NEWS ADSI FLASH
www.adsi.pro

## Índice



# Cena Anual de ADSI 2016

## Jueves 24 de noviembre de 2016

## 20:00 h.

## Cúpula Centro Comercial Arenas de Barcelona

Gran Vía de les Cortes Catalanes, 373-385

**Un año más ADSI celebrará el evento de mayor relevancia de nuestra Asociación, la Cena Anual de ADSI, este año aún si cabe con mayor carga emotiva, pues celebramos además nuestro 20 aniversario.**

**Será un honor para esta Junta Directiva celebrar tan señalado evento acompañado de Socios, Patrocinadores y amigos de ADSI**

1996 - 2016

20 ANIVERSARIO

Asociación de Directivos de Seguridad Integral


www.adsi.pro
somos
FUTURO
ADSI
Asociación de Directivos
de Seguridad Integral
Trabajando para la Seguridad
Trabajando para la Seguridad
1996 - 2016
20
ANIVERSARIO
Visita nuestra web www.adsi.pro e infórmate
"Martes con..."
Participa en nuestras jornadas organizadas en
Barcelona y otros puntos de España

## Nuestros Patrocinadores





















# Cena Anual de ADSI 2016

## Jueves, 24 de noviembre, 20:00 horas.
## Cúpula Centro Comercial Arenas de Barcelona

1996 - 2016
20 Asociación de Directivos de Seguridad Integral
ANIVERSARIO

El jueves 24 de noviembre, un año más, **ADSI** celebrará el evento de mayor relevancia de nuestra Asociación, la **Cena Anual de ADSI**, este año aún con mayor importancia pues celebramos además nuestro **20 aniversario**.

La **Cena Anual de ADSI** se constituye como el mayor punto de encuentro de **socios, patrocinadores** y amigos de nuestra Asociación.

En el transcurso de la Cena se efectuarán los siguientes actos:

- Entrega de los **Premios ADSI 2016**
- Discurso del **Presidente de ADSI, Don. Francisco Poley**

Tras la cena dispondremos de un espacio donde tomar una copa relajadamente y comentar nuestras experiencias de este año y los planes de futuro para el siguiente.

Para evitar que el control de acceso al acto pueda retrasar el inicio de los mismos, os rogamos la máxima puntualidad. El mostrador de acreditaciones se abrirá a las 19:30 h, media hora antes del comienzo del aperitivo.

**Precios de asistencia a la Cena Anual 2016**:
- **Socio de ADSI** **60,00 €**
- **No Socios de ADSI** **85,00 €**

***INSCRIPCION DE SOCIOS A LA CENA ANUAL***

Rogamos a todos los socios de **ADSI** que deseéis asistir a este importante evento de nuestra Asociación, nos lo comuniquéis hasta el **21 de NOVIEMBRE**.

Para ello pulse en INSCRIPCION y rellene el formulario que aparece:

→ ***INSCRIPCION***

Seguidamente recibirán un mail de confirmación.

Como siempre, emitiremos el correspondiente cargo por el evento para facilitar los trámites a nuestros asociados.

***INSCRIPCION DE NO SOCIOS Y EMPRESAS A LA CENA ANUAL***

Aquellas personas, profesionales, amigos o acompañantes que no sean Socios de ADSI, así como empresas que deseen asistir a **la Cena Anual**, **pueden dirigir su petición de reserva de plaza, o de mesas por parte las empresas, hasta el 21 de NOVIEMBRE**, a los correos electrónicos:

**Daniel Páez:** secretario@adsi.pro
**Emilio Herrero:** tesorero@adsi.pro

Indicando en el asunto del correo *"Cena Anual ADSI 2016"* y adjuntando el correspondiente justificante del pago del importe de la cena.

El pago deberá realizarse a la siguiente cuenta bancaria de la Asociación:

**CAIXA D'ENGINYERS ES56 3025 0004 3314 3323 5294**

Indicando como referencia ***Inscripción cena Anual ADSI 2016***, haciendo constar nombre y apellidos de las personas inscritas, o bien el número total de plazas reservadas, cuando se trate de empresas que todavía no conozcan los datos de sus invitados.

CUPULA EVENTS

# Crónica Martes con... Los Presidentes de ADSI

Isidoro Méndez
*Vocal ADSI*

El pasado martes 08 de noviembre se llevó a cabo el anunciado *"Martes con..."* Los Presidentes de **ADSI**.

Pudimos contar con la privilegiada presencia de los expresidentes **D. Santiago Sicart, D. Juan Vilanova y D. Eduard Zamora**, así como con el actual Presidente **D. Francisco Poley**.

Todos ellos hicieron un relato de lo que significó su paso por la Presidencia de **ADSI**, sus experiencias, sus anhelos, aquellos logros alcanzados y los que se quedaron en el tintero, también nos enriquecieron con algunas anécdotas que arrancaron espontaneas carcajadas de los allí asistentes.

Pero no solo hicieron un repaso de lo que fue su presidencia, también formaron un relato cronológico de lo que ha sido **ADSI** en estos veinte años de trayectoria, un relato lleno de sacrificio y tesón de aquellos primeros 39 socios fundadores allá por el año 1996

Se repasaron los inicios, difíciles, como todo lo que se construye desde la nada, los primeros años de andadura, las primeras reuniones, los primeros locales con la sensación de clandestinidad que se daba por aquel entonces, los primeros objetivos y las líneas maestras de lo que querían, o más bien soñaban, en conseguir con esta Asociación, con la unión de los Directivos de Seguridad.

Y así nació **ADSI** hace ahora 20 años.

Los expresidentes siguieron relatando los años posteriores de la Asociación, las metas que se fueron alcanzando, como poco a poco se fue influyendo en la Administración, la relación con la Seguridad Pública y como persona a persona se fueron alcanzando cuotas de asociados cada vez mayores, llegando hasta los casi 400 Socios que forman hoy en día **ADSI**.

Hicieron hincapié en como nacieron los dos elementos que hoy en día distinguen claramente a **ADSI** del resto de asociaciones del sector, los célebres "Martes con..." y la prestigiosa revista News ADSI Flash, por aquel entonces llamada ADSI últimas noticias, nos recordaron lo que cuesta el llevar a cabo cada una de estas ramas de **ADSI** y el impagable tiempo invertido por todas aquellas personas que han tenido responsabilidad en ambas.

También hicieron un repaso a la trayectoria del resto de expresidentes que en un momento u otro estuvieron al frente de **ADSI**, así como de los Secretarios o Tesoreros, todos ellos con una extraordinaria dedicación y sacrificio para con el bien de **ADSI**.

La jornada fue llegando a su fin con la intervención de **Ricardo Domingo**, Defensor del Socio de ADSI, que estuvo de lo más acertado al definir con unas pocas palabras la encomiable labor de cada uno de los ponentes.

Las interacción del resto de asistentes en modo de preguntas dio por finalizada esta enriquecedora jornada que sirvió para que los más jóvenes conocieran un poco mejor lo que significa **ADSI** y para que los más veteranos rememoraran con nostalgia el pasado de la Asociación.


Como no podía ser de otra forma, todos los allí asistentes compartimos un pequeño ágape donde continuamos con los recuerdos, las sonrisas cómplices y la camaradería de la que siempre se ha hecho gala en **ADSI**.

# Bioseguridad; presente y futuro

Roberto Álvarez Díez
*Especialista en defensa nuclear, biológica y química*
*Socio de ADSI*

Cada vez más oímos hablar de bioseguridad. Esta tendencia se ha disparado a partir de la crisis del Ébola y con la llegada del virus Zika. Pero, ¿sabemos qué es? ¿Sabemos las implicaciones que conlleva?

Nos imaginamos que la bioseguridad debe tener algo que ver con laboratorios biológicos, con industrias farmacéuticas, con bioterrorismo, con microorganismos patógenos, con enfermedades emergentes, industria alimentaria, etc.

Pero la **bioseguridad** es un concepto amplio y multidisciplinar, y está dirigido a la protección de los seres vivos y del medio ambiente. Podría decirse que es el conjunto de **normas y medidas preventivas destinadas a mantener el control sobre los factores de riesgo derivados del material biológico**.

La **bioseguridad es gestión del riesgo**, prevención o mitigación del mismo, en tanto que estos riesgos inciden en la vida humana, y en aquello que posibilita la vida humana, como es su entorno y su alimentación. Por tanto, hay múltiples aplicaciones de la bioseguridad en sanidad animal y sanidad vegetal, no solo en sanidad humana.

Los factores de riesgo relacionados con el material biológico **abarcan aspectos y actividades muy diversas** como la manipulación y el uso confinado, la producción, la modificación, el almacenamiento, la custodia, la comercialización, la liberación al medio ambiente (controlada o no), la exportación y la importación, el transporte, la trasferencia, y la destrucción o eliminación de los agentes biológicos y sus productos directos e indirectos, modificados genéticamente o no.

Estas actividades son una muestra de la multidisciplinariedad que conforma la bioseguridad como concepto amplio y genérico. Todas estas actividades tienen el denominador común de incorporar factores de riesgo relacionados con el material biológico en su actividad y normal desarrollo. Todas convergen en el mayor o menor riesgo biológico.

Por eso en 2011 se crea en España la **Asociación Española de Bioseguridad (AEBioS)**, una asociación sin ánimo de lucro fundada para reunir en un mismo foro a profesionales para tratar temas de bioseguridad y dar soporte a sus miembros, y así intentar aumentar los conocimientos en esta área, intercambiando experiencias e inquietudes.

Esta joven asociación ha celebrado el pasado 17 y 18 de octubre, esta vez en Bilbao, su III Congreso Nacional de Bioseguridad y Biocontención.

Quien les escribe estas líneas es miembro de AEBioS al igual que también lo es de **ADSI**, pero el motivo de mi presencia en el III Congreso Nacional de Bioseguridad y Biocontención fue estrictamente profesional, ya que mi jefe suele estar sensibilizado con las cuestiones de bioseguridad y comprende como yo la necesidad de que la Administración para la que trabajamos esté también presente en estos eventos tan importantes. Desde estas líneas quiero agradecer su ayuda.

Para comprender mejor el alcance y la importancia de AEBioS en España, en las siguientes líneas trataré de hacer una breve crónica de éste congreso único a nivel estatal, donde quedará evidenciada la variedad de ámbitos y diferentes puntos de vista que comparten ese nexo común llamado **riesgo biológico**.


Alguno de los perfiles más habituales en los miembros de AEBioS son el de expertos en cualquiera de los diferentes ámbitos relacionados ya dichos, como por ejemplo catedráticos, doctores, profesores, investigadores, técnicos, prevencionistas, directivos, asesores, etc. Los campos técnicos pueden enmarcarse en cualquiera de las especialidades o variantes de la medicina, veterinaria, biología, microbiología, farmacia, biotecnología, terapia génica, consultoría, logística, diseño y construcción, mantenimiento, prevención de riesgos laborales, etc., etc.

Son, en definitiva, personas que desarrollan su actividad profesional asumiendo un rol que frecuentemente incluye la toma de decisiones y la asunción de responsabilidades.

Vemos que existe un evidente paralelismo entre **ADSI** y AEBioS. Los objetivos de ambas asociaciones sin ánimo de lucro son bastante similares. Ambas buscan el fomento y la promoción del intercambio voluntario de experiencias, informaciones, estudios, ideas, y conocimientos, la organización de reuniones, congresos, conferencias, y exposiciones. Todo con el fin de **compartir y difundir el conocimiento especializado** y relacionado con sus respectivas especialidades.

Ambas asociaciones cuentan con apoyo de patrocinadores y con el aval de organizaciones internacionales. Ambas asociaciones son el referente en sus respectivos campos para todo el territorio nacional.

Así, en el congreso se trataron temas de lo más especializado en el campo de la bioseguridad, algunos de ellos totalmente desconocidos fuera de ése círculo tan exclusivo. Se habló de la formación en bioseguridad en el ámbito universitario y en el ámbito profesional, haciéndose especial mención en la necesidad de estandarizarla y reglarla en el primer ámbito, y certificarla profesionalmente en el segundo ámbito.


Al respecto, puedo decir que en España no abunda la formación seria y especializada en bioseguridad, aunque la tendencia está siendo unificar criterios y contenidos para conseguir (quizás con el tiempo) una titulación universitaria oficial de grado o de master. Y sobre la certificación profesional, España a través de AEBioS se está acogiendo a las certificaciones oficiales que otorga la Federación Internacional de Asociaciones de Bioseguridad (IFBA), de manera que es posible que dentro de un tiempo aquél que opte a ciertos puestos de trabajo que impliquen riesgo biológico, deberá estar en posesión de la certificación profesional oficial que le habilita y capacita a ocupar dicho puesto.

En el mundo de la seguridad privada, en cambio, podemos decir que llevamos bastante ventaja en ambos sentidos, ya que está todo más avanzado y reglado tanto en el campo de la formación universitaria oficial como en el de las certificaciones profesionales que permiten, habilitan y capacitan para el desarrollo de la actividad profesional en todas y cada una de sus especialidades.

Otro de los temas punteros actualmente en bioseguridad y que ocuparon varias ponencias del congreso, es del análisis del riesgo enfocado a todo lo que rodea al material biológico, frecuentemente medidas de biocontención que se expresan a través de estructuras arquitectónicas especiales, proyectos de ingeniería aplicados, equipos especiales, procedimientos operativos y de validación de procesos, etc., etc. En definitiva, todo aquello que es necesario para trabajar con el material biológicamente peligroso con las máximas garantías de seguridad para el personal, y sin que exista la posibilidad de que dicho material peligroso salga del lugar del que se encuentra (ni voluntaria ni involuntariamente).

Llegados a este punto quiero matizar dos conceptos importantes. Como he dicho más arriba, la bioseguridad comprende muchos aspectos, entre los cuales está la bioprotección. La diferencia básica está en que la **bioseguridad (biosafety)** son las medidas adoptadas para proteger a las personas de los microorganismos peligrosos. Por otra parte, la **bioprotección (biosecurity)** son las medidas adoptadas para proteger a los microorganismos de las personas peligrosas (robo, distracción, sabotaje, etc.).

El nivel de bioseguridad de una instalación se clasifica en 4 niveles. Internacionalmente se conoce por sus siglas en inglés BSL (biosafety level), siendo el BSL1 el más bajo y el BSL4 el más alto. En España existen más de una cincuentena de centros con BSL3 (sin contar con los centros hospitalarios que también cuentan con laboratorios BSL3). No existe ningún centro con BSL4 en España, pero sí algunos BSL3 que tienen medidas adicionales añadidas a las que les marca la normativa para poder ser BSL3.

Estos centros tienen unos requerimientos muy específicos y concretos para cada nivel, que vienen marcados por la legislación nacional e internacional. Obviamente los de nivel más alto (BSL3 y BSL4) son los más complicados de diseñar, construir, poner en marcha y mantener. Requieren de elevadísimos presupuestos para ello, pero son absolutamente necesarios para realizar de manera segura tareas de investigación y desarrollo, diagnóstico, experimentación, etc.

Un ejemplo de la necesidad de estas instalaciones lo tenemos en la desafortunada crisis del ébola que tuvimos que pasar no hace tanto en España, ya que solo y únicamente pueden realizarse las pruebas para este tipo de enfermedades en estas instalaciones especiales. Cualquier otra enfermedad peligrosa para el ser humano que se pueda transmitir de animales a seres humanos sólo puede gestionarse en este tipo de instalaciones de biocontención. Los patógenos se clasifican también en 4 grupos de riesgo (GR) según la peligrosidad de las enfermedades que causan y las posibles variables que pueden intervenir e influir en el riesgo al manipularlos y trabajar con ellos. Van desde el GR1 hasta el GR4, donde se encuentran, entre otros agentes biológicos peligrosos, aquellos que causan fiebres hemorrágicas como el ébola.

Este tipo de instalaciones suponen un auténtico desafío técnico, arquitectónico, de diseño y de gestión.

Precisamente, varias de las ponencias estuvieron relacionadas con la gestión del ébola en España en varios de sus aspectos. Destacando las lecciones aprendidas en lo

relativo a las salas de aislamiento para pacientes altamente infecciosos, que igualmente deben ser instalaciones con capacidad de contención biológica para impedir la salida al exterior de las enfermedades y evitar su transmisión.

También tuvo especial relevancia la adaptación especial que necesitaron los diferentes transportes de los afectados hasta el hospital de referencia. Como sabemos, se tuvo que aprender a marchas forzadas en todos los aspectos directos e indirectos en los que la crisis incidió; desde la gestión mediática de la comunicación, pasando por la adaptación de habitaciones de aislamiento y el diseño de las nuevas, las adaptaciones del transporte sanitario, la descontaminación segura de espacios, los equipos de protección individual, etc., etc.

Se trataron también ponencias sobre actualidad de otras enfermedades emergentes y reemergentes, como el síndrome respiratorio de oriente medio MERS, la gripe aviar H5N1, virus del Zika, virus del Chikungunya, virus de la fiebre del Valle del Rift y otras fiebres hemorrágicas, etc.

Igualmente se trataron temas tan específicos como la cría, el cuidado, el tratamiento y la gestión de los seres vivos que participan en la transmisión de algunas de estas enfermedades, tanto a seres humanos como a animales y viceversa. Generalmente se trata de artrópodos como mosquitos y garrapatas. Hay que contar con la presencia añadida de animales diana con los que comprobar la competencia vectorial de dichos artrópodos y verificar la eficacia de la infección que se ocasiona según sea el tipo de ganadería cuya protección se está investigando (avícola, ovina, porcina, etc., etc.). Dicho de otro modo, se crían insectos para luego infectarlos de manera controlada en el momento adecuado con las enfermedades de interés, y posteriormente hacer que infecten al ganado. Todo esto se lleva a cabo en estas instalaciones de bioseguridad y biocontención mediante estrictas medidas procedimentales de trabajo, de control y de gestión.

Relacionado directamente y enlazando con lo anterior, se habló también en varias ponencias de la cuestión de los seguros obligatorios de responsabilidad civil para accidentes que pueden tener que afrontar en estas instalaciones. Pensando solamente el ejemplo de la crisis del ébola, hay muchos frentes que cubrir ante el riesgo biológico: por ejemplo el personal médico y de enfermería, el de los servicios de limpieza, el de los transportes, el tipo de enfermedades con las que deba tratar y un largo etcétera de variables.

Dado que hay obligación de notificar a las compañías aseguradoras la temporalidad de cada persona en cada centro para cada tarea, proyecto o trabajo, se planteó la complicación que supone la gestión constante de estos trabajos de corta duración pero abundantes en algunos de estos centros, así como los costes que hay que afrontar para estas coberturas, recordemos de alto riesgo para la salud de los trabajadores. Pero esta es otra de las singularidades inherentes a este tipo de centros y profesiones.

Creo que el III Congreso Nacional de Bioseguridad y Biocontención fue un evento destacado no solo por la importancia de su alcance nacional, sino también por lo específico de sus temas de interés, y por el perfil de los asistentes y ponentes; la gran mayoría personalidades de acreditada reputación y dilatada experiencia, y con una larguísima trayectoria a sus espaldas en el campo de la bioseguridad.

Lo cierto es que por suerte o por desgracia, cada vez resuena más en los medios de comunicación y en boca de muchos, la palabra *bioseguridad*. Ya no solo se limita a los que se dedican a ello en el interior de los laboratorios, sino que parece que va extendiendo sus tentáculos hacia muchos sitios diferentes a medida que la sociedad avanza y evoluciona.

Puede que en años venideros esta tendencia aumente sustancialmente. Puede que en un futuro próximo la palabra bioseguridad nos sea más familiar de lo que lo es ahora. Pero por fortuna para todos esto ya lo sabe AEBioS, y hace tiempo que se ha remangado y se ha puesto a trabajar.

# ¿Estamos preparados para el maremoto que viene?

Jesús Cañas
*Fuente: EL PAÍS*

**España ya cuenta con un sistema de alerta de tsunamis, pero los expertos denuncian la falta de planes de actuación y formación para una catástrofe considerada tabú por su efecto alarmista sobre el turismo**

El capitán de granaderos Manuel Boneo actuó por puro instinto. Una muchedumbre aterrorizada peleaba por salir de Cádiz cuando ordenó cerrar la puerta de la muralla de la ciudad. Fue capaz de vislumbrar lo que iba a ocurrir minutos después: una enorme ola engullía el istmo que conecta Cádiz a tierra y que justo pretendían atravesar en su huida esos centenares de personas. A esa ola le siguieron cuatro más de unos 15 metros de altura, originadas por un devastador terremoto con epicentro al oeste del Cabo de San Vicente y una magnitud 9 en la escala de Richter. Ese 1 de noviembre de 1755, Cádiz acababa de sufrir el que todavía es el último gran tsunami de Europa y que la historia consagró bajo el nombre de maremoto de Lisboa, en alusión a la ciudad que resultó más destrozada. Hoy, tras cuantiosos daños y miles de muertos en Portugal, el sur de España y el norte de África, las preguntas son evidentes: ¿Cuándo se repetirá? Y si eso ocurre, ¿estaremos preparados?

A la primera cuestión, la catedrática de Geofísica y Meteorología en la Universidad Complutense de Madrid, Elisa Buforn, responde con claridad: "No se puede predecir, aunque sí prevenir. Lo que decimos los sismólogos es que donde hubo terremotos los habrá y donde no, puede que los haya". "La Tierra es como un gran móvil que se carga de energía después de cada terremoto. 261 años después no sabemos cuánta energía se ha acumulado ya. Podría ocurrir ahora mismo", sentencia José Antonio Aparicio, presidente del Instituto Español para la Reducción de los Desastres (IERD), una entidad no gubernamental surgida para fomentar la divulgación ante las catástrofes. Con esa premisa, la necesidad de prevención y concienciación se hace evidente, "aunque todavía queda mucho por recorrer", como añade Aparicio. De momento, este 5 de noviembre se celebró, por primera vez, el Día Mundial de Concienciación sobre los Tsunamis, fijado por la Asamblea General de las Naciones Unidas.

En España, el riesgo de un eventual tsunami provocado por un terremoto viene determinado por el gran borde existente entre la placa euroasiática y la africana, que discurre cercano al Golfo de Cádiz, el Estrecho de Gibraltar y las Costas de Argelia. Los movimientos entre ambas placas originan riesgo de maremotos en toda la costa española que va desde el sur occidental hasta las costas de Cataluña. Sin embargo, la peligrosidad es distinta, debido a que el comportamiento de las fallas en el Mediterráneo y el Atlántico también lo es. Tal y como explica Javier Benavente, director general de Investigación de la Universidad de Cádiz, la primera zona "es bastante activa tectónicamente, sin embargo, los tsunamis son más pequeños". Eso se debe a que, frente a las costas de Argelia, existen fallas de desgarre en las que los bloques tienen desplazamientos horizontales y paralelos. Fue el caso del terremoto de 2003 que provocó olas de hasta dos metros en el sur de Mallorca.

## El frente Atlántico, el más expuesto

Frente a ello, en el Atlántico, los maremotos son "menos frecuentes, pero mucho fuertes", como reconoce Benavente, debido a que se trata de fallas normales o inversas en las que los bloques se mueven verticalmente y son capaces de desplazar grandes columnas de agua. De hecho, en el artículo científico **Revisión de fallas tsunamigénicas en el Golfo de Cádiz**, el investigador José A. Álvarez-Gómez lo deja claro: "La zona es una de las de mayor riesgo de tsunami de Europa, en el pasado ya ha generado tsunamis de gran importancia y las estructuras tectónicas activas recopiladas aquí demuestran su potencialidad". Mauricio González, científico del Instituto de Hidráulica Ambiental 'IH Cantabria' estima que, en ese punto se han producido maremotos "cada 300 o 400 años, aunque no existe una certeza y podría repetirse mañana mismo".

Y si en ese mañana se produjese la catástrofe, Buforn cree que "las consecuencias serían mucho peores" que en 1755. González refrenda esta previsión: "El nivel de riesgo no viene

solo determinado por el tamaño de la ola si no porque ataque un punto más o menos vulnerable. Hoy, en la costa hay mucha más población y edificaciones". Se estima que el evento sísmico de 1755 dejó unos 100.000 muertos entre Portugal, Marruecos y España. De ellos, 1.275 fallecieron en las costas españolas. "La mayoría eran pescadores y salineros, los que en ese entonces estaban a pie de costa. Hoy serían muchos más los afectados", apunta Aparicio.

Ante la necesidad de estar preparados para una catástrofe de tal magnitud, desde la UNESCO se impulsó la puesta en marcha en Europa del sistema de alerta temprana de tsunamis (NEAMTWS), integrado por cinco centros europeos que emiten alertas desde Grecia, Francia, Italia, Portugal y Turquía. En el caso de España, se designó al Instituto Geográfico Nacional (IGN) -ya encargado de gestionar alertas de terremotos- para formar parte de esta red europea de alertas. Desde hace un año, cuando detecta un terremoto con potencial de generar un tsunami emite una primera alerta "en menos de cinco minutos", según explica Juan V. Cantavella Nadal, investigador del IGN. Normalmente, eso ocurre cuando tiene más de 5,5 de magnitud y tiene un epicentro marino o cerca de la costa.

### Un plan en fase inicial

Este primer avance se completa con nuevas informaciones procedentes, por ejemplo, de mareógrafos cercanos. A su vez, los datos obtenidos se cruzan con una base de datos que está implementando el IH Cantabria en el que se recogen 5.000 posibles simulaciones de altura de ola y tiempo de llegada, según el epicentro y la magnitud. "Es un sistema que está dando sus primeros pasos y aún queda mucho por hacer", reconoce Cantavella. González es más duro y denuncia que el IGN "realizó una gran labor a coste cero, ya que no tuvo asignación presupuestaria del Estado, como sí ocurrió en el resto de países".

Se supone que si, tras las primeras averiguaciones, la alerta se mantiene, el IGN la deriva a Protección Civil para que la canalice las Comunidades Autónomas y municipios afectados. Desde que se registra el temblor hasta la llegada de la primera ola, el margen para evacuar es variable, pero rara vez superior a una hora. Son justo esos minutos críticos los que aún están pendientes de coordinación. Tras el Real Decreto para el desarrollo de planes de actuación en el caso de maremotos, de noviembre de 2015, cada comunidad autónoma debe desarrollar su plan especial con estudios preliminares de riesgos, zonas inundables y planes de emergencia.

Fue justo lo que González hizo en el marco del proyecto europeo Transfer que perseguía desarrollar metodologías y guías aplicables a zonas de riesgo, como Cádiz o Baleares. Sin embargo, aún no se ha desarrollado esta fase autonómica, de ahí que Aparicio dude de que hoy se pueda canalizar efectivamente una alerta a la ciudadanía. "Vamos retrasados en esto porque los políticos suelen pensar que supone crear una alerta innecesaria en zonas de afluencia turística. Sin embargo, la gente va a Hawái y ve carteles en las playas alertando de este riesgo y no por eso desciende su turismo", añade.

### Sin educación ni autoprotección

El productor Fernando Arroyo lleva meses enfrascado en la realización del documental **La Gran Ola**, para el que ha entrevistado a 40 expertos en la materia. Su idea es estrenarlo la próxima primavera, aunque ya adelanta las conclusiones personales a las que ha llegado tras la grabación: "Existe un cúmulo de incompetencia y miedo con este tema". "En España falta educación, formación y entrenamiento en casos de maremotos. En general, la gente no sabría qué hacer ante una alerta así. Como no se está preparado se genera una angustia lógica", reconoce González.

Buforn comparte el planteamiento: "En el colegio, a todos los niños les educan sobre cómo actuar en caso de incendio, pero no en caso de un terremoto o maremoto". De ahí que Aparicio crea que hay que transmitir a la ciudadanía conocimientos básicos como que, en caso de tsunamis, la huida no es la mejor opción: "Puedes verte atrapado en tu coche en una zona inundable. Lo mejor es la evacuación vertical, subir a una zona alta o a las segundas y terceras plantas de un edificio".

En 1755 fue justo eso lo que hicieron muchos gaditanos, guiados por el instinto. Hubo incluso un sacerdote que, en pleno barrio de La Viña, ante la llegada de la ola no se le ocurrió otra salida más que apelar a la Virgen, mientras portaba un estandarte. Según el supuesto milagro, donde lo plantó, el mar se paró. Hoy en día, cada 1 de noviembre, la Virgen de la Palma sale a la calle en procesión para recordarlo. Ahora, investigadores y expertos esperan que, para el próximo maremoto, la ciencia y la prevención puedan aportar otras salidas más viables que esperar a un milagro.

# Uso de medios de localización y seguimiento por detectives privados

Unidad Central de Seguridad Privada

**ANTECEDENTES** En fecha 04.01.2016, una Unidad Territorial de Seguridad Privada, remite consulta a esta Unidad Central, mediante la que se cuestiona el ajuste a derecho de las actividades de los detectives privados que, mediante el empleo de *"medios técnicos"* en el ejercicio de su labor profesional, podrían estar contraviniendo lo dispuesto en la nueva normativa de seguridad privada y, fundamentalmente, lo dispuesto en la Ley de Enjuiciamiento Criminal cuando, en su artículo 588 quinquies b., hace mención a la *utilización de dispositivos o medios técnicos de seguimiento y localización*.

En este sentido, se concluye que el uso de esos dispositivos por detectives privados debería limitarse a investigaciones *judicializadas y su uso sea autorizado por la Autoridad Judicial competente (…) cuando investiguen delitos perseguibles a instancia de parte*.

**CONSIDERACIONES** Con carácter previo se participa que, los informes o respuestas que emite esta Unidad, tienen un carácter meramente informativo y orientativo –nunca vinculante- para quien los emite y para quien los solicita, sin que quepa atribuir a los mismos otros efectos o aplicaciones distintos del mero cumplimiento del deber de servicio a los ciudadanos.

Partiendo del Informe UCSP 054/2014, citado en el escrito de consulta, parece cuestión pacífica que los servicios de investigación privada, a cargo de detectives privados, no pueden extenderse al ámbito de la vida íntima que se desarrolle en el domicilio u otros lugares reservados, ni puede emplearse en su ejecución ningún medio técnico que atente contra los derechos recogidos en el artículo 18 de la Constitución.

Aunque más adelante se profundizará sobre esta protección de la intimidad, lo sustancial del mencionado Informe 54/2014 radica en que concluye con dos factores muy a tener en cuenta:

- De un lado, la idea de habilitación, con la que, en sentido estricto, hace referencia a la condición profesional de quien ejecuta las investigaciones y, en sentido más amplio, exige de una legitimación en quien solicita esas mismas investigaciones, y
- De otro lado, exige que el principio de proporcionalidad sea rector del caso concreto sobre el que se está cuestionando la legalidad.

Pese a que el contenido del documento UCSP 054/2014 tiene un sustrato básico en una Sentencia del Tribunal Supremo que argumenta los posicionamientos de su Alta Magistratura en relación con el ámbito de *lo Social*, en este Informe se pretende una comprensión más generalizadora, que enfoque su campo de visión en un entorno genérico y trascendente, con el fin de orientar, en la práctica, la correcta actuación de los profesionales de la Seguridad Privada.

Por ello, se necesita repasar una serie de consideraciones que es preciso tener en cuenta, antes de exponer una respuesta a la cuestión planteada:

## I. *En torno a la habilitación en un sentido amplio*

Añadido a los requisitos que la norma exige para el ejercicio de la profesión de detective privado, La Ley 5/2014 perfila el ámbito en el que los detectives privados pueden y deben ejercer sus funciones, como prestadores de servicios de investigación *en relación a personas, hechos o delitos sólo perseguibles a instancia de parte*.

Estas restricciones encauzan dicha actividad de seguridad privada, que debe desarrollarse bajo un paraguas de condicionamientos y exigencias que, en la concreta cuestión que nos ocupa, vienen señalados en el artículo 48.1.a) de la Ley 5/2014, al exceptuar de *las averiguaciones que resulten necesarias para la obtención y aportación, por cuenta de terceros legitimados, de información y pruebas sobre conductas o hechos privados*, aquellos que se desarrollen en los *domicilios o lugares reservados*. A esta exclusión se suma el punto 3 del mismo artículo 48 de la reiterada Ley, cuando establece la prohibición de las investigaciones en torno a la *vida íntima de las personas que transcurra en sus domicilio u otros lugares reservados*, a la vez que limita el uso de *medios personales, materiales o técnicos de tal forma que atenten* contra los derechos incorporados al artículo 18 de la Constitución.

Sobre estos planteamientos, se puede afirmar que el detective privado necesita de un añadido exterior que, también, le es necesario para verse habilitado: el inexcusable deber de trabajar por orden de quien tiene un interés o derecho legítimo, esto es, jurídicamente protegido y que transfiere a la labor profesional del investigador un justo título, convirtiendo al cliente en acreedor del resultado de todo lo averiguado.

Por añadidura y de gran importancia resulta el apartado 5 del reiterado Artículo 48 de la Ley 5/2014, ya que obliga a los profesionales de la investigación a velar por los derechos de sus clientes y *de los sujetos investigados*: como puede apreciarse, la norma convierte al detective privado en el garante de los derechos de la persona que le contrata y de todo aquel que se convierte en su objetivo profesional. Es decir, que el legislador quiere que el primer responsable en la no vulneración de los derechos del investigado sea, como no puede ser de otro modo, el propio investigador.

Para finalizar la síntesis de límites que la Ley impone a la labor del detective, el Artículo 48.6 de la Ley 5/2016 recuerda que todo servicio de investigación debe someterse al juicio de proporcionalidad, del que la doctrina afirma que *"(…) está orientado a resolver conflictos entre derechos, intereses o valores en concurrencia. La ventaja del enfoque de proporcionalidad es que permite decidir esos conflictos sin necesidad de generar jerarquías en abstracto de los derechos, intereses o valores involucrados y por tanto, sin necesidad de prejuzgar su mayor o menor legitimidad, ni producir prohibiciones absolutas.*

*Lo peculiar del juicio de proporcionalidad es el punto de vista desde el que se procede al examen de la controversia una vez se ha fijado el contexto, las circunstancias del caso: (…) lo que se va a analizar es su utilidad (su idoneidad para alcanzar el fin pretendido), su necesidad (en ausencia de otra alternativa igualmente eficaz y menos problemática) y, por fin, su "proporcionalidad", atendido su grado de injerencia en un ámbito protegido así como el carácter y alcance del sacrificio que impone sobre los derechos o intereses afectados.*

*De resultas de este examen se juzgarán inaceptables (…) actuaciones en la medida en que impongan un sacrificio inútil, innecesario, o desequilibrado por excesivo, de un derecho o interés protegido (…)".* En otras palabras, el escenario en el que debe llevarse a cabo un servicio de investigación prestado por un detective, tiene que cumplir con, entro otros, el condicionamiento referido del escrupuloso respeto a la esfera íntima del sujeto investigado, de la que, también, es garante. En este margen es donde el detective estará *habilitado* para desempeñar su profesión.

No obstante y en un notable acierto de previsión, la propia norma, como ya se ha apuntado, hace especial mención de un concreto ámbito de los derechos fundamentales: el de la privacidad, que pasa a desarrollarse a continuación.

## II. La protección constitucional a la esfera íntima

Como ya se había insinuado, es el artículo 18 de la Constitución el que garantiza el derecho a la protección de un núcleo íntimo en la vida de cada individuo: ese ámbito que se preserva del conocimiento y del acceso de terceros por ser patrimonio de la esfera más privada.

Este derecho está garantizado, incluso, para los *"personajes públicos"* o los sometidos al poder coercitivo del estado (reclusos), si bien en distinta medida, según las particularidades de cada caso.

Es, precisamente, este ámbito de protección el que hay que conjugar con las injerencias que pueden limitar el derecho a la intimidad y que, necesariamente, deben responder a la cesión frente a otros bienes jurídicamente protegibles.

Así, el Tribunal Constitucional, en su Sentencia 197/1991, asienta doctrina al determinar el modo en que se puede limitar el derecho a la intimidad, cuando afirma que *"(…) el derecho fundamental a la intimidad personal otorga a su titular cuando menos una facultad negativa o de exclusión, que impone a terceros el deber de abstención de intromisiones, salvo que estén fundadas en una previsión legal que tenga justificación constitucional y que sea proporcionada, o que exista un consentimiento eficaz del afectado que lo autorice, pues corresponde a cada persona acotar el ámbito de intimidad personal que reserva al conocimiento ajeno (…)".*

Según lo establecido por el Alto tribunal, la *esfera íntima* puede ceder a través de dos vías: el consentimiento (eficaz) del titular del derecho y, en segundo término, una imposición normativa con amparo constitucional

Por lo que se refiere a los límites externos, el propio Órgano Constitucional establece que *"(…) los derechos fundamentales reconocidos por la Constitución sólo pueden ceder ante los límites que la propia Constitución expresamente imponga o ante los que de manera mediata o indirecta se infieran de la misma al resultar justificados por la necesidad de preservar otros derechos o bienes jurídicamente protegidos (…) las limitaciones que se establezcan no pueden obstruir el derecho fundamental más allá de lo razonable, de donde se desprende que todo acto o resolución que limite derechos fundamentales ha de asegurar que las medidas limitadoras sean necesarias para conseguir el fin perseguido, ha de atender a la proporcionalidad entre el sacrificio del derecho y la situación en la que se halla aquel a quien se le impone y, en todo caso, ha de respetar su contenido esencial (…)"* (STC 57/1994, de 28 de Febrero). En este sentido y respecto a los medios empleados en la limitación del derecho a la intimidad, la sentencia anterior insiste en que *es necesario emplear aquellos que en menor medida lesionen o restrinjan los derechos fundamentales de la persona*.

Por tanto y a modo de esquema, lo que se está expresando por parte del Árbitro Constitucional es que toda restricción del derecho a la intimidad debe estar sometida al principio de proporcionalidad, del que ya se ha hecho mención.

Sin embargo, hay que tener en cuenta que el investigador privado, por sí, no cuenta con un derecho oponible o en colisión con ese derecho a la intimidad del sujeto investigado. El detective, *habilitado* en sentido amplio y haciendo propio el interés legítimo de su contratante, adquiere un *"derecho a conocer"*, que (por exigencia constitucional) debe basarse, a su vez, en un derecho legalmente reconocido. Por tanto, lo que aquel hace es asumir, por delegación de su cliente, una transmisión de derechos jurídicamente protegidos que sirve de amparo y justifica los servicios de investigación interesados, cuyo producto se pondrá a disposición del contratante.

Como hemos podido comprobar en el ya mencionado Informe UCSP054/2014, la gran mayoría de las ocasiones en que se ha planteado una presunta vulneración del derecho fundamental a la intimidad por la actividad profesional de un detective privado, ello ha sido motivado por temas laborales. Es decir: el contratante esgrime los derechos que le amparan, por ejemplo, en el Estatuto de los Trabajadores, gracias a cuya legitimidad puede encargar al detective un concreto servicio. Sobre ello se tratará a continuación.

## III. La práctica jurisprudencial

La aplicación práctica de la teoría constitucional al caso concreto, es función reservada a jueces y magistrados en su

elevada misión de impartir justicia, esto es, de aplicar la ley a cada caso concreto y determinar consecuencias.

A lo largo de los últimos años, existen numerosas sentencias que han avalado o sancionado la actividad de los detectives privados, en función del ajuste (o no) de la labor profesional a la exigencia normativa.

Respecto de las condiciones subjetivas del investigador privado, es necesario (para centrar la atención en la cuestión planteada por la UTSP de Granada) recordar las limitaciones descritas en el apartado primero de estas consideraciones, denominado "*En torno a la habilitación en un sentido amplio*", que no son necesarias reproducir nuevamente.

A aquellos condicionamientos se añade la exigencia del Tribunal Supremo que –sobre las medidas limitativas de derechos fundamentales– obliga al acomodo al principio de proporcionalidad, ya mencionado, cumpliendo *"(…) los tres requisitos o condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto) (…)."*

Con estos elementos como telón de fondo y acudiendo a las diferentes sentencias que enjuician el comportamiento de los detectives privados, parece que existe una gran relevancia en la jurisdicción social, muy por encima de cualquier otro orden. En este ámbito, la jurisprudencia se ha decantado, sistemáticamente, por admitir la prueba testimonial de detectives, acompañados por pruebas obtenidas con elementos "técnicos" (videograbaciones, fotografías), ya que la ley *"(…) atribuye al empresario, entre otras facultades, la de adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento del trabajador de sus obligaciones laborales (…)*", siempre que esas medidas, entre las que se incluye el empleo de detectives privados y de sus servicios, no supongan "*(…) intromisiones ilegítimas en la intimidad de sus empleados en los centros de trabajo, sino que la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad (…)*".

Un claro ejemplo de estos excesos viene determinado por la ilicitud de la "prueba de detectives", cuando éstos son contratados para controlar a un trabajador "*durante cinco meses, de forma permanente, desde las 6 o 7 de la mañana hasta la noche"*: en este caso, la sentencia declara la nulidad de la prueba practicada al no haber sido ni proporcionada, ni idónea ni necesaria, concluyendo que el uso de un sistema que permite a la empresa tener noticias permanentes respecto de todo tipo de conductas del trabajador en un ámbito que le es privado, constituye una actuación que rebasa ampliamente las facultades que al empresario otorga el Estatuto de los Trabajadores y supone una intromisión ilegítima en el derecho a la intimidad consagrado en el artículo 18.1 de la Constitución, que no ha sido en este caso conforme con el principio de proporcionalidad.

Por lo que se refiere al empleo de medios técnicos, precisamente fue la Sala de lo Social del TSJ Extremadura quien llegó a afirmar que *"(…) si* [los detectives privados] *no pudieran seguir a una persona por la calle, e incluso fotografiarla o filmarla, no se ve cómo podrían desarrollar su actividad para obtener y aportar información y pruebas (…)"*.

Es decir, que el uso de material tecnológico viene avalado por la propia jurisprudencia y, como puede observarse, de forma pacífica. De hecho, el Auto 391/2007 de la Audiencia Provincial de Oviedo, en relación a un seguimiento realizado por dos detectives privados, que colocaron un GPS en el vehículo utilizado por la persona seguida y que después denunció a los investigadores privados, afirma que los hechos descritos *"(…) no integran una conducta susceptible de incardinarse en el art. 197 del C.P. que sanciona el descubrimiento y revelación de secretos, por ausencia de los elementos necesarios para integrar la conducta típica descrita en dicho precepto (…)"*.

A modo de síntesis, puede decirse que la actividad de los detectives ha venido siendo medida, en el seno de los tribunales, por su ajuste al principio de proporcionalidad y el respeto a los límites que este precepto constitucional exige en su conducta que, entre otros, determina la concreción de la finalidad perseguida para la práctica de un seguimiento, lo que enlaza directamente con la idea ya estudiada de la legitimación, como transmisión de un derecho o interés jurídicamente protegido, entre el cliente y el detective.

No obstante, la doctrina ya venía reclamando algún tipo de control al investigador y una regulación de las garantías que permitan al investigado ejercer una efectiva defensa, pues *no siempre las investigaciones son infalibles o ajustadas a derecho.* Esta cuestión se aborda en el siguiente apartado.

## ***IV. La nueva perspectiva de la protección a la intimidad: la doctrina actual en el escenario impuesto por la reforma de la Ley de Enjuiciamiento Criminal***

Aunque la práctica totalidad de los monográficos que sobre el tema de la investigación podemos abordar hacen referencia a la esfera penal público-criminal, es contundente la afirmación del propio Eloy Velasco cuando dice que *"todo* [lo relativo al uso de tecnología en la investigación] *es igualmente predicable de las investigaciones particulares hechas frente a terceros por detectives privados o personas no pertenecientes a los cuerpos policiales, cuando usan tecnologías de vigilancia privadas"*. Esto es así, precisamente, porque la sujeción a la norma que señala el Artículo 9.1 de la Constitución es aplicable tanto a los poderes públicos como a la totalidad de la ciudadanía. Sobre este planteamiento, no se puede hacer distinción en cuanto al sometimiento a la ley, entre una investigación llevada a cabo por la policía y otra llevada a cabo por detectives privados.

Una vez establecido este argumento, hay que indicar que las diversas fuentes doctrinales venían haciéndose eco de la (cada vez más) necesaria regulación del uso de las nuevas tecnologías en la Ley de Enjuiciamiento Criminal que, por su

edad entre otros motivos, no previó el despliegue científico de los últimos años, ni las capacidades invasivas en la intimidad de los ciudadanos.

Los medios de *injerencia no física* en espacios propios de privacidad (Non trespassory surveillance techniques) como el zoom, el GPS, BTS, router… son capaces de saber dónde se encuentra un aparato que no se está viendo y, por extensión, una persona, prácticamente en todo momento.

En los últimos tiempos, la corriente científica ha sostenido que estas injerencias, que permiten investigar tanto al sospechoso de haber cometido un delito, como a un ciudadano honrado, por móviles muy alejados de la imputación de delitos (políticos, religiosos, económicos…), deben ser controladas por el derecho: la intensidad de la injerencia y su duración. En este sentido, en su trabajo *Tecnovigilancia, geolocalización y datos: aspectos procesales penales*, D. Eloy VELASCO NÚÑEZ exigía (Junio de 2014) *"(…) una habilitación legal previa a la injerencia investigadora y debe estar formal y materialmente regulada con cierto detalle por una norma que persiga un fin legítimo, con rango de ley, que determine: -los supuestos habilitantes, - la duración y – el proceso de obtención, custodia, análisis (…) de la información así obtenida (…)"*. Es decir, reclamaba una validación de los sistemas tecnológicos que, previa regulación normativa, tuviese un control tanto en su duración como en los casos en que pueden ser empleados, además de la previsión de reserva y cuidado del resultado obtenido con el empleo de dichos medios.

Por otra parte y respecto de vigilancias o seguimientos ocasionales o con medios técnicos menos "invasivos", el mismo autor señalaba que "no exige mandamiento judicial, dada su apenas despreciable intrusión, salvo que su colocación sea muy intensa (prolongada en el tiempo, sobre terminal de uso privado) o afecte a espacios privados". Por ello (y, como hemos visto, hasta junio del año 2014), la práctica de un seguimiento mediante el empleo de un sistema no invasivo, acompañada del ejercicio inmediato de la labor operativa de los policías actuantes (o, en su caso, los detectives), era una actividad consentida por la ley.

Sin embargo, toda esta teoría está en estos momentos, limitada por el contenido de lo dispuesto en el artículo 588 quinquies b. de la Ley de Enjuiciamiento Criminal, que, sobre la utilización de dispositivos o medios técnicos de seguimiento y localización, establece el control previo judicial de las medidas tecnológicas de seguimiento y localización.

De hecho, la norma no hace distinción en el tipo de sistema de vigilancia, por lo que, en estos momentos, parece haberse producido un salto cualitativo: no solamente se ha regulado, como se venía reclamando, el uso de *medios de injerencia no física*, sino que, al no hacerse precisión alguna, una simple baliza de posicionamiento (beeper) con un radio de acción limitado, se encuentra igualmente sometida a la norma recientemente en vigor.

**CONCLUSIONES** En resumen y como consecuencia de lo anteriormente analizado, se concluye lo siguiente:

1. El detective privado debe actuar investido de habilitación en sentido amplio, por cuanto no solamente debe cumplir escrupulosamente las exigencias formales en su actuación profesional, sino que debe hacerlo mediante la legitimación que su contratante debe ostentar como derecho jurídicamente reconocido y que faculta al investigador para actuar.
2. La actividad del detective exige, como pilar básico, la obligación de defender los derechos de su cliente y los del sujeto sometido a investigación, con especial atención al derecho a la intimidad de éste, de acuerdo a lo establecido en el artículo 18 de la Constitución.
3. El derecho a la intimidad del sujeto investigado puede entrar en conflicto con derechos jurídicamente reconocidos en el contratante, lo que se resolverá mediante el *juicio de proporcionalidad*, que determinará si una intromisión en la esfera íntima tiene las exigencias de útil, necesaria y equilibrada.
4. El uso de medios técnicos debe ajustarse al *juicio de proporcionalidad* por cuanto puede suponer de intromisión en la esfera íntima del investigado.
5. El uso de dispositivos de seguimiento requiere de una orden judicial previa.

Este informe se emite en cumplimiento de lo dispuesto en el artículo 35.g) de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, sobre derecho de información al ciudadano, y fija la posición y el criterio decisor de las Unidades Policiales de Seguridad Privada, en relación con el objeto de la consulta sometido a consideración. No pone fin a la vía administrativa ni constituye un acto de los descritos en el artículo 107 de la citada ley, por lo que, contra el mismo, no cabe recurso alguno.

# Así se protegen los grandes bancos de hackers como los de "Mr. Robot"

Gonzalo Toca
*Fuente: YOROKOBU, Revista nº 77 - 2016*

YOROKOBU
TAKE A WALK ON THE SLOW SIDE

Puedes reírte si quieres, pero la serie estadounidense *Mr. Robot* apasiona a los —siempre quisquillosos y perfeccionistas— expertos en seguridad informática y a los piratas del ciberespacio precisamente porque se acerca a la verdad. A veces se aproxima mucho, como cuando se inspira en ataques como el *presunto* del Moshad, la CIA y la NSA al programa nuclear iraní mediante el virus Stuxnet, y a veces algo menos, como cuando habla de reventar las tripas del sistema financiero y borrar nuestras deudas sin dejar rastro.

Daniel Medianero, gerente de marketing de servicios de la consultora de ciberseguridad s21sec, recuerda lo que haría falta para convertir en realidad esa pesadilla bancaria: «Una ayuda interna de los trabajadores que nos dé pistas sobre su infraestructura, su metodología y sus planes de contingencia, si lo atacan; entrar en unas áreas de acceso muy restringido con unas máquinas que los bancos no suelen tener conectadas a la red; y asumir el riesgo de dejar demasiadas pistas».

Dicho de otro modo, los bancos intentan impedir grandes ataques utilizando armas como los planes de contingencia secretos, los cortafuegos de seguridad que proporcionan las consultoras informáticas y evitando la conexión a internet y el acceso de más de un puñado de técnicos a las máquinas que representan el corazón y los pulmones de la entidad.

Vicente Pérez, gerente de la cuenta que se ocupa de proporcionar seguridad informática a grandes entidades financieras en la consultora Sophos, coincide con Medianero y añade que, a pesar de todo, «lo que cuentan en *Mr. Robot* es posible técnicamente», pero que, siendo sinceros, no sabe «muy bien cómo podrían hacerlo». Ni él ni casi nadie, por supuesto.

Tampoco tiene claro «hasta qué punto podría compensarle a alguien», porque «existen otras posibilidades de atacar sistemas llevándose dinero —con un impacto menor, eso es cierto— sin asumir tantos riesgos». Esta es otra de las estrategias de los bancos: hacer que los atracos espectaculares que puedan prender la desconfianza de sus clientes no les compensen a los criminales, porque los obligan a descender del mundo virtual dejando pistas en el mundo físico, a buscar colaboradores internos entre los empleados y a introducirse a veces personalmente en infraestructuras muy vigiladas.

## Fallos en el sistema

Por supuesto, la lógica que se esconde tras esta protección tiene sus puntos débiles. Este año, sin ir más lejos, unos hackers sustrajeron 101 millones de dólares de las cuentas del Banco Central de Bangladés en la Reserva Federal de Nueva York y quedan por recuperar 63 millones. En mayo, con el reconocimiento por parte de la firma de seguridad FireEye de que se estaban produciendo ataques similares en 12 entidades financieras, casi todas en países emergentes, la agencia Bloomberg concluía que podíamos encontrarnos ante «una campaña amplia y seria para violar el sistema financiero internacional».

Es evidente, por lo tanto, que cientos o quizá miles de personas en todo el mundo están dispuestas a exponerse a un peligro fabuloso a cambio de millones de dólares y la posibilidad de presumir de haber cometido algunos de los atracos más cuantiosos de la historia.

El mundo físico y el virtual no son tan distintos después de todo. En febrero de 2003, unos ladrones se llevaron 100 millones de euros en diamantes de una cámara acorazada de Bruselas y la banda, que se autodenominaba 'La Scuola di Torino' como si se considerasen un grupito de artesanos renacentistas, tuvo la cara dura de alquilar una oficina en frente de la institución que iban a robar y uno de ellos llegó a reunirse con directivos haciéndose pasar por comerciante de piedras preciosas.

El falso comerciante, que casi inevitablemente se llamaba Leonardo (Notarbartolo), fue el único condenado y no cumplió los diez años que le correspondían entre rejas porque salió en libertad condicional. Fue un caballero en prisión, pero los zafiros nunca se recuperaron y la banda se convirtió en leyenda exactamente igual que los hackers que atracaron los bancos de los emergentes y engañaron con códigos a la Reserva Federal de Nueva York.

De todos modos, es verdad que en un escenario en el que los atracos virtuales asedian a las entidades financieras y existen piratas de distinto cuño y habilidad, los bancos han recurrido a especialistas como Daniel Medianero y Vicente Pérez para blindarse con distintos anillos de seguridad que, por lo general, se centran en repeler ataques más modestos que los

que dibuja *Mr. Robot*. Tiene sentido: sería absurdo que Francia se centrase únicamente en evitar un ataque yihadista con bombas nucleares en vez de atentados suicidas, que son los más comunes y probables.

El primer anillo que dibujan los expertos en seguridad informática de las entidades financieras es lo que Vicente Pérez, de Sophos, denomina «perímetro de seguridad». Aquí los ataques son tan directos y toscos como un puñetazo en la mandíbula a traición. Según Daniel Medianero, de s21sec, estos ataques consisten en «rastrear fallos, sobre todo relacionados con la falta de actualización del software, que se venden después en el mercado negro». Los servidores virtuales también se convierten en un raro objeto de deseo.

El segundo anillo, advierte Medianero, es el de «la seguridad de las aplicaciones», entre las que destacan las que hacen posible la banca electrónica. Los hackers intentan manipular los movimientos de la propia entidad financiera para que empiece a enviar transferencias con cargo a las cuentas de sus clientes.

El tercer anillo pasa por que los hackers reconozcan una evidencia: es muy difícil robar directamente a un banco. Aquí es donde optan, según Vicente Pérez, por el «rastreo de vulnerabilidades de los usuarios». Saben que es más fácil robar a un cliente que a su propia entidad y por eso clonan páginas web, cajeros e incluso TPV idénticas a los de los bancos donde metemos nuestros datos alegremente o se hacen pasar por las entidades financieras en correos electrónicos alarmantes para que los clientes les proporcionen toda su información y contraseñas.

El dinero, tanto en el caso de la seguridad de las aplicaciones como en el de impostar la voz amiga del banco, acaba en un sinfín de eslabones de intermediarios y testaferros llamados *muleros* que cobran a veces 1.000 euros al mes por recibir la transacción y reenviársela a otros destinatarios. Estos *muleros* no suelen saber quién les ha contratado ni por qué exactamente: cuando les pregunten, dirán que les ofrecieron cobrar por no hacer nada y, sobre todo, por no hacer preguntas.

**Secuestros y convulsión**

El cuarto anillo es el de los troyanos bancarios. Aquí Daniel Medianero destaca esencialmente la capacidad de que «los delincuentes tomen el control de los ordenadores, los sistemas informáticos o los navegadores y sean capaces de utilizarlos en su beneficio tanto para obtener información sobre las páginas en las que navega el usuario [incluidas las contraseñas que ponemos en tiendas virtuales y bancos digitales] como para coordinarlos para atacar webs [de bancos, por ejemplo] en contra de los deseos de sus dueños». Un buen día observamos un comportamiento extraño en nuestro equipo y descubrimos que está asediando la página de la CIA sin que nosotros podamos hacer nada para evitarlo.

También, advierte el consultor, pueden «pedir un rescate a cambio de liberar los ordenadores». Los ejemplos pueden ser dramáticos y van más allá del sector financiero. Este año múltiples hospitales estadounidenses se han encontrado con que un grupo de piratas no les dejaban acceder a los historiales de sus pacientes y temieron que se los pudieran modificar. Uno de los últimos, en Hollywood, tuvo que pagar 17.000 dólares para volver a acceder a ellos.

Todos estos anillos de seguridad y el éxito de una serie como *Mr. Robot* muestran que vivimos tiempos convulsos en el ciberespacio. También es obvio que internet permite la coordinación de muchos cerebros que trabajan en red y que nunca se hubieran conocido sin ellas.

Además, los sistemas de los bancos nunca habían estado tan expuestos digitalmente porque sus propias estructuras se están *virtualizando* a marchas forzadas (a veces, revelando fallos enormes como Deutsche Bank) y dependen cada vez más de los datos masivos de los servidores. La guinda del pastel es que, por fin, existe un mercado negro y sumamente estructurado en internet, apuntalado por países más o menos permisivos como Rusia o Corea del Norte, donde se pueden vender y comprar los botines de los robos, desde tarjetas de crédito hasta el control de una legión de computadoras.

Es verdad que las entidades financieras rara vez habían sido tan impopulares y que el dinero es sólo uno de los dos grandes motivos que mueven a los hackers. El otro es el prestigio y, en algunos casos, convertirse en leyenda antisistema, en un Che Guevara con sonrisa de bits y ojos de Snowden. Hay miles de hackers dispuestos a arriesgarse a la cárcel para permanecer en la memoria de todos.

La historia decidirá si permanecerán como simples ladrones o como esos héroes contra un sistema opresivo que afirman, con el orgullo de Philip Price, que «la política sólo es para las marionetas». Una parte de la población pagará inevitablemente el precio de sus ambiciones. Tú y yo, para ser exactos.

***Fuente: YOROKOBU, Revista nº 77 – 2016***
***http://www.yorokobu.es/***

# Seguridad, salud en el trabajo y control de accesos

Locken
*Simple key•Smart access*

**Según datos del Ministerio de Empleo y Seguridad Social, ya durante los dos primeros meses del año 2016, un total de 106 trabajadores fallecieron en accidente laboral. Cuando un trabajador no puede regresar a su casa por culpa de un accidente laboral, todos sentimos que los esfuerzos realizados en pro de la seguridad (safety), no han sido suficientes.**

LOCKEN
SMART ACCESS SOLUTIONS

A lo largo del pasado año se registraron casi 450.000 accidentes laborales en España, cerca de un 6% más que en 2014, año que a su vez presentó un crecimiento del 5% sobre el precedente. En 2015 murieron 608 trabajadores y trabajadoras en accidentes laborales, 28 más que en 2014 y casi dos trabajadores muertos cada día, 500 en los lugares de trabajo y 108 en el desplazamiento al trabajo. Con alguna excepción, los accidentes mortales han aumentado en todos los sectores.

Estos datos demuestran un rebrote de la siniestralidad y discuten la eficacia de la normativa, a pesar de que La legislación española en materia de Seguridad y Salud en el Trabajo (Ley 31/1995, de 8 de noviembre, sobre Prevención de Riesgos Laborales) resulta ser una de las normativas más completas y desarrolladas a nivel internacional. Prueba de ello es que en la actualidad, está siendo utilizada como modelo de referencia para muchos países, principalmente latinoamericanos, que se encuentran a día de hoy en fase de promulgación o desarrollo de su legislación de Seguridad y Salud en el Trabajo.

Últimamente asistimos a un interesante debate sobre la convergencia entre Seguridad Física y Seguridad Lógica, una división más del mismo concepto y, también en este caso, no podemos entender la percepción o la garantía de ser o estar seguro, sin cubrir ambos aspectos. Tal vez, sería interesante abrir también un debate sobre la convergencia entre *Security* y *Safety*, o, al menos, estudiar de qué modo los profesionales y empresas del lado *Security*, podemos colaborar con el lado *Safety*.

Garantizar la seguridad y la salud laboral de todos los trabajadores, propios o externos, debe ser un objetivo irrenunciable de cualquier organización, entidad o empresa y, aún más lejos de los sistemas de Coordinación de Actividades Empresariales, campañas informativas, carteles de concienciación, publicación de políticas de Responsabilidad Social Corporativa y compromisos éticos, debemos enfocar nuestros esfuerzos para que las inversiones realizadas en soluciones de seguridad tengan también un retorno expresado en la rebaja objetiva de los niveles de siniestralidad laboral. Está claro que no basta con formar e informar, pues, si fuera así, prácticamente no existirían los accidentes de tráfico. Recibimos formación vial, pasamos exámenes de aptitud y, sin embargo, sufrimos accidentes de tráfico, muchas veces tras infringir la normativa que aprendimos y demostramos conocer.

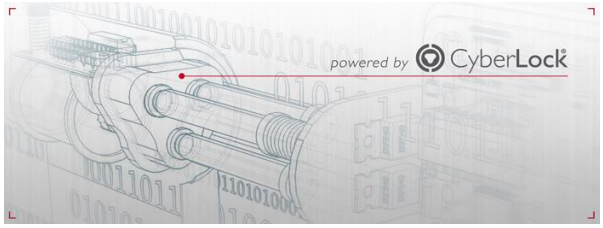
El cambio de cultura empresarial en lo que se refiere a seguridad y salud laboral es, evidentemente, necesario, pero seremos más eficaces y proactivos si, además de poner en marcha planes de educación de plantillas y directivos, también implementamos medidas técnicas de seguridad que empujen en la misma dirección, sin detrimento de su objetivo primario.

Debemos informar a los empleados de los riesgos que corren al acceder a un recinto de riesgo, de las condiciones y factores que afectan, o podrían afectar a la salud y la seguridad de los empleados incluyendo a los trabajadores temporales y personal contratado, visitantes o cualquier otra persona en el lugar de trabajo

Debemos informarles de las medidas de protección y de los recursos técnicos que deben emplear para realizar su trabajo, pero también debemos preguntarnos por la posibilidad de impedir el acceso del trabajador no cualificado o no equipado, al lugar de trabajo, evitando, de este modo, un accidente potencial.

Las posibilidades de utilización de los sistemas de control electrónico de accesos, como instrumento en beneficio de la seguridad laboral, son reales, eficaces y probadas. Desde hace años, muchas empresas se mueven en esta dirección y, especialmente en el caso de empresas y trabajadores subcontratados, se desarrollan e implementan estrategias de verificación del respeto a las normas de protección y salud laboral, embebidas e integradas en los habituales protocolos de autorización de acceso.

La cultura de seguridad, protección y salud laboral debe ser estudiada e implantada de forma colectiva. El comportamiento individual seguro, último eslabón de la cadena, debe y puede ser impuesto y supervisado por medio de la tecnología.




En los procesos de verificación y concesión de autorización de acceso a instalaciones de riesgo deben introducirse criterios y, aún mejor, herramientas software y hardware diseñadas para evitar que trabajadores no cualificados, inconvenientemente documentados o ignorantes de las normas generales o específicas de protección laboral, accedan a los diferentes recintos de una compañía, especialmente si esta compañía y sus instalaciones están normalmente deshabitadas y dispersas en una amplía geografía. Evidentemente, en esta descripción queda perfectamente reflejado el Sector de Utilities.

Reconozcamos que, en estos tiempos tan duramente competitivos, debemos estar muy atentos para evitar situaciones precarias de seguridad laboral, especialmente entre el colectivo de trabajadores de empresas subcontratadas que, cada día, acceden a nuestras instalaciones y, a veces, asumen riesgos para los cuales no están suficientemente preparados, equipados e, incluso, asegurados. Somos corresponsables ante la ley, pero de forma más íntima, ante nuestra propia conciencia.

**Locken**, desde hace años, viene desarrollando herramientas software y hardware orientadas al propósito de gestionar el acceso con la doble vertiente de *security* (impedir el acceso a personas no autorizadas) y *safety* (impedir el acceso a usuarios no cualificados de acuerdo a PRL).

Así, en 2008, con **Locken** Web Request, portal dinámico de petición de acceso y verificación de documentación de Coordinación de Actividades Empresariales, **Locken** da el primer paso en esta dirección.

Hoy en día, en combinación con sistemas de geolocalización o sistemas de posicionamiento por balizas Bluetooth (BLE), **Locken** desarrolla App's personalizadas, bajo el nombre genérico de MyLocken, que verifican automáticamente la aptitud PRL de los trabajadores desplazados y la existencia de órdenes de trabajo que justifiquen el permiso de acceso a recintos aislados y no habitados.

Básicamente, el usuario al llegar a la instalación objeto del trabajo, anuncia vía App su presencia, iniciándose en ese momento un *workflow* de verificación que, por supuesto incluyendo la normativa de riesgos laborales, finaliza con la concesión de permiso de acceso, sólo en el caso de que todo el proceso de verificación culmine en un resultado positivo.

Las empresas usuarias se benefician de un doble retorno de la inversión, garantizando sólo el acceso al personal propio o subcontratado realmente autorizado y encontrándose en regla en cuanto a las normas de salud laboral.

## *RECORDATORIO*

***Próximo 24 de noviembre de 2016, en Cúpula Centro Comercial Arenas de Barcelona:***

- ***Cena Anual de Socios y Amigos de ADSI***
  - ***20:00 horas***
  - ***Fecha límite de inscripción 21.11.2016***

CUPULA EVENTS

# 6 criterios para clasificar y priorizar tus proyectos de ciberseguridad en la empresa

Instituto Nacional de Ciberseguridad

¿Por dónde empiezo? Ésta es una de las preguntas que nos solemos hacemos cuando nos enfrentamos a los resultados de una evaluación de seguridad o una auditoría. Es decir, cuando nos proponemos a abordar las iniciativas y proyectos que hemos definido para subsanar las deficiencias encontradas. Es normal que hayamos identificado aspectos de mejora muy diversos y que no resulte sencillo decidir cuál abordar en primer lugar. Dada esta situación, antes de ponernos en marcha, es muy útil llevar a cabo una clasificación y priorización de los proyectos pendientes. A continuación presentamos una serie de criterios para clasificar y priorizar las distintas iniciativas:

**Tipo de proyecto**. Atendiendo al tipo de proyecto, podemos distinguir entre:

- Organizativo: cuando afecta a la estructura de nuestra empresa, nuestros métodos de trabajo o similares. Por ejemplo, si se trata de definir e implantar políticas de uso de los recursos tecnológicos siguiendo las mejores prácticas en materia de seguridad de la información.
- Técnico: tal y como su nombre indica, son proyectos con un importante contenido técnico. Por ejemplo, securizar la página web corporativa.
- Regulatorio: son proyectos o iniciativas encaminadas a alinear algún aspecto concreto de nuestra organización a alguna norma o regulacion. Por ejemplo, los proyectos encaminados al cumplimiento de la LOPD y el RDLOPD.

**Coste del proyecto**. En algunas ocasiones puede ser complicado hablar del coste económico de un proyecto cuando este se realiza con recursos propios. Sin embargo, al menos es conveniente establecer tres rangos de coste de referencia: bajo, medio y alto. Asignaremos cada proyecto a alguno de estos rangos. Tal y como cabe esperar, lo que para una pyme puede ser coste «alto», para una gran multinacional puede ser coste «bajo».

**Origen del incumplimiento**. Es común que los proyectos e iniciativas para la mejora de la seguridad tengan su origen en un análisis de riesgos, una auditoría o una evaluación de seguridad. Puede resultarnos conveniente clasificar los proyectos atendiendo a este criterio para que una vez finalizados, no resulte sencillo revisar cuál era la situación anterior a fin de comprobar que se han subsanado la causa raíz del problema.

**Tiempo de ejecución**. En algunos casos es requisito indispensable que los proyectos finalicen antes de una fecha determinada. Dada esta situación, clasificar los proyectos atendiendo a su prioridad temporal aporta gran valor para la organización de los mismos.

**Recursos necesarios para la ejecución**. Con este criterio distinguimos aquellos proyectos que pueden ser ejecutados con nuestros recursos propios de los que deberemos externalizar.

Como es lógico, si sabemos que en una época determinada del año necesitamos disponer del 100% de nuestros recursos, entonces únicamente deberemos planificar en este periodo los proyectos que se lleven a cabo por recursos externos. Por ejemplo, si necesitamos que todo el personal del Departamento Administración esté disponible para hacer el cierre del ejercicio contable en un periodo determinado, entonces no planificaremos en este periodo proyectos que requieran de su participación.

**Ratio ganancia / esfuerzo**. Por último, uno de los criterios más utilizados a la hora de priorizar las iniciativas consiste en la relación ganancia / esfuerzo. En este sentido, daremos prioridad alta a los proyectos que nos aportan una fuerte ganancia o beneficio y que requieren de poco esfuerzo para su ejecución.

Hemos podido comprobar que existen múltiples criterios para clasificar y priorizar los proyectos e iniciativas. Ni que decir tiene que no es necesario considerarlos todos a la hora de organizar nuestro trabajo. No obstante sí puede resultar conveniente tener en cuenta varios de ellos. La elección de estos criterios es algo que debe abordar cada empresa antes de empezar a clasificar los proyectos.

Por último, sólo nos queda destacar que hacer una correcta clasificación y priorización de los proyectos no sólo nos hará más cómodo nuestro trabajo, sino que jugará un papel importante de cara a lograr el éxito de los propios proyectos.

# Centro de gestión de incidencias o atención al cliente

Unidad Central de Seguridad Privada

## ANTECEDENTES

Escrito de un representante de una asociación, en relación al concepto y alcance de los "centros de gestión de incidencias o de atención al cliente" asociados al concepto de autoprotección.

## CONSIDERACIONES

Con carácter previo se participa que, los informes o respuestas que emite esta Unidad, tienen un carácter meramente informativo y orientativo –nunca vinculante- para quien los emite y para quien los solicita, sin que quepa atribuir a los mismos otros efectos o aplicaciones distintos del mero cumplimiento del deber de servicio a los ciudadanos.

En el escrito se hace referencia al "concepto de prevención ligado a la autoprotección que puede adoptar el titular de un inmueble no obligado a adoptar medidas de seguridad especificas por la normativa de seguridad privada para la protección de su patrimonio contra todo tipo de riesgos y entre ellos frente a los de robo o intrusión, mediante la adopción de un Plan de Autoprotección sin intervención de los servicios de seguridad privada y se halla recogido en el artículo 7 de la Ley de Seguridad Privada como actividades excluidas".

"Para que las medidas preventivas establecidas por el titular del establecimiento industrial, comercial o de servicios cumplan con su objetivo son necesarios tres aspectos fundamentales:

- Plan de Información Preventiva frente a sus trabajadores y clientes…
- Plan Operativo de Intervención que organiza la preparación y respuesta ante una emergencia…
- Determinar y definir los medios humanos que han de participar, tanto en la fase de prevención como en la de intervención… "

Así mismo se interpreta que "no existe impedimento legal alguno para que los empresarios en relación a sus centros de gestión de incidencias o de atención al cliente, puedan instalar y utilizar a través de su propio personal, sistemas de video vigilancia u otras medidas de seguridad electrónicas para la adecuada vigilancia y protección de su patrimonio, así como controlar la actividad laboral y la relación con sus clientes".

Estos centros son definidos como "locales privados a través de los cuales el personal del empresario pueden emplear las medidas electrónicas e informáticas propias de la autoprotección frente a sus trabajadores y clientes, obviamente sin efectos directos frente a terceros".

Se enumera en las páginas siguientes del documento el concepto de centro de control o de video vigilancia del artículo 39.1 del Reglamento de Seguridad Privada, así como los centros de control de las empresas habilitadas para la actividad de centralización de alarmas e incluso el de las centrales de alarma de uso propio, a fin de diferenciarlos de los denominados "centros de control de incidencias o de atención al cliente", concluyendo que el "personal del empresario asume unas tareas y funciones concretas en su puesto de trabajo que serán totalmente ajenas a lo que constituyen los servicios de seguridad privada definidos en el artículo 2 de la Ley de Seguridad Privada.

Finalmente y de forma exhaustiva se relacionan las tareas que los "operadores" de ese centro de control o atención al cliente podrían realizar, algunas de las cuales son claramente de seguridad:

- Tramitar incidencias de alarmas con los operadores de la central de alarmas contratada, como actuación complementaria a la verificación.
- Control de los sistemas anti incendios o de prevención frente al robo.
- Control del funcionamiento de los sistemas anti hurto instalados en cada local o establecimiento del empresario.

El termino autoprotección al que se refiere el escrito para justificar que los denominados "centros de control de incidencias o de atención al cliente" se encontrarían excluidos de la normativa de seguridad privada, se encuentra definido en el artículo 7.1 de la vigente Ley 5/2014, de 4 de abril: *"No están sujetas a esta ley las actuaciones de autoprotección, entendidas como el conjunto de cautelas o diligencias que se puedan adoptar o que ejecuten por sí y para sí mismos de forma directa los interesados, estrictamente dirigidas a la*

*protección de su entorno personal o patrimonial, y cuya práctica o aplicación no conlleve contraprestación alguna ni suponga algún tipo de servicio de seguridad privada prestado a terceros.*

*Cuando los interesados tengan el carácter de empresas o entidades de cualquier tipo, en ningún caso utilizarán a sus empleados para el desarrollo de las funciones previstas en la presente ley, reservadas a las empresas y el personal de seguridad privada".*


Conforme al artículo transcrito, los titulares de establecimientos industriales, comerciales o de servicios, no podrían utilizar a sus empleados para realizar funciones sujetas a la normativa de seguridad privada como el uso de medidas electrónicas o sistemas de video vigilancia con la finalidad de prevenir posibles hechos delictivos, debiendo contratar empresas de seguridad autorizadas para estas actividades o bien ser los propios dueños o empresarios quienes directamente las lleven a cabo.

## CONCLUSIONES

En los denominados centros de gestión de incidencias o de atención al cliente, el personal empleado en los mismos solo podrá realizar aquellas tareas o funciones que sean de carácter empresarial o laboral y no tengan relación con la seguridad, ya que el concepto autoprotección para la normativa de seguridad privada exige que sea el interesado directamente y para sí mismo el que ejecute las acciones tendentes a proteger su persona o patrimonio.

Este informe se emite en cumplimiento de lo dispuesto en el artículo 35.g) de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, sobre derecho de información al ciudadano, y fija la posición y el criterio decisor de las Unidades Policiales de Seguridad Privada, en relación con el objeto de la consulta sometido a consideración. No pone fin a la vía administrativa ni constituye un acto de los descritos en el artículo 107 de la citada ley, por lo que, contra el mismo, no cabe recurso alguno.

# Noticias


## Controles de identidad a los jóvenes de París

Recientemente se ha publicado un estudio sobre **el perfil de los jóvenes detenidos en París**. El estudio parte de una encuesta dirigida a los jóvenes que se llevó a cabo en el año 2010 en el marco de la convocatoria de la defensa y la ciudadanía. El Observatorio Francés de las Drogas y las Toxicomanías (OFDT) aprovecha siempre la convocatoria para hacer una encuesta sobre el consumo de sustancias psicoactivas entre los jóvenes. En la edición de 2010, el Ayuntamiento de París financió una ampliación de la encuesta dirigida a averiguar los índices de solicitudes policiales de identificación de jóvenes, así como las características de los que son objeto de esta medida.

La primera conclusión de la encuesta nos muestra un dato conocido: **la policía detiene a los jóvenes para identificarlos con más frecuencia que al resto de la población** (un 28% de jóvenes frente a un 16% del total de entrevistados). La mayoría de jóvenes son hombres, no están escolarizados, tienden al sobrepeso, tienen poca confianza en la policía, han consumido alcohol o cannabis y han estado implicados previamente en una pelea.

A partir de los datos, se configuran dos grandes grupos de jóvenes a quienes la policía detiene con más frecuencia:

Al primer grupo se les llama epicúreos desafiantes. **Se trata de jóvenes a quienes controlan en el espacio público el doble de veces que al resto**. Son mayoritariamente hombres, con amigos sobre todo masculinos, y que salen, como mínimo, una vez por semana (a todo tipo de lugares). La mayoría de las veces los padres no saben los sitios que frecuentan sus hijos. Viven en barrios mayoritariamente con un buen nivel económico (están orgullosos de vivir allí) y sus padres suelen ser profesionales liberales. Acostumbran a consumir mucho tabaco (77%) y algunos también alcohol y cannabis. Normalmente tienen algún antecedente por alguna pelea o por algún tipo de agresión. No tienen un buen concepto de la policía y les gusta enfrentarse.

El segundo grupo no está tan sobrerepresentado (jóvenes a quienes controlan sólo un 1,6% más que a la media). **La mayoría viven en barrios populares de la ciudad que no les hacen sentirse orgullosos**, ya que suelen tener problemas de drogas, de delincuencia o de inseguridad. Los hombres también están sobrerepresentados, pero sus amistades son fundamentalmente femeninas. No acostumbran a declarar tener muchos amigos. Salen menos que los anteriores y consumen poco alcohol o drogas. La familia suele saber los lugares que frecuentan sus hijos y tener sobrepeso u obesidad.

Las características del grupo de jóvenes que no son sometidos a controles inferiores son: se trata mayoritariamente de mujeres, cursan algún tipo de estudios, están orgullosas de los barrios donde viven y consumen poco alcohol y prácticamente ninguna droga. Reciben como mínimo 100 euros a la semana como dinero de bolsillo. **No les gusta enfrentarse a la policía**. Algunas viven en barrios populares, pero otras en barrios intermedios y acomodados. Frecuentemente los padres (algunos, al menos) tienen una profesión liberal. No acostumbran a tener antecedentes por ningún tipo de pelea.

Precisamente **el hecho de haber estado previamente involucrado en una pelea o consumir drogas son factores que tienen una gran influencia para facilitar los controles policiales a los jóvenes**.

**Fuente: Notes de Seguretat**

# Formación

FESEI
DOCENS

## MÁSTER en Liderazgo, Diploma e Inteligencia

**Organiza FESEI:** Fundación de Estudios Estratégicos e Internacionales

**Lugar de organización del Máster:** Madrid
**Fecha de realización:** noviembre 2016 a octubre 2017

*Inscripción y programa en el siguiente enlace*

**Jornada de reflexión sobre los refugiados en el Institut de Ciències Polítiques i Socials (ISCP)**

Una respuesta necesaria desde los principios jurídicos y los valores cívicos

**Lugar de la jornada:** c/ Mallorca, 244 pral. Barcelona
**Fecha de realización:** 24 de noviembre de 2016

*Inscripción y programa en el siguiente enlace*

Desde la **Escola de Prevenció i Seguretat Integral**, de la Universitat Autònoma de Barcelona lanzan estos estudios que pretenden proporcionar una formación específica en relación al mundo del perro de trabajo, con tal de poder ejercer la profesión de instructor de perros de trabajo, aportando nuevas tecnologías y herramientas que consigan potenciar al máximo la eficacia en las intervenciones de estos profesionales y, mejorando el proceso de aprendizaje del perro de trabajo.

Los asociados que se inscriban y que vengan de parte de **ADSI** podrán acogerse al precio reducido que se ofrece a alumnos y ex-alumnos de la escuela

- **Curso de Adiestramiento Canino de Base**: *Más información en el siguiente enlace*
- **Postgrado de Instructor de Unidades Caninas de Trabajo**: *Más información en el siguiente enlace*
- **Postgrado en Instrucción de Unidades Caninas de Asistencia**: *Más información en el siguiente enlace*

# Legislación

**LEY 9/2016, DE 28 DE OCTUBRE, DE LA GENERALITAT, DE REGULACIÓN DE LOS PROCEDIMIENTOS DE EMERGENCIA CIUDADANA EN LA ADMINISTRACIÓN DE LA COMUNITAT VALENCIANA**

*PDF de la disposición en el siguiente enlace*

**ORDEN DEF/1756/2016, DE 28 DE OCTUBRE, POR LA QUE SE APRUEBAN LAS NORMAS DE UNIFORMIDAD DE LAS FUERZAS ARMADAS**

*PDF de la disposición en el siguiente enlace*

# Revistas


**Seguritecnia Nº 435. Octubre**

Nuevo número de **SEGURITECNIA**, con reportajes, entrevistas y artículos, destacando:

- **Editorial:** El futuro ha empezado ya
- **Seguripress**
- **Especial Seguridad Aeroportuaria**
- **Entrevista:** David Paja, presidente de Honeywell Security and Fire

*Enlace:* ver revista digital


### Cuadernos de Seguridad Nº 316. Noviembre

En este número de **CUADERNOS DE SEGURIDAD**, además de las secciones habituales de «Seguridad», «Cuadernos de Seguridad estuvo allí», «Estudios y Análisis», o «Actualidad, el lector encontrará:

- **Editorial:** «Security Forum, cinco años al lado del sector».
- **En Portada:** «Seguridad en entidades bancarias».
- **Entrevistas:** «Eduard Zamora, Dirección de Seguridad Personal y Protección, Grupo Banco Sabadell».
- **Artículos:** «La banca ante su más difícil despegue».

*Enlace:* ver revista digital

### red seguridad Nº 74. tercer trimestre 2016.

Nuevo número de **RED SEGURIDAD**, con reportajes, entrevistas y artículos, destacando:

- **Editorial bajo el título** «Un enorme avance para Europa».
- **Trofeos Red Seguridad** «Los trofeos de la Seguridad TIC alcanzan su décima edición».
- **Reportajes:** «Especial Firma Digital».
- **Entrevistas:** «Miguel Ángel Thomas, Director ejecutivo de Ciberseguridad en everis Aeroespacial».

*Enlace:* ver revista digital

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

Para iniciar el proceso de alta como Asociado, envíe un e-mail a secretario@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 – Asociación de Directivos de Seguridad Integral?

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.