NEWS ADSI FLASH
www.adsi.pro

Índice

Asamblea General Ordinaria 2017

Crónica "Martes con..."

Compliance Corporativo en el ámbito de la Seguridad Privada

Carta del Presidente

Nuestros Patrocinadores

Asamblea General Ordinaria 2017

Junta Directiva

El pasado 19 de diciembre, tras la oportuna convocatoria en plazo y forma, celebramos en el Auditorio AXA, la Asamblea General Ordinaria de nuestra Asociación, correspondiente al ejercicio 2017.

Se inició la Asamblea en segunda convocatoria con el siguiente Orden del Día:

1. Lectura y Aprobación del Acta de la Asamblea General Ordinaria celebrada el 20 de diciembre de 2016.
2. Informe del Vicepresidente 1º: Organización Interna.
3. Informe del Vicepresidente 2º: Relaciones Externas.
4. Informe y ratificación del Defensor del Socio.
5. Informe de Tesorería.
6. Auditoría.
7. Informe del Presidente: Gestión ADSI 2017
8. Premios ADSI 2017.
9. Ruegos y Preguntas.

Inició la Asamblea el Secretario de **ADSI**, *Luis Miguel Gómez*, sometiendo a aprobación el acta de la Asamblea anterior, siendo ésta aprobada por unanimidad de los presentes, tras lo que se pasó a los siguientes puntos resumidos a continuación.

Organización Interna

Se detallaron las funciones que tiene encomendadas la vocalía, siendo las más sobresalientes las de captación de nuevos patrocinios, nuevos socios y la publicación de la revista **News ADSI Flash**. Se dieron datos de patrocinios actuales, número de socios, total revistas publicadas durante el ejercicio 2017, así como total de notas informativas.

Relaciones Externas

Se dio buena cuenta de las visitas institucionales que **ADSI** ha realizado en el presente año 2017, así como la asistencia a actos y jornadas de seguridad.

También informó de la totalidad de *"martes con..."* celebrados durante el año 2017, dando detalles de sus contenidos y ponentes.

Memoria del Defensor del Socio 2017

Ricardo Domingo dio detalles de sus actividades llevadas a cabo en el año 2017 como Defensor del Socio de **ADSI**

Informe Tesorería

Se detallaron las cuentas del presente ejercicio y el presupuesto previsto para el próximo año.

- Informe financiero – fiscal 2016 para aprobación en Asamblea Ordinaria 2017.
- Informe previsión financiero – fiscal 2017.
- Presupuesto 2018.

La contabilidad de la Asociación se realiza según normas del Ministerio de Hacienda para las entidades, organizaciones y asociaciones sin ánimo de lucro, las cuales deben llevar los libros de contabilidad debidamente cumplimentados, no debiendo presentarlos en ninguna entidad de la Administración y estando a disposición de los Socios, que podrán revisarlos, previa solicitud en la Asamblea General Ordinaria.

Informe Auditoría

ONESEVEN Auditoría Consultoría SL, explicó el resultado de la Auditoría llevada a cabo sobre las cuentas anuales simplificadas del ejercicio cerrado a 31 de diciembre de 2016, con el siguiente contenido:

- Introducción
- Ajustes y reclasificaciones de auditoría
- Balance de situación a 31 de diciembre de 2016
- Cuenta de resultados de 2016
- Principales procedimientos de auditoría y conclusiones
- Opinión de auditoría

Informe de Gestión del Presidente

El Presidente *Francisco Poley*, expuso su informe de gestión, elaborado en los siguientes puntos:

- Resumen año 2017.
- Proyectos año 2018.

Premios ADSI 2017

La convocatoria de premios **ADSI** 2017 quedó aplazada para el 2018.

Artículo 22 del R.R.I.

Para finalizar, los Socios, durante el turno de "Ruegos y Preguntas", pudieron efectuar preguntas a la Junta Directiva que deberá contestar en el plazo máximo de diez días naturales si no fuera posible durante el Acto.

Los ruegos se analizarán en la siguiente reunión de la Junta Directiva, comunicando al Socio el resultado correspondiente.

Carta del Presidente

Francisco Poley
Presidente ADSI

Apreciados soci@s.

Como por todos es sabido, el pasado día 19 de diciembre tuvo lugar la Asamblea General Ordinaria Anual 2017.

Tras las elecciones del 7 de marzo y, en cumplimiento de los compromisos electorales adquiridos, la Junta que presido se marcó como objetivo un plan de acción fundamentado en tres ejes:

- ✓ Definir las prioridades de **ADSI**, tanto las externas; actividades, colaboraciones, etc. como las de todos los ámbitos de gestión interna.
- ✓ Desarrollar e implantar un plan de acción que fomente la transparencia, la participación y el liderazgo.
- ✓ Establecer controles regulares que permitan hacer un seguimiento eficaz de los resultados.

En consecuencia se adoptó la decisión de auditar, por una empresa externa, la gestión del ejercicio 2016.

Los resultados de la misma fueron presentados por el equipo auditor a los socios asistentes a la Asamblea General que refrendaron en votación por mayoría absoluta la gestión 2016.

En este punto debo comunicar que para cumplir con los plazos establecidos se ha tenido que realizar un ímprobo trabajo de documentación y archivo que, a su vez ha generado divergencias y opiniones encontradas entre los integrantes de la Junta Directiva. Diferencias que culminaron con la dimisión de varios miembros de Junta entre los días 17 y 18 de diciembre.

No dudo que se hayan podido cometer errores pero no me resigno ante las dificultades que, en un primer instante, me hicieron dudar.

Lo ocurrido me ha exigido un sincero ejercicio de autocrítica. Asumo la responsabilidad de no haber podido cohesionar las diferentes opiniones o ideas surgidas pero pongo en valor que, todas las decisiones, sin excepción, se han tomado en el seno de las reuniones ordinarias de la Junta Directiva y posteriormente, sometidas a refrendo en el máximo órgano de representación como es la Asamblea General, cuya función principal, es dotar de voz y voto a todos los asociados.

Quiero transmitir mi más sincero agradecimiento hacia los compañeros de Junta por su esfuerzo, empeño y trabajo que, desde ahora como socios, no dudo continuarán realizando en pro y para **ADSI**.

Ilusionado, como estoy, por el futuro, creo que es el momento de abrir caminos y seguir avanzando con constancia, esfuerzo y trabajo para la consecución de los objetivos fijados.

Creo que durante estos nueve meses se ha hecho un buen trabajo que ha concluido con la presentación del informe de auditoría. Había que actuar y había que explicarlo para que discurso y realidad fueran concomitantes.

El mérito de las organizaciones asociativas no es todo lo que llegan a hacer, que en mi opinión es mucho, sino que lo hagan a pesar de las dificultades. Intentar hacer las cosas bien por el simple gusto de hacerlas bien hechas.

Finalizo con las palabras de un célebre filósofo: *"Desde la humildad la vida nos recuerda que somos imperfectos, que los planes, en ocasiones, no salen como queremos, que lo que hacemos tiene consecuencias y que, a veces, las consecuencias llegan sin haberlas buscado"*.

Me despido deseando un esperanzador año 2018.

Francisco Poley Herrera
Presidente de ADSI

Crónica "Martes con..." Compliance Corporativo en el ámbito de la Seguridad Privada

Junta Directiva

El pasado 12 de diciembre, desde **ADSI**, se organizó esta jornada para nuestros socios y patrocinadores en formato mesa-debate sobre Corporate Compliance.

Contamos con la inestimable presencia de tres ponentes de contrastada reputación, como son;

D. Fernando Carlos De Valdivia González; Doctor en Derecho por la UB y la Universidad Roma. Magistrado de Juzgado de 1ª Instancia de Barcelona.

D. Eligio Landin López; Facultativo del CNP, Licenciado en Derecho y Ciencias Políticas.

D. Iván Bayo Roque; Licenciado en Derecho y Profesor Asociado de la UB. Socio de MBC Iuris.
D. David A. SanMartín; Detective Privado y Licenciado en Derecho.

Una jornada específica y adaptada a la actividad de Seguridad Privada, la figura del Director de Seguridad y sus posibles responsabilidades jurídicas y penales.

Durante la misma, los ponentes nos ofrecieron información relativa al cumplimiento normativo de carácter legal y reglamentario que regula la actividad de Seguridad Privada con especial énfasis en su tratamiento orientado a su encaje y posterior desarrollo dentro de un sistema de "Compliance Corporativo", en base a lo estipulado, entre otras normas, en la UNE 19601.

Se debatió el reciente régimen de responsabilidad penal que afecta a todas las organizaciones, a raíz de la reforma del Código Penal y, en particular en todo lo referente a la figura del Director de Seguridad.

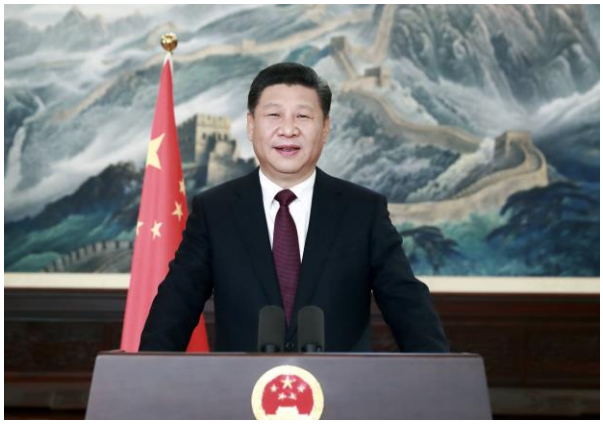
Dentro de este debate se obtuvieron respuestas a la actual encrucijada normativa en la que se encuentra el sector. Pendiente de la publicación de un nuevo Reglamento que desarrolle la actual Ley 5/2014, la reforma de la Ley Orgánica 15/1999 de Protección de Datos y al RGPD UE 2016/67, de obligada aplicación a partir del 25 de mayo de 2018.

A la finalización de la jornada pudimos disfrutar de un agradable ágape en las instalaciones del hotel AC Diagonal.

2018 presenta un elevado riesgo de una crisis geopolítica global

Fuente: El País
Alicia González

Eurasia Group alerta de la creciente amenaza de una nueva guerra fría tecnológica



No presenta buenas perspectivas el recién estrenado 2018. El riesgo de una crisis geopolítica severa, el "equivalente a la crisis financiera internacional de 2008", es muy elevado, según el diagnóstico de la consultora de riesgo Eurasia Group. El peligro procede tanto del ámbito de la ciberseguridad y del terrorismo como de un error de cálculo en los conflictos abiertos con Corea del Norte, Siria o Rusia, que pueden desatar una crisis en cualquier momento. De fondo, la ausencia de un liderazgo mundial ante el deliberado paso atrás del Estados Unidos de Donald Trump.

Cada mes de enero Eurasia Group presenta su lista de los principales riesgos que afronta el mundo en ese año, una base para los debates que a finales de mes tienen lugar en el Foro Económico Mundial que se celebra en la estación suiza de Davos. Y no van a ser buenas noticias para los delegados a la cita alpina. Pese a la recuperación económica sincronizada a nivel global y la carrera al alza de las bolsas, el mundo va a tener que lidiar con la creciente amenaza de un accidente imprevisto, lo que en la jerga se denomina un cisne negro, que puede desatar una crisis global. "2018 presenta el escenario con mayores riesgos geopolíticos desde 1998", explicaba este martes por teleconferencia su presidente, Ian Bremmer.

El 'América primero' de la Administración de Donald Trump ha erosionado el orden político internacional que ha liderado Estados Unidos desde la Segunda Guerra Mundial, dando pie a un vacío de poder que, según la consultora que preside Bremmer, por primera vez China se muestra dispuesta a ocupar. Y ahí surge el primer riesgo: que lo hará según sus propias reglas, las de un Estado autoritario que lidera la inversión en nueva tecnología —frente al sector privado que es quien lleva la batuta en los países occidentales—, con una nueva arquitectura comercial y de inversión guiada por intereses puramente bilaterales y con el valor de la no intervención como máxima en sus relaciones internacionales. "China está fijando los estándares internacionales con menor resistencia que nunca", advierte el documento de la consultora. Y Bremmer matiza: "China no reemplazará a EE UU como potencia mundial, su único interés es el liderazgo económico y tecnológico".

Con esa política, China ya ha logrado superar a Estados Unidos en número de robots operativos (340.000 frente a 250.000), usuarios de Internet (773.000 frente a 246.000) o en los avances de la economía digital, con 5,5 billones de pagos por teléfono móvil frente a los 112.000 millones de Estados Unidos.

Ese escenario en el que los Estados tienen un creciente papel en la carrera tecnológica y económica agrava el riesgo de ciberataques, uno de los cisnes negros de 2018, junto a Corea del Norte, Siria, Rusia o nuevos ataques terroristas porque puede provocar una sobrerreacción y abrir un nuevo conflicto. Y suscita, a juicio de la consultora, la amenaza de un nuevo proteccionismo 2.0, azuzado a su vez por el nuevo entorno de creciente protagonismo de los populismos. "No estamos al borde de una tercera guerra mundial", tranquiliza la consultora, pero en la ausencia de un garante de la seguridad global, con la proliferación de actores regionales y privados con capacidad de desestabilización, el mundo es un lugar mucho más peligroso".

Eurasia Group pone, asimismo, el acento en el incierto futuro que afronta México, con el riesgo creciente de que las negociaciones sobre el acuerdo de libre comercio con EE UU y Canadá no tengan buen fin y la celebración de unas elecciones, cuya carrera lidera en estos momentos el líder de Morena, Andrés Manuel López Obrador, que puede provocar inestabilidad en los mercados conforme se acerque la fecha electoral.

Las relaciones entre Estados Unidos e Irán son otro de los riesgos más destacados para 2018, tanto a nivel político como para los mercados, por su implicación sobre el sector energético. Las recientes protestas que viven diversas ciudades iraníes "no se veían venir", según admite Bremmer, por más que la demanda de los jóvenes iraníes sean similares a las de otras economías en crisis, que exigen empleo y cierta apertura. "Pero no creo que esto vaya a ser como las protestas de 2009 aunque obligará a Rohaní a acometer reformas", apunta. En ese enfrentamiento con las autoridades de Teherán, Trump se ha apoyado en Arabia Saudí, sumida a su vez en un programa reformista que "va demasiado rápido, demasiado lejos y demasiado tarde", por lo que la consultora no le augura un gran éxito. "Riad está fracasando en todas sus operaciones exteriores, desde Yemen a Líbano y si me preguntas qué pasará de aquí a cinco o diez años, yo apostaría que esta política va a fracasar y restará protagonismo" al Reino del Desierto, explica Bremmer.

Lista de las 10 novedades del nuevo borrador del Reglamento de Seguridad Privada

Fuente: Red Minerva

Nos hemos leído las 388 páginas del último borrador del Reglamento de Seguridad Privada y hemos realizado el análisis de todas las novedades y las noticias relacionadas. Más abajo te ofrecemos el PDF en versión actualizada, pero **para que no te lo tengas que leer entero, te destacamos sus puntos principales**. Si el Ministerio del Interior cumple con su palabra, este Reglamento verá la luz este 2017. Recordemos que ya hace 3 años de la publicación de la Ley 5/2014, de 4 de abril, de Seguridad Privada (en adelante, Ley de Seguridad Privada), pero es que **hace más de 12 años que se aprobó el Reglamento de Seguridad Privada que está vigente a día de hoy**.

Este desfase normativo hace que **el sector de la seguridad privada esté desordenado, tenga ineficiencias, falta de regulación y control, ausencia de herramientas, descoordinación con las Fuerzas y Cuerpos de Seguridad y, sobre todo, falta de adaptación a la realidad, riesgos y amenazas** que afectan al personal de seguridad, a nuestros ciudadanos, a las empresas y, por ende, a las instituciones.

A continuación, desgranamos las principales novedades que previsiblemente incluirá el Reglamento:

1. Su objetivo principal: Aumentar la eficacia de los servicios de seguridad a los que tienen derecho los ciudadanos y **dar respuesta a las necesidades reales de seguridad en cada momento, lo que obliga a permitir cierta flexibilidad en el marco jurídico** para que la seguridad se pueda adaptar con cierta rapidez a las necesidades de seguridad de la sociedad.

2. Creación de un nuevo Registro: Se creará un Registro Nacional de Seguridad Privada único para todo el territorio nacional que permitirá tener actualizado un mapa de los servicios de seguridad privada a nivel estatal **facilitando la integración y coordinación con las Fuerzas y Cuerpos de Seguridad**.

3. Relación con las Fuerzas y Cuerpos de Seguridad: De sumisión, dependencia y subordinación a **coordinación, colaboración y corresponsabilidad**. Ya lo establecía la Ley de Seguridad Privada de 2014, pero ahora se hace aún más énfasis con el objetivo de mejorar la calidad, eficacia y eficiencia de los servicios en favor de la preservación de la seguridad ciudadana y la lucha contra el delito.

4. Incentivos económicos, sí… ¿pero para quién?
A. Para los que quieran crear empresas de seguridad privada (y a las ya existentes) **se reducen o eliminan exigencias que provocaban desembolsos desproporcionados e innecesarios**, excepto en lo relativo a medidas de seguridad obligatorias (ver punto 9).

B. **En lo que se refiere a concursos públicos para contratar servicios de seguridad, a partir de ahora, se priorizarán los criterios cualitativos en vez de tener en cuenta solo el precio**. Esta priorización es positiva porque debería provocar que las empresas no compitan en reducir el precio/hora de vigilante de seguridad a toda costa, con lo que ello implica para los sueldos del profesional de la seguridad. Estos criterios cualitativos dependerán principalmente de los Directores de Seguridad y de los Directores de Compras que podrán tener en cuenta factores como la formación permanente por parte de la empresa a su propio personal, la rotación de servicios, las vacaciones del personal de seguridad, la inversión en herramientas tecnológicas de soporte al vigilante, entre otras, con la intención de **que las empresas de seguridad que aporten más valor y no las más baratas sean las que ganen más contratos**.

5. Consideración de Agente de Autoridad:
Un tema especialmente necesario, a la vez que delicado, es el de la consideración de agente de autoridad al personal de seguridad privada en el ejercicio de sus funciones. Este reglamento **prevé la protección jurídica al profesional de seguridad cuando se le agreda o desobedezca cuando está cooperando y bajo el mando de las Fuerzas y Cuerpos de Seguridad**, aunque éstas no estén presentes en el lugar de los hechos. Falta ver cómo se traduce esto en la práctica. En la actualidad la jurisprudencia exige que haya un convenio o acuerdo por escrito entre la Policía y la empresa contratante de los servicios de seguridad en la que se definan el marco temporal, geográfico y funcional de los servicios de seguridad, **acuerdo que rara vez existe provocando que rara vez se pueda considerar a un vigilante de seguridad como agente de autoridad, con la merma que eso supone en su seguridad y en la eficacia de su función**. Esperemos que en la práctica se pueda llevar a cabo la flexibilización de este punto.

6. Servicios mínimos ante situaciones de huelga: Se incluye en este Reglamento la posibilidad de que la autoridad laboral decrete servicios mínimos del personal de seguridad ante situaciones de huelga en supuestos en los que los servicios de seguridad se declaren esenciales, tales como:

1. La vigilancia y protección en centrales nucleares, refinerías, transporte y distribución de materias inflamables, fábricas de armas de fuego, centros de telecomunicaciones, hospitales y juzgados.
2. El Depósito, custodia, recuento y clasificación de monedas y billetes.
3. Protección personal a autoridades y cargos públicos.
4. Operadores en centrales receptoras de alarmas.
5. Personal de seguridad de establecimientos, instalaciones o actividades en los que los servicios de seguridad privada se hubieran impuesto con carácter obligatorio.

7. Servicios de control de accesos: por primera vez en la legislación sobre seguridad privada, se especifican los

requisitos, obligaciones y facultades que debe cumplir el personal de seguridad privada en la ejecución de los servicios de control de accesos.

8. Ampliación de las tipologías de servicio de seguridad reguladas: Se ha hecho una recopilación de las tipologías de servicio de seguridad que se prestan en la actualidad para regularlas, ponerles condiciones y requisitos varios. Los servicios que contemplará el Reglamento son:

1. La protección de bienes en vías públicas.
2. La vigilancia y protección de buques mercantes y pesqueros.
3. La protección de cajeros automáticos.
4. La protección de medios de transporte.
5. La realización de rondas o vigilancia discontinua.
6. La vigilancia perimetral de centros penitenciarios y centros de internamiento de extranjeros.
7. La vigilancia de edificios o instalaciones de organismos públicos.
8. La participación en servicios encomendados a la seguridad pública.
9. La vigilancia de polígonos industriales y urbanizaciones, complejos o parques comerciales y de ocio.
10. La vigilancia de recintos y espacios abiertos que se encuentren delimitados y acontecimientos culturales, sociales o deportivos.
11. Los servicios de videovigilancia.
12. Los servicios de protección para personas o grupos de personas determinadas.
13. El transporte, protección y depósito de dinero, joyas u otros objetos valiosos, de obras de arte y antigüedades, así como de armas, explosivos y sustancias peligrosas.
14. La instalación y mantenimiento de sistemas de seguridad.
15. Los servicios de alarmas de seguridad.
16. Los servicios de investigación privada (detectives privados).

9. Regulación de las medidas de seguridad privada para ciertas empresas:

A. Se regulan las medidas de seguridad privada, sus características, naturaleza, exigibilidad y finalidades, qué organismo puede imponerlas y definición de responsabilidades. Esto es un poco delicado (sobre todo para las empresas pequeñas) que estarán obligadas a invertir en medidas de seguridad. Esperamos que se flexibilice y se haga progresivo para que esta no provoque problemas económicos en las empresas de seguridad, lo que repercutiría también en el personal que trabaja en ellas.

B. Se establece que **la principal medida de seguridad organizativa es la constitución de un Departamento de Seguridad en las empresas**, acompañado de los planes de seguridad, cuya elaboración y actualización queda atribuida únicamente a la figura del Director de Seguridad.

C. Otro paso importante en la creación (y en los mejores casos consolidación) de los Departamentos de Seguridad en las empresas es la **específica y amplia regulación sobre las Centrales receptoras de alarmas de uso propio así como de los Centros de Control o de Videovigilancia** cada vez más habituales en empresas de mediano y gran tamaño.

10. ¿Y la Seguridad de la Información y Ciberseguridad que está tan de moda?

A. Una gran novedad, aunque no podía ser de otra manera, es la inclusión (por fin) de la seguridad informática en el reglamento. **Se establecen requisitos y condiciones a las empresas que presten este tipo de servicios de Seguridad de la Información o Ciberseguridad para garantizar la calidad de sus servicios** en función de para qué tipo de cliente estén trabajando. Aunque seguramente escaso, este constituye el primer desarrollo reglamentario de la Seguridad Informática en España. Histórico.

B. En línea con lo anterior, otra novedad es la **necesidad obligatoria de que las empresas de seguridad informática y las empresas de seguridad privada que quieran prestar servicios en sectores estratégicos definidos en la normativa de Infraestructuras Críticas se sometan a una auditoría externa obligatoria**. Esta obligatoriedad es una tendencia cada vez más habitual en todos aquellos sectores económicos y esenciales tales como el sector financiero o el sector sanitario, ejemplo de la importanica que el legislador le atribuye al sector de la seguridad privada.

PUNTOS POSITIVOS DE ESTA PROPUESTA DE REGLAMENTO DE SEGURIDAD PRIVADA

Como siempre, depende. Depende de si eres un vigilante de seguridad, un detective privado que está pagando autónomos, una empresa de seguridad pequeña o una empresa de seguridad grande.

En términos generales el Reglamento es positivo al:

1. **Regular más el sector y dar más seguridad jurídica a profesionales y empresas** por estar ejerciendo funciones que están previstas en la ley.
2. **Mantener vigentes indefinidamente las TIP ya obtenidas así como los diplomas expedidos** hasta la fecha de cualquier vigilante de seguridad, sus especialidades y los grados y cursos de detective privado y Director de Seguridad.
3. **Regular el intercambio de información, no solo hacia la Policía sino hacia el personal de seguridad privada** para que pueda: (1) adoptar medidas de protección adecuadas ante riesgos e incluso (2) facilitar datos personales para prevenir peligros reales para la seguridad ciudadana o para evitar comisión de delitos.
4. **Reconocer social e institucionalmente al sector**, estableciendo oficialmente el Día de la Seguridad Privada, concediendo reconocimientos honoríficos al personal de seguridad privada.
5. **Establecer medidas de seguridad obligadas para las empresas de seguridad privada:** (1) sistema de seguridad físico y electrónico, (2) área restringida destinada a la custodia de información y documentación sensible, (3) sistema informático acorde con la clasificación del nivel de criticidad, (4) un plan de seguridad frente a riesgos y amenazas y (5) un plan de contingencia para garantizar la continuidad de la actividad cuando se materialicen las amenazas. Estas medidas son coherentes tratándose del sector en cuestión, aunque la

clave está en cuánto tiempo permitirán dar de alta estas medidas de seguridad y si darán ayudas a las que las empresas puedan acogerse.

6. **Darle mayor contenido a la figura del Director de Seguridad al considerarle interlocutor y enlace con la Administración** en relación a los siguientes ámbitos. En la mayoría de empresas esos ámbitos están diseminados entre diferentes departamentos por lo que el hecho de que lo incluya el Reglamento da fuerza para que dichas competencias las acabe vehiculando el Director de Seguridad:
   a) Materias clasificadas.
   b) Infraestructuras críticas.
   c) Seguridad de la información y las comunicaciones.
   d) Blanqueo de capitales y financiación del terrorismo.
   e) Protección contra incendios.
   f) Seguridad laboral.
   g) Intercambio de información con las Fuerzas y Cuerpos de Seguridad sobre cuestiones relativas a delincuencia, de las que se tuviesen indicios o conocimiento en su entidad.
   h) Actuación ante situaciones de emergencia que afecten a la propia empresa o cuando esta aporte recursos en caso de situaciones de catástrofe o emergencia pública.
   i) Cualquier acción de colaboración público-privada en el marco de la Estrategia de Seguridad Nacional.
   j) Cualquier otro que afecte a la seguridad de su organización y contribuya a la persecución de delitos e infracciones.

PUNTOS NEGATIVOS DEL REGLAMENTO

Aún así, creemos que este borrador de Reglamento es mejorable en los siguientes puntos:

1. Se pierde una oportunidad de profesionalizar el sector: cada vez hay menos gente que quiere ser vigilante de seguridad por las condiciones laborales y económicas que lleva asociadas una profesión con tantos riesgos intrínsecos. Si no se hace atractiva la profesión, difícilmente se atraerá a personas que quieran dedicarse a la seguridad privada vocacionalmente.

2. Se podría haber aprovechado para exigir mayor calidad en la formación impartida en los Centros de Formación y Universidades: las formaciones de seguridad privada no tienen un método pedagógico moderno, dinámico ni interactivo; los contenidos impartidos son cada vez más teóricos y las prácticas solo se hacen cuando son imprescindibles, sin importar si el candidato ha adquirido realmente los conocimientos y habilidades que lleva asociada la TIP. **Tampoco está previsto el reciclaje en cursos complementarios que ayudarían al profesional a ampliar sus capacidades y habilidades**, tales como cursos de ciberseguridad, autoprotección, gestión de conflictos, entre otros, que va a necesitar a lo largo de su trayectoria profesional.

3. Flexibilizar en términos prácticos y viables la figura de agente de autoridad (como pasa en algunos países de nuestro entorno): se ha producido un avance no exigiendo la presencia de FCS en el lugar de los hechos y reconociéndola en algunos supuestos concretos pero, aún así, con el actual redactado, será difícil que jurídicamente se reconozca esta protección jurídica en todos los casos en los que se produzca una agresión o desobediencia a un profesional de la seguridad en el ejercicio de sus funciones.

En resumen, este borrador del Reglamento es un avance en muchos ámbitos. Aún así, ha dejado algunos temas a medias que podría haber consolidado en una norma de tanta repercusión para el sector y para la seguridad en general.

Si aún así quieres leer las 388 páginas del borrador completo o ampliar algunos de los apartados, *aquí lo tienes en formato PDF*.

2017, el año en que las empresas se concienciaron en ciberseguridad

Instituto Nacional de Ciberseguridad

Este año comenzamos ofreciéndoos una serie de consejos para que empezarais el mismo con buen pie en lo relativo a la ciberseguridad. Diez buenos hábitos en el uso de las tecnologías que nos permitirían, y nos permiten, hacer un uso seguro de Internet y los servicios que ofrece la Red. Además, este año más que nunca tendríamos que hacer uso de ellos porque sin duda ha sido uno de los más prolijos en cuando a ciberincidentes.

Durante el primer trimestre, entre las oleadas de phising y de malware que nuestros sistemas de inteligencia detectaron y de las que os informábamos a través de nuestro servicio de avisos y boletines, desaparecía el soporte para Windows Vista, otro sistema operativo de Microsoft que nos deja para pasar a mejor vida o quizás, en algunos casos, seguir viviendo pero sin actualizaciones como le ha ocurrido a su predecesor Windows XP del que aún quedan bastantes dispersos por todo el mundo. Además, al servicio de respuesta a incidentes de INCIBE, CERTSI_, llegan las primeras alertas relativas al "whaling" o también conocido como el "Fraude del CEO". ¡Los "peces gordos" también están en la mira de los ciberdelincuentes! Aunque en realidad todos somos objetivos potenciales.

Pero sin duda, el incidente que nadie olvidará y que formará parte de la historia de la ciberseguridad, fue el que sucedió el viernes 12 de mayo, que bien podría haber sido 13 y que afectaba a **todos los sistemas operativos Windows**. Mencionar que aunque el malware o virus de tipo **ransomware** ya era bastante conocido por muchos, será un concepto que todo el mundo recordará gracias a la amplia difusión y repercusión que el ciberincidente tuvo en los medios. Expertos y legos en ciberseguridad van a asociar durante mucho tiempo "ransomware=WannaCry" algo que perdurará en la memoria del sector informático durante años. En muy poco tiempo esta amenaza afectó a miles de ordenadores en distintas empresas las cuales desconocían cómo hacer frente al problema, y no hay nada más desesperante que tratar de poner barreras a algo de lo que no sabes cómo defenderte, algo que en ciberseguridad es bastante común. Por fortuna y gracias a la experiencia y colaboración entre los diferentes CERT's, empresas del sector de la ciberseguridad, afectados y demás protagornistas, se pudo contener la amenaza. En este caso concreto, se podía haber prevenido instalando la actualización que Microsoft publicó dos meses antes.

Aún con las camisas remangadas por el incidente de WannaCry y apenas un mes después, el 27 de junio, conocimos a Petya (o una variante de este), otro ransomware "primo" del primero, ya que aprovechaba entre otros vectores de ataque, la misma vulnerabilidad MS17-010 con la que se propagaba. No obstante, este malware era más sofisticado y más dañino, pues además inutilizaba el equipo pero afortunadamente, en España tuvo un escaso impacto.

Mientras, entre estos dos importantes incidentes, y aprovechando el pánico, miedo, sensación de inseguridad que Wannacry había generado, los ciberdelincuentes en su afán de lucro económico comenzaron a generar campañas de correos en las que se instaba a las empresas que lo recibía a pagar un bitcoin a cambio de no ser "hackeadas". Este mensaje con intención de extorsionar a las empresas evolucionó en julio incluyendo en su lista de ataques los del tipo DDoS (Denegación de Servicio distribuida), algo que en principio es muy difícil de evitar. El objetivo, atemorizar. Como vemos, la imaginación de los delincuentes de Internet no tiene límites.

Pasada la primera mitad de año, vivimos el verano entre actualizaciones de seguridad de gestores de contenidos, fugas de información, más oleadas de ransomware y phishing, vulnerabilidades en el software y demás amenazas con las que desde INCIBE estamos muy acostumbrados a lidiar. No es hasta octubre donde se descubre otra de las vulnerabilidades más importantes de este 2017: un fallo en el protocolo WPA2 pondrá en riesgo la seguridad de las redes wifi. A priori se trata de un problema muy serio ya que aunque la vulnerabilidad no permite obtener la contraseña para acceder a la red, sí que es posible espiar el tráfico de la misma que no vaya por canales cifrados, esto es, navegar por webs que usen SSL (https://www.incibe.es) por poner un ejemplo. Afortunadamente los fabricantes publicaron actualizaciones rápidamente.

Todos estos incidentes y muchos más, han hecho que estudios recientes estimen que el cibercrimen tenga un impacto global en términos macroeconómicos cercano al 1% del PIB, un 0,2 más que el pasado año aproximándose a un incremento en torno a 70.000 millones de euros haciendo casi un total de 350.000.

El PIB generado por el cibercrimen ha pasado del 0,8% en 2016 al 1% en 2017

La inteligencia competitiva en los países del entorno de competencia de Españpa

Fuente: Grupo de Estudios en Seguridad Internacional
http://www.seguridadinternacional.es/

Se realiza una comparativa acerca de qué es lo que se hace en los países referentes de la Inteligencia Competitiva (IC). Se distingue si la IC se potencia desde el Estado Top-Down o si es desde las empresas Bottom-Up.

Con la Inteligencia Competitiva, en adelante IC, nos encontramos ante una práctica empresarial destinada a la mejora en la toma de decisiones de las empresas. La IC constituye una disciplina que ha tenido un gran desarrollo en las últimas décadas del siglo XX y, en especial, en el siglo XXI, propiciado por la desaparición de las fronteras financieras y la apertura de las fronteras económicas, tal y como indica Olier (2013). Sin embargo su grado de implantación en los distintos países ha sido heterogéneo. Factores como la cultura país, la necesidad de competir ante una escasez de recursos o una crisis económica y el entorno empresarial han influido en ello. A continuación enunciamos los principales países referentes en la materia y las características de su implantación.

Francia

Es un ejemplo donde la IC es fundamental en la estrategia del país, estableciéndose sobre distintas capas por organizaciones territoriales y con un modelo impulsado desde la Administración *Top-Down* hasta el punto que la IC se conozca como Inteligencia Económica. (Harbulot y Baumard (1997).

(Montero y Martín, 2008) y (Debelque y Pardini, 2011) destacan, como aspectos clave, la consideración de la Inteligencia Económica como propiedad del Estado con visión a largo plazo y la existencia de un órgano público que gestione la materia y soporte a las empresas de su *know how* en distintos ámbitos de Inteligencia.

Con cierto retraso respecto a otros países y después de crearse una cultura de identidad nacional en las décadas posteriores a la Segunda Guerra Mundial y a la pérdida de sus colonias, como Indochina o Argelia, Francia se incorpora con interés, a partir de la década de los 90, con un enfoque de inteligencia más cercano a la concepción escandinava de "inteligencia social" que a la anglosajona. Un factor que procede destacar es la inteligencia colectiva del modelo francés, de intercambio de información, de elaboración de sinergias y de enfoque a través de distintas perspectivas que den una visión integral, así como de progreso de capacidades individuales (Bahouka-Debat, 2011).

Como hitos relevantes en el desarrollo de la IC en Francia:

- El Informe Martre en 1994 publicado por el Centro de Análisis Estratégico que desarrollaba qué debía ser la IC y propuso los objetivos de: 1.- Difundir la práctica de la inteligencia económica en la empresa. 2.- Optimizar el flujo de información entre el público y el sector privado. 3.- Diseñar Bases de datos de diseño basados en las necesidades del usuario. 4.- Movilizar el mundo de la educación y la formación.
- El Caso Gemplus por la pérdida de control de esta empresa dedicada a la criptología.
- La creación en 1995 del Comité para la Competitividad y la Seguridad Económica (CCSE) por Eduardo Balladur.
- La creación de la Agencia para la Difusión de la Información Tecnológica (ADIT) en 1995.
- La fundación de la Escuela de Guerra Económica (EGE) por el General Jean Pichot-Duclos en 1997.
- La creación como cargo público de Allain Juilet como responsable de la Inteligencia Económica en el año 2003. *Haut Responsable à l'Intelligence Economique* (HRIE).
- El Informe *Intelligence économique, compétitivité et cohésion sociale* realizado por el diputado (Bernard Carayon, 2003) para el Primer Ministro.

La IC en Francia se estructura en cuatro aspectos básicos (Gonzalvo, 2015) que son los siguientes:

- Se entiende la inteligencia como necesaria para el Estado y con orientación a largo plazo.
- Se crea un órgano encargado de fomentar la inteligencia y ayudar al desarrollo de las empresas.
- Se presta apoyo para establecer modelos en las empresas de las distintas tipologías de inteligencia adaptada a sus necesidades.
- Se establece un modelo de inteligencia territorial alineando los recursos de los órganos locales, provinciales, regionales y nacionales.

En relación a su organización, Kossou y Smith, (2008):

- Presenta como eslabón clave el papel de las Cámaras de Comercio, que utilizan la red de 58 países de habla francesa y que está apoyado por la estructura militar, como sirven de ejemplo las intervenciones de 2013 en Mali.
- Se establece una red donde participan asociaciones, patronales (por ejemplo destacar el apoyo de la organización patronal MEDEF formada principalmente por PYME), en la que el poder público ayuda, integra y reduce incertidumbre.
- En el ámbito formativo, además de la EGE, hay que reseñar los programas de la Escuela Militar INHESJ, la Escuela europea de Inteligencia Económica, Universidad Paris-Est Marne-la-Vallée, la Escuela Internacional del procesamiento de la información, la Universidad Montesquieu Bordeaux IV y Universidad de Aix-Marsella.
- La inteligencia francesa ha servido de modelo en sus antiguas colonias, tales como Argelia, Marruecos o Túnez, destacando la celebración de actividades como el *Fórum d´intelligence Economique et Development* celebrado en Dakar en 2008, la creación de una escuela de Inteligencia Económica en el Congo en el año 2009 o la creación de la agencia marroquí de Inteligencia Económica (AMIE).

En el continente africano destaca el grupo francés Bolloré por su poder en la gestión estratégica del transporte y la logística, mientras que entre las empresas africanas con sistemas de Inteligencia Competitiva, de un nivel similar al de países occidentales, destacan las denominadas cinco hermanas: SGMB Bank (Marruecos), KeniaAirways (Kenia), Orascom (Egipto), MTN y Vodacom (Sudáfrica).

Estados Unidos

Los países anglosajones se caracterizan por la no intervención directa en cuestiones privadas, las ideas ultra-liberales de la época, impedían aplicar una IC de carácter nacional (Martre, Clerc y Habulot, 1994) pero sí en el asesoramiento, en el apoyo en el extranjero y, sobre todo, en asociar el dominio económico con el militar (Gilad, 2008). Especialmente, en este último aspecto, a partir de la Segunda Guerra Mundial, en el esfuerzo de captación de información y análisis de datos, frente a sus rivales al otro lado del telón de acero.

El apoyo institucional se plasma en 1992, rompiendo el histórico carácter poco intervencionista de su ejecutivo, cuando la Administración Bush decide que del presupuesto de la CIA se destinen dos tercios para información económica. (Herring, 1999). Para ello se apoya en la *Intelligence Community*, formada por 17 agencias de inteligencia como la CIA, NSA o DIA, que recolectan y transmiten la información esencial que a los poderes estatales y las empresas del país necesitan para la toma de decisiones.

Otro apoyo se realiza a través del *Department of Commerce* para favorecer el desarrollo internacional de las empresas estadounidenses. Esta ayuda, que se lleva a cabo a través de las 12 oficinas que la forman, se realiza mediante la confección de informes país, labores de ciberseguridad o de *lobby*. Entre las oficinas se encuentran la *Economic and Statistic Administration, el Bureau of Economic Analysis, la International Trade Organization, el Bureau of Industry and Security o la US Patent and Trade Office.*

Sin embargo la IC en las PYME no tiene apenas desarrollo (Agencia de Información de la Diputación Foral de Bizkaia, 2007) mientras que la U.S. Chamber es el primer lobby mundial en importe invertido en sus acciones (Steinbach, 2013) con más de mil millones de dólares en operaciones de influencia.

También ha gozado de una legislación que protege sus actividades, como la Ley de Espionaje Económico (1996), de protección del patrimonio de las empresas y, ese mismo año, la creación del Advocacy Center, para alinear los recursos del país en la gestión de los contratos internacionales que considerasen capitales.

Es de destacar el grado de implantación de la Inteligencia Competitiva en las grandes empresas norteamericanas. Sirva como dato que, ya en el año 1999, según recogen (Prescott y Miller, 2001), el 80% de las compañías, con un nivel de facturación superior a 10.000 millones de dólares, disponía de un departamento de Inteligencia Competitiva. A ello han ayudado consultoras como Kroll o SRI International entre otras.

Entre las revistas especializadas destacan dos: el *Daily Economic Intelligence Brief* (DEIB) y el *Economic Intelligence Weekly* (EIW), como fuentes de difusión de información relevante sobre la materia. También es de reseñar el *Advocacy Center* del Departamento de Comercio de los EEUU, dedicado a canalizar trabajos para la internacionalización de la empresa estadounidense y el Consejo de Economía Nacional (CEN) impulsado por la Administración Clinton.

En el ámbito formativo destacan:

- Los programas, en grados o masters universitarios sobre IC, como el de la *Mercyhurst University*, la *National Intelligence University*, el *Institute of World Politics* y la *University of Marylang*
- Los certificados, como los expedidos por la *Academy of Competitive Intelligence*, el *Institute for Competitive Intelligence*, la *Johns Hopkins University* o la *SCIP University*
- Los cursos, como los del *Champlain College, California Institute of Technology* o de la *City University of New York*

- Sherman Kent, autor, entre otras, de las *obras Strategic Intelligence for American World Policy* (1949) y *The Theory of Intelligence* (1968), está considerado uno de los padres del análisis en inteligencia estratégica
- La obra *Organizational Intelligence: Knowledge and Policy in Government and Industry* (Harold Wilensky, 1967), que desarrolla conceptos de Inteligencia Económica destaca las ventajas de la colaboración (Estado-empresas) y el conocimiento de la economía como motor de la mejora
- En 1986 se funda en Washington D.C. el *Strategic and Competitive Intelligence Professionals*, (SCIP) como asociación no lucrativa para fomentar el uso de la inteligencia en las organizaciones donde sus miembros trabajen.

Suecia

El país escandinavo destaca por su capacidad de asociación entre distintos sectores: universitario, bancario, público e industrial que le ha permitido desarrollar la implantación de la IC. Propiciado, entre otros aspectos, por sus características geográficas, lingüísticas y poblacionales que le obligaban a desarrollar mecanismos para competir.

LUND UNIVERSITY

La llamada Escuela Sueca de IC tiene a Stevan Dedijer, profesor de la Lund University como principal referente. Un aspecto interesante de esta es el referente a la Inteligencia Social, en el que se valoran no sólo aspectos tradicionalmente económicos como rentabilidad o beneficio, sino también medioambientales, sociales, educativos. Acorde con la idiosincrasia escandinava, basada en una interpretación, donde lo social y lo educativo son las bases de su modelo económico. Se podría entender como una evolución de la Inteligencia Anglosajona, si bien con una mayor preocupación por aspectos sociales y de entorno medioambiental (Dedijer, 1983).

En este caso, en vez de ser impulsada la Inteligencia desde el Estado hacia las empresas, son las empresas *from bottom to top* y los distintos grupos de interés (universidades, lobbies, multinacionales, congresos, centros de investigación…), las que fomentan el modelo y el Estado, quien las ayuda a través del Poder Federal y de sus Agencias de Inteligencia (Bahouka-Débat, 2011).

Estos aspectos han influido en que las principales compañías suecas cuenten con áreas de IC. Las cuales se complementan las labores de las embajadas entre las que están la de recopilar y suministrar información relevante a las empresas del país, así como las de las universidades las cuales realizan programas especializados en la materia.

Suecia no es un país recién llegado a la Inteligencia Competitiva, no en vano uno de los precedentes de la materia fue la revista *Den Goteborg Spionen*, en el siglo XVIII, sobre sistemática fabril en otros países competidores (Escorsa y Maspons, 2011). Esta revista fue pionera de lo que en el siglo XX se desarrollaría, destacando la labor de los servicios de inteligencia suecos desde los años 70, la creación del *Business Intelligence and Security Network of Sweden* (BISNES).

Entre las organizaciones gubernamentales implicadas, destacan, según el estudio de la Agencia de Información de la Diputación Foral de Bizkaia (2007), la *Confederation os Swedish Enterprises, Institute for Future Studies, Swedish Emergency Management Association* (SEMA), *Swedish Institute for Growth Policy Studies* (ITPS), la *Swedish Technical Attaches* (STTAT), y el trabajo conjunto de la Oficina de Aduanas Sueca, la Dirección de Impuestos y la Gerencia Nacional Sueca, en el intercambio de información.

En el entorno de PYME se desarrolla un proceso de "*escaneo espontáneo del entorno*" Hamrefors (1998), que aplica en el "Center for Entrepreneurship & Business Creation" de la Universidad de Estocolmo. Según este concepto, los empresarios, más que implementar departamentos de IC, lo que realizan es una descentralización de los medios de captación de la información donde cada PYME contribuya a la alimentación del sistema de IC. En esta línea están también los estudios de Sigurdson y Nelson, (1991) donde utilizan modelos japoneses de IC que replicar en otros países.

Otro aspecto relevante es su eficaz sistema educativo, con nueve universidades que tienen entre sus planes de estudios programas relacionados con la Inteligencia Económica y Competitiva. Entre ellos destacan los de la Lund University, Dalarna University, Lulea Technology University y los de la Universidad de Estocolmo. El concepto educativo va también ligado a la formación en idiomas (al menos tres por habitante), lo que compensa, en cierta manera, la limitada difusión internacional de su lengua oficial, el sueco. (Agencia de Información de la Diputación Foral de Bizkaia, 2007).

Destacan los estudios sobre la implantación de la Inteligencia Competitiva en Suecia de Dedijer, (1998) y Hedin (2005), así como Porter (1985) en el desarrollo del Center for Strategy and Competitiveness, y Stevan Dedijer (1983) del Research Policy Institute sobre la aplicación de la inteligencia británica en la inteligencia escandinava.

También procede destacar el papel de las empresas privadas dedicadas a la consultoría de Inteligencia, como son *Docere Intelligence* o *Infosphere*, asociaciones sectoriales como la *Global Intelligence Alliance* o la *Global Intelligence Network*, proveedores de información como *Novintel* o especialistas en cursos de formación para empresas como *Infonaut o Kairos* (Hedin, 1993).

Es de reseñar, en un país con una población de 9,5 millones de habitantes, consciente de la necesidad de tener un sistema económico que lo proteja (Olier, 2011), el número de empresas suecas líderes. Sirva como ejemplo: Ericsson, H&M, Volvo, Electrolux, ABB, Securitas, Nordea Bank, IKEA, Telia Sonera, SCA Svenska Cellusola o SSAB, la mayoría de ellas con unidades de Inteligencia.

El desarrollo de la IC en Suecia ha influido en los países de su entorno: en concreto Finlandia, como recogen los estudios de Pirttimäki (2007) y de Hirvensalo (2005), donde los trabajos realizados muestran que el tejido empresarial finés ya reconoce la IC como un elemento crucial para sus operaciones y, con un desarrollo tardío. Finlandia tuvo el impulso en la materia con motivo de la crisis económica de inicio de los años 90 que supuso la pérdida de medio millón de empleos en un país de 5 millones de habitantes, lo que hizo reorganizar su estructura empresarial y hacerla más competitiva. Otro país con reciente implantación es Lituania como muestran los estudios sobre su implantación por parte de Jucevicius, Oržekauskas y Stankeviciute (2004).

Japón

Japón presenta un elemento de religiosidad, entre confucionismo y budismo, con una abnegación individual en beneficio del bien colectivo, una arraigada noción de grupo, que ayuda en una IC eficiente (Achard & Bernat, 1998). Es un país con escasos recursos naturales, especialmente energéticos, con un mercado interno, en cierta manera, blindado ante la competencia extranjera y, por otro lado, muy competitivo en la expansión exterior y en la exportación de sus productos.

Los inicios de su inteligencia, en este caso aplicada desde el Estado hacia las empresas *Top-down*, se pueden ubicar (Gonzalvo, 2015) en la Revolución Meiji (1866-1869), que supone el cambio de una economía autárquica, cerrada a las influencias extranjeras y con un sistema social basado en castas, hacia la apertura, posterior, a Occidente.

Este proceso supuso un incremento de la industrialización, la militarización, los intercambios comerciales y la protección ante las grandes potencias vecinas, en concreto ante Rusia y China, con los cuales acabaría entrando en guerra (Kahaner, 1997).

La implantación de la IC (Wang, 2001), muestra durante la primera mitad del siglo XX, la importancia de la participación de los *Zaibatsu,* como corporaciones empresariales con base militar, interrelacionada con el Estado. Y que tras la Segunda Guerra Mundial y después de adaptarse a la normativa Anti Monopolio, implantada por los Estados Unidos durante la ocupación, volvieron a tener protagonismo. También, la Segunda Guerra Mundial supuso la obligación de disolución del ejército japonés, lo que hizo que oficiales de alta graduación fueran destinados al Ministerio de Economía y Finanzas, donde incorporaron y adaptaron los conocimientos adquiridos en materia militar.

Era necesario conocer qué hacían otras potencias para poder competir contra ellas. El sentimiento de pertenencia y de lealtad al emperador predisponía a compartir información. Para ello se realiza un proceso: captar, analizar, filtrar y difundir la información entre la empresa y con otras empresas del grupo. Todo ello englobado en un proceso de mejora continua denomina*Kaizen* (Kobuko, 1989).

Este proceso se plasma en una concepción del aprendizaje mediante la observación *learning by watching,* frente al occidental de acierto / error del *learning by doing* (Guiromaes, Sato y Kitanada, 1999).

Considerado uno de los líderes mundiales de la Inteligencia aplicada al mundo empresarial, (Agencia Bizkaia, 2007) desarrolla su estrategia mediante los siguientes organismos públicos:

- El *Ministry of International Trae and Industry* (MITI). Éste mantiene una posición intervencionista en el mercado similar al caso francés, con interrelación entre la esfera pública y la esfera privada y trata tanto de controlar el mercado doméstico, como de ayudar a la internacionalización de sus empresas con una importante relación entre este Ministerio y las empresas privadas ya que les proporciona información, orientación y protección
- El *Japan External Trade Organisation*, (JETRO), organismo público adscrito al MITI con 73 oficinas en el extranjero y 36 en Japón, y que analiza el entorno económico, desarrolla nuevos sectores tecnológicos y asesora a las PYME sobre los mercados extranjeros y su posible externalización
- El *Japan Information Center of Science and Technology*, (JICST), dependiente del JST (Agencia de Ciencia y Tecnología de Japón) bajo el mandato del Primer Ministro. Se encarga, entre otras materias, de la difusión de información tecnológica del extranjero y la gestión de patentes
- El *Chui Joho Kyodu*, que depende del Ministerio de Asuntos Exteriores, para el tratamiento de información relativa a cuestiones políticas de los países donde se pudiese operar.

En las asociaciones privadas enfocadas a la obtención de información, destacan los *Sogo Shosha,* de apoyo a la exportación, y los *Keiretsu*, como organizaciones empresariales, con un componente científico pensado en el desarrollo de productos a largo plazo y los aspectos relacionados con financiación o definición estratégica.

En el plano formativo, destaca el *Institute for Industrial Protection,* para la formación de analistas en empresas. Así como la labor de *Juro Nakagawa* de la *Tokyo-Keizai*

University y *Yoshio Sugasawa* de la*Nihon University* ambos miembros del consejo editorial del *Journal of Competitive Intelligence and Management.*

Por lo tanto, nos encontramos en Japón a un país de grandes multinacionales, Toyota, Mitsubishi, Nippon Telegraph & Tel, Softbank, Honda, Sumimoto Mitsui Financial o Hitachi, acostumbrado a competir en un entorno hostil y con un sentimiento cultural muy fuerte de pertenencia a la organización en la que trabajan sus empleados y al Estado del que forman parte (Kahaner, 1997).

El sistema japonés se articula en las siguientes líneas estratégicas, (Olier, 2013):

- Doble enfoque: global y local de las empresas japonesas (glocalización).
- Adaptación al contexto económico y modo de vida de cada país.
- Gestión selectiva de la información y de divulgación selectiva con sistemas de *reporting* tipo Alemania.
- Visión económica a largo plazo.
- Integración vertical y horizontal de las grandes corporaciones.
- Formación, en especialización de países, de jóvenes profesionales en sus empresas.

En el siguiente gráfico se muestra la integración en la economía nacional japonesa, desde la mencionada cultura de información de grupo, a la estrategia del largo plazo de las empresas (hasta 30 años). Así como un enfoque global, ligado a una correlación de interés económico y nacional.

Gráfico 1: Sistema de Inteligencia en Japón

Fuente: Adaptación del 11éme plan de Francia. Inteligencia Economique. Recopilado de *Agencia de Información de la Diputación Foral de Bizkaia (2007)*

Corea del Sur

Corea del Sur es un país con un fuerte desarrollo tecnológico auspiciado, entre otros aspectos por la situación de tensión bélica que llevan viviendo sus habitantes en las últimas décadas y por una fuerte conciencia de país.

En Corea del Sur se cumplen los factores característicos a la hora de la implantación de la IC en países asiáticos (Fleisher y Wright, 2009):

- Rol fundamental del Gobierno en cuestiones de política económica de las empresas.
- Mercado posicionado entre grandes corporaciones urbanas y pequeños comerciantes rurales.
- Fuertes barreras de entrada en el mercado local a competidores extranjeros.

El país es un aliado tradicional de EEUU quien ha intervenido su economía durante décadas y sigue criterios anglosajones en el fomento de su estructura empresarial, tras la guerra de Corea y de su entrada en el marco de influencia norteamericana (Blenkhorn, 2005).

En los inicios de la IC en Corea del Sur se encuentra el *Je-Kook-Ik-Luna-Je-Kook-Ik-Moon-Sa*encargada de obtener información sobre los países competidores. En 1945 se creó el servicio de inteligencia del ejército centrada en la seguridad nacional que sirvió de referente para la creación del *Korea Trade Promotion Corporation* (KOTRA) y del *Korea Institute os Science and Technology Information* (KISTI), así como el desarrollo de los *Chaebols* (Bustelo, 1991)

- KOTRA. Su función es la promoción de negocios e inversiones del país. Depende del Ministerio de Asuntos Exteriores y Comercio Exterior. Se encarga de la recolección y el análisis sistemático de la información sobre inversiones de o en países extranjeros. Tiene a su cargo las Instituciones encargadas de la transferencia tecnológica e I+D+i
- KISTI. Su función es desarrollar la infraestructura de comunicación tecnológica. Depende del Primer Ministro. Se encarga del conocimiento e información de las empresas y gestión de la información relevante para los actores económicos
- Chaebols. Es la denominación de conglomerados de empresas diversificadas en distintos sectores desarrolladas durante el mandato de Park Chung-hee (1962-1979) siguiendo el modelo de los Zaibatsus de Japón (Jensana Tanehashi, 2004). Su objetivo inicial era prestar apoyo a las empresas de alto valor añadido para el país, sin embargo a partir de los años 90 se van estableciendo modelos de IC que incluían información de los competidores, tanto económica como política.

Un aspecto relevante fue la creación en los años 60 de los organismos *Je-Kook-Ik-Luna-Je-Kook-Ik-Moon-Sa*, como medio de captación de datos de personas clave (empresarios, políticos, diplomáticos…), y también de la *Korean CIA*, que apoyó a las grandes corporaciones, *chaebols,* las cuales han ido desarrollando procesos de recopilación de información para la inversión y, desde los años 80, programas específicos de Inteligencia (Kim y Kim, 2005).

A partir de 1997, el país entró en crisis económica, lo que obligó a las empresas a modificar su estrategia. En la esta crisis se decidió potenciar diez sectores que se consideraron clave, entre los que destacaban los sectores de electrónica y alta tecnología. Se tomaron de referencias criterios de IC japoneses y de EEUU.

En el tejido empresarial coreano destacan empresas como Samsung, Hyundai, Posco, LG o Kia. (Agencia de Información de la Diputación Foral de Bizkaia, 2007). Destaca la formación en la*Konkku University*, las consultoras como Asesoramiento IBS, Encielasen Korea, 3mecca, Korea Economic Resecar o CIB Comunicación.

Alemania

La IC alemana, como en el resto de países, hay que contextualizarla por sus aspectos históricos y sus rasgos culturales.

Los inicios corresponden a la creación de la Liga Hanseática, fundada en 1358, como federación comercial y defensiva de ciudades de influencia alemana en el Mar Báltico (Braudel, 1984) y que servía para compartir conocimientos comerciales y acceso a rutas marítimas. Un posterior impulso es con el desarrollo de Prusia y su pugna frente a las potencias francesas y británicas. En este momento se intensifica la labor de recopilación y difusión de información a través de consulados y sociedades de comercio. Así como la creación de asociaciones entre los grandes grupos industriales y bancarios del país.

En el aspecto cultural (Hofstede, 2012), destaca los aspectos de ser una nación competitiva, beligerante en ocasiones, con una limitada distancia al poder, lo que favorece el flujo de información y el factor de la diáspora de alemanes que viven en el extranjero, pero mantienen vinculación con el país. Actualmente hay 80 millones de alemanes viviendo en otros países.

El país presenta una estructura federal con un alto nivel de coordinación entre sus diferentes organismos territoriales. Así como entre estos y los bancos, industrias, asociaciones sindicales, servicios de Inteligencia de los *länder* y pactos entre partidos políticos con el fin de apoyar el desarrollo del tejido empresarial alemán (Palop y Vicente, 1999).

El esquema alemán (Olier, 2013), sigue las siguientes pautas:

- La alineación de los principales grupos de interés económicos: bancos, grupos industriales, etc
- La flexibilidad y aproximación coordinada a los mercados objetivos
- La posibilidad de sacar provecho de modo coordinado de la masa emigrante alemán en el extranjero
- El objetivo de prevalencia de los intereses comunes alemanes frente a los intereses individuales, lo que potencia las actividades de inteligencia.

En la actualidad, el 86% de las grandes empresas alemanas tienen un departamento de IC (M-Brain, 2015). En las que destacan los sectores farmacéuticos y salud así como el de telecomunicaciones y tecnología.

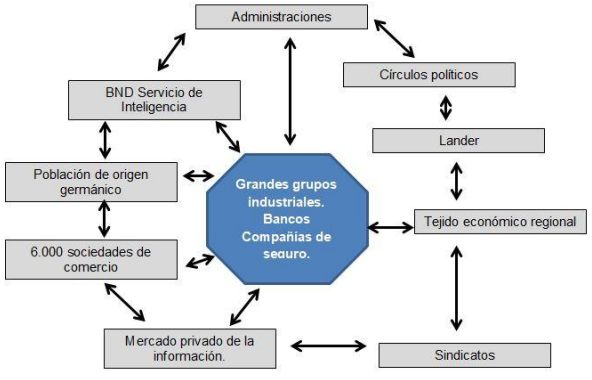
En el mismo estudio sobre empresas alemanas se llegó a los siguientes resultados del gráfico, que muestran un convencimiento de los beneficios de la IC, si bien los porcentajes bajan cuando se pregunta si la inversión en IC ha dado sus frutos.

Entre los organismos destaca Michaeli (2004):

- La Oficina Federal de Protección de la Constitución, *Bundesamt für Verfassungsschutz,* (BFV), cuya razón de ser es la aplicación de la inteligencia para la protección de la constitución, el orden democrático, la seguridad del país y el promover la cooperación entre el gobierno federal y los länder.
- Otras medidas que realiza la BfV son charlas y conferencias de sensibilización, el Congreso de Seguridad anual de la BfV, boletines de noticias dirigidos a sus empresas, la realización de un Informe extraordinario sobre protección de la economía y la feria *Secutiry Essen.*
- *Bundesnachrichtendienst* (BND), la agencia alemana de inteligencia extranjera. Nace en 1945, como la Organización Gehlen, y es financiada por la CIA, si bien en 1956 pasa a depender del Gobierno de Alemania occidental. En los años 80 se centra en la defensa de los intereses económicos alemanes, con gran peso en los países eslavos y de influencia alemana en Centroeuropa.
- Cámaras de Comercio. Tiene 79 oficinas en Alemania y 90 en otros países y se integran en la asociación alemana de cámaras de comercio e industria (DIHK).
- La educación en IC a través de las universidades. Entre otras destacan los programas de IC de la Escuela de Economía y Derecho de Berlín, la Escuela de Negocios de la Universidad de Mannheim o la Escuela de Negocio de Münster.

A continuación se anexa el esquema de Inteligencia en Alemania. Este plan pivota en los grandes grupos industriales, bancos y compañías de seguro y en la conexión a los distintos canales de información: diáspora, sociedades de comercio administraciones, etc… Asimismo la conexión con los niveles regionales se realiza a través del peso de los sindicatos y círculos políticos.

Gráfico 2: Sistema de Inteligencia en Alemania



Fuente: Palop y Vicente (1999)

Reino Unido

En este país, como en Estados Unidos, la política es de no intervención en la esfera privada, si bien hay apoyo a través de instituciones, como la Cámara de Comercio Británica en materia de ayudas a la exportación. Hay que entender al

Reino Unido como una potencia económica que fomentó su poder en el ámbito naval y, por tanto, dominadora de las rutas comerciales más rentables, que garantiza gracias a su poderío militar (Mahan, 1987).

No obstante, la iniciativa de apoyo en cuestiones de inteligencia se deja en mano de las empresas privadas y no del sector público, como ocurre entre otros en el caso japonés o francés. Dentro de una concepción ética de cuáles son los límites de actuación del Estado en la esfera privada (Weber, 2003). Un embrión de IC fue el sistema de palomas mensajeras que utilizó Nathana Rothschild para conocer el desenlace de la batalla de Waterloo antes que los demás y utilizar esa información para actuar en la bolsa londinense (Ferguson, 1999).

El poco apoyo público ha generado que el desarrollo en la materia provenga de las iniciativas privadas. Hay que señalar que en 1989 Andrew Pollard crea la consultora de Inteligencia Competitiva EMP Intelligence Service, que también destaca por el aspecto de formación docente en la materia. Hay que reseñar a City Information Group (CIG) como asociación de profesionales, en línea con la Sociedad de Profesionales de Inteligencia Competitiva (SCIP), que, en el caso del Reino Unido, su departamento se crearía en 1990.

Entre las consultoras más significativas se encuentran *Aware Consulting* (fundada en 1993), CIS (1994), *FreshMinds* (2000), *Fuld&Co* (1979), *Infonortics* (198 7) o *EMEA Consulting* (2001). (Agencia de Información de la Diputación Foral de Bizkaia, 2007).

En el aspecto de formación, destaca el postgrado de Gestión de un entorno competitivo que, desde 1987, la *Open University* ha ido impartiendo, así como otros estudios de la *Leicester Business School.* O la *Brunel University* en Londres, con estudios sobre Inteligencia y sobre seguridad. Así como la *London Business School,* con seminarios en Inteligencia Competitiva. En cuanto a la difusión, hay que destacar publicaciones como *The Economist Intelligence Unit,* perteneciente a *The Economist.*

Entre los principales autores de Inteligencia Competitiva en el Reíno Unido destacan Sheila Wright autor entre otros junto al canadiense Jonathan Calof de *Competitive intelligence: a practioner, academic and interdisciplinary perspective* (2006) y de *The quest for competitive, business and marketing intelligence: A country comparison of current practices* (2008) y ambos con el británico David Pickton de *Competitive intelligence in UK firms: a typology* (2002) y sus labores de estudio y difusión.

Entre otros países anglosajones es necesario destacar los estudios sobre la implantación de la Inteligencia Competitiva en Australia por Bensoussan y Densham (2005) con su obra *Australian CI Practices: A Comparison with the U.S.* y Sudáfrica por Muller y Viviers (2004) con *The Evolution of Competitive Intelligence in South Africa: Early 1980s-2003.* O Canadá donde se sigue un sistema mixto entre lo público y lo privado, con interrelación entre los órganos centralizados y descentralizados. Así como una doble estructura de IC, una a nivel federal centralizada y otra regional con variaciones según los distintos territorios (Tanev y Bailetti, 2008).

Conclusiones

Las principales potencias económicas realizan labores de Inteligencia Competitiva, si bien la relación entre lo público y lo privado está condicionada por el grado de liberalismo y de intervención pública de su respectiva Administración, así como del entorno competitivo en el que se mueven sus empresas.

Tabla 1: Cuadro resumen.

País	Enfoque	Características
Francia	Top-Down.	La Inteligencia necesaria para el Estado. Órganos específicos e interconexión con un modelo territorial de Cámaras de Comercio.
Alemania	Mixto.	Alineación de grandes grupos industriales. Cultura competitiva. Prevalencia de intereses comunes. Tradición de siglos.
Estados Unidos	Bottom-Up.	No intervención directa hasta los años 90. Grandes recursos públicos y gestión muy desarrollada a nivel privado.
Corea del Sur	Top-Down.	Conglomerados industriales (Chaebols). Foco en sectores tecnológicos. Integra modelo japonés y estadounidense. Dependencia del Primer Ministro.
Suecia	Bottom-Up.	Inteligencia social. Integración sectorial. Escaneo del entorno. Difusión universitaria. Tradición histórica cultural.
Reino Unido	Bottom-Up.	Poca intervención pública. Desarrollo de consultoras y asociaciones privadas. Formación especializada.
Japón	Top-Down.	Cultura colectiva de información. Conquista de mercados exteriores. Reflexión prospectiva a largo plazo. Rentabilidad del secreto.

Fuente: Izquierdo Triana (2016)

Nota sobre los autores

Dr. Héctor Izquierdo Triana es Profesor en el Instituto de Empresa (ie, business school) y en la Universidad Pontificia Comillas.

Dr. Fernando Velasco es Director de la Cátedra Servicios de Inteligencia y Sistemas Democráticos de la Universidad Rey Juan Carlos y Editor Jefe de The International Journal of Intelligence, Security, and Public Affairs.

Dr. José Luis Fernández es Director de la Cátedra de Ética Económica y Empresarial de la Universidad Pontificia de Comillas.

Los accidentes de tráfico se cobran la vida de 1.200 personas durante el año pasado

Dirección General de Tráfico

Balance de Seguridad Vial 2017

Se reduce en 336 personas el número de heridos graves

Las distracciones, la velocidad inadecuada, el cansancio o sueño y el alcohol y las drogas son los principales factores que aparecen en los accidentes mortales o graves.

Aumenta en 26 el número de fallecidos en turismo o furgoneta que no hacían uso del cinturón de seguridad en el momento del accidente. 149 en 2016 y 175 el pasado año.

Se han registrado un total de 408,5 millones de desplazamientos de largo recorrido, 16,4 millones más, lo que supone un aumento de la movilidad de un 4,2% respecto al año anterior y se han matriculado 1.787. 242 de vehículos.

A principios de 2017 se aprobó un plan de choque contra la siniestralidad vial con 15 medidas urgentes. De las 15 medidas urgentes anunciadas se ha ejecutado el 90%.

Los proyectos para 2018 se concentran en varios bloques: Más reformas, más control, más educación/formación y comunicación, más investigación y más compromisos entre administraciones y sector privado.

Durante el año 2017 se han producido 1.067 accidentes mortales en vías interurbanas, en los que han fallecido 1.200 personas y 4.837 heridas hospitalizadas, lo que supone un aumento del 3% en lo que a accidentes mortales (+28) y fallecidos (+39) se refiere y una disminución de un 6% (-336) en lo relativo a heridos hospitalizados.

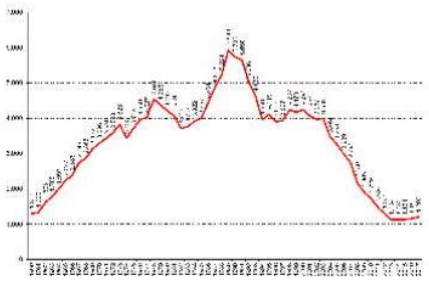
Estos datos han sido comunicados por el director general de Tráfico, Gregorio Serrano, en la presentación del balance anual de siniestralidad vial 2017.

Las cifras dadas a conocer hoy son provisionales y únicamente referidas a los accidentes mortales ocurridos en vías interurbanas y victimas tomadas hasta las 24 horas de producirse el accidente. Las cifras definitivas ya consolidadas en la que se incluirán las victimas a 30 días de accidentes ocurridos en vías urbanas e interurbanas estarán disponibles en los próximos meses.

A pesar de este repunte, la cifra de fallecidos sigue por debajo de los registrados en 1960, primer año en el que se tienen estadísticas, cuando hubo 1.300 muertos, con un escenario de movilidad absolutamente distinto (en 1960 había un millón de vehículos y en 2017 el parque automovilístico es de casi 33 millones).

Según el Director General de Tráfico *"A pesar de que España sigue siendo uno de los países más seguros en carretera tanto del mundo (8º) como de Europa (5º), tenemos que seguir haciendo grandes esfuerzos entre todos para reducir las cifras de siniestralidad"*. *"Estoy seguro que con la nueva Ley de Tráfico y Seguridad Vial y con más medidas de control, educación, formación, comunicación e investigación lograremos entre todos reducir el número de fallecidos en nuestras carreteras"*. Además ha añadido *"que ninguna medida es eficaz si no cuenta con la implicación de los conductores y del resto de la administración pública"*

Evolución del número de fallecidos en vías interurbanas (24 horas) 1960 – 2017



Con estos datos, la accidentalidad en carretera se mantiene en el promedio diario de víctimas mortales, que ha pasado de los 11,6 muertos diarios en carretera en 2.000 a los 3,3 fallecidos diarios en 2017.

A DESTACAR

En la siniestralidad de 2017 destacan las siguientes circunstancias:

- Movilidad: Se ha constatado un aumento de 16,4 millones de viaje de largo recorrido por carretera, lo que supone un 4,2% más que respecto al año anterior. En total se han registrado 408,5 millones de desplazamientos de largo recorrido en 2017, lo que representa un incremento acumulado del 14,5% en los cuatro últimos años.

- Aumento del parque: Durante 2017 se han matriculado 1.787.242 vehículos, lo que supone un parque automovilístico de casi 33 millones.

Envejecimiento del parque. Pese a las nuevas matriculaciones, en 2017 la antigüedad media de los vehículos implicados en accidentes mortales se sitúa en 12 años para los turismos, porcentaje que aumenta hasta los 13,8 años en el caso de los turismos en los que viajaban los fallecidos.

CARACTERÍSTICAS DE LA SINIESTRALIDAD

Por sexos: Se sigue observando un mayor porcentaje de fallecidos de sexo masculino. La proporción de varones sobre el total ha sido del 78%, porcentaje que se mantiene respecto a 2016.

Por edades: Se produce un descenso importante de fallecidos entre los mayores de 65 años. En 2017 han fallecido 181 personas, frente a los 240 del año anterior.

Los grupos de edad en los que más aumentado el número de fallecidos han sido el de 25 a 34 años, con un incremento del 37% y el de 55 a 64 años, con un aumento del 16%. Los niños fallecidos (hasta 14 años) han sido 21, tres más que en 2016.

Por Comunidades Autónomas: Registran incrementos todas las comunidades autónomas, excepto Galicia (-29), la Comunidad Valenciana (-17); País Vasco (-6) Navarra (-3), La Rioja y Castilla y León (-1) y Baleares que mantiene la misma cifra de fallecidos que el año anterior.

CCAA	2016	2017	Di % 2017/2016	Dif Nº 2017/2016
Andalucía	186	200	8%	14
Aragón	55	58		3
Asturias, Principado de	26	27		1
Balears, Illes	48	48		0
Canarias	38	44		6
Cantabria	9	13		4
Castilla-La Mancha	93	112		19
Castilla y León	124	123	-1%	-1
Cataluña	154	169	10%	15
Extremadura	45	50		5
Galicia	106	77	-27%	-29
Madrid, Comunidad de	52	68		16
Murcia, Región de	34	46		12
Navarra, Comunidad Foral de	18	15		-3
Rioja, La	20	19		-1
Comunidad Valenciana	117	100	-15%	-17
País Vasco	36	30		-6
Ceuta y Melilla	0	1		1
Total	**1.161**	**1.200**	**3%**	**39**

Por tipo de vía: El 77% de los fallecidos tienen lugar en vías convencionales. Concretamente el año pasado fallecieron en este tipo de vías 792 personas, 30 más que en 2016.

En las vías de alta capacidad los fallecidos disminuyen de un 24% a un 23%, pasando de los 245 en 2016 a los 239 de 2017.

Por tipo de accidente: En las vías de gran capacidad, el 41% de los fallecidos en 2017 se han producido en accidentes que fueron salidas de la vía, el 20% en accidentes con colisión trasera y múltiple y el 15% en atropellos a peatones. En las carreteras convencionales, el 42% de los fallecidos se debió a accidentes en los que el vehículo se salió de la vía, mientras que un 28% se debió a colisiones frontales.

Por factores contribuyentes: La conducción distraída o desatenta (32%); la velocidad inadecuada (26%), el cansancio o el sueño (12%); el alcohol (12%) y otras drogas (11%), son los factores que en mayor medida contribuyen a los siniestros.

Por tipo de usuario: Los fallecidos por tipo de usuario presentan diferentes comportamientos. Aumentan los fallecidos en turismo, moto, furgoneta y bicicleta y disminuye de forma importante los fallecidos peatones

Tipo de Vehículo	2016	2017	Dif. % 2017/2016 (1)	Dif. Nº 2017/2016
Bicicleta	33	44		11
Ciclomotor	22	20		-2
Motocicleta	214	240	12%	26
Turismo	603	646	7%	43
Furgoneta	58	75		17
Camión ≤ 3.500 kg	18	6		-12
Camión > 3.500 kg	48	47		-1
Autobús	18	2		-16
Otros Vehículos	27	29		2
Peatón	120	91	-24%	-29
Total	**1.161**	**1.200**	**3%**	**39**

Uso de accesorios de seguridad: El 24% de los conductores y pasajeros fallecidos en turismos y furgonetas en 2017 no llevaban puesto el cinturón de seguridad en el momento del accidente. Aumenta en 26 el número de fallecidos que no hacían uso de dicho dispositivo de seguridad en estos vehículos pasando de los 149 en 2016 a los 175 el pasado año.

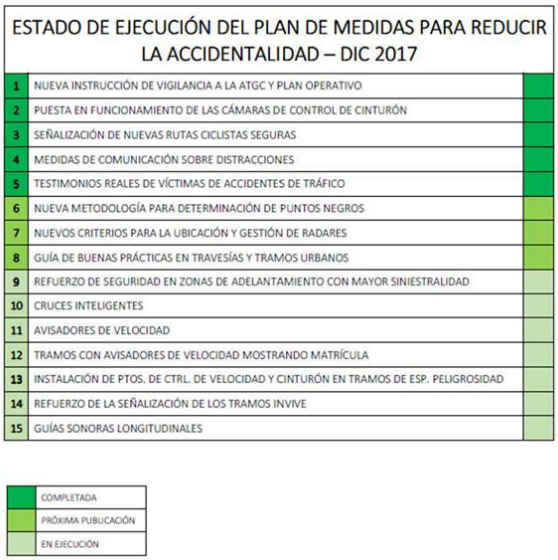
De los 240 fallecidos en motocicleta, 2 no utilizaban casco. En el caso de los ciclistas, de los 44 fallecidos, 8 no lo llevaban, pese a ser obligatorio en vías interurbanas.

De los 16 niños hasta 12 años fallecidos en turismo o furgoneta, 4 no utilizaba ningún accesorio de seguridad en el momento del accidente.

El no uso del cinturón de seguridad se produce tanto en vías de alta capacidad (22%) como en vías convencionales (27%).

MEDIDAS ADOPTADAS

A principios de 2017 se aprobó un plan de choque contra la siniestralidad vial con 15 medidas urgentes. De las 15 medidas urgentes anunciadas se ha ejecutado el 90%.



Además se ha aprobado una nueva instrucción de medidas especiales de regulación de tráfico de mercancías y otra sobre el consumo de drogas en la conducción y se han adquirido 300 nuevas motocicletas para la ATGC, 156 nuevas furgonetas con equipos de alcohol y drogas para la ATGC así como la compra de 746 etilómetros integrados y 500 lectores de drogas.

Se ha aprobado también el Plan básico de Educación Vial y de las Comisiones Provinciales de Educación vial, que ya están en marcha.

Además de todas estas acciones, durante 2017, los 52 grupos de trabajo creados en el seno de del Consejo Superior de Tráfico y Seguridad Vial se han reunido para debatir sobre los cambios y mejoras que se puede realizar en la Ley de Seguridad Vial para posteriormente la DGT desarrollar la nueva Ley que Tráfico tiene previsto enviar al Ministerio en el primer trimestre del año.

PROYECTOS PARA 2018

Los proyectos para 2018 se concentran en varios bloques: Más reformas, más control; más educación/formación y comunicación, más investigación y más compromisos entre administraciones y sector privado.

• Más reformas:

- Nueva Ley de Tráfico y Seguridad Vial; Reglamento General de vehículos y Reglamento de auxilio en carretera.
- Aprobación del Plan estratégico estatal de la bicicleta.
- Estrategia de seguridad vial 2018-2020.
- Puesta en funcionamiento de la plataforma del vehículo conectado DGT 3.0.
- Plan estratégico del vehículo.
- Plan de medidas contra la siniestralidad de vulnerables.

• Más control:

- Aprobación nuevo plan contra la velocidad y publicación de una nueva Instrucción de radares.
- Aprobación del protocolo para la aplicación del Art. 36 del Reglamento de Conductores en los reincidentes por alcohol y otras drogas.
- Nuevo plan integral de lucha contra el alcohol y drogas en la conducción.
- Adquisición de drones para el control del tráfico

• Más educación, formación y comunicación:

- Desarrollo de los Planes básicos de coordinación en Educación Vial.
- Adquisición más materiales pedagógicos para centros escolares.
- Adquisición de 50 parques infantiles de tráfico móviles.
- Aprobación convocatoria de ayuda a asociaciones de víctimas de accidentes de tráfico, con especial atención a la educación vial de adolescentes.
- Reforma del modelo de formación vial en España.
- Ingreso de 100 nuevos examinadores.
- Realización de campañas de comunicación en todos los soportes (TV, radio, digital…) sobre el colectivo de vulnerables: peatones y motoristas.
- Realización de nuevas campañas de comunicación, publicidad exterior y acciones directas.

• Más investigación

- Inversión de 1 M€ en ayudas a la investigación

• Más compromisos:

- Aprobación de convenios para el impulso de la educación vial con las CC.AA.
- Aprobación acuerdo marco de colaboración con la FEMP.
- Celebración de convenios de colaboración en materia de seguridad vial con los titulares de las vías.
- Aprobación de convenios bilaterales con Ayuntamientos en materia de seguridad vial de vulnerables.
- Continuar impulsando en colaboración con empresas la seguridad vial laboral.

Prestando atención a los negocios que aparecen en las tarjetas de Google Maps

Oficina de Seguridad del Internauta

La evolución de las nuevas tecnologías y del software asociado a las mismas, ha provocado también una evolución de la ciberdelincuencia. A pesar de la existencia de numerosos sistemas de seguridad y empresas especialistas en esta materia, siguen apareciendo nuevos fraudes. En esta ocasión, hablaremos de las tarjetas de negocios fraudulentas que se podrían encontrar en Google Maps.

Estudios llevados a cabo por expertos en seguridad recogen que un ciberdelincuente podría derivar a un usuario que acceda a la información sobre una determinada empresa a través de Google Maps, a páginas web de su interés para llevar a cabo actividades maliciosas, aun teniendo en cuenta que Google Maps cuenta con un potente filtro y un fuerte sistema de verificación para evitar precisamente este tipo de situaciones.

¿Por qué puede suceder esto?

Teóricamente es el propietario de una tienda o comercio quien debiera dar de alta su propio negocio en Google Maps. Pero el sistema con el que Google verifica este tipo de datos, a día de hoy permite que cualquiera pueda realizar un alta, ya que al hacer efectivo este proceso, únicamente enviará un correo postal a la dirección que se haya introducido, con un código que el receptor deberá introducir para confirmar la identidad del mismo. Dicho correo podría ser sustraído si se tiene acceso físico al buzón de dicho domicilio.

La mecánica que utilizan para engañar al usuario es la siguiente:

1. El usuario accede a la información de una empresa a través de Google Maps.
2. Entre la información que se ofrece sobre la misma, se encuentran los datos correspondientes a su página web.
3. Cuando el usuario haga clic sobre el enlace, se materializará el engaño. En lugar de acceder a la web legítima de la empresa, lo hará a una web fraudulenta.
4. Terminará siendo víctima de un caso de phishing.

Se podría utilizar esta misma situación para perjudicar a un determinado negocio, manipulando la información de la ficha de Google. Por ejemplo, informar de un cierre permanente sin que realmente se haya producido, dotar de falsos números de teléfono, etc.

¿Cómo puede afectar esto al usuario?

Si se consigue falsear la información de una determinada tarjeta de manera fraudulenta de un establecimiento o negocio publicado en Google Maps con las artimañas comentadas anteriormente, sería posible, por ejemplo, redirigir al usuario a páginas web dotadas de formularios orientados a robar las datos personales, credenciales de acceso, información bancaria o cualquier otra información que se os ocurra. También podrían engañarle con el teléfono de contacto, de tal forma que el usuario acabase llamando a número de tarificación especial sin darse cuenta.

En cualquier caso, el ciberdelincuente sabe en qué zonas ubicar este tipo de tarjetas fraudulentas para que las posibilidades de que el engaño se materialice sean mayores. No es lo mismo intentar colar un fraude en una pequeña ciudad o pueblo donde en mayor o menor medida, se conocen perfectamente todos los comercios y servicios que hay, que realizarlo en grandes ciudades con cientos de negocios.

Consejos para evitar caer en engaños de características similares:

1. Accede a las direcciones de las tiendas o negocios directamente tecleando la URL en el navegador. Evita utilizar enlaces desde páginas de terceros o de correos electrónicos si no son de tu total confianza.
2. Contrasta la información encontrada a través de Google Maps así como en cualquier otro servicio o página web de Internet.
3. En caso de duda, consulta directamente con la empresa o servicio implicado o con terceras partes de confianza como pueden ser las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) y la Oficina de Seguridad del Internauta (OSI) para contrastar la información.
4. En la medida de lo posible, no navegues desde ordenadores públicos, no confiables o que estén conectados a redes wifi públicas para evitar riesgos. No sabes si están correctamente configurados, libres de malware, etc. que puedan manipular tu navegación.

Si no hay certificado, o si no corresponde con el sitio que quieres visitar, no facilites ningún tipo de información personal: nombre de usuario, contraseña, datos bancarios, etc.

Noticias

La DGT elevará a los Ministerios del Interior y de Fomento un informe que recogerá de manera precisa y detallada las mejoras en los procedimientos y protocolos

La Dirección General de Tráfico pide disculpas a los conductores que se quedaron bloqueados en carretera, especialmente a los de la AP-6, por los fallos que se pudieron cometer.

Ha agradecido al personal dela UME, de la ATGC, Cruz Roja así como policías locales y personal de mantenimiento de las carreteras las actuaciones realizadas en el rescate y atención a los conductores.

Los responsables de la Dirección General de Tráfico mantendrán una reunión con los responsables de la Dirección General de Carreteras para mejorar la coordinación interinstitucional para evitar colapsos por condiciones climatológicas en las carreteras

El Comité de Seguridad Vial reunido en la tarde de hoy y presidido por el Director General de Tráfico para analizar las actuaciones llevadas a cabo durante el episodio de nevadas del pasado fin de semana y estudiar mejoras para evitar situaciones como las acaecidas el pasado fin de semana, pide disculpas a los conductores que se quedaron bloqueados en carretera, especialmente a los de la AP-6, por los fallos que se pudieron cometer.

Asimismo, ha agradecido a los miembros de la Unidad Militar de Emergencias, de la Agrupación de Tráfico de la Guardia Civil, Cruz Roja así como a los policías locales de los ayuntamientos próximos a la zona de la nevada y a los operarios de mantenimiento de carreteras las actuaciones realizadas en el rescate y atención a los conductores.

Durante la reunión se han analizado las actuaciones llevadas a cabo desde esta Dirección General y desde la Agrupación de Tráfico de la Guardia Civil, a través de la presentación de los documentos emitidos por la Subdirección General de Operaciones y Movilidad de la DGT; los Centros de Gestión de Tráfico de Madrid y Valladolid; la Jefa Coordinadora de Tráfico de Castilla y León y de la Agrupación de Tráfico de la Guardia Civil. En todos ellos se detectan importantes y graves defectos de procedimiento y de comunicación por parte de la Concesionaria, que en muchos aspectos actuó de manera negligente en un episodio de nevada intensa y de operación regreso de Navidad.

También se han analizado los procedimientos tanto de los Centros de Gestión de Tráfico como de la Agrupación de Tráfico de la Guardia Civil, proponiendo mejoras de actuación en estos casos.

La Dirección General de Tráfico elaborará un informe exhaustivo, en base a todos estos documentos, donde se recoja de manera concreta, todos los procedimientos de gestión y coordinación que hay que modificar para mejorar la gestión de los episodios de fenómenos meteorológicos extremos. Este informe que se elevará para su consideración al Ministerio del Interior y al Ministerio de Fomento, recogerá de manera precisa y detallada las mejoras en los procedimientos y protocolos.

También se ha valorado introducir en la nueva Ley de Tráfico y Seguridad Vial, el equipamiento que deberán llevar los vehículos de manera obligatoria, cuando se transite por lugares de nevadas frecuentes.

Además, en los próximos días, los responsables de la Dirección General de Tráfico mantendrán una reunión con los responsables de la Dirección General de Carreteras para mejorar la coordinación interinstitucional para evitar colapsos por condiciones climatológicas en las carreteras.

Asimismo, a nivel interno, el próximo 30 de enero, el Director General de Tráfico se reunirá en el Centro de Gestión de Zaragoza con los directores de los 8 centros de Gestión de Tráfico de España y con los jefes de sala de cada uno de ellos para unificar criterios de mejora en los protocolos de actuación en caso de episodios de nevadas.

También se va a proceder a incorporar nuevas acciones para mejorar los canales de comunicación con los ciudadanos a través de los diferentes medios de los que dispone el Organismo.

Organizada por IFEMA, SICUR 2018 se celebrará del 20 al 23 de febrero de 2018 en Feria de Madrid

SICUR 2018, el gran referente internacional del sector de la seguridad integral que organiza **IFEMA, del 20 al 23 de febrero de 2018** en **Feria de Madrid**, prepara la que será una de sus más completas ediciones, confirmando sus expectativas iniciales de crecimiento.

Más Información en el siguiente enlace

Formación

Formaciones de enfoque práctico sobre áreas y sectores de conocimiento de AECOC

Más Información en el siguiente enlace

Cursos Especializados de Dirección 2018

Más información y programa en el siguiente enlace

Oferta formativa de la Escuela de Prevención y Seguridad Integral

La **Escola de Prevenció i Seguretat Integral (EPSI)**, adscrita a la Universitat Autònoma de Barcelona, ofrece estudios universitarios en el ámbito de la prevención y la seguridad integral.

Programa en el siguiente enlace

Legislación

REAL DECRETO 1036/2017, DE 15 DE DICIEMBRE, POR EL QUE SE REGULA LA UTILIZACIÓN CIVIL DE LAS AERONAVES PILOTADAS POR CONTROL REMOTO, Y SE MODIFICAN EL REAL DECRETO 552/2014, DE 27 DE JUNIO, POR EL QUE SE DESARROLLA EL REGLAMENTO DEL AIRE Y DISPOSICIONES OPERATIVAS COMUNES PARA LOS SERVICIOS Y PROCEDIMIENTOS DE NAVEGACIÓN AÉREA Y EL REAL DECRETO 57/2002, DE 18 DE ENERO, POR EL QUE SE APRUEBA EL REGLAMENTO DE CIRCULACIÓN AÉREA.

PDF de la disposición en el siguiente enlace

DIRECTIVA (UE) 2017/2398 DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 12 DE DICIEMBRE DE 2017 POR LA QUE SE MODIFICA LA DIRECTIVA 2004/37/CE RELATIVA A LA PROTECCIÓN DE LOS TRABAJADORES CONTRA LOS RIESGOS RELACIONADOS CON LA EXPOSICIÓN A AGENTES CARCINÓGENOS O MUTÁGENOS DURANTE EL TRABAJO

PDF de la disposición en el siguiente enlace

Revistas

Seguritecnia Nº 448. Diciembre

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

- **Editorial:** Intenso fin de año
- **Seguripress**
- **Especial Seguridad e Inteligencia**
- **Entrevista:** Juan Yera. Director General de Gunnebo Iberia

Enlace: ver revista digital

Cuadernos de Seguridad Nº 328. Diciembre

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:** «2018, un año de desafíos y oportunidades».
- **En Portada:** «Seguridad en museos y patrimonios».
- **Entrevistas:** «Sonsoles Navas. Jefa de Seguridad de Museos Estatales».
- **Artículos:** «Traslado de obras de arte: de la teoría a la carretera».

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.