FORO PARA LA PAZ
EN EL MEDITERRÁNEO

ACTAS DE LAS XII JORNADAS DE SEGURIDAD, DEFENSA Y COOPERACIÓN

TOMO I

INFRAESTRUCTURAS CRÍTICAS Y GEOECONOMÍA

AUTORES

Rafael Vidal Delgado, Carmen Cristófol Rodríguez y María del Mar Gallardo Quero

Coordinadoras: Dra,s. Elena Ruiz Romero de la Cruz y Elena Cruz Ruiz

Edita: Foro para la Paz en el Mediterráneo
ISBN: 978-84-09-10456-7

Depósito Legal: MA 506-2019

EL MARCO REGULATORIO DE LAS INFRAESTRUCTURAS CRÍTICAS

ÍNDICE

EL MARCO REGULATORIO DE LAS INFRAESTRUCTURAS CRÍTICAS

AUTORES: Dr. Rafael Vidal Delgado, Coronel de Artª, DEM (Ret.), Director del Foro para la Paz en el Mediterráneo y miembro del Comité Científico del Centro Internacional de Formación de Autoridades y Líderes (CIFAL Málaga de UNITAR); Dra. Carmen Cristófol Rodríguez, Profesora de Comunicación de la UMA; y Doña Mar Gallardo, Responsable financiera del Foro para la paz en el Mediterráneo.

1. CONSIDERACIONES PREVIAS

Los últimos diez años han sido de intensa labor legislativa en los ministerios de Defensa e Interior, encontrándose en toda la normativa promulgada un factor común: la de responsabilizar sobre la seguridad a las distintas administraciones públicas y al sector privado.

Este hecho se reitera hasta la saciedad y en la ley aprobada a finales de 2015, la de la "Seguridad Nacional" [1], se recalca en su preámbulo:

En este contexto aparece el campo de la Seguridad Nacional como un espacio de actuación pública nuevo, enfocado a la armonización de objetivos, recursos y políticas ya existentes en materia de seguridad.
En este sentido, la Seguridad Nacional se entiende como la acción del Estado dirigida a proteger la libertad y el bienestar de sus ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en cumplimiento de los compromisos asumidos; concepto que, hasta la fecha, no había sido objeto de una regulación normativa integral.
Este esfuerzo de integración reviste tanta mayor importancia cuanto que la Seguridad Nacional debe ser considerada un objetivo compartido por las diferentes Administraciones, estatal, autonómica y local, los órganos constitucionales, en especial las Cortes Generales, ***el sector privado y la sociedad civil****, dentro de los proyectos de las organizaciones internacionales de las que formamos parte.* (VIDAL DELGADO & ALONSO RUSSI, 2015)

[1] En este libro se diseccionan las distintas seguridades y su evolución conceptual a través de los últimos años. Descarga gratuita en:
http://www.uma.es/foroparalapazenelmediterraneo/?p=3583

La participación del sector privada en las responsabilidades de la Seguridad Nacional, no es nueva, aunque sí lo es, el que se exprese con carácter de obligatoriedad en una Ley, y de hecho en el artículo 7 de la 36/2015, de 28 de septiembre, de Seguridad Nacional, al hablar de la "colaboración privada", expresa con rotundidad:

Las entidades privadas, siempre que las circunstancias lo aconsejen y, en todo caso, cuando sean ***operadoras de servicios esenciales y de infraestructuras críticas que puedan afectar a la Seguridad Nacional****, deberán colaborar con las Administraciones Públicas. El Gobierno establecerá reglamentariamente los mecanismos y formas de esta colaboración*.

Se ha subrayado el verbo "deber", porque significa que se está obligado a ello por una ley, natural, divina o positiva, según la acepción española en el diccionario de la Real Academia Española, en este caso por una "positiva" como es la de Seguridad Nacional y por toda la normativa en que se desarrolla. De hecho en el segundo párrafo del artículo anteriormente citado se indican los cauces reglamentarios para llevar a efecto este mandado legal: *El Gobierno, en coordinación con las Comunidades Autónomas, establecerá cauces que fomenten la participación del sector privado en la formulación y ejecución de la política de Seguridad Nacional*.

Insiste en el artículo 10: “Ámbitos de especial interés de la Seguridad Nacional”, entre los que destaca los de preservar los derechos y libertades de los ciudadanos y garantizar el suministro de los servicios y recursos esenciales, y volviendo a hacerlos en el 11, mencionando expresamente a las infraestructuras críticas:

Asimismo, sin perjuicio de lo establecido en la normativa reguladora de protección de infraestructuras críticas, las Administraciones Públicas citadas anteriormente asegurarán la disponibilidad de los servicios esenciales y la garantía del suministro de recursos energéticos, agua y alimentación, medicamentos y productos sanitarios, o cualesquiera otros servicios y recursos de primera necesidad o de carácter estratégico, entre ellos, como posteriormente veremos los “financieros” [2].

La Ley 36/2015 no es de carácter orgánico, aunque crea legalmente el “Sistema de Seguridad Nacional” y subordina a él, otros sistemas de carácter más sectorial, como por ejemplo en el de infraestructuras críticas,

[2] DEPARTAMENTO DE SEGURIDAD NACIONAL (en adelante DNS). La seguridad económica y financiera se erige cada vez de forma más clara y patente en requisito esencial y parte integral de la Seguridad Nacional, debido a su repercusión en la puesta en marcha de actuaciones gubernamentales y en el bienestar de los ciudadanos.
http://www.dsn.gob.es/es/sistema-seguridad-nacional/qu%C3%A9-es-seguridad-nacional/%C3%A1mbitos-seguridad-nacional/seguridad-econ%C3%B3mica Consultada el 08.10.2018.

protección civil, crisis, etc., sin embargo no los contradice, sino que pretende armonizar lo ya legislado.

Debe quedar claro en la mente de los directivos de las empresas de servicios esenciales, entre ellas, las económico-financieras, que forman parte del Sistema Nacional de Seguridad, con todas las obligaciones que ello conlleva.

En el artículo 21.7, da pie a que sea convocado al Consejo de Seguridad Nacional, *las personas físicas y jurídicas cuya contribución se considere relevante a la vista de los asuntos a tratar en el orden del día*. En este sentido no podemos obviar que el sector económico financiero es un bien esencial y además con el que se puede dañar el bienestar de los ciudadanos a causa de ataques o sabotajes a sus infraestructuras, por lo que con toda seguridad, en ocasiones serán convocados uno o varios representantes del sector financiero, tal como ya se hace con otro cualquier sector de las infraestructuras críticas.

En la Ley se hace mención a que se elaborará un catálogo de recursos privados y su contribución a la seguridad nacional. Y de hecho:

Comprende más de 3.500 instalaciones e infraestructuras sensibles dentro de las siguientes áreas estratégicas:

1. *Energía*

2. *Industria Nuclear*
3. *Tecnológicas de la Información*
4. *Transportes*
5. *Suministro de Agua*
6. *Suministro de Alimentos*
7. *Salud*
8. ***Sistema Financiero***
9. *Industria Química*
10. *Espacio*
11. *Recursos*
12. *Administración*

El catalogo contiene la descripción de las infraestructuras, los medios de contacto con las mismas, el tipo de instalación, datos geográficos y de localización, información de seguridad, riesgos evaluados, información de las fuerzas de seguridad, e información audiovisual. [3]

[3] https://www.intelpage.info/centro-nacional-de-proteccion-de-infraestructuras-criticas8.html

Consejo de Seguridad Nacional, presidido por S.M. El Rey

A lo largo del presente análisis, se tratará el repertorio legislativo que a continuación se relaciona, sin que el mismo tenga el carácter excluyente:

1. Comunicación de la Comisión al Consejo y al Parlamento Europea COM(2004) 702 final de 20.10.2004
2. Libro Verde sobre el Programa Europea para la Protección de las IC. COM(2005) 576 final de 17.11.2005
3. Directiva 2008/114/CE del Consejo de 8 de diciembre de 2008, sobre la identificación y designación de IC Europas y la evaluación de la necesidad de mejorar su protección.
4. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las Infraestructuras Críticas.

5. Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de Protección de IC.
6. Estrategia global para la política exterior y de seguridad de la Unión Europea: “Una visión común, una actuación conjunta: una Europa más fuerte” (2016). Sustituye a la Estrategia Europea de Seguridad 2003
7. Estrategia de Seguridad Nacional 2017.
8. Ley 5/2014, de 4 de abril, de Seguridad Privada.
9. Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.
10. Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos
    a) Seguridad documental.
        - OR-ASIP-04-01.04 – Orientaciones para el Manejo de Información Clasificada con Grado de Difusión Limitada.
    b) Seguridad en el Personal.
        - OR-ASIP-04-02.02 – Instrucción de Seguridad del Personal para acceso a Información Clasificada.
    c) Seguridad Física.
        - OR-ASIP-01-01.03 – Orientaciones para el Plan de Protección de una Zona de Acceso Restringido.

- OR-ASIP-01-02.03–Orientaciones para la Constitución de Zonas de Acceso Restringido.

d) Seguridad de los Sistemas de Información y Comunicaciones.
   - OR-ASIP-03-01.04 – Orientaciones para la Acreditación de Sistemas de Información y Comunicaciones para el manejo de Información Clasificada.

11. Directiva Europea (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión.
12. Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Este RD-L se observa el "apresuramiento" en su elaboración y redacción, debido a que el plaza de transposición de la Directiva UE, finalizaba en agosto de 2018, de esta forma, se hace constantemente referencia a normativas europeas, que deben tenerse en cuenta, contándose entre ellas:
    a) Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas, recogiéndose todo ello en el artículo 2 de la citada Recomendación.
    b) Reglamento (UE) 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de

2012, sobre normalización europea, sin que quede claro a qué normalización expresa se refiere, teniéndose en cuenta que en España funciona la Norma UNE-ISO/IEC 27001, la cual trata de tecnologías de la información, técnicas de seguridad, sistemas de gestión de seguridad de la información y requisitos.

La anterior normativa es la que directamente afecta a las IC y Seguridad Nacional, relacionándose a continuación otra, que tiene nexos comunes con las de IC:

13. LEY 9/1968, de 5 de Abril (BOE. Núm. 84, de 6 de Abril de 1968), MODIFICADA POR LEY 48/78, de 7 de Octubre (BOE. Núm. 243) sobre SECRETOS OFICIALES.
14. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
15. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
16. REAL DECRETO 393/2007, de 23 de marzo, por el que se aprueba la Norma Básica de Autoprotección de los centros, establecimientos y

dependencias dedicados a actividades que puedan dar origen a situaciones de emergencia.

17. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
18. Reglamento (UE) nº 526/2013 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) nº 460/2004 Texto pertinente a efectos del EEE.
19. Ley 15/2015, de 9 de julio, del Sistema Nacional de Protección Civil. Esta ley y todo su desarrollo, afecta a los sectores de IC que están relacionados con el terreno, con bienes materiales o pueden afectar a personas. Los riesgos son de carácter natural o antrópicos, entre estos últimos destaca el terrorismo.
20. Ley Orgánica 4/2015, de 30 de marzo de Protección de la Seguridad Ciudadana. En esta Ley se hace una referencia explícita a los operadores críticos, expresando que todos ellos tienen obligación de disponer de medidas de seguridad y por ende del correspondiente Plan de Seguridad.

Artículo 26. Establecimientos e instalaciones obligados a adoptar medidas de seguridad.

1. *Reglamentariamente, en desarrollo de lo dispuesto en esta Ley, en la legislación de seguridad privada, en la de infraestructuras críticas o en otra normativa sectorial, podrá establecerse la necesidad de adoptar medidas de seguridad en establecimientos e instalaciones industriales, comerciales y de servicios, así como en las infraestructuras críticas, con la finalidad de prevenir la comisión de actos delictivos o infracciones administrativas, o cuando generen riesgos directos para terceros o sean especialmente vulnerables.*

1.1.SERVICIO ESENCIAL

La Ley 8/2011 de Protección de Infraestructuras Críticas, define lo que es "servicio esencial" a efectos de la citada ley, aunque dada la conexión entre toda la normativa que se va a desarrollar con posterioridad, debiera entenderse que la definición afecta a toda ella, aunque el Real Decreto-Ley 18/2018, de 7 de septiembre, establece matices en la definición, como luego veremos:

> *a) Servicio esencial: el servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.*

b) Sector estratégico: cada una de las áreas diferenciadas dentro de la actividad laboral, económica y productiva, que proporciona un ***servicio esencial*** *o que garantiza el ejercicio de la autoridad del Estado o de la seguridad del país. Su categorización viene determinada en el anexo de esta norma.*

c) Subsector estratégico: cada uno de los ámbitos en los que se dividen los distintos sectores estratégicos, conforme a la distribución que contenga, a propuesta de los Ministerios y organismos afectados, el documento técnico que se apruebe por el Centro Nacional de Protección de las Infraestructuras Críticas.

d) Infraestructuras estratégicas: las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los ***servicios esenciales****.*

e) Infraestructuras críticas: son las infraestructuras estratégicas, cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los ***servicios esenciales****.*

El carácter de "servicio esencial" ha sido ampliamente debatido, aunque no en lo concerniente a la protección de infraestructuras ni seguridad nacional, sino en el

terreno laboral, precisamente para establecer criterios sobre el mantenimiento de un “servicio público”, en caso de convocatoria de huelga.

Eduardo López Aranguren, en su artículos sobre “Huelga, servicios esenciales y servicios mínimos”, escribe [4]:

> *Primer problema: la definición de “servicios esenciales. El Tribunal Constitucional (TC) intentó una definición en su sentencia 26/1981 de 17 de julio que ha sido invocada en otras sentencias posteriores del mismo tribunal: “Para que el servicio sea esencial deben ser esenciales los bienes e intereses satisfechos. Como bienes e intereses esenciales hay que considerar los derechos fundamentales, las libertades públicas y los bienes constitucionales protegidos” (Fundamento jurídico 10). Más en sentencia posterior, 43/1990 de 15 de marzo, el TC razona que “a priori no existe ningún tipo de actividad productiva que, en sí misma, pueda ser considerada como esencial” y que “los servicios esenciales no quedan lesionados o puestos en peligro por cualquier situación de huelga, siendo necesario examinar en cada caso las circunstancias concurrentes en la misma” (Fundamento jurídico 5). Como*

> *escribiera poco tiempo después de esta última sentencia María Emilia Casas, una de las dificultades más notables del sistema español y de la jurisprudencia constitucional sobre la huelga es la imprecisa y amplia fórmula delimitadora de la esencialidad de los servicios. Está pendiente pues, una definición operativa de "servicio esencial" que sea generalmente aceptada. Ello da origen a la queja sindical de que en la práctica es la autoridad gubernativa quien decide qué es un servicio esencial.* (López Aranguren, 2011)

El artículo, publicado el 7 de agosto de 2011, no tiene en cuenta la definición que se fija en la Ley 8/2011, de 28 de abril.

Por otra parte en el Real Decreto-Ley 18/2018, en su artículo 3, define "servicio esencial" y "operador de servicio esencial", como:

> c) *Servicio esencial: servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas, que dependa para su provisión de redes y sistemas de información.*

d) *Operador de servicios esenciales: entidad pública o privada que se identifique considerando los factores establecidos en el artículo 6 de este Real Decreto-Ley, que preste dichos servicios en alguno de los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril.*

Es decir, que este segundo texto legal, tiene el añadido de “redes y sistemas de información”, bien es verdad que la norma se refiere a ellos.

1.2. RESPECTO AL SECTOR FINANCIERO

La finalidad del presente trabajo es que las empresas del sector financiero, dispongan de una herramienta de consulta para cualquier situación que pueda presentársele relacionado con la protección como Infraestructura Crítica.

No siendo experto en el sector financiero, solamente se tratarán de forma tangencial algunos aspectos del mismo, dejando a criterio de los que trabajan en el mismo, rellenar los huecos que puede dar lugar en este repertorio legislativo.

Se reseña alguna normativa referente al sector financiero:

21. Real Decreto 1080/1991, de 5 de julio, por el que se determinan los países o territorios a que se

refieren los artículos 2.º, apartado 3, número 4, de la Ley 17/1991, de 27 de mayo, de Medidas Fiscales Urgentes, y 62 de la Ley 31/1990, de 27 de diciembre, de Presupuestos Generales del Estado para 1991.

22. Ley 12/2003, de 21 de mayo, de prevención y bloqueo de la financiación del terrorismo.
23. Orden EHA/2963/2005, de 20 de septiembre, reguladora del Órgano Centralizado de Prevención en materia de blanqueo de capitales en el Consejo General del Notariado.
24. Orden EHA/1439/2006, de 3 de mayo, reguladora de la declaración de movimientos de medios de pago en el ámbito de la prevención del blanqueo de capitales
25. Orden EHA/2444/2007, de 31 de julio, por la que se desarrolla el Reglamento de la Ley 19/1993, de 28 de diciembre, sobre determinadas medidas de prevención del blanqueo de capitales, aprobado por Real Decreto 925/1995, de 9 de junio, en relación con el informe de experto externo sobre los procedimientos y órganos de control interno y comunicación establecidos para prevenir el blanqueo de capitales
26. REGLAMENTO (UE) Nº 575/2013 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 26 de junio de 2013, sobre los requisitos prudenciales de las entidades de crédito y las empresas de inversión, y por el que se modifica el Reglamento (UE) nº 648/2012.

27. Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.
28. Orden EHA/114/2008, de 29 de enero, reguladora del cumplimiento de determinadas obligaciones de los notarios en el ámbito de la prevención del blanqueo de capitales.
29. Circular 5/2010, de 28 de septiembre, del Banco de España, a entidades de crédito, sobre información que debe remitir el adquirente potencial en la notificación a la que se refiere el artículo 57.1 de la Ley 26/1988, de 29 de julio, sobre disciplina e intervención de las entidades de crédito. Hace referencia al terrorismo en el Anejo: *Lista de información que debe suministrar el adquirente potencial en cumplimiento de la obligación a que se refiere el artículo 57.1 de la Ley 26/1988, de 29 de julio, sobre disciplina e intervención de las entidades de crédito, para la evaluación cautelar de las adquisiciones de participaciones significativas y de los incrementos de participaciones en entidades de crédito.*
30. Ley 21/2011, de 26 de julio, de dinero electrónico.
31. Real Decreto 778/2012, de 4 de mayo, de régimen jurídico de las entidades de dinero electrónico.
32. Real Decreto 1559/2012, de 15 de noviembre, por el que se establece el régimen jurídico de las sociedades de gestión de activos. Hace referencia al terrorismo en determinados artículos, entre ellos los 24 y 47.

33. Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo
34. Orden ECC/2402/2015, de 11 de noviembre, por la que se crea el Órgano Centralizado de Prevención del blanqueo de capitales y de la financiación del terrorismo del Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles.
35. Ley 22/2015, de 20 de julio, de Auditoría de Cuentas. El artículo 60 hace referencia explícita al terrorismo.

Puede parecer excesiva la normativa que queda afectada, a causa de la declaración del sector financiero como infraestructura crítica y como servicio esencial, pero en esencia gran parte de esta legislación, circulares y órdenes, ya se lleva a efecto en el sector.

El sector abarcaba inicialmente el financiero y tributario, pero el equipo de trabajo, nombrado "ad hoc" para su estudio decidieron *"separar la parte financiera y tratarla de manera aislada, dejando la parte tributaria para su inclusión dentro del Plan Estratégico Sectorial que se dedicará a la Administración, estimando que tendría mejor encaje dentro del citado sector"* [5] (SÁNCHEZ CAMPS, 2014)

2. ANTECEDENTES LEJANOS

Tras el atentado en Nueva York del 11 de septiembre de 2001, el Gobierno norteamericano estableció un sistema de protección del país contra posibles ataques terroristas, al que denominó Homeland Security.

Con la información que en aquel momento se disponía, Rafael Vidal (Vidal, 2003), llevó a cabo unas reflexiones de las que se toman algunas consideraciones útiles para lo que se pretende:

2.1 HOMELAND SECURITY

Es difícil traducir el concepto de "Homeland Security" a nuestra lengua y mucho más adecuarla a nuestra manera de ser y sentir a la Nación. Se podría traducir como "Seguridad de la Patria", "Seguridad de la Tierra Natal", porque, tanto el gobierno como el pueblo norteamericano, lo que quieren expresar con el título es que quieren proteger el territorio nacional contra cualquier acción terrorista, poniendo en ello el empeño no sólo de las autoridades y medios estatales, sino también el personal de los mundos económicos y social.

Norteamérica no duda en echar mano de su Ejército, de sus sistemas de información, militares y civiles, de sus fuerzas guardacostas, de su guardia nacional, de sus policías federales, estatales y locales, de las distintas instituciones públicas que tienen relación con extranjeros

y de todas las empresas, comercios y población en general, porque todos están unidos contra el terrorismo, todos quieren vencerlo y todos desean olvidar, como una mala pesadilla, el fatídico 11 de septiembre.

España ha sufrido un millar de víctimas del terrorismo, no de golpe, sino en un continuo goteo que llega a ser más desesperante, pero nuestra conciencia nacional aún no se ha despertado contra esa lacra social.

"Homeland Security" propicia que el que no esté directamente en contra del terrorismo que amenaza a EE.UU. (la Patria), está implícitamente a favor de él, y por tanto es un enemigo público que hay que erradicar, es como un traidor a la "Patria".

¿Podría ese argumento implantarse en España? Hoy por hoy, no (está escrito en 2003)*, porque existen fuerzas políticas, principalmente determinadas nacionalistas que*

están francamente en contra de cualquier presión legal contra los grupos que apoyan directamente al terrorismo, defendiendo incluso algunos planteamientos conjuntamente con los terroristas. Hay también fuerzas de índole nacional, que se muestran tibias en recriminar determinadas acciones violentas. Desde luego, estas posturas serían perseguidas claramente en EE.UU.

España debe aprender, los americanos han creado el concepto de "Homeland Security", tal vez la traducción "Seguridad de la Patria" no tendría acogida en nuestro País, desde el momento que algunos grupos preconizan que España es una nación de naciones, cuando no se muestran como antiespañoles, pero si la expresión "Seguridad de la Tierra Natal". Para dar credibilidad al concepto hay que proporcionarle los medios necesarios, tanto materiales, como morales y sociales, y cuando esté implantado, cuando todos los españoles y sus estamentos comprendan que estamos en guerra contra el terrorismo, entonces estaremos dando los pasos decididos para erradicarlo, pero ¿es que necesitamos mil muertos de golpe para hacerlo? (Vidal, 2003)

2.2.LA SEGURIDAD

La "Homeland Security" de EE.UU. está comenzando a modificar el concepto de seguridad colectiva y de defensa nacional de los países occidentales, sin embargo su concepto, aún no han entrado en el ámbito de la empresa y de las instituciones europeas, lo que les

provocará a medio plazo un aumento de sus riesgos y vulnerabilidades.

La "Homeland Security", "Seguridad de la Patria" o "Seguridad de la Tierra Natal", como se quiera denominar en Europa y España, quiere representar un concepto integral de la seguridad colectiva, es decir la coordinación de todos los elementos que proporcionan protección a los estadounidenses contra cualquier agresión exterior.

El concepto de "Homeland Security" está sustentado en un superministerio de seguridad nacional, que controlará no solamente todos los resortes que proporcionan seguridad, sino también y muy especialmente a los sistemas de información o inteligencia, que "alertan" de cualquier amenaza que pueda materializarse en daño para la población o los bienes norteamericanos.

*¿**Por dónde pueden introducirse los sujetos causantes del daño?**, por múltiples lugares, desde las fronteras terrestres y marítimas, el espacio aéreo, el ciberespacio, la biotecnología, los alimentos y un largo etcétera, que por supuesto tienen perfectamente analizados y diseñados. Como es imposible cubrir todo el conjunto de la nación, los americanos han definido unas infraestructuras críticas, cuya carencia o disminución a causa de un riesgo materializado, provocaría gran quebranto al sistema de vida. Entre estas infraestructuras se encuentra la energía, las*

telecomunicaciones, la alimentación, el sistema financiero, etc.

El autor, en sus planteamientos operativos y formativos ha preconizado desde hace años la necesidad del "mando único", de la total coordinación, de todas las facetas que proporcionan seguridad a una organización, trasladando el concepto de "Homeland Security" al mundo civil con la denominación de "Seguridad Global", no integral, sino mirada la seguridad de la empresa o de la institución pública o privada, desde una perspectiva de conjunto, abarcando como una cúpula la global seguridad de la organización, despiezándola a continuación en otras seguridades más específicas, como corporativa, industrial, de la información, medioambiental, etc., uniendo a todo este conjunto los elementos que proporcionan inteligencia competitiva (Intelligence Competitive), pilar básico de la seguridad, como está demostrado en el esquema norteamericano.

Sin embargo la empresa y las instituciones españolas no comprenden aún esa necesidad, y la seguridad se encuentra desperdigada en numerosos departamentos, como recursos humanos, explotación, producción, operaciones, incluso económico-administrativo, no siendo posible su coordinación, ni su perspectiva global, por la cuestión evidente que el único que podría hacerlo es el presidente o el director general de la organización, lo cual es imposible.

No solamente se encuentra desperdigada, sino que los responsables de cada una de las parcelas de seguridad, tienen un rango de cuarto o quinto nivel en la organización, no respondiendo tampoco al esquema norteamericano, en donde el responsable de la "Homeland Security" se encontrará directamente debajo del presidente de EE.UU.

Los directivos españoles y europeos tienen que cambiar y empezar a dar a la Seguridad Global la importancia que tiene, porque como en otros artículos veremos, la seguridad, en definitiva la protección del patrimonio de una empresa, es la que más beneficios proporciona a la misma, al reducir drásticamente pérdidas a causa de las constantes inseguridades (Vidal, 2003).

2.3 EN EL ANIVERSARIO DEL 11S

El 11 de septiembre no debe considerarse una fecha exclusivamente norteamericana, sino que afecta a todo el orbe, porque significa una escalada cualitativa y cuantitativa del terrorismo internacional, habiéndose producido, un poco como consecuencia de dicha operación terrorista, otras que en distintas partes del mundo, han llevado la muerte y la desesperación, tanto a países islámicos como a los que no lo son.

Si nos atenemos a los hechos, la organización maligna de Osama bin Ladem y otras similares, ya habían atentado contra intereses occidentales, por ejemplo en 1993 una bomba de fabricación artesanal, hizo explosión en las torres del World Trade Center, matando a seis personas, hiriendo a más de mil e interrumpió las actividades comerciales de centenares de empresas próximas al centro financiero de Nueva York; la destrucción de dos aviones de pasajeros implicó al gobierno libio, de tal forma que parece que Gadafi, no

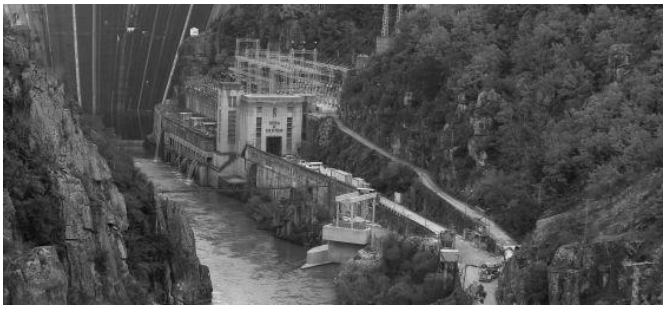
solamente ha entregado a los autores materiales del hecho, sino que está dispuesto a indemnizar a las víctimas inocentes de ese hecho tan absurdo. Estas tragedias, acaecidas en el pasado, han servido de indicadores de lo que podría venir en el futuro, como fue el 11 de setiembre, aunque su magnitud y la forma de llevar a cabo el acto terrorista, eran casi impensables de imaginar.

Con respecto al hecho terrorista se produce una situación singular en las mentes de las personas, las cuales por lo general, consideran que a ellos nunca les va afectar, cuestión que estamos viviendo día a día, con las declaraciones de los algunos políticos que alegan que la ayuda de España a George Bush, ha incrementado el peligro del terrorismo islámico. Sin embargo, mis propias vivencias, me indican que esa percepción es un gravísimo error, para ello pongo dos ejemplos de nuestro país: En 1980 la escalada terrorista de ETA en la País Vasco se había incrementado espectacularmente, con atentados y asesinatos semanales; me encontraba destinado en el estado mayor del gobierno militar de Guipúzcoa, cuyo gobernador, Pedro Arístegui, un hombre de gran valía y extraordinario valor, sufrió en sus carnes el terrorismo en Argentina y pocos años después sería asesinado en un atentado en Beirut, pues bien en el gobierno militar se encontraba destinado un coronel, cuyo cargo era el de director del economato militar, y al recordarle que debía de cumplir las medidas de seguridad individual, contestó que a él no

le afectaban porque tenía dos hijos afiliados a herri batasuna, sin embargo fue asesinado y según dicen, sus hijos no se desentendieron de la organización; Díaz Arcocha, superintendente de la policía autónoma vasca, teniente coronel de infantería, tampoco creía que le podría pasar a él, por sus vinculaciones vascas, sin embargo también fue asesinado. Sólo dos muestras de que la espiral del terror no entiende de opiniones y simpatías, pretendiendo exclusivamente imponer su doctrina y poder por este medio, sin importarle que la tragedia afecte a uno de los que considera afecto.

Todo gobierno occidental, toda institución pública y todas las empresas privadas, deben de analizar, estudiar y precaverse en lo posible, de un atentado terrorista, sin pensar en ningún momento "que eso no me puede pasar a mí", porque precisamente esa indefensión les hace ser proclive a padecer la furia terrorista.

La lacra del siglo XXI es el terrorismo, el gobierno y la sociedad norteamericanos así lo han comprendido y han implantado su sistema de "seguridad de la Patria" (Homeland Security), colaborando a la misma todas las instituciones federales, estatales, las grandes empresa estratégicas y hasta los mismos ciudadanos, que se han convertido en fuentes de información.



La Unión Europea y España deben actuar de la misma manera, pero mientras nos encontremos con políticos y personas irresponsables que piensen que eso no me puede pasar, estaremos inermes ante el terrorismo internacional, uno de cuyos pilares es ETA. [6]

2.4 NOTAS DE LOS AUTORES

Desde 2001 el coronel Vidal ha sido apóstol de la protección de las infraestructuras, escribiendo incansablemente tras los atentados de Atocha y del metro de Londres, viendo que a partir de este último atentado, la Unión Europea, empezaba a preocuparse el tema, ya que hasta dicha fecha el terrorismo era solamente un problema español, las dos coautoras se sienten identificadas con ello y preconizan, dentro de sus respectivos ámbitos la misma preocupación.

[6] VIDAL DELGADO, Rafael. *En el aniversario del 11S*. www.belt.es 11.09.2003

3. LAS INFRAESTRUCTURAS CRÍTICAS Y SUS SECTORES ESPECÍFICOS

3.1 LA GÉNESIS DE LAS IC [7] EN LA UNIÓN EUROPEA

En el año 2004, tras el atentado del 11 de marzo en España, la Unión Europea comprendió que el terrorismo yihadista era una amenaza que se debía tener muy en cuenta y por el Consejo Europeo en su reunión de junio de 2004, solicitó de la Comisión y del Alto Representante, en aquel momento Javier Solana, que prepararan una estrategia global contra el terrorismo.

COMUNICACIÓN DE LA COMISIÓN AL CONSEJO Y AL PARLAMENTO EUROPEA COM (2004) 702 FINAL DE 20.10.2004

Como resultado del encargo, la Comisión presentó una Comunicación con fecha 20 de octubre, en la cual se definía por primera vez el concepto de IC. Dicha definición ha permanecido casi inalterable a lo largo de los años, efectuándosele exclusivamente ligeros matices:

Definición:

Las infraestructuras críticas son aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz

[7] Acrónimo de Infraestructura/s Crítica/s que se emplearé en el texto.

funcionamiento de los gobiernos de los Estados miembros. Las infraestructuras críticas están presentes en numerosos sectores de la economía: actividades bancarias y financieras, transporte y distribución, energía, servicios, salud, abastecimiento de alimentos, comunicaciones, administraciones públicas clave.

Relacionaba los llamados posteriormente "Sectores Críticos", encontrándose entre ellos:

- *Finanzas (por ejemplo banca, valores e inversión)*

Dentro de la brevedad de la Comunicación, marcó las directrices que iban a desarrollarse en el transcurrir de los años, tanto por la Unión Europea (UE) como por los países miembros.

Un aspecto importante de la Comunicación fue establecer los criterios para declarar que una infraestructura de un estado tuviera que conceptuarse como crítica.

Criterios:

- *Alcance - la pérdida de un elemento de infraestructura crítico se mide por el tamaño del área geográfica que pudiera verse afectada por su pérdida o indisponibilidad, internacional, nacional, provincial, territorial o local.*
- *Magnitud - el grado del impacto o de la pérdida puede evaluarse como nulo, mínimo, moderado o*

principal. Entre los criterios que podrían utilizarse para evaluar la magnitud potencial se encuentran los siguientes:

a) *Impacto público (cantidad de población afectada, pérdidas de vidas, enfermedades, lesiones graves, evacuación);*
b) *Económico (efecto PIB, volumen de pérdida económica y/o degradación de productos o servicios);*
c) *Ambiental (impacto en el lugar y sus alrededores);*
d) *Interdependencia (con otros elementos de infraestructura críticos).*
e) *Político (confianza en la capacidad de las administraciones públicas);*

- *<u>Efectos en el tiempo</u> - estos criterios determinan en qué plazo la pérdida de un elemento podría tener un impacto importante (inmediato, 24-48 horas, una semana, otros).*

Estos criterios se han mantenido a lo largo de los años. La normativa española añade un criterio nuevo, el de "redundancia", es decir cuando el problema no puede paliarse por otros medios.

En el estudio y análisis de los "medios" disponibles, de acuerdo con el Método de Planeamiento, que posteriormente se tratará, se deberá contar con estos medios adicionales, para el mantenimiento del sector financiero.

Gestión compartida

La gestión de la seguridad de una IC, aunque, según la Comunicación, debe ser responsabilidad del estado miembro, pero debido a que es imposible para las capacidades de los estados atender todas las vulnerabilidades, se recomienda que exista una "gestión compartida":

La protección de infraestructuras críticas (PIC) requiere un partenariado firme y cooperativo entre los propietarios y gestores de infraestructuras críticas y las autoridades de los Estados miembros. La responsabilidad principal de la gestión del riesgo en las instalaciones físicas, cadenas de suministro, tecnologías de la información y redes de comunicaciones corresponde a sus propietarios y gestores.

La responsabilidad compartida es recurrente en toda la normativa actual de seguridad, tanto europea, como la más reciente de seguridad nacional española.

Habría que preguntarse si una de las partes no asume su cuota de responsabilidad, estaría infringiendo la ley y por tanto podría ser sancionado administrativa e incluso penalmente, en este caso a los gestores del sector financiero por dejación de sus funciones

LIBRO VERDE [8] SOBRE EL PROGRAMA EUROPE PARA LA PROTECCIÓN DE LAS IC. COM(2005) 576 FINAL DE 17.11.2005

En julio de 2005 se produce el atentado en el metro de Londres, pareciendo que en aquellos primeros años, el Gobierno de la UE, se moviera a impulsos de estos ataques terroristas yihadistas.

El objetivo del documento, presentado por la Comisión al Consejo, era establecer un Programa Europeo de Protección de Infraestructuras Críticas (PEPIC), con la colaboración de todas las partes interesadas, no solamente los estados miembros, sino incluso empresas y otras organizaciones.

Niveles de protección

Como tal libro verde, se plantea como un marco de reflexión, y de esta forma se exponen las amenazas posibles sobre las que debe precaverse el PEPIC:

1. Frente a todo los peligros, constituyéndose una amalgama entre terrorismo, catástrofes naturales, sabotajes, etc.
2. Similar al anterior, pero fijando como línea prioritaria la amenaza terrorista.

[8] Los Libros Verdes son documentos publicados por la Comisión Europea cuyo objetivo es estimular una reflexión a nivel europeo sobre un tema concreto. En ellos se invita a las partes interesadas (organismos y particulares) a participar en un proceso de consulta y debate sobre las propuestas que presentan.

3. Centrarse exclusivamente en la amenaza terrorista.

A la postre, el Programa Europea, se ha centrado en la tercera opción, aunque con el matiz, de que debe estar perfectamente coordinado con el resto de las amenazas a las IC, bien sea por causas antrópicas o naturales.

Principios

Aunque la UE es muy dada a establecer un buen número de principios, en este caso, se marcó únicamente cinco:

- **Subsidiariedad:** el principio de subsidiariedad estaría en el núcleo mismo del PEPIC; la protección de las infraestructuras críticas sería, ante todo, responsabilidad nacional. Las responsabilidades primordiales en cuanto a protección de estructuras críticas incumbirían a los Estados miembros y a los propietarios/ operadores, actuando bajo un marco común.
- **Complementariedad**: el marco común del PEPIC sería complementario con respecto a medidas ya vigentes.
- **Confidencialidad**: el intercambio de información sobre protección de infraestructuras críticas tendría lugar en un entorno de confianza y confidencialidad.
- **Cooperación de los agentes interesados**: todos los agentes interesados, incluidos los Estados

miembros, la Comisión, las asociaciones sectoriales o profesionales, los organismos de normalización y los propietarios, operadores y usuarios (entendiéndose por «usuarios» las organizaciones que explotan y utilizan la infraestructura para fines comerciales y de prestación de servicios) deben desempeñar un papel en la protección de las infraestructuras críticas.

- **Proporcionalidad**: las estrategias y medidas de protección serían proporcionales al grado de riesgo en cuestión, pues no todas las infraestructuras pueden protegerse frente a todas las amenazas

De estos principios se deducen dos actores primordiales:

1. Estado.
2. Operador Crítico.

Pero al mismo tiempo, se recomienda en este Libro Verde:

a) La necesidad de aprovechar los medios existentes, es decir que la seguridad de que ya se dispone debe ser complementada.
b) Los agentes interesado, es decir las empresas, deben actuar, no por “imperativo legal”, sino por propia convicción de la necesidad de su seguridad.
c) La proporcionalidad es necesaria, este principio va unido a un eficaz análisis de riesgos, de tal forma

que no deben ser los mismos medios lo que deban de instalarse en una instalación financiera situada en un barrio conflictivo a otro que está en el centro de un núcleo urbano, sin embargo, desgraciadamente, bastantes empresas, instalan las mismas medidas de protección en ambas, lo cual es un despilfarro económico.

En España nos movemos por "imperativos legales", dado que no existe una "cultura" de seguridad[9].

Tal vez, la UE, debería de haber incidido en otro principio: el de la "economía de medios", porque la seguridad y las medidas a instalar, deben ser las suficientes, ni más ni menos. De hecho una de las críticas de los operadores, declarados críticos, es la necesidad de fuertes inversiones en seguridad y protección, debido principalmente a una cultura nociva existente en nuestro país, relacionado con la seguridad, en el sentido de que si queremos hacernos una casa, recurrimos a un arquitecto que nos la diseñe y a una constructora que la edifique, siempre vigilada por el

[9] Desde finales de la década de los ochenta he actuado como consultor-asesor de numerosas entidades públicas y privadas, y casi siempre los gestores de las mismas han querido circunscribirse únicamente a lo que se marca en la normativa "para que no me multen o no tenga responsabilidad judicial". Judicialmente puede argumentarse que una empresa que presta un servicio público, como es el abastecimiento de agua, aunque por su entidad, no haya sido declarada como crítica, en caso de una manipulación del mismo, debido a agentes externos, podría el juez encontrar indicios penales en el gestor de la infraestructura.

“arquitecto de la propiedad”; sin embargo, cuando se quiere montar un sistema de protección, en vez de recurrir a un ingeniero, técnico competente, según la legislación vigente, que diseñe el sistema, recurrimos directamente a la empresa de seguridad, que al mismo tiempo que hace el proyecto, lo ejecuta y ahí está el error, porque el operador crítico, no tiene un “ingeniero de la propiedad”. No quiere significarse con ello, que a las empresas instaladoras de seguridad, se les “va la mano” a la hora de colocar medios de protección, sino que tienen unos estándares y el análisis de riesgo hay que efectuarlo instalación por instalación, porque ninguna es igual que otra.

El papel de los operadores críticos

Ya en el Libro Verde se señalan las responsabilidades de los operadores críticos, entre ellos designación de uno o varios funcionarios de enlace para la seguridad, entre el operador y la autoridad competente del estado miembro; el diseño, ejecución y actualización de un Plan de seguridad del operador y ***la participación en la elaboración de un plan de intervención*** *relativo a las infraestructuras críticas, conjuntamente con las autoridades competentes en materia de* ***protección civil de los Estados miembros****, así como las* ***autoridades represivas***.

Esta última responsabilidad se ha transcrito de forma textual, dada su referencia explícita a la Protección Civil y a las Fuerzas y Cuerpos de Seguridad.

En el Libro Verde habla de la posibilidad de que el operador crítico, no sea declarado como tal por una autoridad competente del estado miembro, sino que la empresa que tiene a su cargo un servicio esencial, proponga a dicha autoridad, esta declaración, cuestión que no se ha dado en España, en donde se espera que sea catalogada como tal para actuar en consecuencia.

En este sentido, el desarrollo normativo, podría haber seguido una línea similar a la de los “planes de autoprotección”, en donde se fijan unos mínimos, a partir de los cuales todas las actividades (empresas, centros, establecimientos, etc.), que entran dentro de esos mínimos, asumen su propio Plan de Autoprotección, presentándolo a la autoridad competente, como un documento más, para que se le autorice el inicio de la actividad.

Este procedimiento hubiera permitido una mejor concienciación y una progresiva asunción de responsabilidades por parte de las empresas de servicios esenciales, entre ellos el que nos ocupa, que es el sector financiero.

3.2 PRIMERAS ACTUACIONES ESPAÑOLAS

El 2 de noviembre de 2007, el Consejo de Ministros aprobó el marco estructural para la protección de las IC en España, basándose en la Comunicación de la Comisión de 2004 y en el Libro Verde.

Se crea el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), dentro de la Secretaría de Estado de Seguridad, debiendo ser custodio del Plan de Seguridad y del Catálogo Nacional.

De forma previa, con fecha 7 de mayo de 2007, el Secretario de Estado de Seguridad, aprobó el Plan Nacional de Protección de IC, creando además un esbozo de instalaciones sensibles contra atentados terroristas.

Define, por primera vez, que son las instalaciones críticas en España:

Son aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción pueden tener una repercusión importante en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados miembros.

*Entre estas instalaciones sensibles destacan las centrales y redes de energía, las comunicaciones, **las finanzas**, el sector sanitario, la alimentación, el agua - embalses, almacenamiento, tratamiento y redes-, los*

transportes -aeropuertos, puertos, etc-, monumentos nacionales, así como la producción, almacenamiento y transporte de mercancías peligrosas, como material químico, biológico o nuclear.

También se fijó como una posible instalación sensible, determinados monumentos, que posteriormente no han pasado a la legislación, aunque en la actualidad parece que desde el Gobierno de la Nación, se pretende tenerlo en cuenta.

DIRECTIVA 2008/114/CE DEL CONSEJO DE 8 DE DICIEMBRE DE 2008, SOBRE LA IDENTIFICACIÓN Y DESIGNACIÓN DE IC EUROPEAS Y LA EVALUACIÓN DE LA NECESIDAD DE MEJORAR SU PROTECCIÓN

Un largo período de tiempo había transcurrido para que por fin la UE se decidiera a aprobar una Directiva, la cual tenía que ser obligatoriamente transpuesta a la legislación de todos los países miembros.

Aparte de todos los "considerando", propios de una directiva europea, es interesante remitirse a las definiciones:

«Infraestructura crítica», *el elemento, sistema o parte de éste situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o*

destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones.

***«Análisis de riesgos»**, el estudio de hipótesis de amenazas posibles, para evaluar las vulnerabilidades y las posibles repercusiones de la perturbación o destrucción de infraestructuras críticas.*

***«Protección»**, todas las actividades destinadas a garantizar la funcionalidad, continuidad e integridad de las infraestructuras críticas con el fin de prevenir, paliar y neutralizar una amenaza, riesgo o vulnerabilidad.*

***«Propietarios u operadores de infraestructuras críticas europeas »**, las entidades responsables de las inversiones en, o del funcionamiento diario de, un elemento, sistema o parte del mismo concreto, designado como ICE con arreglo a la presente Directiva.*

Del conjunto de definiciones, aunque se deberían destacar todas, se han seleccionado estas cuatro, para señalar no solamente lo que es una IC, sino que debemos siempre realizar un análisis de riesgos y de acuerdo con ellos, establecer una medidas de protección, siendo los responsables los “titulares de la actividad” de que se trata.

Es precisamente ese análisis de riesgo el que se criticaba, desde estas líneas, cuando es efectuado por una empresa instaladora, que tiende por propio negocio, a incrementar los medios y sistemas, al de un verdadera

analista que tamiza los riesgos que aparecen a través del principio de “economía de medios”. La protección y la seguridad son cuestiones basadas en la organización y buenas prácticas internas, más que una reiteración de medios físicos.

No se harán más menciones a la Directiva base de toda la legislación española, precisamente, por la obligatoriedad de asumirla en su totalidad, pudiendo el estado miembro, en este caso, España, como así ha hecho, reforzar determinadas actuaciones y supuestos, dada la experiencia en la lucha y protección contra el terrorismo que desgraciadamente tiene nuestra Patria.

4. NORMATIVA ESPAÑOLA EN VIGOR

4.1 LEY 8/2011, DE 28 DE ABRIL, POR LA QUE SE ESTABLECEN MEDIDAS PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

Preámbulo

Aunque parezca paradójico, el preámbulo o la exposición de motivos es una parte muy importante en nuestro repertorio legislativo, dado que en él, se fija el "espíritu del legislador", sirviendo posteriormente para poder "interpretar" adecuadamente algunos aspectos que pudieran estar confusos en el articulado.

En este preámbulo, aparte de bucear en la historia normativa para llegar a la necesidad de la Ley, se marca como prioritario, que la norma no es exclusiva de un Ministerio, en este caso el de Interior, sino que toda la Administración General del Estado, todas las Administraciones Públicas, organismos públicos y sector privado, se encuentran involucrados en la misma, siendo debidamente coordinados por el Ministerio del Interior, a través del CNPIC, al que expresamente se señala en el preámbulo (aunque expone que se "crea", cuando ya lo estaba desde 2007).

La finalidad de esta norma es, por lo tanto, el establecimiento de medidas de protección de las infraestructuras críticas que proporcionen una base adecuada sobre la que se asiente una eficaz ***coordinación*** *de las Administraciones Públicas y de las entidades y* ***organismos gestores o propietarios de infraestructuras*** *que presten servicios esenciales para la sociedad, con el fin de lograr una mejor seguridad para aquéllas.*

La Ley 8/2011, tiene una "anormalidad" dentro de la tradición de las leyes españolas no orgánicas, y es su carácter organizativo, repitiéndose por ello muchos conceptos en el reglamento de desarrollo.

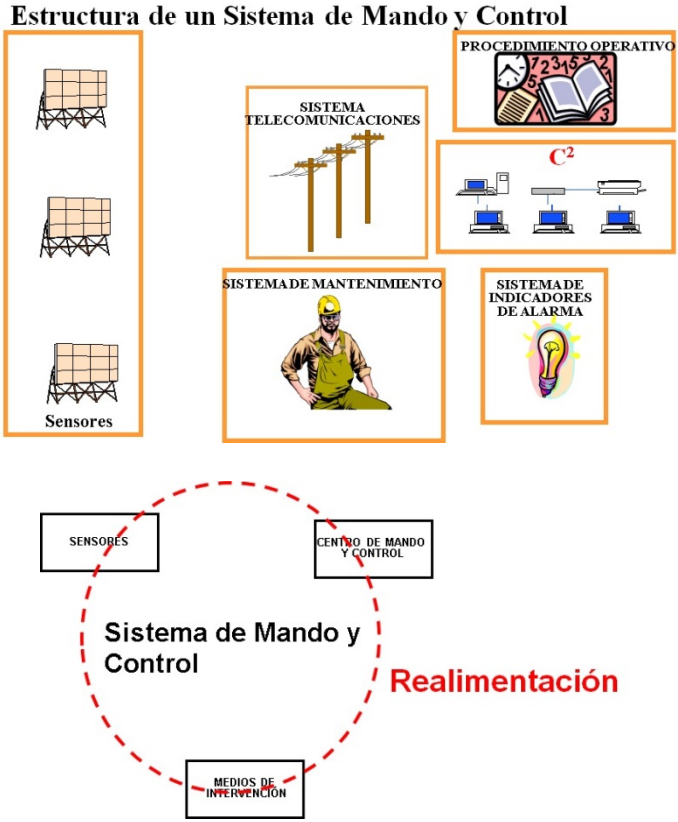
Definiciones**:**

No vamos a relacionar todas las definiciones, aunque cabría reseñar una, algo diferente de la europea, sobre el concepto de IC, *las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales*. Con ello incide en un principio, muy propio de las telecomunicaciones, el de "redundancia", es decir que siempre hay que tender a la existencia de "dos caminos" para llegar al mismo destino.

Operador Crítico

En las nuevas leyes españolas referentes a emergencias, crisis, seguridad, etc., se habla constantemente de “sistema”, pero ¿qué es un sistema?

Al margen de los llamados en informática “sistemas operativos”, el concepto de sistema debe entenderse como un conjunto de elementos que interactúan entre ellos, con la finalidad de alcanzar un objetivo.



Todo sistema tiene unas entradas, unos procesos y unos resultados, los cuales y con objeto de mejorarlos, vuelven a entrar en el sistema, para sufrir el mismo ciclo, es decir todo sistema se realimenta y al mismo tiempo recibe entradas nuevas.

Por ello en el sistema de IC y focalizado el ejemplo en una instalación crítica, de acuerdo con la “misión” que debe cumplir la instalación en el conjunto del operador, del territorio y de la población, sus vulnerabilidades y sus riesgos, necesita disponer de una serie de medios de protección, existiendo una o varias formas de aplicarlos en el terreno y en consonancia con los riesgos. Ese primer diseño sistémico, afronta a lo largo del tiempo una serie de riesgos patentes, los cuales exigen tomar decisiones, para ajustar el conjunto a las amenazas y mantener la continuidad del negocio. Esas formas de actuar sirven de entrada en el sistema, para volver a realizar el ciclo completo, unido todo ello a los nuevos riesgos latentes. Esta es la razón por la que en la normativa en vigor se exijan las revisiones, actualizaciones y auditorías con una determinada periodicidad.

El Sistema de Protección de IC dispone de una serie de agentes (los elementos que antes hemos reseñado), entre ellos, los que nos interesan: los operadores críticos

del sector financiero, tienen las siguientes funciones[10], de acuerdo con el artículo 13 de la Ley:

1. *Los operadores considerados críticos en virtud de esta Ley deberán colaborar con las autoridades competentes del Sistema, con el fin de optimizar la protección de las infraestructuras críticas y de las infraestructuras críticas europeas por ellos gestionados. Con ese fin, deberán:*

   a) *Asesorar técnicamente al Ministerio del Interior, a través del CNPIC, en la valoración de las infraestructuras propias que se aporten al Catálogo, actualizando los datos disponibles con una periodicidad anual y, en todo caso, a requerimiento del citado Ministerio.*
   b) *Colaborar, en su caso, con el Grupo de Trabajo en la elaboración de los Planes Estratégicos Sectoriales y en la realización de los análisis de riesgos sobre los sectores estratégicos donde se encuentren incluidos.*
   c) *Elaborar el* ***Plan de Seguridad del Operador*** *en los términos y con los contenidos que se determinen reglamentariamente.*
   d) *Elaborar, según se disponga reglamentariamente, un* ***Plan de Protección Específico*** *por cada una de las infraestructuras consideradas como críticas en el Catálogo.*

[10] En el presente estudio se quiere diferenciar los conceptos de "función" y de "misión", que se emplean como sinónimos sin serlos.

e) *Designar a un **Responsable de Seguridad y Enlace** en los términos de la presente Ley.*

f) *Designar a un **Delegado de Seguridad** por cada una de sus infraestructuras consideradas Críticas o Críticas Europeas por el Ministerio del Interior, comunicando su designación a los órganos correspondientes.*

g) *Facilitar las inspecciones que las autoridades competentes lleven a cabo para verificar el cumplimiento de la normativa sectorial y adoptar las medidas de seguridad que sean precisas en cada Plan, solventando en el menor tiempo posible las deficiencias encontradas.*

2. *Será requisito para la designación de los operadores críticos, tanto del sector público como del privado, que al menos una de las infraestructuras que gestionen reúna la consideración de Infraestructura Crítica, mediante la correspondiente propuesta de la que, en todo caso, el CNPIC informará al operador antes de proceder a su clasificación definitiva.*

3. *La designación como tales de los operadores críticos en cada uno de los sectores o subsectores estratégicos definidos se efectuará en los términos que reglamentariamente se establezcan.*

4. *Los operadores críticos tendrán en el CNPIC el punto directo de interlocución con el Ministerio del Interior en lo relativo a sus responsabilidades, funciones y*

obligaciones. En el caso de que los operadores críticos del Sector Público estén vinculados o dependan de una Administración Pública, el órgano competente de ésta podrá erigirse, a través del CNPIC, en el interlocutor con el Ministerio del Interior.

El artículo 16, recoge el perfil profesional del Responsable de Seguridad y Enlace (RSE), denominación que en España se ha dado al funcionario responsable de interlocución con las autoridades competentes, que señalaba la Directiva europea:

*… deberá contar con la habilitación de **Director de Seguridad** expedida por el Ministerio del Interior según lo previsto en la normativa de seguridad privada o con la habilitación equivalente, según su normativa específica*

En lo que respecta al sector crítico financiero, habría que añadir, que el RSE debe ser un técnico cualificado en su sector específico, con el nivel adecuado en la escala jerárquica de la empresa designada como Operador Crítico.

Por cada instalación [11] crítica, debe de existir un Delegado de Seguridad (DS), recogido en el artículo 17.

[11] Se debería haber diferenciado en la normativa los conceptos de infraestructura crítica e instalación crítica, empleada indistintamente y que puede dar motivos a confusión.

Ya las distintas normas europeas indicaban la necesidad de la “confidencialidad” de la información sensible, para ello el operador crítico, debe comprometerse a su seguridad, cumpliendo para ello con las normas dictadas por la autoridad competente de certificación de la información, cuestión que posteriormente se tratará.

Este tema de la información es muy importante, dado que en aras de una mal extendida transparencia, se cuelgan datos en la red internet, que tomados uno a uno, no son relevantes, pero que recopilados en su conjunto ya analizados adecuadamente, presentan una información muy detallada del operador crítico [12].

Coordinación con otros planes

No se puede poner coto a la seguridad. Ya se indicaban los niveles que en el Libro Verde se pretendía cubrir con respecto a los operadores críticos y se decía que la normativa de IC en vigor, se dirige precisamente a precaverse contra el terrorismo, pero no se puede olvidar que un acto de estas características, tiene necesariamente que dar pie a la activación de otros planes. Por ejemplo en el atentado del 11M en Madrid, se activaron, aparte de los planes antiterroristas, el de protección civil de la capital, los planes de catástrofes externas de los hospitales, el de RENFE y otros. Por eso en la Disposición final segunda de la Ley, se titula

[12] Las experiencias de osl autores de las presentes líneas pueden afirmar con rotundidad que se cuelga demasiada información en la red.

"Competencias en materia de Protección Civil", exponiéndose textualmente:

Lo dispuesto en esta Ley se entiende sin perjuicio de lo que establezca la normativa autonómica en materia de protección civil, de acuerdo con las competencias correspondientes a cada territorio en virtud de lo dispuesto en los correspondientes Estatutos de Autonomía.

4.2 REAL DECRETO 704/2011, DE 20 DE MAYO, POR EL QUE SE APRUEBA EL REGLAMENTO DE PROTECCIÓN DE IC

CNPIC

El artículo 7 del Reglamento trata sobre este órgano, al cual se le encarga la máxima coordinación en cuestiones de planificación, de tal manera que establecerá los contenidos mínimos de los Planes de Seguridad del Operador y los de Protección Específica, recordándose que por Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad (BOE nº 224 de 18.09.2015) se dictan dos Guías con los contenidos mínimos.

También el CNPIC es el órgano de interlocución y enlace entre el operador crítico y la estructura del Estado.

PSO y PPE

En estos planes se reitera el énfasis que debe darse al análisis de riesgos, única forma de que los planes resultantes se ajusten a la realidad.

Vivimos en la sociedad del riesgo. No tenemos más que recordar los atentados del 11S en Norteamérica, o los del 11M en España. ¿Debían haber previsto en sus análisis de riesgos, las entidades financiera que había en las Torres Gemelas que un avión podría abatirse sobre ellas?, por supuesto que no, pero sí, como disponían varias de ellas, de planes de crisis o continuidad del negocio, es decir que para una entidad financiera el riesgo no es el acto terrorista que se ha abatido sobre ella, sino la posibilidad de que se quede inoperativa, por cualquier causa una de sus instalaciones, debiéndose mantener el negocio por otros procedimientos.

Compatibilidad con otros planes existentes

En la Disposición final segunda de la Ley se trataba el tema de la coordinación con los planes de protección, el Reglamento, en su artículo 29, hace explícita referencia a la Protección Civil a través de la Norma Básica de Autoprotección (NBA) y de los propios planes de autoprotección, sobre los que se insiste, que son planes de protección civil y no de riesgos laborales. Este lapsus que existe en muchas empresas, es debido a que la NBA fue aprobada por Real Decreto 393/2007, es decir relativamente reciente, no existiendo con anterioridad

nada más que unas guías y unos planes de emergencia interior para determinados sectores, mientras que en la legislación laboral se insiste constantemente en los riesgos laborales y en la autoprotección de los trabajadores.

Todos los planes de contingencia que tiene un operador tienen que estar coordinados, siendo por ello muy conveniente que dentro del organigrama de una empresa o corporación y en el nivel adecuado, se encuentre la dirección, departamento, división o como quiera denominarse, que tenga a su cargo toda la "protección del patrimonio", tangible e intangible de la misma.

Los autores, han podido comprobar, que un operador del sector financiero, declarado crítico, tiene por un lado un Responsable de Seguridad y Enlace que coordina toda la información clasificada, estableciendo medidas y procedimientos para que su custodia y protección, y por otro lado exista un Responsable de Seguridad o Delegado de Protección de Datos de Carácter Personal, el cual también dicta sus propias medidas y procedimientos, llegándose a duplicar, cuando todo se solucionaría, si los dos son el mismo o tienen un mando por encima de ellos que los coordine y dirija.

Seguridad de las comunicaciones

El artículo 33 del Reglamento trata de las comunicaciones, pero entiende únicamente, la seguridad desde el operador crítico hacia el exterior, cuando

debería haber efectuado alguna referencia a las características técnicas que debiera tener la red de telecomunicaciones de las empresas, desplegadas en cientos de kilómetros cuadrados y con varios centenares de instalaciones, unas pequeñas y otras grandes.

Posteriormente podrá comprobarse que la Directiva Europea (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión complementa, precisamente, esta importante cuestión.

Plazos

La normativa española de seguridad se configura como una normativa de mínimos, es decir que muy pocos usuarios se encuentran de lleno inmersos en ella.

El legislador pretende la concienciación en seguridad a todos los niveles y que cuando se promulga una ley, todos los que pudieran verse afectados, deben dirigir sus esfuerzos a adaptarse en lo posible a sus requerimientos. Esa es la razón por la que se da tan corto plazo entre la declaración de operador crítico e instalación crítica y el nombramiento de RSE y DE.

4.3 OTRA NORMATIVA ESPAÑOLA EN MATERIA DE SEGURIDAD

4.3.1 LEY 36/2015, DE 28 DE SEPTIEMBRE, DE SEGURIDAD NACIONAL

Es una Ley aprobada recientemente, siendo, junto con la Estrategia Española de Seguridad, la primera que tendría que haberse aprobado, dado que implica a todas las demás, incluidas a las precedentes de infraestructuras críticas.

Dada su importancia se ha tratado ampliamente en las consideraciones previas.

5. ESTRATEGIAS DE SEGURIDAD

5.1 ESTRATEGIA DE SEGURIDAD DE LA UNIÓN EUROPEA

En el año 2003 la Unión Europea aprobó una Estrategia de Seguridad, en la cual se indicaba:

La Unión Europea, como unión de veinticinco Estados con más de 450 millones de habitantes y la cuarta parte del producto nacional bruto mundial, es, inevitablemente, un actor de envergadura mundial… tiene que estar dispuesta a asumir su responsabilidad en el mantenimiento de la seguridad mundial y la construcción de un mundo mejor.

Detallaba las amenazas mundiales y planteaba los objetivos estratégicos de la UE y consideraba y sigue considerando la multilateralidad como una ventana para la seguridad internacional, de la cual, aunque con cautela, trata el sector financiero:

Las principales instituciones el sistema internacional, como la Organización Mundial del Comercio (OMC) y las instituciones financieras internacionales, han incorporado nuevos miembros. China ha pasado a formar parte de la OMC y Rusia está negociando su ingreso. Nuestro objetivo debe ser ampliar el número de miembros de

estos organismos manteniendo, al mismo tiempo, el alto nivel de sus normas.

5.2. ESTRATEGIA DE SEGURIDAD NACIONAL DE 2011

La primera Estrategia de Seguridad Nacional fue aprobada en 2011, por el Gobierno de José Luis Rodríguez Zapatero. El coordinador de la misma: Javier Solana.

Con respecto al sector financiero, enunciaba:

Tanto la prevención como la mitigación de sus efectos requiere luchar contra las actividades delictivas, asegurar una correcta supervisión y regulación de los mercados, avanzar en la gobernanza económica europea y global, potenciar la presencia internacional de España, garantizar el funcionamiento de los servicios e infraestructuras críticos económicos y financieros, y promover un desarrollo económico sostenible que minimice los desequilibrios y garantice el crecimiento económico y la cohesión social. Con el fin de analizar la información relevante y facilitar la acción del Estado mediante una mejor toma de decisiones en este ámbito, se creará un Sistema de Inteligencia Económica (SIE).

5.3 REAL DECRETO 1008/2017, DE 1 DE DICIEMBRE, POR EL QUE SE APRUEBA LA ESTRATEGIA DE SEGURIDAD NACIONAL 2017

Esta estrategia de Seguridad Nacional, aprobada mediante Real Decreto, tal como fijaba la Ley de Seguridad Nacional, podría considerarse como continuación y actualización de la de 2011, haciendo mención a las de 2015, la cual en su aprobación por el Presidente del Gobierno, así lo afirmaba.

Tras analizar los desafíos, las vulnerabilidades y en definitiva las amenazas y los riesgos, en el capítulo V, se establecen los objetivos que se pretende, siendo, aunque no novedoso, sí para el sector financiero el "promover una cultura de seguridad nacional", resultando de ellos quince ámbitos de actuación, entre ellos el de la "ciberseguridad", considerada por el sector financiero como protección de sus sistemas de información, se debe producir un salto cualitativo, al entender que la seguridad en las redes y sistemas que proporcionan, no son exclusivas de ellos mismos, sino que afectan a la Seguridad Nacional, tal como veremos que las incidencias que se produzcan, afectan también a la globalidad del Estado, incluso de la UE.

La Seguridad Nacional se constituye como un servicio público, compartido por el Estado y por los operadores de servicios esenciales y de infraestructuras críticas.

En este documento estratégico se hace una especial anotación a la libertad, en estos momentos donde existen movimientos que quieren desgajar de la unidad de la Patria a algunas de sus partes:

En España se puede defender cualquier proyecto político siempre que se haga en estricta observancia de la legalidad y de los derechos y libertades de todos sus ciudadanos.

En cierto modo es una declaración extemporánea e inusitada que una estrategia de nivel político se haga mención al riesgo del separatismo y del nacionalismo.

Trata como una de las seguridades del Estado la "económica".

En lo que concierne a las infraestructuras críticas, uno de cuyos sectores es el financiero, expone:

Cualquier interrupción en los servicios proporcionados por estas infraestructuras de sectores estratégicos (Administración, espacio, industria nuclear, industria química, instalaciones de investigación, agua, energía, salud, tecnologías de la información y de comunicaciones, transporte, alimentación y sistema financiero y tributario) podría tener graves consecuencias en los flujos de suministros vitales o en el funcionamiento de los servicios esenciales, además de provocar perturbaciones y disfunciones graves en materia de seguridad.

Como se expuso con anterioridad, se modifica el concepto genérico de "sector financiero", por dos, uno propiamente de finanzas y el otro tributario, que entraría dentro del sector de la administración pública.

Entre los desafíos a los que se enfrenta la seguridad nacional en España, se encuentra la "inestabilidad económica y financiera":

Los factores que pueden desestabilizar el sistema económico y financiero son de muy diversa naturaleza, no exclusivamente económica, y normalmente sus efectos son transversales, materializándose en más de un ámbito. De ahí la necesidad de adoptar un enfoque integral, que no sólo aborde los aspectos estrictamente económico-financieros, sino que contemple también su dimensión de seguridad.

El fraude, la corrupción, los paraísos fiscales, el blanqueo de capitales, etc. es una gestión compartida entre la Administración del Estado y los Operadores de Servicios Financieros.

5.4 SEGURIDAD ECONÓMICA Y FINANCIERA

En el Departamento de Seguridad Nacional, se recoge[13]:

La seguridad económica y financiera se erige cada vez de forma más clara y patente el requisito esencial y parte integral de la Seguridad Nacional, debido a su repercusión en la puesta en marcha de actuaciones gubernamentales y en el bienestar de los ciudadanos.

[13] http://www.dsn.gob.es/es/sistema-seguridad-nacional/qu%C3%A9-es-seguridad-nacional/%C3%A1mbitos-seguridad-nacional/seguridad-econ%C3%B3mica Consultado el 15.10.2018.

La Estrategia de Seguridad Nacional plantea como ***objetivo*** *en el ámbito de la seguridad económica y financiera, potenciar un modelo de crecimiento económico sostenible, mitigar los desequilibrios de los mercados, luchar contra las actividades delictivas, potenciar la presencia económica internacional de España y garantizar la resiliencia de los servicios esenciales económicos y financieros.*

Las ***líneas de acción estratégica*** *que propone para alcanzar este objetivo son las siguientes:*

- *Potenciación de un modelo de crecimiento económico sostenible que minimice los desequilibrios tanto públicos como privados, potencie la productividad, el tejido empresarial, la innovación y la competitividad, intensifique los sectores de alto valor añadido, cree empleo de calidad, mantenga unas finanzas públicas saneadas y la estabilidad de precios a lo largo del ciclo económico, y garantice la cohesión social.*
- *Establecimiento de un marco socio-laboral que contribuya a una gestión eficaz de las relaciones laborales, basado en el diálogo social con vistas a la adopción de medidas consensuadas que coadyuven a reducir los niveles de conflictividad y favorezcan la paz social, que facilite la estabilidad en el empleo, la creación de puestos de trabajo y la eficiencia del mercado de trabajo.*

- *Promoción de una economía internacional abierta con un sistema estable de libre comercio e inversión en el marco de los foros internacionales en los que está presente España. Se fomentarán los consensos internacionales para dotar de mayor transparencia al sistema financiero. Se promoverá la seguridad jurídica en los entornos de inversión de las empresas españolas con actividad en el exterior.*
- *Refuerzo de los actuales mecanismos de regulación y supervisión, para conseguir que su labor sea efectiva y se eviten crisis sistémicas. Establecimiento de nuevos mecanismos de regulación y supervisión que garanticen una gobernanza económica y financiera global eficaz, como los propuestos por el G20, foro en el que participa España en calidad de invitado permanente.*
- *Contribución a una gobernanza económica y financiera efectiva de la UE, que asegure la sostenibilidad y el buen funcionamiento de la UEM y la fortaleza del euro. Se cooperará activamente en la construcción de un gobierno económico europeo con instrumentos comunes y políticas económicas coordinadas que incluirán igualmente el estudio de medidas de vigilancia de los paraísos fiscales.*
- *Fomento de los mecanismos de coordinación adecuados que permitan el desarrollo de la seguridad económica y de sus herramientas de*

apoyo -como por ejemplo, el Sistema de Inteligencia Económica (SIE)-.

- *Esfuerzo estratégico de acción y comunicación permanente en favor de la reputación e imagen de España, defensa de nuestros intereses en foros e instituciones económicas y apoyo a la internacionalización de empresas y emprendedores españoles con el objetivo de contribuir a construir una "marca España" sólida y positiva, tanto desde el entorno público como el privado.*
- *Definición de un procedimiento de estrecha cooperación entre las entidades privadas y las autoridades públicas responsables de la seguridad de las infraestructuras y los servicios financieros.*

En el año 2014, las acciones desarrolladas se han dirigido fundamentalmente a potenciar una economía internacional abierta, recuperar competitividad y luchar contra aquellas actividades que desequilibran la estabilidad económica.

En el sentido de promover una economía internacional abierta con un sistema estable de libre comercio e inversión, en el ámbito del G20 se han producido importantes avances como la creación de un centro global de infraestructuras como plataforma de intercambio de información y red de contacto entre gobiernos, el sector privado, los bancos de desarrollo y

otras organizaciones internacionales o la aprobación del Plan de acción contra la corrupción 2015-2016.

Son relevantes también las acciones emprendidas en el marco del Consejo de Estabilidad Financiera (FSB por sus siglas en inglés) para la mejora de los requerimientos prudenciales de incremento del grado de resistencia de los bancos con actividad internacional. En esta línea, destacan las medidas normativas y orgánicas de apoyo a los emprendedores y su internacionalización, así como las acciones de atracción de inversión extranjera generadora de actividad y empleo.

Se han impulsado, además, nuevos mecanismos de regulación y supervisión, para garantizar una gobernanza económica y financiera global eficaz, reforzándose a través del Servicio Ejecutivo de Prevención de Blanqueo de Capitales el esfuerzo contra el blanqueo de capitales y la corrupción pública. España es además parte activa en los foros internacionales de lucha contra los paraísos fiscales y en los acuerdos internacionales existentes en la materia.

La seguridad económica y financiera se erige cada vez de forma más clara y patente en requisito esencial y parte integral de la Seguridad Nacional, debido a su repercusión en la puesta en marcha de actuaciones gubernamentales y en el bienestar de los ciudadanos.

La Estrategia de Seguridad Nacional plantea como ***objetivo*** *en el ámbito de la seguridad económica y*

financiera, potenciar un modelo de crecimiento económico sostenible, mitigar los desequilibrios de los mercados, luchar contra las actividades delictivas, potenciar la presencia económica internacional de España y garantizar la resiliencia de los servicios esenciales económicos y financieros.

*Las **líneas de acción estratégica** que propone para alcanzar este objetivo son las siguientes:*

- *Potenciación de un modelo de crecimiento económico sostenible que minimice los desequilibrios tanto públicos como privados, potencie la productividad, el tejido empresarial, la innovación y la competitividad, intensifique los sectores de alto valor añadido, cree empleo de calidad, mantenga unas finanzas públicas saneadas y la estabilidad de precios a lo largo del ciclo económico, y garantice la cohesión social.*
- *Establecimiento de un marco socio-laboral que contribuya a una gestión eficaz de las relaciones laborales, basado en el diálogo social con vistas a la adopción de medidas consensuadas que coadyuven a reducir los niveles de conflictividad y favorezcan la paz social, que facilite la estabilidad en el empleo, la creación de puestos de trabajo y la eficiencia del mercado de trabajo.*
- *Promoción de una economía internacional abierta con un sistema estable de libre comercio e inversión en el marco de los foros internacionales*

en los que está presente España. Se fomentarán los consensos internacionales para dotar de mayor transparencia al sistema financiero. Se promoverá la seguridad jurídica en los entornos de inversión de las empresas españolas con actividad en el exterior.

- *Refuerzo de los actuales mecanismos de regulación y supervisión, para conseguir que su labor sea efectiva y se eviten crisis sistémicas. Establecimiento de nuevos mecanismos de regulación y supervisión que garanticen una gobernanza económica y financiera global eficaz, como los propuestos por el G20, foro en el que participa España en calidad de invitado permanente.*
- *Contribución a una gobernanza económica y financiera efectiva de la UE, que asegure la sostenibilidad y el buen funcionamiento de la UEM y la fortaleza del euro. Se cooperará activamente en la construcción de un gobierno económico europeo con instrumentos comunes y políticas económicas coordinadas que incluirán igualmente el estudio de medidas de vigilancia de los paraísos fiscales.*
- *Fomento de los mecanismos de coordinación adecuados que permitan el desarrollo de la seguridad económica y de sus herramientas de apoyo -como por ejemplo, el Sistema de Inteligencia Económica (SIE)-.*

- *Esfuerzo estratégico de acción y comunicación permanente en favor de la reputación e imagen de España, defensa de nuestros intereses en foros e instituciones económicas y apoyo a la internacionalización de empresas y emprendedores españoles con el objetivo de contribuir a construir una "marca España" sólida y positiva, tanto desde el entorno público como el privado.*
- *Definición de un procedimiento de estrecha cooperación entre las entidades privadas y las autoridades públicas responsables de la seguridad de las infraestructuras y los servicios financieros.*

En el año 2014, las acciones desarrolladas se han dirigido fundamentalmente a potenciar una economía internacional abierta, recuperar competitividad y luchar contra aquellas actividades que desequilibran la estabilidad económica.

En el sentido de promover una economía internacional abierta con un sistema estable de libre comercio e inversión, en el ámbito del G20 se han producido importantes avances como la creación de un centro global de infraestructuras como plataforma de intercambio de información y red de contacto entre gobiernos, el sector privado, los bancos de desarrollo y otras organizaciones internacionales o la aprobación del Plan de acción contra la corrupción 2015-2016.

Son relevantes también las acciones emprendidas en el marco del Consejo de Estabilidad Financiera (FSB por sus siglas en inglés) para la mejora de los requerimientos prudenciales de incremento del grado de resistencia de los bancos con actividad internacional. En esta línea, destacan las medidas normativas y orgánicas de apoyo a los emprendedores y su internacionalización, así como las acciones de atracción de inversión extranjera generadora de actividad y empleo.

Se han impulsado, además, nuevos mecanismos de regulación y supervisión, para garantizar una gobernanza económica y financiera global eficaz, reforzándose a través del Servicio Ejecutivo de Prevención de Blanqueo de Capitales el esfuerzo contra el blanqueo de capitales y la corrupción pública. España es además parte activa en los foros internacionales de lucha contra los paraísos fiscales y en los acuerdos internacionales existentes en la materia.

5.5 OTRAS ESTRATEGIAS

Por otra parte, otros sectores sociales, como seguridad y salud, formulan su propia estrategia: Estrategia Española de Seguridad y Salud en el Trabajo, o Estrategia del Sistema Nacional de Protección Civil:

La Estrategia del Sistema Nacional de Protección Civil consiste en analizar prospectivamente los riesgos que pueden afectar a las personas y bienes protegidos por la protección civil y las capacidades de respuesta

necesarias, y en formular en consecuencia las líneas estratégicas de acción para alinear, integrar y priorizar los esfuerzos que permitan optimizar los recursos disponibles para mitigar los efectos de las emergencias.

Como en la propia normativa de IC, también implica a la sociedad civil, como ya cita el Presidente del Gobierno Español, y los títulos que se expresan para cada uno de los dos documentos, no pueden ser más aleccionadores, siendo en el de 2011 “una responsabilidad de todos” y en la de 2017 “un proyecto compartido”.

Todas estas estrategias parten, tal como se ha indicado anteriormente, de la Estrategia Europea de Seguridad, que con el título de “Una Europa segura en un mundo mejor”, fue aprobada en 2003, bajo los auspicios del español Javier Solana.

6. SEGURIDAD DE LAS REDES Y SISTEMA DE INFORMACIÓN

6.1 DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 8 DE JULIO DE 2016, RELATIVA A LAS MEDIDAS DESTINADAS A GARANTIZAR UN ELEVADO NIVEL COMÚN DE SEGURIDAD DE LAS REDES Y SISTEMAS DE INFORMACIÓN DE LA UNIÓN

El consejero delegado del Banco Santander, José Antonio Álvarez (izquierda), y la presidenta de la Comisión, Ana Oramas (derecha), durante su comparecencia en la comisión parlamentaria que investiga la crisis financiera. Santi Donaire EFE

"Uno de los grandes y crecientes retos del sector financiero es el aumento geométrico de las amenazas de ciberseguridad y el fraude que suele acarrear", según ha declarado el número dos del gigante bancario español, quien ha recordado que las amenazas de ciberseguridad en el mundo provienen del crimen. "Las mafias se están especializando en diferentes tipos de cibercrimen e incluso hay grupos especializados en cada banco", expuso en el Congreso. Esta declaración publicada el 9 de septiembre de 2018, por Cinco Días, siendo la autora Ángeles Gonzalo Alconada, era una

realidad, sentida por la Unión Europea y transpuesta la Directiva por España con fecha 7 de del mismo mes y año.

Según fuentes del Fondo Monetario Internacional, las pérdidas del sector financiero por ataques informáticos se acerca a los cien mil millones de dólares, lo que supone unas pérdidas del 9%.

La Directiva se dirige fundamentalmente a los estados miembros, aunque hace referencias explícitas a los operadores de servicios esenciales, para que aquellos obliguen al cumplimiento de las especificaciones de seguridad, incluso con la posibilidad de sanciones que, aunque graduadas por los estados, deben ser significativas.

Le da gran importancia a los “sectores de la banca y las infraestructuras del mercado financiero”, no definiéndolo como “sector financiero” como en la normativa de las infraestructuras críticas, aunque reconoce que las regulaciones y supervisiones de la banca y las finanzas, han sido objeto de armonizaciones anteriores por parte de la UE, habiéndose aplicado controles estrictos para su seguridad, notificación de incidencias y gestión de las mismas.

En el considerando 26, la Directiva entiende que todas las entidades bancarias que sean declaradas operadores esenciales, extienden su actividad en todos o en varios Estados de la UE, por lo que ello obligará de

conversaciones bilaterales o multilaterales, seguramente para identificar la incidencia que pudieran tener, estas entidades, en los distintos países donde se encuentran implantadas.

En el considerando 52 expresa que solidariamente los operadores de servicios esenciales y los proveedores de servicios digitales de las redes y sistemas que utilicen, al tratarse fundamentalmente de redes y sistemas privados, gestionados por personal interno al banco o externo al mismo, mediante contrata, señalando en el considerando siguiente que los requisitos exigibles no deben aplicarse, en el caso de empresas de servicios digitales a la microempresas ni a las pequeñas empresas.

Ya en el articulado de la Directiva, concretamente en su artículo 1 señala explícitamente la complementariedad de la misma, con respecto a otras normas estatales que tengan por finalidad salvaguardar objetivos esenciales, en particular los concernientes a la seguridad nacional.

La Directiva obliga a los estados miembros, en su artículo 7.1., a dictar una “Estrategia Nacional de Seguridad de las Redes y Sistemas de Información”, considerándose en la transposición a España, por el Real Decreto-Ley 12/2018, que esta función la cumple la “Estrategia de Ciberseguridad Nacional” de 2013, conociéndose que se está produciéndose a su actualización.

Es significativo el Capítulo VII, ·Disposiciones Finales", al tratar las "sanciones" que pueden imponer los estados miembros, siendo una novedad legislativa en materia de seguridad nacional y servicio esencial, vista seguramente el incumplimiento de las infraestructuras críticas y servicios esenciales de la seguridad nacional, por parte de los operadores privados, al menos en España, precisamente por falta de un régimen sancionador.

Uno de los autores, asesorando a una entidad que había sido declarada infraestructura críticas, el máximo responsable de la misma, le comentó que no pensaba cumplir nada, porque no existían sanciones por incumplimiento, incluso llegó a decirle que para él era más importante cumplir escrupulosamente la Ley Orgánica de Protección Datos Personales (LOPD) que la de Seguridad Nacional o Infraestructuras Críticas, porque con la primera podrían multarle y con las segundas no.

Evidentemente, aunque en el derecho español, la ley debe especificar si existe sanción, en el caso que nos ocupa, lo hace a través del derecho supletorio, concretamente la Ley de Protección de la Seguridad Ciudadana, la de Seguridad Privada y el Código Penal.

6.2. APLICACIÓN DE LAS SANCIONES CON OTRAS LEYES SUPLETORIAS [14]

Esta Directiva de la UE, palia el tema de la sanciones, exponiéndose en este apartado algunos argumentos para indicar que sin la misma y su correspondiente transposición a España en Real Decreo-Ley, también podía sancionarse por incumplimiento de la legislación anterior sobre IC y Seguridad Nacional.

6.2.1 LEY ORGÁNICA DE PROTECCIÓN DE LA SEGURIDAD CIUDADANA

La Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, especifica en su *Disposición adicional segunda. Régimen de protección de las infraestructuras críticas. La protección de las infraestructuras críticas se regirá por su normativa específica y supletoriamente por esta Ley.* Es decir que la Ley 4/2015 es "supletoria" de la 8/2011, de 28 de abril de protección de las infraestructuras críticas[15].

[14] Este apartado forma parte de una ponencia, que el coronel Rafael Vidal, dictó en la Escuela de Caminos, Canales y Puertos de Granada, dedicada al servicio esencial del agua, aunque puede perfectamente trasponerse al sector financiero.

[15] DERECHO SUPLETORIO: lo forman aquellas normas de un ordenamiento jurídico que tienen la facultad de regir situaciones que no le son específicamente propias, pero obligadas por el hecho de que la rama específica del ordenamiento que debería haberla regulado no lo ha hecho. Por lo tanto, el Derecho supletorio suple la ausencia de una norma específica y sirve para cubrir la laguna

El Artículo 26 de la citada LO, trata el tema de los *"Establecimientos e instalaciones obligados a adoptar medidas de seguridad":*

Reglamentariamente, en desarrollo de lo dispuesto en esta Ley, en la legislación de seguridad privada, en la de infraestructuras críticas o en otra normativa sectorial, podrá establecerse la necesidad de adoptar medidas de seguridad en establecimientos e instalaciones industriales, comerciales y de servicios, así como en las infraestructuras críticas, con la finalidad de prevenir la comisión de actos delictivos o infracciones administrativas, o cuando generen riesgos directos para terceros o sean especialmente vulnerables.

Hemos subrayado lo relativo a infraestructuras críticas y de forma discontinua, las instalaciones de servicios que, en este caso de la seguridad nacional, tendría el calificativo de "esenciales", es decir necesarios para el normal funcionamiento de la convivencia ciudadana.

Al haberse aprobado el Reglamento de desarrollo de la Ley de Infraestructuras Críticas con la omisión de las

---

jurídica. Se extiende a todos aquellos aspectos no regulados por un Derecho específico. Es normal que cada ordenamiento jurídico establezca un derecho supletorio básico. La principal utilidad de la existencia de los Derechos supletorios es cubrir las lagunas de las distintas ramas del derecho. En caso de ausencia de regulación, el juez se dirige al Derecho supletorio antes de acudir a otras fuentes del derecho como la costumbre o los principios generales del derecho. www.es.wikipedia.org

infracciones y sanciones, quedaría por ser recogidas la mención en el de Seguridad Privada, que se desarrollará en el apartado siguiente. No obstante, también se intentará profundizar en la normativa sectorial específica, relacionadas con los distintos grupos de infraestructuras críticas, para comprobar si de algunas manera si la omisión de medidas de seguridad pudiera ser motivo de sanción para el titular correspondiente.

En el Capítulo quinto, corresponde a “sanciones” y la Sección 1ª: *Sujetos responsables, órganos competentes y reglas generales sobre las infracciones y la aplicación de las sanciones.*

Artículo 30. Sujetos responsables.
1. La responsabilidad por las infracciones cometidas recaerá directamente en el autor del hecho en que consista la infracción.

Queda claro que la responsabilidad de la infracción es del autor en que consista la infracción. Si un establecimiento, espacio o actividad, está obligados a disponer de unas determinadas medidas de seguridad privada, y el titular no las adopta, habiéndose sido requerido para ello, queda inmerso en la presente Ley de Seguridad Ciudadana.

Además, las leyes de Infraestructuras Críticas y Seguridad Nacional, pretenden preservar los servicios esenciales de ataques de agentes externos que pretendan subvertir la normalidad y convivencia

ciudadana, por lo que las infracciones contra las normativas anteriores, quedan bajo la autoridad competente del Ministro del Interior, Secretario de Estado de Seguridad o Delegado del Gobierno, según la importancia de la infracción cometida y de la sanción que le corresponda.

En lo relativo a sanciones, se dividen en “muy graves”, “graves” y “leves”. En el párrafo segundo del artículo 35 se señala que serán autores de una infracción grave: la *omisión, insuficiencia, o falta de eficacia de las medidas de seguridad o precauciones que resulten obligatorias, siempre que en tales actuaciones se causen perjuicios muy graves*. Es decir que un “Operador Crítico”, podría ser sancionado, desde luego siempre que se produzca un hecho contra sus instalaciones, con grave perjuicio para la comunidad a la que debe servir y se demuestre que ha omitido las medidas de seguridad exigibles en la correspondiente Ley, en este caso las de Infraestructuras Críticas y Seguridad Nacional.

Se omite el análisis de las faltas “graves” y “leves”, dado que la relación de las infracciones, se encuentra en la misma línea que las “muy graves”, aunque causantes de menor perjuicio a la comunidad.

Con respecto a la cuantía de la sanción, teniendo en cuenta que, para las infraestructuras críticas y servicios esenciales, casi siempre se incluiría en la relación de

infracciones muy graves, conllevaría una multa de 30.001 a 600.000 euros (artículo 39).

En el supuesto que el acto vandálico o terrorista, cometido en la instalación crítica o servicio esencial, afecte gravemente a terceros, el titular de la instalación y/o servicio a reponer a su situación original los daños que hay podido causar. Por ejemplo, si se comete un acto terrorista en una instalación de agua y se provoca una inundación, siempre que la instalación no disponga de las medidas de seguridad que le correspondan, podría ser obligado a pagar los daños causados (artículo 42).

6.2.2.LEY DE SEGURIDAD PRIVADA Y SU FUTURO REGLAMENTO [16]

En el preámbulo de la Ley ya advierte de infracciones y sanciones:

En el título VI se da solución a algunas de las principales carencias de la anterior legislación referidas al régimen sancionador. Así, se contemplan con la debida separación las infracciones que pueden ser cometidas por las entidades, el personal o los usuarios de seguridad privada, incluyendo junto a estos últimos, a los centros de formación en la materia.

[16] Se dispone de un borrador de reglamento, en el cual se tipifican las sanciones, refiriéndose en múltiples ocasiones a infraestructuras críticas o a operadores estratégicos, a la postre "servicios esenciales" para el mantenimiento de la normalidad ciudadana.

Una instalación crítica o un servicio esencial son "usuarios de seguridad privada".

El artículo 12, *"Competencias de la Administración General del Estado y de las comunidades autónomas"* de la Ley 5/2014, de 4 de abril de 2014, de Seguridad Privada, relaciona entre las mismas, en su apartado 1, subapartados:

i. La determinación reglamentaria de los establecimientos obligados a disponer de medidas de seguridad privada, así como la fijación del tipo y alcance de las medidas obligatorias que ha de cumplir cada tipo de establecimiento.

j. La autorización, inspección y sanción de los establecimientos e instalaciones industriales, comerciales y de servicios que estén obligados a adoptar medidas de seguridad, cuando el ejercicio de esas facultades no sea competencia de las comunidades autónomas.

A falta de la aprobación reglamentaria, uno de los puntos más conflictivos es la relación de los "sujetos obligados" a disponer de seguridad privada, encontrándose entre ellos las empresas e instituciones declaradas "operador crítico-infraestructura crítica" y las consideradas como "servicios esenciales", encontrándose afectadas las primeras por la Ley de Infraestructuras Críticas y los segundos por la de Seguridad Nacional.

De esta forma se paliaría la grave omisión de no recoger un título sobre infracciones y sanciones en las dos anteriores leyes.

No obstante, la propia Ley adelanta en su:

Artículo 51. Adopción de medidas.

1. *Las personas físicas o jurídicas, públicas o privadas, podrán dotarse de medidas de seguridad privada dirigidas a la protección de personas y bienes y al aseguramiento del normal desarrollo de sus actividades personales o empresariales.*
2. *Reglamentariamente, con la finalidad de prevenir la comisión de actos delictivos contra ellos o por generar riesgos directos para terceros o ser especialmente vulnerables, se determinarán los establecimientos e instalaciones industriales, comerciales y de servicios y los eventos que resulten obligados a adoptar medidas de seguridad, así como el tipo y características de las que deban implantar en cada caso.*
7. *Los titulares de los establecimientos, instalaciones serán responsables de la adopción de las medidas de seguridad que resulten obligatorias en cada caso.*

Los operadores críticos quedan inmersos en los apartados 2 y 7, ya que la propia Ley 8/2011 les ordena

disponer de un Plan de Seguridad del Operador (PSO) para el conjunto de la actividad que realizan y Planes de Protección Específicos (PPE) para cada una de las instalaciones declaradas críticas. Por ejemplo, una empresa de agua, declarada “Instalación Crítica”, debe disponer de un PSO para el conjunto y de los correspondientes PPE para las críticas, como pueden ser las Estaciones de Tratamiento de Agua Potable (ETAPs.), así como otras que se consideren. Aparte de los PPE, cada una de las instalaciones de dicha empresa, deben disponer de sus planes de seguridad y de autoprotección.

Con respecto a los operadores de servicios esenciales, aspecto mucho más amplio que el de infraestructuras críticas, tienen la opción de acogerse de forma voluntaria al primer apartado.

Con respecto a la regulación de las infracciones, en esta ley hay que trasladarse al artículo 59, relativo a los “usuarios de seguridad”, es decir la empresa de abastecimiento y saneamiento de agua:

f) La falta de adopción o instalación de las medidas de seguridad que resulten obligatorias.

Como en el caso de la seguridad ciudadana, recogemos únicamente las infracciones “muy graves”.

Por su parte el artículo 63 establece la cuantía de las sanciones a los usuarios de seguridad privada, volviendo a insistir en las empresas de agua:

Las autoridades competentes podrán imponer, por la comisión de las infracciones tipificadas en el artículo 59, las siguientes sanciones:

a) Multa de 20.001 a 100.000 euros

No pudiéndosele aplicar a un servicio esencial, como es el abastecimiento y saneamiento de agua, el apartado c), es decir la suspensión de la actividad.

Aspecto importante y que significaría una "multa a la reputación y/o política", es la publicidad de la sanción:

Artículo 71. Publicidad de las sanciones.
Las sanciones, así como los nombres, apellidos, denominación o razón social de las personas físicas o jurídicas responsables de la comisión de infracciones muy graves, cuando hayan adquirido firmeza en vía administrativa, podrán ser hechas públicas, en virtud de acuerdo de la autoridad competente para su imposición, siempre que concurra riesgo para la seguridad de los usuarios o ciudadanos, en infracciones de naturaleza análoga o acreditada intencionalidad.

Estando claro que la infracción en seguridad de una empresa de agua afecta totalmente a la seguridad de los ciudadanos a los que se presta el servicio esencial. Las empresas públicas de agua, la inmensa mayoría, se

rigen por criterios políticos de representatividad, por lo que, al darle publicidad a la sanción, saldría perjudicada la opción política que en ese momento ostenta la presidente del consejo de administración, representante del “titular de la actividad”.

6.2.3 LEY 17/2015, DE 9 DE JULIO, DEL SISTEMA NACIONAL DE PROTECCIÓN CIVIL

Al centrar este trabajo en las empresas de agua, aplicaremos los preceptos a la misma, aunque son perfectamente extrapolables a otras actividades que pueden generar riesgos.

En primer lugar, en una de las disposiciones adicionales de esta Ley establece:

Disposición adicional segunda Sistemas de Seguridad Nacional, Defensa Nacional e Infraestructuras Críticas y los derivados de tratados internacionales.
Lo dispuesto en esta ley se entiende sin perjuicio de lo que establezca la normativa vigente para los sistemas de Seguridad Nacional, Defensa Nacional e Infraestructuras Críticas y los derivados de tratados internacionales suscritos por España.

En este sentido debe entenderse que en todo lo no regulado por las normativas anteriores, quedará sujeta su inobservancia a la de Protección Civil.

El artículo 2.7 define “servicio esencial”, siendo todos ellos los afectados por las leyes de infraestructuras críticas y seguridad nacional:

7. *Servicios esenciales. Servicios necesarios para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las instituciones del Estado y las Administraciones Públicas.*

En el artículo 3.3 se expresa la participación de las “personas jurídicas” (empresas de abastecimiento y saneamiento de agua) en el Sistema Nacional de Protección Civil, encontrándose entre esta participación el “deber de colaborar a informar a los ciudadanos”, tal como se recoge en al artículo 7.bis.7:

7. *Los titulares de centros, establecimientos y dependencias, en los que se realicen actividades previstas en el artículo 9.2.b) que puedan originar emergencias, deberán informar con regularidad suficiente a los ciudadanos potencialmente afectados acerca de los riesgos y las medidas de prevención adoptadas, y estarán obligados a:* … en definitiva informar.

El servicio esencial del agua es una “actividad” y un conjunto de instalaciones, en las cuales se pueden materializar unos riesgos para la población, unos provocados por la acción del hombre, como terrorismo, vandalismo o sabotaje y otros por causas naturales. Una

empresa de agua se compone de un conjunto de obras hidráulicas [17], las cuales veremos con posterioridad al analizar el texto refundido de la Ley de Aguas, pero en las cuales pueden producirse contaminación, inundación, corte del suministro, sustancias peligrosas, etc., estando en consecuencia la empresa de agua, obligada a informar a la población circundante de estos riesgos que pueden afectarles, incidiendo además en las medidas de protección que se han impuesto para impedirlos, paliarlos o reducirlos, pero que en caso de que se materialicen, deben disponer de los medios y medidas de detección y de los medios, medidas y procedimientos de aviso a la población. En definitiva, deben disponer de un Plan de Seguridad del Operador, denominación del Plan de Autoprotección de la actividad "gestión del agua".

[17] *A los efectos de esta Ley (de Aguas), se entiende por obra hidráulica la construcción de bienes que tengan naturaleza inmueble destinada a la captación, extracción, desalación, almacenamiento, regulación, conducción, control y aprovechamiento de las aguas, así como el saneamiento, depuración, tratamiento y reutilización de las aprovechadas y las que tengan como objeto la recarga artificial de acuíferos, la actuación sobre cauces, corrección del régimen de corrientes y la protección frente avenidas, tales como presas, embalses, canales de acequias, azudes, conducciones, y depósitos de abastecimiento a poblaciones, instalaciones de desalación, captación y bombeo, alcantarillado, colectores de aguas pluviales y residuales, instalaciones de saneamiento, depuración y tratamiento, estaciones de aforo, piezómetros, redes de control de calidad, diques y obras de encauzamiento y defensa contra avenidas, así como aquellas actuaciones necesarias para la protección del dominio público hidráulico (artículo 122).*

Por su parte el artículo 7, ter.2, expresa las obligaciones de los titulares de las actividades que pueden generar riesgos:

Los titulares de los centros, establecimientos y dependencias, públicos o privados, que generen riesgo de emergencia, estarán obligados a adoptar las medidas de autoprotección previstas en esta ley, en los términos recogidos en la misma y en la normativa de desarrollo.

Cuando analicemos la Norma Básica de Autoprotección, veremos que las actividades que pueden generar riesgos están obligadas a disponer de los correspondientes planes de autoprotección, con estudios, medios y disposiciones regulados en una serie de capítulos, aunque en caso de "sectores específicos", se atendrán a su propia normativa en materia de autoprotección y desde luego una empresa de agua, declarada infraestructura crítica, tiene para autoprotección y proteger a la población a la que presta servicio, el Plan de Seguridad del Operador (PSO) y los Planes de Protección Específico (PPE)

El artículo 7.bis.7 hace mención al 9.2.b) de la misma Ley, en la cual se expresa:

Los catálogos oficiales de actividades que puedan originar una emergencia de protección civil, incluyendo información sobre los centros, establecimientos y

dependencias en que aquéllas se realicen, en los términos que reglamentariamente se establezcan.

Trataremos este catálogo de actividades en la Norma Básica de Autoprotección, pero no debemos olvidar que el catálogo genérico de infraestructuras críticas fue relacionado ampliamente por una directiva[18], una comunicación [19] y un "libro verde" [20] de la Unión Europea, abarcando los siguientes sectores estratégicos:

1. Centrales y redes de energía
2. Tecnologías de las comunicaciones y la información
3. **Finanzas**
4. Salud
5. Alimentación
6. Agua (por ejemplo, embalses almacenamiento, tratamiento, redes).
7. Transporte
8. Producción, almacenamiento y transporte de mercancías peligrosas
9. Estado (por ejemplo, servicios críticos, instalaciones, redes de información, activos, sitios y monumentos principales).

Tenemos pues que el agua y por tanto las empresas que la gestionan, está considerado dentro del concepto y

[18] DIRECTIVA 2008/114/CE DEL CONSEJO, de 8 de diciembre de 2008.
[19] COM (2004) 702 final de 20.10.2004
[20] COM (2005) 576 final, de 17.11.2005.

grupo de “infraestructuras críticas”, así como “servicio esencial”, por manifestación explícita en la Ley de Seguridad Nacional.

En el artículo 45 se recogen las infracciones, declarando como “muy grave”, la ya tipificada en el artículo 7.bis.7:

c) *El incumplimiento de los deberes previstos en el artículo 7 bis.7 de esta Ley, cuando suponga una especial peligrosidad o trascendencia para la seguridad de las personas o los bienes.*

Podrían ser declaradas “graves” e incluso “leves”, la misma infracción, aunque son gran trascendencia para la población a la que presta servicio.

La sanción que podría conllevar el incumplimiento de las medidas de protección adecuadas, siendo requerido para ellos, al ser declarado “Operador Crítico una Empresa de Agua”, según el artículo 46 de la misma ley, oscila entre 30.001 y 600.000 euros.

Entidad de Crédito

Independientemente del glosario de términos y definiciones, en su Anexo II, se relacionan los “Sectores” y al relacionar el de la Banca, señala: “Entidades de crédito, tal como se definen en el artículo 4, punto 1, del Reglamento (UE) nº. 575/2013 del Parlamento Europeo y del Consejo”, en el cual se indica: ***«Entidad de crédito»****: una empresa cuya actividad consista en recibir del*

público depósitos u otros fondos reembolsables y en conceder créditos por cuenta propia.

6.2.4. REAL DECRETO-LEY 12/2018, DE 7 DE SEPTIEMBRE, DE SEGURIDAD DE LAS REDES Y SISTEMAS DE INFORMACIÓN

En agosto de 2018 terminaba el plazo para la transposición de la Directiva UE a la normativa legal española, pero por circunstancias que se desconocen se ha sobrepasado el tiempo y ante un apercibimiento de la Comisión Europea, se ha promulgado por carácter de urgencia este Real Decreto, el cual adolece precisamente de la premura en su tramitación, de tal manera que en la Disposición final segunda, indica que se "incorpora la ordenamiento jurídico interno" la Directiva del epígrafe anterior, así como en la Disposición final tercera, prevé un desarrollo reglamentario, sin perjuicio de que se fijen obligaciones específicas a operadores de servicios esenciales, mediante órdenes ministeriales diversas.

En el preámbulo, apartado II es suficientemente explícito al reconocer, recordar y obligar que la norma *"se aplicará a las entidades que presten servicios esenciales para la comunidad y dependan de las redes y sistemas de información para el desarrollo de su actividad"*.

La Banca entra dentro del Sector Financiero, tanto como infraestructura crítica como servicio esencial, aunque evidentemente ello no debe preocuparle, debido a que

desde el inicio de la actividad bancaria a través de redes, se aplican unas estrictas medidas de seguridad en los sistemas y redes de telecomunicaciones, sin que ello quiera significar que no existan ciberataques:

Los bancos siguen siendo vulnerables a los ciberataques. Es una de las conclusiones del último Security Report 2018 de Check Point, proveedor líder especializado en ciberseguridad a nivel mundial. Según este informe, el sector financiero se enfrenta principalmente a tres ***ciberamenazas****: las ofensivas contra la red SWIFT, el malware que ataca a la* ***banca móvil y el robo de información****.* [21]

Un ***ataque cibernético a gran escala*** *ha obligado a varios bancos en Perú a activar sus protocolos de seguridad este viernes, limitando temporalmente varios de sus servicios para proteger las cuentas de los usuarios.* [22]

El RD-Ley recalca la necesidad de tener en cuenta los estándares europeos, así como las recomendaciones que emanen del grupo de cooperación y de la red CSIRT, remitiendo en este sentido al Reglamento (UE) nº 526/2013 del Parlamento Europeo y del Consejo, de

[21] https://intereconomia.com/tecnologia/el-sector-bancario-desprotegido-frente-a-los-nuevos-ciberataques-20180531-1235/ Intereconomía de 31.05.2018. Consultada el 18.10.2018.

[22] https://actualidad.rt.com/actualidad/285564-ciberataque-financiero-mundial-suspenso-bancos-peru RT. 18.08.2018. Consultada el 18.10.2018.

21 de mayo de 2013 , relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) nº 460/2004 Texto pertinente a efectos del EEE, en el cual, aunque es más de utilidad para los estados miembros, recogen una serie de definiciones que deben ser tenidas muy en cuenta, por ejemplo, indica que se entenderá por *«seguridad de las redes y de la información» la capacidad de las redes o los sistemas de información para resistir, con un nivel de confianza dado, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios conexos que dichas redes y sistemas ofrecen o hacen accesibles*. El resto del Reglamento trata de la creación y constitución orgánica y operativa de ENISA, teniendo presente que se puede acceder a ella, a través de los Equipos de Intervención ante incidentes de seguridad informática (CSIRT) y los Equipos de Intervención ante emergencias informáticas (CERT).

Todo lo concerniente al CERT se encuentra en la web https://www.ccn-cert.cni.es/ del Centro Criptológico Nacional, órgano dependiente del Centro Nacional de Inteligencia. El acceso al CSIRT se efectúa a través de la web https://www.csirt.es/index.php/es/

Importante en lo que respecta a la comunicación de incidencias, es que no son sólo los proveedores de

servicios digitales los que deben hacerlo sino también los “operadores de servicios esenciales”, y mucho más importante es el régimen sancionador, recogido no solo en el apartado III del preámbulo, sino también en el artículo 37, en el cual se determina que para infracciones consideradas muy graves, pueden sobrevenir multas de hasta un millón de euros; hasta 500.000 € en caso de infracciones graves; y en las leves hasta 100.000 €, es decir que pueden considerarse bastante elevadas.

La competencia sancionadora recae, según el artículo 41, en el Ministro competente, ejerciéndose la potestad sancionadora de acuerdo con las leyes 39/2015, de 1 de octubre de Procedimiento Administrativo Común de las Administraciones Públicas y 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

6.3 CONCLUSIÓN A ESTE APARTADO DE LA SEGURIDAD DE SISTEMAS Y REDES

Las leyes de Infraestructuras Críticas y Seguridad Nacional, adolecían de ausencia de régimen sancionador, aunque podía aplicarse con carácter subsidiario las leyes de Seguridad Ciudadana y Seguridad Privada, pero con la nueva Directiva y el nuevo Real Decreto-Ley se obliga, mediante coacción sancionadora al cumplimiento de los operadores de infraestructuras críticas y de servicios esenciales.

7. PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA

7.1 RESOLUCIÓN DE 8 DE SEPTIEMBRE DE 2015, DE LA SECRETARÍA DE ESTADO DE SEGURIDAD, POR LA QUE SE APRUEBAN LOS NUEVOS CONTENIDOS MÍNIMOS DE LOS PLANES DE SEGURIDAD DEL OPERADOR Y DE LOS PLANES DE PROTECCIÓN ESPECÍFICOS

En los Anexo I y II de la Resolución se recogen los contenidos mínimos del Plan de Seguridad del Operador y del Plan de Protección Específico, especificándose en sus apartados 1.5 la Protección y Gestión de la Información y Documentación, debiéndose de tener en cuenta que esta gestión de la información clasificada, no debe entenderse exclusiva para los planes operativos, sino para cualquier comunicación que se efectúe con terceros e incluso dentro de la entidad financiera en relación con información sensible, el cual indica los siguiente:

La información es un valor estratégico para cualquier organización, siendo ésta de carácter sensible, por lo que en este sentido, el operador debe definir sus procedimientos de gestión y tratamiento, así como los estándares de seguridad precisos para prestar una adecuada y eficaz protección de esa información, independientemente del formato en el que ésta se encuentre.

Además, los operadores designados como críticos, deberán tratar los documentos que se deriven de la aplicación de la Ley 8/2011 y su desarrollo normativo a través del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, según el grado de clasificación que se derive de las citadas normas.

En virtud de la disposición adicional segunda de la ley 08/2011, la clasificación del PSO (PPE) constará de forma expresa en el instrumento de su aprobación. A tal fin, el tratamiento de los PSO (PPE) deberá estar regido conforme a las orientaciones publicadas por la ***Autoridad Nacional para la Protección de la Información Clasificada*** *del Centro Nacional de Inteligencia en lo que se refiere al manejo y custodia de información clasificada con grado de* ***Difusión Limitada****.*

Las orientaciones de referencia se encuentran recogidas en los siguientes documentos:

Seguridad documental.

OR-ASIP-04-01.04 – Orientaciones para el Manejo de Información Clasificada con Grado de Difusión Limitada.

Seguridad en el Personal.

OR-ASIP-04-02.02 – Instrucción de Seguridad del Personal para acceso a Información Clasificada.

Seguridad Física.

OR-ASIP-01-01.03 – Orientaciones para el Plan de Protección de una Zona de Acceso Restringido.

OR-ASIP-01-02.03–Orientaciones para la Constitución de Zonas de Acceso Restringido.

Seguridad de los Sistemas de Información y Comunicaciones.
OR-ASIP-03-01.04 – Orientaciones para la Acreditación de Sistemas de Información y Comunicaciones para el manejo de Información Clasificada.

7.1.1 CONSIDERACIONES GENERALES SOBRE INFORMACIÓN CLASIFICADA

A tal efecto es conveniente desarrollar estas orientaciones, clarificando su manejo por los operadores críticos del sector financiero, así como el resto de los operadores de este servicio esencial.

Una apreciación importante se debe de efectuar, en el sentido que las normas que implican a la información clasificada, no alteran el normal funcionamiento de la entidad, ni le exigen recursos adicionales para llevarla a efecto, sino que los procedimientos son más de organización y de concienciación del personal.

La Ley 11/2002 reguladora del Centro Nacional de Inteligencia, en su artículo 4, encomienda a este organismo la función de *«Velar por el cumplimiento de la normativa relativa a la protección de la información*

clasificada» [23], afectando no solamente a los organismos públicos, sino también a las entidades privadas.

La normativa legislativa española para la protección de la información clasificada nacional está constituida actualmente por la Ley 9/1968, modificada por la Ley 48/78, sobre Secretos Oficiales, y su Decreto de desarrollo 242/1969, manteniendo su vigencia aunque sean preconstitucionales.

Desde hace años se intenta en medio políticos elaborar una nueva ley que, incluso cambiaría de nombre, para designarse como de "Información Clasificada". Parecía hace unos meses que iba a llegarse a un acuerdo entre los grupos PP y PSOE, pero los acontecimientos vividos dan pocas esperanzas al cambio [24].

En el apartado 5 de las Normas se desarrolla la Infraestructura Nacional de Protección de la Información Clasificada, llegando hasta la entidad privada (entidad bancaria o financiera en este caso) que manipula este tipo de información, especificándose:

[23] PRESIDENCIA DE GOBIERNO. Normas de la Autoridad Nacional para la Protección de la Información Clasificada de 15 de diciembre de 2012.

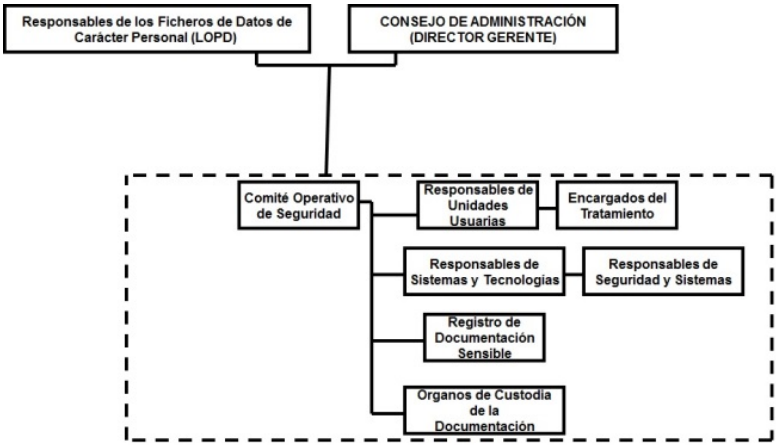
[24] PALACIOS, José Miguel. Grupo GESI. *Hacia la reforma de la Ley de Secretos Oficiales*. http://www.seguridadinternacional.es/?q=es/content/hacia-la-reforma-de-la-ley-de-secretos-oficiales-de-1968 Consultada el 18.10.2018.

El Presidente/Director es el responsable de la adecuada protección de la información clasificada (apartado 5.4.1.), tanto en su custodia como en su manejo. Para asegurar el cumplimiento de sus cometidos en este aspecto, deberá disponer de los medios y recursos adecuados, es decir, de una estructura funcional y orgánica responsable de la ejecución de dicha protección. Esta estructura, desde el punto de vista del más alto nivel de la organización recibe el nombre de servicio de protección de información clasificada.

No hace referencia en las Normas anteriores, de forma específica, a las entidades de servicios esenciales con documentación clasificada, aunque en el artículo 16.3 del RD-Ley expresa que “Los operadores de servicios esenciales designarán y comunicarán a la autoridad competente, en el plazo que reglamentariamente se establezca, la persona, unidad u órgano colegiado responsable de la seguridad de la información, como punto de contacto y de coordinación técnica con aquella”.

Tenemos pues un Responsable de Seguridad y Enlace, por Ley de IC y un Responsable de Seguridad de la Información, por RD-Ley, los cuales en pùra lógica podrían ser el mismo, estableciéndose en el segundo caso la posibilidad de que sea un órgano colegiado, como por ejemplo un “Comité Operativo de Seguridad”

Se puede aducir que estamos creando un servicio nuevo, aunque bien pudiera superponerse al ya creado y obligado por la Ley Orgánica de Protección de Datos, en donde ya existe un Responsable de Seguridad, que tiene bajo su responsabilidad la custodia y tratamiento de los datos de carácter personal de la empresa.



Ejemplo de organización para la protección de datos de carácter personal LOPD

Sin entrar en muchas profundidades, en el reglamento de desarrollo de la Ley Orgánica de Protección de Datos, en su artículo 5, definiciones, se cita a un “Responsable de Seguridad”, como persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables. En el nuevo Reglamento de la Unión Europea 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016

relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), en su artículo 39 habla de un Delegado de Protección de Datos, así como de un Responsable del Tratamiento, aunque al no haberse transpuesto a la normativa española, podría quedar identificado con el "Responsable de Seguridad".

El artículo 36 de la Ley de 5/2014, de 4 de abril, de Seguridad Privada, indica:

Los usuarios de seguridad privada situarán al frente de la seguridad integral de la entidad, empresa o grupo empresarial a un director de seguridad cuando así lo exija la normativa de desarrollo de esta ley por la dimensión de su servicio de seguridad; cuando se acuerde por decisión gubernativa, en atención a las medidas de seguridad y al grado de concentración de riesgo, o cuando lo prevea una disposición especial.

Este "Director de Seguridad", debe tener a su cargo la "seguridad integral" de la entidad, por lo que se presupone que también tiene responsabilidades, al menos operativas, en los sistemas de información y telecomunicaciones.

Tenemos, pues tres o cuatro responsables de seguridad. ¿Deben existir tantos?, ni mucho menos, sino que el Responsable de Seguridad y Enlace, debe al mismo

tiempo ser responsable de la información y jefe del propio departamento de seguridad de la entidad, lo único es que debe disponer del nivel directivo adecuado y tener una formación acorde con los sectores de actividad de la entidad.

7.1.2 GRADOS DE CLASIFICACIÓN EN ESPAÑA

En España, al igual que en los demás países de nuestro entorno y de la OTAN, se emplean, bien que con distintas denominaciones, los mismos niveles de clasificación:

- SECRETO.
- RESERVADO
- CONFIDENCIAL
- DIFUSIÓN LIMITADA

Aparte de los anteriores, recogidos en la normativa sobre información clasificada, debemos de incluir en el mismo servicio los:

- DATOS DE CARÁCTER PERSONAL [25].
- RESTRINGIDA: Información sobre los factores claves del éxito de la empresa [26].

[25] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Persona (texto consolidado de 05.03.2011) y Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (texto consolidado de 08.03.2012)

[26] Relacionado con la propiedad industrial e intelectual de una empresa.

Los grados de Secreto y Reservado se emplean para aquella información que precisa un alto grado de protección por perjudicar gravemente los intereses españoles en el ámbito internacional, mientras que los de Confidencial y Difusión Limitada son más de "consumo interno":

> *2. MATERIAS DE RESERVA INTERNA*
> *2.1. Grado CONFIDENCIAL*
> *La clasificación de **CONFIDENCIAL** se aplicará a la información cuya revelación no autorizada o utilización indebida pueda causar una amenaza o perjuicio para los intereses de España en los siguientes ámbitos:*
> *a) El efectivo desarrollo de las políticas del Estado o el funcionamiento del sector público;*
> *b) negociaciones políticas o comerciales de España frente a otros Estados;*
> *c) los intereses económicos o industriales;*
> *d) funcionamiento de los servicios públicos;*
> *e) dificultar la investigación o facilitar la comisión de delitos, o*
> *f) cualquier otro que pueda causar una amenaza o perjuicio para los intereses de España.*
> *2.2. Grado DIFUSIÓN LIMITADA*
> *La clasificación de **DIFUSIÓN LIMITADA** se aplicará a la información cuya revelación no autorizada o utilización indebida pueda ser contraria a los intereses de España en*

cualquiera de los ámbitos relacionados en los apartados anteriores.

En el caso de las entidades financieras, al ser un servicio esencial, el conocimiento indebido por terceros podría afectar, en un grado limitado, cualquiera de los ámbitos anteriores.

7.2.OR-ASIP-04-01-04 ORIENTACIONES PARA EL MANEJO DE INFORMACIÓN CLASIFICADA EN GRADO DE DIFUSIÓN LIMITADA

Anteriormente hemos visto que se declara “difusión limitada” toda la información contenida en el Plan de Seguridad del Operador (PSO) y en los Planes de Protección Específicos (PPE,s), que es prácticamente toda la de la de la entidad o banco, lo cual aunque parezca excesivo, lo que nos debe llevar a adoptar una actitud de “cautela” [27] con respecto a toda la información de la entidad, debiendo tomar conciencia de ello todas las personas que trabajan en ella.

Esta “cautela” también debe plasmarse en la información pública que se cuelga de internet, en algunos casos excesiva y que lo único que puede ocasionar en perjuicio para la empresa y ningún beneficio.

[27] RAE: Cuidado y reserva de una persona al hablar o actuar para prevenir un daño o un peligro.

Para todas las clasificaciones de seguridad se necesita que la persona se encuentre “acreditada” (habilitación personal de seguridad o HPS) para su manipulación, por la Autoridad Nacional, menos las de difusión limitada, de carácter personal y restringida, por lo que es más exigible el sentido cautelar sobre la información.

En realidad en una entidad financiera, todos los trabajadores tienen acceso a una parte, al menos, de información clasificada como “difusión limitada”, por ello en el apartado 4 de las orientaciones, se indica que con carácter general, las personas que tratan este tipo de información no deben revelar su contenido al público ni a otro personal de la propia empresa, que no esté autorizado para acceder a la misma; que la información solo estará disponible para el personal que “necesite conocerla” por razón de su trabajo; y que todo el personal de la empresa debe estar instruido en el manejo de la información.

Lo expresado en este apartado no es nuevo, ya el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos, define al “usuario” como aquel sujeto autorizado para acceder a datos o recursos, reflejándose esta autorización el en Documento de Seguridad, que también regula la forma de acceso a los recursos informático o no.

Al igual que en protección de datos, la información clasificada como “difusión limitada” se puede ceder a

terceros, debiendo de recogerse en los documentos contractuales la cautela en el trato de dicha información.

De idéntica forma que en la LOPD, es preciso designar a un “Responsable de Seguridad”, preconizándose que sea el Responsable de Seguridad y Enlace, bien que constituyendo como órgano colegiado un “Comité Operativo de Seguridad”, tal como se verá con posterioridad, así como el Consejo de Administración o Junta de Gobierno, debe constituirse para los temas relacionados con la seguridad en “Comité de Seguridad”, porque la seguridad entra dentro de la política de la empresa. De hecho en los contenidos mínimos del PSO, en su apartado 2, se recoge:

Política General de Seguridad del Operador y Marco de Gobierno.

2.1 Política General de Seguridad del Operador Crítico.

2.2 Marco de Gobierno de Seguridad.

2.2.1 Organización de la Seguridad y Comunicación.

2.2.2 Formación y Concienciación.

2.2.3 Modelo de Gestión Aplicado.

2.2.4. Comunicación

En el Documento de Seguridad de datos de carácter personal, se establecen las distintas responsabilidades en el tema del tratamiento de los datos, existiendo unas normas generales, definidas como “Directrices generales de Seguridad”, que deben cumplir todo el personal, pues

bien un documentos similar debe de elaborarse para el personal de la entidad financiera, documento que debe ser conocido y firmado su conocimiento, por el trabajador que acceda por primera vez al puesto de trabajo, debiendo figurar en un lugar visible en la intranet de la empresa, para que pueda ser consultado en caso de duda [28].

En las presentes orientaciones se especifican determinada normas de seguridad física, las cuales son las normales que cualquier ciudadano que tenga un "bien preciado" dispone. Por ejemplo la información clasificada solo debe de manejarse en los lugares designados para ello.

La información clasificada debe ser reconocida como tal y para ello deberá figurar en la cabecera y al pie de cada página, en letras mayúsculas y negritas, DIFUSIÓN LIMITADA. ¿Qué debe hacer una persona que encuentra una documentación con esta clasificación?, por ejemplo una limpiadora, simplemente, sin leerla, entregarla al Responsable de Seguridad o a su superior jerárquico.

Con respecto a la distribución, reproducción y destrucción de la información de difusión limitada, se rige

[28] La Junta de Andalucía dictó la Resolución de 27 de septiembre de 2004, de la Secretaría General para la Administración Pública por la que se establece el manual de comportamiento de los empleados públicos en el uso de los sistemas informáticos y redes de comunicaciones de la Administración de la Junta de Andalucía (BOJA nº. 200, de 13 de octubre de 2004), la cual se encuentra en vigor y se cumple con normalidad.

por criterios lógicos, es decir distribuyéndose a quién debe conocerla y mediante un registro de salida del documento y en caso que así lo disponga el Comité de Seguridad o el Operativo de Seguridad, mediante recibo al que lo se hace cargo de la misma.

Es necesario restringir el fotocopiado, solo cuando sea indispensable.

A contratistas o terceros, se entrega documentación clasificada, debiéndose exigir en los contratos, un acuerdo tácito de confidencialidad con respecto a la documentación. Esto no es solamente para la declarada por difusión limitada, sino también para la restringida y para la de datos de carácter personal. Por ejemplo si una gestoría lleva toda la gestión de nóminas, debe de exigírsele, de acuerdo con el reglamento de desarrollo de la LOPD, la cautela necesaria con respecto al tratamiento de los datos personales, debiéndose emplear el mismo sistema para los otros.

Una documentación de difusión limitada que haya dejado de ser útil para un acto concreto, aunque siga sirviendo para la empresa, debe destruirse, mediante una trituradora de papel del corte apropiado para evitar su reconstrucción.

8. SEGURIDAD PRIVADA

8.1. LEY 5/2014, DE 4 DE ABRIL, DE SEGURIDAD PRIVADA

Plan de Seguridad

Toda organización, desplegada en un territorio, debe disponer de un Plan Director de Seguridad, el cual a su vez se sectoriza, de acuerdo con las características de la misma, hasta llegar al Plan de Seguridad de una instalación, por pequeña que sea.

En ninguna normativa legal se recoge la definición de Plan de Seguridad. Como profesor en el Master Ejecutivo de Dirección de Seguridad Global de la Universidad Camilo José Cela de Madrid, en donde el autor ha impartido, entre otras, la asignatura de "Planes operativos de seguridad", lo define como un:

> *Documento de carácter clasificado que recoge las características del sistema de protección y donde se describen los recursos humanos técnicos y organizativos necesarios para hacer frente a los riesgos.*

Tampoco la legislación es muy explícita al referirse sobre lo que es un plan de seguridad ni quién está obligado a elaborar, redactar e implantar uno de ellos.

Sin embargo hay que hacer constar que para que exista un Plan, que es un documento operativo, tiene que existir previamente un “proyecto técnico de seguridad”, en donde se plasmen los medios técnicos de alarma, detección, prevención y reacción, complementados con los medios humanos necesarios para su activación.

La Ley de Seguridad Privada es poco explícita en el concepto de plan o planes de seguridad, de tal manera que en el artículo 36, al tratar sobre los Directores de Seguridad de las empresas, en este caso el Responsable de Seguridad y Enlace de la entidad financiera, declarada infraestructura crítica, apunta en el apartado c), entre sus funciones:

La planificación, organización y control de las actuaciones precisas para la implantación de las medidas conducentes a prevenir, proteger y reducir la manifestación de riesgos de cualquier naturaleza con medios y medidas precisas, mediante la elaboración y desarrollo de los ***planes de seguridad*** *aplicables*.

En el desarrollo de las medidas de seguridad, indica en el artículo 52, apartado d):

De seguridad organizativa, dirigidas a evitar o poner término a cualquier tipo de amenaza, peligro o ataque deliberado, mediante la disposición, programación o planificación de cometidos, funciones o tareas formalizadas o ejecutadas por personas; tales como la creación, existencia y funcionamiento de ***departamentos***

de seguridad *o la elaboración y aplicación de todo tipo de planes de seguridad, así como cualesquiera otras de similar naturaleza que puedan adoptarse.*

Entrando en el campo de la lógica, dado que si se configuran medidas electrónicas, físicas, informáticas, etc., debe existir un documento coordinador, que no puede ser otro que un Plan de Seguridad.

Se ha resaltado "departamentos de seguridad", aunque es la única referencia en la Ley, dado que los autores consideran de suma importancia la existencia de esta medida de seguridad organizativa.

8.2. SOBRE EL DEPARTAMENTO DE SEGURIDAD

Encontrándose en tramitación parlamentaria la Ley de Seguridad Privada, en un afán de aportar la experiencia de más de diez años en el tema, uno de los autores, Rafael Vidal, escribió algunos artículos publicados en la página www.belt.es [29].

ALEGACIONES AL CAPÍTULO II DEL TÍTULO PRELIMINAR

FUNDAMENTO

Resulta verdaderamente sorprendente que el artículo 12, en donde se relacionan las competencias de la

[29] http://www.belt.es/expertos/HOME2_experto.asp?id=6555

Administración General del Estado no exista ninguna referencia a los "Departamentos de Seguridad", cuando en el actual Reglamento de Seguridad Privada, aprobado por Real Decreto 2364/1994, de 9 de diciembre, en su artículo 112 "Enumeración de los servicios o sistemas y circunstancias determinantes", se expone:

> ***1.*** *Cuando la naturaleza o importancia de la actividad económica que desarrollan las empresas y entidades privadas, la localización de sus instalaciones, la concentración de sus clientes, el volumen de los fondos o valores que manejen, el valor de los bienes muebles u objetos valiosos que posean o cualquier otra causa lo hiciesen necesario, el Secretario de Estado de Interior para supuestos supraprovinciales, o los Gobernadores Civiles, podrán exigir a la empresa o entidad que adopte, conjunta o separadamente, los servicios o sistemas de seguridad siguientes:*
>
> *a)* ***Creación del departamento de seguridad****.*
>
> *b) Establecimiento del servicio de vigilantes de seguridad, con o sin armas a cargo de personal integrado en empresas de seguridad.*
>
> *c) Instalación de dispositivos y sistemas de seguridad y protección.*

d) Conexión de los sistemas de seguridad con centrales de alarmas, ajenas o propias, que deberán ajustarse en su funcionamiento a los establecido en los artículos 46, 48 y 49, y reunir los requisitos que se establecen en el apartado 6.2 del anexo del presente Reglamento; no pudiendo prestar servicios a terceros si las empresas o entidades no están habilitadas como empresas de seguridad.

***2.** En todo caso deberá existir **Departamento de Seguridad** cuando concurran las circunstancias de los párrafos b) y c) del artículo 96.2 de este Reglamento.*

Hoy en día son cada vez más las empresas, instalaciones, actividades, establecimientos, organizaciones, etc., y más desde la aprobación de la normativa sobre Infraestructuras Críticas, que se les va a exigir la disposición, como orgánico (plantilla) de un Departamento de Seguridad, figurando al frente del mismo, un técnico con la titulación de Director de Seguridad (grado universitario a partir de la aprobación de la Ley).

Posteriormente en el artículo 115 se detalla el procedimiento para crear el Departamento de Seguridad a través de diversos organismos administrativos

dependientes del Ministerio del Interior y comunicarlo al Director General de la Policía y al Delegado/Subdelegado del Gobierno. Posteriormente en los artículos 116 y 117 se configura el Departamento de Seguridad y sus cometidos.

Se podría argüir que esas referencias explícitas al Departamento de Seguridad ya se harán en el Reglamento que se apruebe con posterioridad a la ley, pero es que el texto del anteproyecto, relaciona diez competencias, incluidas la de los despachos de detectives privados, centros de formación y otros de menor relevancia e importancia que el Departamento de Seguridad.

¿Nos imaginamos, por poner un ejemplo concreto, que el Departamento de Seguridad que debe tener ENDESA, al igual que cientos y cientos de otras entidades españolas, no está referenciado en la ley y si lo esté una pequeña empresa de veinte o treinta vigilantes?

El artículo 13 del anteproyecto es un "saludo al sol" en este estado de las autonomías, en la cual si una entidad se erradica en una comunidad autónoma tiene que hacer los trámites pertinentes, ¿incluidos o no los del Departamento de Seguridad? en los homónimos del Estado en la misma, con el hándicap que si esa entidad quiere sobrepasar su mercado u su acción a otras comunidades, tiene que volver a efectuar nueva petición, esta vez ante el Ministerio del Interior. Si tenemos en

cuenta que hay varias autonomías uniprovinciales, nos encontraremos con obstáculos administrativos que en teoría se pretenden superar, pero que cada vez dificultan más la vida de la sociedad.

Además, dentro de unos años, nos encontraremos que cada Comunidad Autónoma he legislado y ha establecido pautas de comportamiento y de procedimiento, diferentes a los de otras CC.AA., con lo cual tendremos que adecuar la seguridad privada a cada territorio.

En la actual seguridad privada, la guía para la elaboración y redacción de un plan de seguridad es distinto entre CC.AA., al menos en formato. Ya está ocurriendo en Protección Civil, que tenemos diecisiete sistemas distintos, cuando tendría que ser único.

Si nos vamos al Estatuto de Autonomía de Cataluña, en su artículo 163 se consigna la "seguridad privada" y se plasma el mismo texto, con imperceptibles modificaciones, del anteproyecto:

> ***Corresponde a la Generalitat la ejecución de la legislación del Estado en las siguientes materias:***
>
> *a. La autorización de las empresas de seguridad privada que tengan su domicilio social en Cataluña y cuyo*

ámbito de actuación esté limitado a su territorio.

b. *La inspección y sanción de las actividades de seguridad privada que se realicen en Cataluña.*

c. *La autorización de los centros de formación del personal de seguridad privada.*

d. *La coordinación de los servicios de seguridad e investigación privadas con la Policía de la Generalitat y las Policías Locales de Cataluña.*

En algunos estatutos de autonomía, por ejemplo el de Andalucía, en su artículo 66, recoge que tiene "competencias exclusivas" en protección civil, lo cual no deje de ser un contrasentido, por no expresar una cuestión de inconstitucionalidad. La normativa estatal es muy clara al respecto, pero estas expresiones dan pie a embrollos jurídicos posteriores, y nos referimos a la autoprotección y seguridad privada, tema que ya se ha hecho mención en las alegaciones al capítulo I. En igual sentido y casi con las mismas palabras se recogen en el artículo 132 del Estatuto catalán.

La realidad es que ya no hay marcha atrás en el estado de las autonomías, lo que complicará la vida de los españoles ahora y aún más en el futuro, pero en lo

concerniente al Departamento de Seguridad y Director de Seguridad, debe mantenerse en el ámbito del Ministerio del Interior.

La Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (IC), establece en su Preámbulo y en su articulado que la dirección y coordinación de la protección de las IC pertenece al Estado a través de la Secretaria de Estado de Seguridad, incluyéndose como "agentes", entre otros a las CC.AA., con claras competencias, pero siempre en beneficio del conjunto del territorio español.

En diferentes artículos recoge como elemento de enlace entre el Sistema de Protección de Infraestructuras Críticas y los Operadores Críticos, un Responsable de Seguridad y Enlace con la titulación de Director de Seguridad.

Desde julio a octubre de 2011 escribí una serie de columnas en www.belt.es, sobre este importante tema, cuyo diagrama general puede verse en la figura:

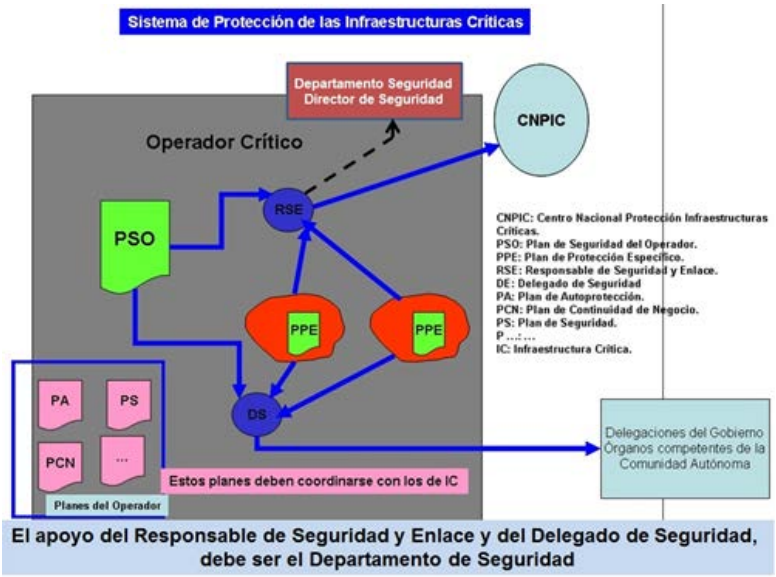
El artículo 13 de la Ley de IC indica que los "operadores críticos", similar en definición a los titulares que necesitan servicios de seguridad privada, designarán a un Responsable de Seguridad y Enlace. Posteriormente en el artículo 16 remacha que "los operadores críticos nombrarán y comunicarán al Ministerio del Interior un Responsable de Seguridad y Enlace con la

Administración en el plazo que reglamentariamente se establezca".Es decir que existe una relación directa en el nombramiento y en el posterior control de este importante cargo, no delegable ni desconcentrada la función en las CC.AA.

PROPUESTA

- *Relacionar, entre las competencias de la Administración General del Estado, como apartado 1 a) "La autorización para la creación de un Departamento de Seguridad en los titulares definidos en el artículo 2 de la presente Ley, así como su inspección y sanción en caso de incumplimiento de sus obligaciones legales y reglamentarias. Esta competencia será exclusiva del Estado".*

De esta forma el Ministerio del Interior dispondrá de unos elementos materiales y procedimentales y unos recursos humanos, los directores de seguridad, que tenderán a una mejor coordinación de la seguridad privada desplegada y repartidas sus responsabilidades entre las CC.AA.



NOTA: [30] *En la presente entrega se analizan los títulos I y II del anteproyecto.*

ALEGACIONES AL TÍTULO I

FUNDAMENTO

Se vuelve a reiterar la "inexistencia" de los departamentos de seguridad para el anteproyecto. El artículo 14 parece muy claro y tendente a que exista una relación fluida entre las seguridades privada y pública, pero lo que no parece tan claro es el procedimiento, concretamente el expresado en el apartado 2, que recoge que "las empresas y el personal de seguridad privada deberán comunicar a las Fuerzas y Cuerpos de Seguridad competentes …", en donde parece existir una

[30] http://www.belt.es/expertos/home2_experto.asp?id=6567

prelación en su relación con las FCS y que podría conllevar a errores de bulto en la seguridad de una instalación.

¿Sería admisible que el jefe de turno de una empresa de seguridad que presta servicios en una instalación que cuenta con departamento de seguridad, se comunicara directamente con las FCS, o lo lógico es que se comunique al departamento y que éste enlace con las FCS? En el reglamento de Seguridad Privada actualmente vigente, que en realidad podría considerarse una norma reglamentaria que desarrolla las leyes Orgánica de Protección de la Seguridad Ciudadana y ordinaría de Seguridad privada, indica lo contrario en sus artículos 66, 95, 96, 97, 98, 116 y 117.

A lo largo de todo el anteproyecto se habla de "empresas", que se refiere a las de seguridad y de "personal de seguridad privada", el cual, según la definición del artículo 2 son las personas físicas que, habiendo obtenido la correspondiente habilitación, desarrollan funciones de seguridad privada, con lo cual el llamado "usuario" de la seguridad no tiene nada que opinar en este tema, ni comunicar nada, lo cual entra en clara contradicción con la ley de Infraestructuras Críticas, en la cual la relación con la seguridad pública se realiza a través de los Responsables de Seguridad y Enlace (Departamento de Seguridad) y de los Delegados de Seguridad, que son orgánicos de los operadores críticos.

El anteproyecto emplea indistintamente los conceptos "empresas", "personal de seguridad privada", "servicios de seguridad privada" y otros, sin llegar a alcanzar al

lector del texto si se está refiriendo a los definidos en el artículo 2. Por ejemplo en el artículo 16.1 se pretende coordinar los servicios de seguridad privada con las Fuerzas y Cuerpos de Seguridad, cuando en buena lógica lo que deben de coordinarse son con los servicios de las FCS.

PROPUESTA

Eliminar la expresión "las empresas y el personal de seguridad privada" y sustituirlo por Seguridad privada, de esta forma el apartado 1 quedaría La especial obligación de colaboración entre la Seguridad privada con las Fuerzas y Cuerpos de Seguridad … El apartado 2 La Seguridad privada deberá comunicar, por sus cauces jerárquicos, o directamente el personal que lo detecte en caso de urgencia, cualesquiera … El 3. Debería quedar Las Fuerzas y Cuerpos de Seguridad podrán facilitar a la Seguridad privada, en el ejercicio de sus funciones, …

ALEGACIONES AL TÍTULO II

FUNDAMENTOS

El propio título ya es de por sí desconcertante, parece como si nada más que existieran para el anteproyecto, las empresas de seguridad privada y los despachos de detectives privados.

Ha parecido olvidar el equipo redactor del anteproyecto que existen miles de departamentos de seguridad en, también miles, empresas españolas no de seguridad.

Puedo indicar con seguridad que son miles, porque a lo largo de muchos años de formación, han pasado por las aulas en donde impartí, junto con un buen número de profesionales/profesores, de Belt Ibérica, S.A. y sucesivamente la Universidad Autónoma de Madrid, Antonio de Nebrija, Europea de Madrid y en la actualidad Camilo José Cela, alrededor de dos mil quinientos alumnos, que tras obtener el diploma acreditativo de haber superado el curso/master, lo homologaron en el ministerio del Interior para obtener el título de "Director de Seguridad".

Es seguro que existen más departamentos de seguridad en España que despachos de detectives privados y sin embargo ni se tiene en cuenta este aserto, con el agravante que más del 95% de la seguridad privada está regida por directores de seguridad a través de sus correspondientes departamentos de seguridad.

En el artículo 19, al relacionar los requisitos generales que tienen que disponer las empresas de seguridad, incide en la protección de las Infraestructuras Críticas, cuando precisamente por la propia Ley 8/2011, son los Responsables de Seguridad y Enlace (Directores de Seguridad/Departamentos de Seguridad) los que tienen, y valga la repetición, la responsabilidad en la seguridad tanto del operador crítico como en las diversas instalaciones del mismo.

Los artículos 20 y 24 del anteproyecto exigen la inscripción registral de las empresas de seguridad y los despachos de detectives privados, sin mencionar para nada a los departamentos de seguridad. Sin embargo en

los artículos 95 y siguientes del Reglamento de Seguridad Privada, aprobado por R.D. 2364/1994, de 9 de diciembre, aunque con múltiples modificaciones, entre ellos los artículos mencionados, exige departamentos de seguridad en empresas y organizaciones por disposición general o decisión gubernativa, y en las que sin estar obligadas legalmente, deseen crear su propio departamento de seguridad, deben comunicarlo a la autoridad gubernativa, es decir, el Reglamento, está reconociendo la existencia de un registro de departamentos de seguridad.

El hecho que se pretenda desarrollar todo lo concerniente a los departamentos de seguridad a la vía reglamentaria, no deja de sorprender, cuando como se ha expuesto anteriormente el 95% de la seguridad privada recae sobre ellos, siendo las empresas de seguridad privada meros ejecutores de sus órdenes y consignas, en lo que respecta a su propia empresa usuaria de seguridad privada.

PROPUESTA

Denominar al título II: Departamentos de seguridad, empresas de seguridad privada y despachos de detectives privados.

Dedicar el Capítulo I a los Departamentos de seguridad, el II a las empresas de seguridad y el III a los despachos de detectives privados.

En total Rafael Vidal escribió ocho columnas con distintas alegaciones y proponiendo mejoras. Algún

grupo de la Comisión del Congreso que se ocupaba de la tramitación, propuso su presencia, como técnico en la materia, pero el comité de expertos que se constituyó se formó con profesionales de “empresas de seguridad privada” y no de “usuarios de la seguridad”, resultando con ello, una ley con grandes lagunas, agravadas por la inexistencia de un reglamento que la desarrolle, aunque han pasado cuatro años largos desde su promulgación.

8.3. MISIONES Y FUNCIONES DEL DEPART6AMENTO Y DEL DIRECTOR DE SEGURIDAD

Las competencias del Director de Seguridad quedan recogidas en las diversas disposiciones relacionadas en el apartado de referencias legales. Al objeto de una mayor claridad, enumeraremos los cometidos por bloques legales:

Normativa de Seguridad Privada

En esta relación de responsabilidades, se van exponer las que recoge la Ley 5/2014 y las del Reglamento aún en vigor.

Veamos lo que se indica en el artículo 36 de la Ley:

1. En relación con la empresa o entidad en la que presten sus servicios, corresponde a los directores de seguridad el ejercicio de las siguientes funciones:

a) La organización, dirección, inspección y administración de los servicios y recursos de seguridad privada disponibles.

b) La identificación, análisis y evaluación de situaciones de riesgo que puedan afectar a la vida e integridad de las personas y al patrimonio.

c) La planificación, organización y control de las actuaciones precisas para la implantación de las medidas conducentes a prevenir, proteger y reducir la manifestación de riesgos de cualquier naturaleza con medios y medidas precisas, mediante la elaboración y desarrollo de los planes de seguridad aplicables.

d) El control del funcionamiento y mantenimiento de los sistemas de seguridad privada.

e) La validación provisional, hasta la comprobación, en su caso, por parte de la Administración, de las medidas de seguridad en lo referente a su adecuación a la normativa de seguridad privada.

f) La comprobación de que los sistemas de seguridad privada instalados y las empresas de seguridad privada contratadas, cumplen con las exigencias de homologación de los organismos competentes.

g) La comunicación a las Fuerzas y Cuerpos de Seguridad competentes de las circunstancias o informaciones relevantes para la seguridad ciudadana,

así como de los hechos delictivos de los que tenga conocimiento en el ejercicio de sus funciones.

h) La interlocución y enlace con la Administración, especialmente con las Fuerzas y Cuerpos de Seguridad, respecto de la función de seguridad integral de la entidad, empresa o grupo empresarial que les tenga contratados, en relación con el cumplimiento normativo sobre gestión de todo tipo de riesgos.

i) Las comprobaciones de los aspectos necesarios sobre el personal que, por el ejercicio de las funciones encomendadas, precise acceder a áreas o informaciones, para garantizar la protección efectiva de su entidad, empresa o grupo empresarial.

2. Los usuarios de seguridad privada situarán al frente de la seguridad integral de la entidad, empresa o grupo empresarial a un director de seguridad cuando así lo exija la normativa de desarrollo de esta ley por la dimensión de su servicio de seguridad; cuando se acuerde por decisión gubernativa, en atención a las medidas de seguridad y al grado de concentración de riesgo, o cuando lo prevea una disposición especial.

Este apartado 2. es bastante explícito, debido a que la normativa de Infraestructuras Críticas expresa que en cada Empresa/Operador Crítico existirá en plantilla un Director de Seguridad.

Considerado la existencia de un director y de un Departamento de Seguridad en la empresa, veamos ahora lo que se recoge en el actual reglamento.

El artículo 116 especifica cuáles deben ser sus cometidos:

> *El departamento de seguridad obligatoriamente establecido, único para cada entidad, empresa o grupo empresarial y con competencia en todo el ámbito geográfico en que éstos actúen, comprenderá la administración y organización de los servicios de seguridad de la empresa o grupo, incluso, en su caso, del transporte y custodia de efectos y valores, correspondiéndole la dirección de los vigilantes de seguridad o guardas particulares del campo, el control del funcionamiento de las instalaciones de sistemas físicos y electrónicos, así como del mantenimiento de éstos y la gestión de las informaciones que generen.*

Tal como se observa, el departamento de seguridad, dirigido por un director de seguridad [31], son órganos de la entidad, al igual que lo son el departamento financiero

[31]La denominación de director de seguridad como persona al frente de un departamento no quiere expresar que tenga el rango administrativo de Director, dado que el "Director de Seguridad" es un título expedido por una Universidad y homologado por el Ministerio del Interior para ejercer como tal.

o cualquier otro, cuyas misiones generales se recogen en el presente artículo 116:

a) *Administración del departamento.*

b) *Organización de los servicios de seguridad.*

c) *Organización del servicio de transporte y custodia de efectos y valores.*

d) *Dirección de los vigilantes de seguridad: asignación de misiones y cometidos a cada puesto de vigilante.*

e) *Control de las instalaciones de los sistemas físicos y electrónicos: generalmente se efectúa a través de una central de alarma, servida por vigilantes de seguridad (empresa externa de seguridad), pero que informan directamente al departamento de seguridad.*

f) *Mantenimiento de las instalaciones y medios técnicos: contratando a una empresa de mantenimiento de sistemas de seguridad.*

g) *Gestión de la información que se genere: las incidencias en el servicio y la coordinación con las fuerzas y cuerpos de seguridad es competencia del departamento de seguridad.*

Aparte de los anteriores debe asumir otros cometidos recogidos en los artículos 66, 95, 96, 97, 98 y 117 del Reglamento:

- Análisis de riesgos (art. 95 RSP)
- Planificación y programación de los servicios de seguridad (art. 95 RSP)
- Organización, dirección e inspección del personal y servicios de seguridad privada. (art. 95 RSP)
- Propuesta y supervisión de los sistemas de seguridad (art. 95 RSP)
- Coordinación de servicios de seguridad en casos de emergencia (art. 95 RSP)
- Asegurar la colaboración de los servicios de seguridad con las FF y CC de Seguridad (art. 95 RSP)
- Velar por la observancia de la regulación de seguridad (art. 95 RSP)
- Mandar sobre los servicios de seguridad (art. 96.2 RSP)
- Comunicar a las Fuerzas y Cuerpos de Seguridad, tan pronto como sea posible, cualesquiera circunstancias o informaciones relevantes para la prevención, el mantenimiento o restablecimiento

de la seguridad ciudadana, así como todo hecho delictivo de que tuviesen conocimiento en el ejercicio de sus funciones (art. 66 RSP)

— Comparecer a las reuniones informativas o de coordinación convocadas por las autoridades policiales (art. 97 RSP)

— Proponer o adoptar medidas oportunas para subsanar las deficiencias de los servicios o sistemas de seguridad (art. 98 RSP).

— Organizar y dirigir el departamento de seguridad (art. 117 RSP).

Normativa sobre Infraestructuras Críticas

El artículo 13 del Reglamento de protección de las infraestructuras críticas, aprobado por Real Decreto 704/2011, de 20 de mayo, detalla las responsabilidades que adquieren los "Operadores Críticos". Estos operadores son designados como tales mediante catálogo elaborado por el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), el cual ha iniciado su labor hace relativamente poco tiempo, por lo que la relación de entidades, empresas y organizaciones, declaradas "críticas" son relativamente pocas, aumentándose las mismas con el paso de los años.

Ello no es óbice para que las entidades que, por razón de su actividad, puedan ser declaradas "críticas", inicien

las acciones necesarias para asumir las responsabilidades fijadas en la normativa de forma inmediata.

Las misiones/funciones que tiene que llevar a cabo un Operador Crítico son las que recogidas en el artículo 13, desarrollando las mismas a través del Responsable de Seguridad y Enlace, el cual tiene que disponer la titulación de Director de Seguridad homologada por el Ministerio del Interior, según el artículo 16 de la Ley 8/2011, de 28 de abril.

Por su parte el artículo 34.2 del Reglamento expresa: *El Responsable de Seguridad y Enlace representará al operador crítico ante la Secretaría de Estado de Seguridad en todas las materias relativas a la seguridad de sus infraestructuras y los diferentes planes especificados en este reglamento, canalizando, en su caso, las necesidades operativas e informativas que surjan al respecto*.

Por tanto, el Director de Seguridad como Responsable de Seguridad y Enlace y asesor principal en seguridad de Operador Crítico (empresa de agua), tendría las siguientes funciones.

a) Prestar su colaboración técnica a la Secretaría de Estado de Seguridad, a través del CNPIC, en la valoración de las infraestructuras propias que se aporten al Catálogo. Por ello, deberán actualizar los datos disponibles con una periodicidad anual

y, en todo caso, a requerimiento o previa validación del CNPIC.

b) Colaborar, en su caso, con el Grupo de Trabajo, en la elaboración de los Planes Estratégicos Sectoriales y en la realización de los análisis de riesgos sobre los sectores estratégicos donde se encuentren incluidos.

c) Elaborar el Plan de Seguridad del Operador y proceder a su actualización periódicamente o cuando las circunstancias así lo exijan, conforme a lo que establece el Capítulo III, Título III del presente reglamento.

d) Elaborar un Plan de Protección Específico por cada una de las infraestructuras consideradas como críticas en el Catálogo así como proceder a su actualización periódicamente o cuando las circunstancias así lo exijan, conforme a lo establecido en el Capítulo IV, Título III del presente reglamento.

e) Designar a un Responsable de Seguridad y Enlace, en virtud de lo dispuesto en el artículo 34 del presente reglamento (sería responsabilidad del Operador Crítico).

f) Designar a un Delegado de Seguridad por cada una de sus infraestructuras consideradas Críticas o Críticas Europeas por la Secretaría de Estado

de Seguridad, comunicando su designación a los órganos correspondientes en virtud de lo dispuesto en el artículo 35 del presente reglamento (Sería responsabilidad del Operador Crítico, asesorado por el Director de Seguridad).

g) Facilitar las inspecciones que las autoridades competentes lleven a cabo para verificar el cumplimiento de la normativa sectorial, en el marco de lo establecido en el Título III de este reglamento.

La SEGURIDAD no debe ser impuesta por imperativo legal, dado que la seguridad genera beneficios al disminuir pérdidas; por ello siempre es aconsejable que las organizaciones y entidades asuman de forma voluntaria algunos de los requisitos exigidos como tales a las infraestructuras críticas, principalmente en los Planes de Seguridad del Operador y Planes de Protección Específico.

Un aspecto muy importante y que se encuentra presente en las infraestructuras críticas es el relacionado con los sistemas de información tal, como se ha señalado con anterioridad.

En el preámbulo de la Ley se recoge:

> *Estas infraestructuras críticas dependen cada vez más de las tecnologías de la información, tanto para su gestión como para su*

> *vinculación con otros sistemas, para lo cual se basan, principalmente, en* ***medios de información y de comunicación de carácter público y abierto****.*

En el mismo preámbulo se hace referencia a las acciones terroristas, a las cuales no puede estar ajena la empresa de aguas, dado que sus instalaciones se encuentran desplegadas en un extenso territorio, poblado o no y con personas de distinto nivel educacional:

> *Las actuaciones necesarias para optimizar la seguridad de las infraestructuras se enmarcan principalmente en el ámbito de la protección contra agresiones deliberadas y, muy especialmente, contra ataques terroristas, resultando por ello lideradas por el Ministerio del Interior.*

El vandalismo es una lacra social, haciéndose daño a instalaciones con el único fin de hacerlo, sin que sea consecuencia de una reivindicación. A este vandalismo se une el robo/hurto, existiendo bandas que se llevan todo lo que de aprovechable puede haber en una pequeña instalación que se encuentra aparentemente abandonada. Se ha podido comprobar que en casetas, derivaciones, pozos, etc., se han llevado las puertas, las ventanas, motores, etc., lo que refuerza la necesidad de una adecuada planificación de la seguridad, que

solamente puede hacerse a través del correspondiente director de seguridad y su departamento.

Normativa sobre Autoprotección

Las distintas instalaciones de la empresa de agua se regulan por la Norma Básica de Autoprotección (NBA), aprobada por Real Decreto 393/2007.

Se suele identificar la responsabilidad en autoprotección con la correspondiente a riesgos laborales, sin embargo, ambas normativas, aunque coincidentes en algunos aspectos, tienen leyes generadoras de distinta procedencia, siendo por otra parte el ámbito de la autoprotección mucho más amplio que el de riesgos laborales.

La propia “Exposición de motivos” del Real Decreto 393/2007, así lo aclara:

> *Es evidente que la protección de los trabajadores de una determinada dependencia o establecimiento, especialmente en cuanto se refiere a riesgos catastróficos, implica, las más de las veces, la protección simultánea de otras personas presentes en el establecimiento, con lo que, en tales casos, se estará atendiendo simultáneamente a la seguridad de los trabajadores y a la del público en general. En otras ocasiones, sin embargo, el ámbito de protección abarcado por la Ley 31/1995, de 8*

de noviembre, no será coincidente con el que debe corresponder a la autoprotección a que se refiere la Ley 2/1985, de 21 de enero. Así, por ejemplo, determinados riesgos, los estrictamente laborales, lo serán únicamente para los trabajadores de un determinado establecimiento, sin afectar al resto de las personas presentes en el mismo. Por el contrario, otros riesgos, derivados del desarrollo de una determinada actividad, lo son fundamentalmente para un colectivo de ciudadanos, a veces enormemente extenso, que por, diferentes razones, se encuentran expuestos. En ciertos casos, la generación del riesgo puede no derivarse incluso de una actividad económica o vinculada a una actividad propiamente laboral.

En consecuencia, la actividad protectora de la seguridad y la salud, derivada de la Ley 31/1995, de 8 de noviembre, teniendo un campo común con la autoprotección a que se refiere la Ley 2/1985, de 21 de enero, no cubre los requerimientos de prevención o reducción de riesgos para la población de los que esta última se ocupa.

…

La autoprotección ha sido asimismo abordada en las Directrices Básicas de Planificación de Protección Civil y en los Planes Especiales ante riesgos específicos.

Los vigilantes de seguridad junto con los técnicos de mantenimiento, son las piezas fundamentales en los diversos planes de autoprotección, dado que conforman los equipos de intervención y el de apoyo. Los primeros dependen orgánicamente del Jefe de Seguridad de la empresa de seguridad que ha sido contratada, dependiendo a su vez del Director de Seguridad, tal como lo expresa el artículo 71.3. Por ello es totalmente lógico que el Director de Seguridad, que es el "mando natural" sea al mismo tiempo responsable de ejecutar el Plan de Autoprotección que se haya diseñado para cada una de las instalaciones de la empresa de aguas.

La consideración de "mando natural" se recoge en el artículo 71.3 del Reglamento de Seguridad Privada:

3. En la organización de los servicios y en el desempeño de sus funciones, los vigilantes dependerán del jefe de ***seguridad*** *de la empresa de* ***seguridad*** *en la que estuviesen encuadrados. No obstante, dependerán funcionalmente, en su caso, del jefe del*

*departamento de **seguridad** de la empresa o entidad en que presten sus servicios.*

Por todo ello es necesario para la eficacia y eficiencia de la autoprotección que el Director de Seguridad homologado por el Ministerio del Interior, tenga responsabilidades en la misma, bien como Director del Plan de Autoprotección, del Plan de Actuación ante Emergencias, u otra figura de las recogidas en la NBA, siendo además asesor para esta cuestión para la dirección de la empresa.

La Directriz Básica aprobada por el anteriormente citado Real Decreto 393/2007. Indicándose con ello que la autoprotección forma parte del Sistema Nacional de Protección Civil, quedando bajo la tutela del Ministerio del Interior y no de los riesgos laborales, los cuales dependen del Ministerio de Trabajo.

Se cuestionó la competencia de la protección civil, si era exclusiva del Estado o de las Comunidades Autónomas. En este sentido cabe indicar que cuando se promulgó la Ley 2/1985 [32], se produjo un conflicto de constitucionalidad, presentado por el Gobierno Vasco a una ley autonómica que legislaba sobre la misma materia de protección civil.

[32] Esta Ley se encuentra derogada por la Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil, pero los pilares fundamentales permanecen inalterables.

La Sentencia nº 133/1990 de Tribunal Constitucional, Pleno, 19 de Julio de 1990, cuyo ponente fue el magistrado Don Luis López Guerra, sobre el Recurso de Inconstitucionalidad nº 355/1985, es bastante clara al insertar la protección civil dentro del contexto de la seguridad, la cual es competencia exclusiva del Estado:

> *B) De este modo, la Ley parte de la premisa de que las Comunidades Autónomas carecen de competencia sobre la protección civil mientras que la Sentencia indicada reconocía expresamente la competencia de la Comunidad Autónoma del País Vasco. Por consiguiente, la Ley incurre en una clara invasión de competencias. Esto se hace evidente en el apartado II de la Exposición de Motivos de la Ley cuando se dice que la protección civil es un problema de organización que corresponde principalmente al Estado en cuanto competencia para la protección de personas y bienes integrada en la seguridad pública; y que esta competencia tiene como mecanismos de actuación técnicas de planificación y de coordinación a nivel superior y jurídicamente, pues se da respecto de esta materia, «el supuesto del núm. 3 del art. 149 de la Constitución».*

La Seguridad se compone de dos pilares básicos: Privada y Pública, teniendo las dos responsabilidades en

la ejecución de los planes de protección civil y por ende en los de autoprotección, que son parte de los primeros, por lo que no cabe la menor duda que la persona más idónea para responsabilizarse de todo lo concerniente a autoprotección debe ser el Director de Seguridad.

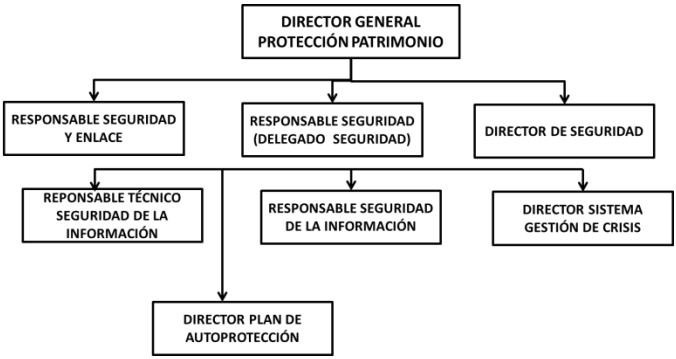
8.4. ORGANIZACIÓN DE LA SEGURIDAD

El Reglamento de Seguridad privada, recoge en su artículo 117, sobre organización del departamento de seguridad:

> *En aquellas entidades y empresas de **seguridad** en las que el departamento de **seguridad** se caracterice por su gran volumen y complejidad, en dicho departamento existirá, bajo la dirección de **seguridad**, a la que corresponderán las funciones del director de **seguridad**, la estructura necesaria con los escalones jerárquicos y territoriales adecuados, al frente de los cuales se encontrarán los delegados correspondientes.*

Por otra parte, existe una tendencia clara en todas las organizaciones occidentales de disponer de la SEGURIDAD (PROTECCIÓN DEL PATRIMONIO), en un organismo único y que se encuentre al máximo nivel jerárquico.

Veamos un organigrama de la SEGURIDAD, en una empresa de Servicio Esencial o de Infraestructura Crítica:



9. CONCLUSIONES

9.1. SERVICIO ESENCIAL E INFRAESTRUCTURA CRÍTICA: DOS CONCEPTOS SIMILARES**.**

El concepto de “servicio esencial” venía recogido en la normativa de la Organización Internacional del Trabajo, transponiéndose a las legislaciones nacionales, con la finalidad de que los servicios mínimos, en caso de huelgas, afectaran lo mínimo imprescindible a la normalidad y convivencia ciudadana.

La amenaza terrorista, principalmente, pero también otra serie de amenazas antrópicas y naturales, aconsejaron a raíz del atentado del 11S contra las Torres Gemelas a tomar una serie de medidas de protección, sobre aquellas infraestructuras, cuya perturbación o anulación, podían llegar a quebrar la voluntad de dirección de un gobiernos sobre los asuntos del Estado. Estas infraestructuras se denominaron críticas.

Posteriormente se amplió algo el concepto y dentro de la Unión Europea se consideró la “seguridad europea”, transpuesta a los estados miembros como “seguridad nacional”, pues bien todos aquellos servicios que pudieran interferir en la preservación de esa seguridad nacional, se denominaron “servicios esenciales”.

Las diferencias entre “infraestructuras críticas” y “servicios esenciales” son en cierto modo semánticas, corrigiéndose en el segundo caso, tanto en la UE como en los estados miembros, por el carácter sancionador contra el que atentare contra un servicio esencial, mientras que un atentado contra una infraestructura crítica, tenía que ser objeto del llamado derecho supletorio: ley de protección de la seguridad ciudadana, ley de protección civil, ley se seguridad privada y otras.

9.2. OPERADORES (TITULAR) “DEBEN” COLABORAR CON LAS AA.PP.

Tanto en las infraestructuras críticas como en los servicios esenciales, las responsabilidades se reparten entre los operadores y las Administraciones Públicas, correspondiendo este deber por imperativo legal, conllevando su incumplimiento una sanción administrativa e incluso una penal.

9.3. SE DISPONE DE LEGISLACIÓN NACIONAL

Desde 2011 se traspuso la Directiva Europea de Protección de Infraestructuras Críticas a la legislación española, siendo la última, el reciente Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información

9.4. CARÁCTER SANCIONADOR

Artículo 36. Infracciones.

1. Las infracciones de los preceptos de este real decreto-ley se clasifican en muy graves, graves y leves.

2. Son infracciones muy graves:

a) La falta de adopción de medidas para subsanar las deficiencias detectadas, de acuerdo con lo dispuesto en los artículos 32.2 o 33.1, cuando éstas le hayan hecho vulnerable a un incidente con efectos perturbadores significativos en el servicio y el operador de servicios esenciales o el proveedor de servicios digitales no hubiera atendido los requerimientos dictados por la autoridad competente con anterioridad a la producción del incidente.

b) El incumplimiento reiterado de la obligación de notificar incidentes con efectos perturbadores significativos en el servicio. Se considerará que es reiterado a partir del segundo incumplimiento.

c) No tomar las medidas necesarias para resolver los incidentes con arreglo a lo dispuesto en el artículo 28.1 cuando éstos tengan un efecto perturbador significativo en la prestación servicios esenciales o de servicios digitales en España o en otros Estados miembros.

3. Son infracciones graves:

a) El incumplimiento de las disposiciones reglamentarias o de las instrucciones técnicas de seguridad dictadas por la autoridad competente referidas a las precauciones mínimas que los operadores de servicios esenciales han de adoptar para garantizar la seguridad de las redes y sistemas de información.

b) La falta de adopción de medidas para subsanar las deficiencias detectadas en respuesta a un requerimiento dictado de acuerdo con los artículos 32.2 o 33.1, cuando ese sea el tercer requerimiento desatendido que se dicta en los cinco últimos años.

c) El incumplimiento de la obligación de notificar incidentes con efectos perturbadores significativos en el servicio.

d) La demostración de una notoria falta de interés en la resolución de incidentes con efectos perturbadores significativos notificados cuando dé lugar a una mayor degradación del servicio.

e) Proporcionar información falsa o engañosa al público sobre los estándares que cumple o las certificaciones de seguridad que mantiene en vigor.

f) Poner obstáculos a la realización de auditorías por la autoridad competente.

4. Son infracciones leves:

a) El incumplimiento de las disposiciones reglamentarias o de las instrucciones técnicas de seguridad dictadas por la autoridad competente al amparo de este real decreto-ley, cuando no suponga una infracción grave.

b) La falta de adopción de medidas para corregir las deficiencias detectadas en respuesta a un requerimiento de subsanación dictado de acuerdo con los artículos 32.2 o 33.1.

c) No facilitar la información que sea requerida por las autoridades competentes sobre sus políticas de seguridad, o proporcionar información incompleta o tardía sin justificación.

d) No someterse a una auditoría de seguridad según lo ordenado por la autoridad competente.

e) No proporcionar al CSIRT de referencia o a la autoridad competente la información que soliciten en virtud del artículo 28.2.

f) La falta de notificación de los sucesos o incidencias para los que, aunque no hayan tenido un efecto adverso real sobre los servicios, exista obligación de notificación en virtud del párrafo segundo del artículo 19.2.

g) No completar la información que debe reunir la notificación de incidentes teniendo en cuenta lo dispuesto en el artículo 23, o no remitir el informe

justificativo sobre la imposibilidad de reunir la información previsto en dicho artículo.

h) No seguir las indicaciones que reciba del CSIRT de referencia para resolver un incidente, de acuerdo con el artículo 28.

Artículo 37. Sanciones.

1. Por la comisión de las infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones:

a) Por la comisión de infracciones muy graves, multa de 500.001 hasta 1.000.000 euros.

b) Por la comisión de infracciones graves, multa de 100.001 hasta 500.000 euros.

c) Por la comisión de infracciones leves, amonestación o multa hasta 100.000 euros.

2. Las sanciones firmes en vía administrativa por infracciones muy graves y graves podrán ser publicadas, a costa del sancionado, en el «Boletín Oficial del Estado» y en el sitio de Internet de la autoridad competente, en atención a los hechos concurrentes y de conformidad con el artículo siguiente.

Artículo 38. Graduación de la cuantía de las sanciones.

El órgano sancionador establecerá la sanción teniendo en cuenta los siguientes criterios:

a) El grado de culpabilidad o la existencia de intencionalidad.

b) La continuidad o persistencia en la conducta infractora.

c) La naturaleza y cuantía de los perjuicios causados.

d) La reincidencia, por comisión en el último año de más de una infracción de la misma naturaleza, cuando así haya sido declarado por resolución firme en vía administrativa.

e) El número de usuarios afectados.

f) El volumen de facturación del responsable.

g) La utilización por el responsable de programas de recompensa por el descubrimiento de vulnerabilidades en sus redes y sistemas de información.

h) Las acciones realizadas por el responsable para paliar los efectos o consecuencias de la infracción.

9.5. FALTA DE CONCIENCIACIÓN

La eficacia de las Fuerzas y Cuerpos de Seguridad del Estado en su lucha contra el terrorismo y el crimen

organizado, ha sido tan eficaz que ha restringido la concienciación ciudadana de que también es su responsabilidad.

Las empresas públicas y privadas, en general todas las que prestan servicios esenciales, deberían, a instancia del Poder Ejecutivo, a realizar una concienciación de sus directivos y trabajadores en general, de la importancia que tiene el mantenimiento de la “continuidad del servicio que se presta a la sociedad a pesar de cualquier contingencia que pudiera acaecer”.

9.6. EN LA CIBERGUERRA NO HAY FRENTES

En la actualidad, todo se mueve a través de las redes de información. Las redes de agua, telecomunicaciones energía, todas son controladas por sistemas, cuya manipulación desde el exterior puede provocar un cataclismo. Hoy día “con un teclado se puede hacer más daño que con una bomba nuclear”.

Pero todos los empleados de una organización tienen acceso a su sistema de información, debiendo cada uno acceder a la parte y a los datos del mismo, que sean necesarios e imprescindibles para su trabajo ordinario.

9.7.CONCLUSIÓN DE CONCLUSIONES

Todos somos soldados, implicados en una guerra donde el frente de combate está en todas partes.

BIBLIOGRAFÍA

López Aranguren, E. (2011). Huelgas, servicios esenciales y servicios mínimos. *www.sinpermiso.info*. Obtenido de http://www.sinpermiso.info/textos/huelgas-servicios-esenciales-y-servicios-mnimos

SÁNCHEZ CAMPS, J. (2014). Obtenido de http://www.seguritecnia.es/seguridad-publica/administraciones-publicas/plan-estrategico-sectorial-del-sector-financiero: http://www.seguritecnia.es/seguridad-publica/administraciones-publicas/plan-estrategico-sectorial-del-sector-financiero

VIDAL DELGADO, R., & ALONSO RUSSI, E. (2015). *España y la Seguridad Compartida para el Mediterráneo (Análisis jurídico y conceptual). Málaga, 2015. En este libro se diseccionan las distintas seguridades y su e*. Málaga: Foro para la Paz en el Mediterráneo.

Vidal, R. (2003). Obtenido de www.belt.es.