenarios. Para cumplir con ambos marcos, el equipo de ingeniería de COLLBAIX desarrolla soluciones que integran tecnologías de alta precisión y materiales de última generación, logrando adaptarse a diversos entornos de operación.

El compromiso de COLLBAIX con la actualización normativa y los ensayos de resistencia asegura que sus puertas no solo cumplan con los estándares globales actuales, sino que se adelanten a las futuras exigencias del mercado. La combinación de cumplimiento normativo, innovación y capacidad de adaptación convierte a COLLBAIX en un referente en la protección de infraestructuras críticas, ofreciendo productos que responden eficazmente a la evolución constante de las amenazas. ■





Las ciudades son cada vez más inteligentes y sostenibles gracias a iLOQ

Las ciudades actuales tienen que acoger a un número cada vez mayor de personas en áreas geográficas más pequeñas. Es esencial un cambio de perspectiva para satisfacer la creciente necesidad de:

- Servicios públicos fiables para mantener la infraestructura en funcionamiento.
- Hospitales para atender a los enfermos.
- Escuelas y campus para captar las mentes de la próxima generación.
- Lugares de trabajo que conecten e involucren a los empleados con su entorno.

Nuestras ciudades tienen que ser más inteligentes y sostenibles mediante el uso de soluciones digitales y la implantación de mayores niveles de tecnología.

¿Cómo contribuye iLOQ al desarrollo de ciudades inteligentes?

El propósito de iLOQ es hacer la vida accesible. Las soluciones de iLOQ están diseñadas para maximizar la seguridad, minimizar el tiempo de administración y el impacto en el medio ambiente, reducir los costes del



ciclo de vida y aumentar el valor de las propiedades.

Desde 2003, iLOQ ha venido desarrollando soluciones de cierre digital y acceso compartido móvil que ahora pueden verse en todos los sectores de una ciudad inteligente; en nuestras propiedades residenciales, viviendas para estudiantes, escuelas e instalaciones públicas, oficinas, hospitales y emplazamientos de infraestructuras críticas. Garantizan altos niveles de seguridad y capacidades de gestión de accesos sin precedentes, junto con costes de ciclo de vida competitivos y ahorros significativos, a propietarios de edificios, usuarios y poseedores de llaves.

Las soluciones de iLOQ no contienen pilas. Esto ahorra 100.000 kg de residuos de pilas al año, lo que las convierte en las más sostenibles del mercado. También ahorra a las empresas tiempo, dinero y el impacto medioambiental relacionado con los desplazamientos asociados a las actividades de mantenimiento.

¿Cuáles son las ventajas de las soluciones de iLOQ?

El sistema de cierre digital de iLOQ:

- Particularmente ideal para propiedades residenciales y



comerciales, para garantizar un flujo seguro y fiable de personas por el edificio - se puede programar una llave con los derechos de acceso para todas las puertas y áreas que son importantes para los usuarios.

- Las cerraduras funcionan con la energía cinética que se produce al introducir la llave: no se necesitan pilas ni cables, lo que reduce los costes de mantenimiento y elimina los desechos de pilas.

- Las llaves perdidas o robadas pueden bloquearse rápida y fácilmente, y sus derechos de acceso pueden reprogramarse de forma segura con una nueva llave.

- Los cilindros son fáciles de instalar y pueden adaptarse a cualquier cerradura moderna sin modificaciones.

- La comunicación de dispositivo a dispositivo permite que los datos (como una lista de llaves bloqueadas, limitaciones de tiempo, última hora, registros de auditoría y accesos de la llave) se actualicen a distancia y se compartan en ambas direcciones entre el software de gestión y los lectores, llaves y cerraduras de un edificio antes de que se desbloqueen las puertas.



- Amplia cartera de productos.

La solución móvil de compartición de accesos de iLOQ:

- La energía necesaria para confirmar los derechos de acceso y abrir las cerraduras proviene de un smartphone (no se necesitan baterías ni cables) reduciendo los costes de mantenimiento y eliminando los desechos de baterías.

- Los derechos de acceso pueden compartirse, actualizarse y cancelarse de forma instantánea a través de una aplicación que se ejecuta en un teléfono móvil. Esto elimina por completo los riesgos de uso indebido relacionados con las llaves físicas.

- Diseñado originalmente para proveedores de infraestructuras críticas (como empresas de producción y distribución de energía, servicios de redes de telecomunicaciones y centros de datos) y servicios inmobiliarios que tienen numerosos emplazamientos, un gran número de cerraduras y una enorme cantidad de llaves en circulación.

- Cada vez más propiedades residenciales y comerciales están adoptando soluciones móviles de acceso compartido a medida que la gente es más consciente de las ventajas de las soluciones sin llave.

- Funcionamiento fiable incluso en caso de corte del suministro eléctrico.

En el futuro, iLOQ se centrará en desarrollar soluciones digitales y de software que ofrezcan aún más posibilidades para crear entornos de vida y de trabajo más inteligentes. Esto garantiza no solo el crecimiento, sino, lo que es más importante, el crecimiento sostenible de nuestras ciudades. ■



Soluciones de Seguridad para el hogar: cajas fuertes de lujo y habitaciones del pánico

La seguridad personal y la protección de bienes de valor son prioridades crecientes para muchas personas, quienes buscan opciones que no solo ofrezcan una protección efectiva, sino que también se integren adecuadamente en sus espacios y se adapten a sus necesidades específicas. En este contexto, han surgido soluciones de seguridad de alta gama, diseñadas para brindar el máximo nivel de protección sin renunciar a la estética y la funcionalidad.

Entre los productos más destacados en esta categoría están las cajas fuertes de alta seguridad (desde grado IV hasta grado VI según la Norma Europea UNE-EN 1143-1), las habitaciones del pánico y las cajas fuertes de lujo para la protección de relojes de alta gama y otros artículos de valor.

A continuación, exploraremos las características, ventajas y funciones de estas opciones, que están redefiniendo el estándar de seguridad en el hogar.

Cajas Fuertes de Alta Seguridad: grados IV a VI

Las cajas fuertes de Grado IV hasta Grado VI representan la cúspide de la seguridad en lo que respecta a la protección de bienes. La clasificación de grado, regulada según la norma EN 1143-1 en Europa, asegura que cada nivel corresponde a una mayor resistencia contra intentos de robo y ataques.

Características

Las cajas fuertes de Grado IV a VI están construidas con materiales de alta resistencia, como acero reforzado que soportan ataques con herramientas de corte, taladro y hasta explosivos. Cada incremento en el grado representa una resistencia mayor, así como un nivel más elevado de tecnología aplicada a su mecanismo de cierre y estructura interna.

1. Resistencia certificada: estas cajas fuertes han pasado por pruebas rigurosas, y solo aquellas que superan todos

los protocolos de resistencia son certificadas con estos grados.

2. Sistemas avanzados de cerradura: Incorporan cerraduras electrónicas de alta tecnología, combinadas en ocasiones con cerraduras biométricas, que aseguran que solo las personas autorizadas puedan acceder a su contenido.

3. Aislamiento térmico: además, muchos modelos cuentan con sistemas de protección contra incendios, factores críticos cuando se almacenan objetos delicados como relojes de lujo, documentos importantes y obras de arte.

Estas cajas fuertes son especialmente útiles para



almacenar grandes sumas de dinero en efectivo, joyas de alto valor, documentos irremplazables y colecciones privadas que requieren de un alto nivel de seguridad.

Habitaciones del Pánico: Protección Integral y Personal

Las habitaciones del pánico son espacios seguros diseñados para proteger tanto a las personas como a sus bienes en situaciones de emergencia, tales como intentos de allanamiento, ataques o desastres naturales. Originalmente diseñadas como refugios de emergencia, hoy en día estas habitaciones están integradas en muchos hogares como una medida de seguridad adicional que proporciona un nivel completo de protección personal y familiar.

Características

Estas habitaciones de seguridad suelen personalizarse para adaptarse tanto a las necesidades de sus ocupantes como a las especificaciones del espacio en que serán instaladas. Sus principales características incluyen:

1. Estructura reforzada y blindada: las paredes, puertas y suelos de estas habitaciones están contruidos con materiales de alta resistencia, capaces de soportar impactos, explosiones y el uso de herramientas de corte y perforación.

2. Sistema de comunicación avanzado: para garantizar la conexión con el exterior, estas habitaciones están equipadas con sistemas de comunicación de emergencia independientes del resto de la casa, tales como líneas telefónicas dedicadas, acceso a redes de radio y cámaras



de vigilancia que permiten monitorear el exterior en tiempo real.

3. Suministro autónomo de energía y aire: las habitaciones del pánico cuentan con generadores de energía y sistemas de purificación de aire, lo cual permite a los ocupantes permanecer en el interior por periodos prolongados, asegurando su seguridad en situaciones extremas.

4. Acabados de lujo y diseño personalizado: este tipo de habitaciones no solo están diseñadas para ser funcionales, sino que también cuentan con acabados de lujo y decoración adaptada al gusto de sus propietarios, logrando una integración armoniosa dentro de la vivienda.

La función principal de una habitación del pánico es actuar como un refugio seguro donde los residentes puedan resguardarse y contactar a las autoridades hasta que la amenaza sea controlada, siendo un elemento fundamental en las propiedades de particulares que priorizan su seguridad personal y familiar.

Cajas fuertes de lujo para relojes de alta gama

Para los coleccionistas de relojes de alta gama, una caja fuerte convencional puede no ser suficiente. Los relojes de lujo no solo representan una inversión significativa, sino que también requieren condiciones especiales de almacenamiento para mantener su valor y funcionalidad. En respuesta a esta demanda, hemos desarrollado cajas fuertes especializadas que ofrecen una protección adecuada sin descuidar el diseño estético.



Características

Estas cajas fuertes combinan la tecnología de seguridad avanzada con diseños exclusivos y personalizables, ofreciendo un entorno seguro y elegante para el almacenamiento de relojes de lujo y otros bienes.

1. Rotores automáticos: estas cajas incluyen rotores que permiten que los relojes de movimiento automático se mantengan en funcionamiento, lo cual previene la necesidad de ajustes de hora y garantiza su precisión.

2. Diseño estético y personalización: diseñadas con materiales de lujo como cuero, madera noble y acabados en metales preciosos, que no solo protegen sino también exhiben los relojes con distinción.

3. Tecnología avanzada de seguridad: integran sistemas de apertura biométrica, cerraduras electrónicas y, en algunos modelos, mecanismos de reconocimiento facial o de voz, que ofrecen una experiencia de acceso cómoda y segura.

Este tipo de cajas fuertes también son adecuadas para almacenar otros artículos de valor, como documentos importantes y joyas, siendo ideales para particulares que desean combinar seguridad, lujo y funcionalidad.

Showroom Ferrimax

En nuestro showroom de Barcelona, ofrecemos un espacio exclusivo donde podrá conocer de primera mano nuestras soluciones de seguridad de alta gama. Aquí, podrá explorar en detalle nuestras cajas fuertes de Grado

IV a VI, habitaciones del pánico y cajas fuertes de lujo diseñadas especialmente para relojes de alta gama y otros objetos de valor. Cada producto está exhibido en un ambiente que combina seguridad y diseño, permitiéndole experimentar tanto su tecnología avanzada como sus acabados de lujo.

Nuestro equipo de expertos estará a su disposición para ofrecerle una atención personalizada y asesorarle en cada detalle, desde las características técnicas hasta las opciones de personalización y adaptación a su espacio. Visítenos en nuestro [showroom de Barcelona](#) y descubra cómo nuestras soluciones exclusivas pueden brindarle la máxima seguridad y tranquilidad. ■

Pide cita previa y descubre nuestro nuevo espacio exclusivo en el centro de Barcelona.

ferrimax.com/es/luxury

Gran Via de les Corts Catalanes, 623
08010 Barcelona





CURSO SUPERIOR



DIRECCIÓN DE SEGURIDAD DIGITAL Y GESTIÓN DE CRISIS

FORMACIÓN PARA NO TÉCNICOS

10%
Desuento Socios ADSI

TERCERA EDICIÓN

MÁS
INFORMACIÓN



UCAV
www.ucavila.es



MÁS
INFORMACIÓN



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

UNIVERSIDAD CATÓLICA DE ÁVILA

DIRECTOR: Dr. Alberto Barea Vera

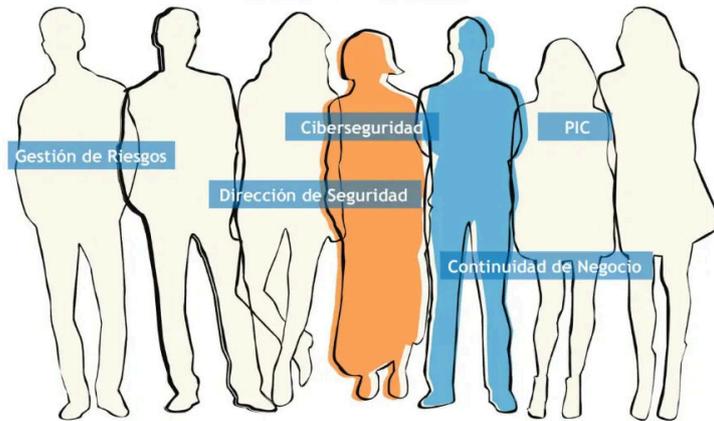
CODIRECTOR: Coronel José Luis Calvo Albero





**DESCARGAR
INFORMACIÓN**

CURSOS PARA LA ESPECIALIZACIÓN DE DIRECTIVOS DE SEGURIDAD 2024 - 2025



Aumento de la Profesionalización de la Seguridad GRUPO ESTUDIOS TÉCNICOS diseña e imparte desde 1988 convocatorias (cursos, seminarios, congresos, jornadas y presentaciones) para la formación, capacitación y especialización.

Dirigido a: Directores de Seguridad, Fuerzas y Cuerpos de Seguridad Pública, Jefes y Responsables de empresas de Seguridad, Ingenieros, Consultores, Técnicos y Prescriptores, Instaladores, mantenedores y operadores, Responsables de gestión y Profesionales, Usuarios de sistemas y servicios.

Gracias al acuerdo de colaboración entre GET y ADSI, los asociados a ADSI disponen de un 20% de descuento en Cursos bonificables. 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 23/24

[Enlace](#)



UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Master de Formación Permanente en Cibersecurity Management

[Enlace](#)



UNIVERSITAT DE BARCELONA

Máster en Dirección de Seguridad Privada

[Enlace](#)



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

[Enlace](#)



Grado de Criminología y Dirección de Seguridad

[Enlace](#)





Sesiones Técnicas AEINSE

Evaluación del riesgo en los proyectos de seguridad

Por Ivan Ballesteros Ballesteros
21 de noviembre de 2024 – 18:00h

Programa de la sesión

- ¿Cuál es el contexto de la evaluación de riesgos de seguridad?
- ¿Cómo aportar valor a partir de la evaluación de riesgos de seguridad?
- ¿Cuál es el papel del ingeniero de seguridad en la evaluación de riesgos?

[Regístrate pinchando sobre este enlace](#)



Esta sesión forma parte del programa de formación continua Sesiones Técnicas de AEINSE,



Revista Securitecnia.
Nº 509 Sep/Oct 2024.

[Enlace](#)



Revista Red Seguridad.
Nº 377 Jul/Sep 2024.

[Enlace](#)



"Lecciones Aprendidas de los Tatuajes en FCSE, FAS y Fuerzas Especiales", da continuación al anterior artículo publicado en la revista de ADSI del pasado mes de Septiembre.

[Enlace](#)



MINISTERIO
DEL INTERIOR

Balance de Criminalidad segundo trimestre 2024. Evolución de la criminalidad en España de los primeros seis meses del año por las Fuerzas y Cuerpos de Seguridad del Estado.

[Enlace](#)



El ministro José Manuel Albares, preside el acto de presentación del Plan Director de la Cooperación Española 2024-2027. PDF en el artículo

[Enlace](#)



Directiva NIS2 para cambiar la Ciberseguridad. Repercusión en las organizaciones.

[Enlace](#)



Siglo XXI: ¿Un nuevo orden mundial!... ¿Y un nuevo poder?. PDF en el artículo

[Enlace](#)



DSN

Reunión del Consejo de Seguridad Nacional - 15 de octubre 2024.

[Enlace](#)



¿Están España y la UE progresando adecuadamente hacia los objetivos europeos de la Década Digital 2030?

[Enlace](#)



Informe: El uso de las tecnologías en personas mayores, Edición 2023 - Datos 2022. PDF en el artículo

[Enlace](#)



ASA DE S. M. EL RE'

Conmemoración XIX aniversario de la Unidad Militar de Emergencias (UME) y XV aniversario de la entrega de la Enseña Nacional

[Enlace](#)

Port Aventura Park: entradas 2x1 para socios

La Dirección de Port Aventura Park, como deferencia hacia ADSI, nos ha facilitado unos cupones de descuento (2x1) para distribuir entre nuestros asociados.

Los socios de ADSI que quieran disfrutar de esta promoción podrán recibirlas en los próximos eventos de la asociación, si algún socio, por imposibilidad de acompañarnos en los eventos presenciales, podrá contactar vía mail con nuestra Vicepresidenta, Elvira Márquez, a la siguiente dirección: vicepresidente@adsi.pro.

Se adjudicará un máximo de 2 entradas por petición y serán atendidas por orden de llegada del mail y hasta fin de existencias.

La Junta Directiva de ADSI agradece a la Dirección de Port Aventura Park este detalle con nuestra asociación y recomienda a todos visitar estas instalaciones lúdicas, uno de los mejores destinos de ocio familiar de Europa. ■



La venganza de la geografía: Cómo los mapas condicionan el destino de las naciones



ROBERT D.
KAPLAN



La venganza
de la geografía



La geografía cambia el destino de las naciones



Autor: Robert D. Kaplan

En el pasado, el contexto geográfico y las realidades naturales de los imperios y las naciones siempre fueron determinantes en los conflictos internacionales. Así ha sido hasta ahora y así será en el futuro, por encima de cualquier condicionante que la globalización imponga. Esa es la sorprendente y brillante tesis que se postula en *La venganza de la geografía*. Serán la distribución del

espacio, el clima y otras circunstancias exclusivamente físicas los parámetros que definirán el devenir de las diferentes regiones mundiales durante el próximo siglo.

Robert D. Kaplan, uno de los más agudos y reputados analistas políticos de la actualidad, repasa en este impactante libro las teorías y los descubrimientos geopolíticos más recientes, así como también examina algunas reveladoras páginas de la historia, para a continuación proponer una lectura global del mundo en que vivimos y definir cuál será el posterior desarrollo de los acontecimientos en el escenario internacional.

Sobre el autor

Robert D. Kaplan (Nueva York, 1952) es periodista, analista geopolítico, viajero y escritor. Redactor y colaborador habitual en prensa especializada y otros medios, ha trabajado como corresponsal en diversos países durante más de dos décadas, ha sido profesor de Seguridad Nacional en la Academia Naval de Annapolis y miembro del consejo asesor del Departamento de Defensa estadounidense. Gracias a sus ensayos sobre relaciones internacionales y el poder en Estados Unidos, la revista *Foreign Policy* lo ha incluido en la lista de los Top 100 Global Thinkers en dos ocasiones. Entre sus obras destacan *Fantasmas balcánicos*, *La anarquía que viene* y *El retorno de la antigüedad*, así como *El retorno del mundo de Marco Polo* y su fundamental *La venganza de la geografía*, estas dos últimas publicadas por RBA. ■





ADISI

asociación de directivos
de seguridad integral