Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

La Ciberseguridad en las infraestructuras críticas

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: Alberto Francoso Figueredo

DIRECTORES: Javier Vales Alonso

Norberto Fernández García

CURSO ACADÉMICO: 2019-2020

Universidade Vigo

Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

La Ciberseguridad en las infraestructuras críticas

Máster Universitario en Dirección TIC para la Defensa
Especialidad de Sistemas y Tecnologías de la Información

Universidade Vigo

RESUMEN

Con este trabajo se pretende dar a conocer la importancia de la ciberseguridad en la protección de las infraestructuras críticas españolas, así como el marco normativo que la regula en este ámbito y los nuevos proyectos en los que se está trabajando para la mejora de la misma.

Para ello, se hace un repaso por la normativa más importante que regula esta materia a nivel europeo y nacional y por los estándares internacionales más importantes en seguridad de la información. Además, se realiza un somero estudio sobre la problemática de la aplicación de la normativa sectorial en distintos sectores con marcadas diferencias entre ellos.

Se realiza un estudio del caso de transposición de la Directiva NIS a la legislación española, mediante la reutilización de estructuras y procedimientos previamente establecidos y en vigor, como es la normativa relacionada con la protección de las infraestructuras críticas o normativa PIC.

En el siguiente apartado se pone en contexto la ciberseguridad con el marco estratégico establecido por la Ley de Seguridad Nacional y se citan y estudian los documentos y actores más importantes recogidos en dicha Ley.

Así mismo, se hace un repaso por las agencias estatales de ciberseguridad y cómo se relacionan entre ellas a partir del nuevo marco de actuación definido a raíz de la transposición de la Directiva NIS

Por último, se analizan los nuevos retos a los habrá que afrontar a medio plazo y largo plazo, haciendo especial mención a la lucha contra la criminalidad.

.

PALABRAS CLAVE

Infraestructura crítica, ciberseguridad, protección, normativa, gobernanza, cibercriminalidad

AGRADECIMIENTOS

Quiero expresar mi especial agradecimiento a los directores de este trabajo fin de master: Javier Alonso Vales y Norberto Fernández García por el tiempo que han dedicado a proponer ideas y sugerencias para mejorar este trabajo.

También me gustaría agradecer al director del Centro Nacional de Protección de Infraestructuras Críticas, Teniente Coronel de la Guardia Civil D. Fernando José Sánchez Gómez y al jefe de la Oficina de Coordinación de Ciberseguridad, Comisario del Cuerpo Nacional de Policía D. Juan Carlos López Madera por todo lo que me han enseñado en estos años de trabajo en la Secretaría de Estado de Seguridad del Ministerio del Interior.

Por último, me gustaría agradecer a todos los compañeros del Máster Universitario en Dirección TIC para la Defensa en su edición 2019/2020 por su compañerismo y atención demostrada, y a los profesores del Centro Universitario de la Defensa y de la Universidad de Vigo por su profesionalidad, compromiso y buen hacer en la impartición de las distintas asignaturas.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 INTRODUCCIÓN Y OBJETIVOS

I

A raíz de una serie de atentados terroristas ocurridos en los primeros años de la década de los 2000, como el atentado contra las torres gemelas ocurrido en Nueva York el 11 de septiembre de 2001 (figura 1-1) o el ocurrido en Madrid el 11 de marzo de 2004 (figura 1-2), la Unión Europea se ve en la necesidad de proteger las infraestructuras críticas europeas, entendiendo como tales, "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 funcionamiento de las instituciones del Estado y de las Administraciones Públicas[1]".

Con esta finalidad, se publica la DIRECTIVA 2008/114/CE DEL CONSEJO de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras criticas europeas y la evaluación de la necesidad de mejorar su protección, mediante el establecimiento de un procedimiento de identificación y designación de infraestructuras criticas europeas y un planteamiento común para evaluar la necesidad de mejorar la protección de dichas infraestructuras, con el fin de contribuir a la protección de la población.

Figura 1-1 Atentado torres gemelas. New York 2001 (fuente: www. antena3.com)

[1] DIRECTIVA 2008/114/CE DEL CONSEJO de 8 de diciembre de 2008 (art.2, a)

Figura 1-2. Atentados Renfe. Madrid 2004 (fuente: www.antena3.com)

II

El 28 de abril de 2001, se publica en España la *Ley 8/2011, por la que se establecen medidas para la protección de las infraestructuras críticas* (en adelante, Ley PIC), e inmediatamente después, el *Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas* (en adelante, Reglamento PIC). Con la dicha ley y su reglamento de desarrollo, se establecen los instrumentos de planificación del Sistema de Protección de Infraestructuras Críticas y constituyen los elementos esenciales para garantizar la protección de las infraestructuras críticas y, por tanto, los servicios esenciales provistos por éstas.

En esta normativa, además de la creación del Centro Nacional de Protección de Infraestructuras Críticas (en adelante CNPIC), se contempla la elaboración de unos planes de actuación por parte de los operadores críticos, que conforman el conjunto de medidas de seguridad integral para elevar al máximo nivel de capacidad en la protección de las infraestructuras críticas, comprendiendo tanto aspectos estratégicos como tácticos.

Para la elaboración de estos planes, el Secretario de Estado de Seguridad dictó la *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.*

Dicha Resolución es complementada mediante la elaboración por parte del CNPIC de las "*Guías de Buenas Prácticas para la elaboración de los Contenidos Mínimos de los Planes de Seguridad del Operador"* y *"Guías de Buenas Prácticas para la elaboración de los Contenidos Mínimos de los Planes de Protección Específicos",* donde se dan una serie de líneas maestras para la correcta elaboración de los mencionados planes.

En el transcurso de estos años, y de manera progresiva, la naturaleza de las amenazas a las infraestructuras críticas va variando desde el ámbito físico al ámbito cibernético. El uso cada vez más extendido de las tecnologías de la información y la comunicación (en adelante TIC) para la provisión de los servicios esenciales, el aumento de la dependencia energética y su elevada transversalidad e interconexión, hacen variar los ataques a dichas instalaciones, lo que hace aconsejable la revisión del enfoque de la seguridad para su protección.

En palabras de la Secretaria de Estado, directora del Centro Nacional de Inteligencia: "el ciberespacio permite operar con un alto grado de impunidad y de anonimato"[2].

La definición del ciberespacio, la podemos encontrar en la Estrategia de Ciberseguridad de 2019, donde lo define de la siguiente forma:

"...es un espacio común global caracterizado por su apertura funcional y su dinamismo. La ausencia de soberanía, su débil jurisdicción, la facilidad de acceso y la dificultad de atribución de las acciones que en él se desarrollan definen un escenario que ofrece innumerables oportunidades de futuro, aunque también presenta serios desafíos de seguridad"[3].

La Dirección del CNPIC, consciente del incremento de las amenazas provenientes del ciberespacio, en 2017, lleva a cabo una mejora de los contenidos mínimos del PSO y PPE, especialmente en el ámbito de la ciberseguridad y pone en marcha, junto con el Instituto de Ciberseguridad del Estado (en adelante INCIBE), un proyecto de creación del Esquema Nacional de Seguridad Industrial.

En desarrollo de la Resolución *de 8 de septiembre de 2015, de la Secretaria 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,* se contemplan otros aspectos en los que se profundizará en el futuro esquema de certificación de infraestructuras críticas y servicios esenciales, tales como:

- Carácter Integral de la Seguridad.
- Visión holística de la Seguridad.
- Certificaciones en materia de seguridad.
- Procedimientos operativos para la monitorización, supervisión y evaluación/auditoría, tanto de los activos físicos de la infraestructura como los activos lógicos (ciberseguridad) o de sistemas de operación.

Dichos aspectos, que fueron ampliados en las dos guías de buenas prácticas "Plan de Seguridad del Operador (PSO)" y "Plan de Protección Específico (PPE)", detallan las medidas de seguridad, de carácter organizativo, procedimental y técnicas, que han de adoptar los operadores críticos para garantizar la seguridad integral de sus infraestructuras.

III

De forma paralela, en el 2010 se publica el 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.

Dicho esquema (en adelante ENS), aunque regula un ámbito distinto, como es el de la Administración Pública, para la que es de obligado cumplimiento, inspirará en materia de ciberseguridad el enfoque futuro de la protección de las infraestructuras críticas, destacando la consideración de sus dimensiones de seguridad, o la división de las medidas de seguridad en tres marcos definidos como son el organizativo, operacional y de protección.

[2] Conferencia de la directora del CNI, Paz Esteban López. XXXII SEMINARIO INTERNACIONAL DE SEGURIDAD Y DEFENSA: "AMENAZAS DESDE EL CIBERESPACIO"

[3] Estrategia Nacional de Ciberseguridad 2019, Presidencia del Gobierno. P. 17-18.

La exigencia de una certificación, que acredite su cumplimiento para los organismos públicos, introdujo de manera muy temprana el concepto de obligatoriedad en la implementación de medidas de seguridad para los sistemas de información de la Administración Pública española.

IV

El Acuerdo Marco suscrito en 2015 entre la Secretaría de Estado de Seguridad, y la Secretaría de Estado para la Sociedad de la Información y Agenda Digital del Ministerio de Energía, Turismo y Agenda Digital, permitió la adopción de un conjunto de actuaciones comunes dentro del ámbito de la prevención y reacción ante incidentes de ciberseguridad que pudiesen afectar a las redes y sistemas de información de los operadores de infraestructuras críticas y consiguientemente, a los servicios esenciales que éstos prestan.

Entre dichas actuaciones comunes, el INCIBE y el CNPIC iniciaron el desarrollo del Esquema Nacional de Seguridad Industrial (en adelante, ENSI), como instrumento para mejorar la seguridad de los sistemas de operación industrial[4] (*operation technologies*, en adelante sistemas OT) de las infraestructuras críticas y que podría ser adoptado para el resto de los entornos industriales, aunque no estuviesen catalogados como infraestructuras críticas.

El ENSI se basaba en cuatro pilares fundamentales:

- Metodología de Análisis de Riesgo Ligero de Seguridad Integral (en adelante, ARLI-SI)
- Indicadores para la Mejora de Ciberresiliencia (en adelante, IMC).
- Modelo de Construcción de Capacidades en Ciberseguridad de la Cadena de Valor (en adelante, C4V).
- Sistema de Acreditación en Ciberseguridad (en adelante, SA).

A lo largo del tiempo, dichos pilares han ido derivando en otros modelos, como por ejemplo el C4V, que se constituye como el motor del futuro esquema de certificación para infraestructuras críticas y servicios esenciales o continúan funcionado de manera autónoma como el IMC.

Otros como el ARLI-SI, han quedado sin desarrollo hasta el día de hoy.

V

Con la entrada en vigor de la *Directiva (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 en la Unión* (en adelante, Directiva NIS), cambia radicalmente el panorama de la ciberseguridad, no sólo en España, sino en toda Europa.

Pese a ser una directiva con un marcado carácter económico, tal y como se recoge en su articulado: "La *presente Directiva establece medidas con el objeto de lograr un elevado nivel común de seguridad de las redes y sistemas de información dentro de la Unión a fin de mejorar el*

[4] Tecnología diseñada para la automatización de los procesos industriales mediante el uso de sistemas informáticos

funcionamiento del mercado interior."[5], ha establecido obligaciones en ciberseguridad en sectores tradicionalmente híper regulados en esta materia como es el sector financiero, así como en sectores muy regulados en el ámbito físico pero sin regulación específica en el ámbito cibernético, como por ejemplo el subsector del transporte aéreo.

La escasa o nula regulación en la Unión Europea en esta materia, dio lugar a retrasos generalizados a la hora de su transposición a las legislaciones de los estados miembros. Tanto es así, que España tuvo que adoptar la fórmula del real decreto-ley para su transposición para evitar los largos tiempos legislativos de una ley ordinaria, y evitar las sanciones que un retraso en su transposición hubiese conllevado.

Dicha transposición se materializó en el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, convalidado mediante Resolución de 20 de septiembre de 2018, del Congreso de los Diputados, por la que se ordena la publicación del Acuerdo de Convalidación del citado Real Decreto-ley.

A día de hoy, se encuentra en trámite parlamentario el reglamento de desarrollo correspondiente, encontrándose en su última fase de aprobación.

VI

En abril del pasado 2019, se aprobó *el REGLAMENTO (UE) 2019/881 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación* y por el que se deroga el Reglamento (UE) n.o 526/2013 («Reglamento sobre la Ciberseguridad») de 2013 por encontrarse obsoleto.

Este reglamento, refuerza las funciones de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) e intenta poner orden la hora de la certificación de productos, sistemas y procesos de la ciberseguridad, en un panorama caótico donde cada estado miembro posee sus propios esquemas de certificación, o utilizan estándares internacionales.

Este galimatías hace que dichas certificaciones tengan un carácter local, lo que evita el reconocimiento entre países de la Unión, convirtiéndose en un problema para los operadores, que necesitan diferentes certificaciones para operar internacionalmente o basarse en estándares ajenos como por ejemplo el "*Common Criteria*", cuyo origen se remonta a 1990 y que surge como resultado de la necesidad de armonización de criterios de seguridad a la hora de evaluar productos de software, hardware y firmware ya utilizados por diferentes países con el fin de que el resultado del proceso de evaluación pudiese ser aceptado internacionalmente.

El objetivo por tanto de este trabajo es dar a conocer la importancia de la ciberseguridad en la protección de las infraestructuras críticas españolas, así como el marco normativo que la regula, la problemática en su aplicación y los nuevos proyectos en los que se está trabajando para la mejora de la misma.

Así mismo, se hace un repaso por la gobernanza en la ciberseguridad española, identificándose además los principales actores en ciberseguridad de la Administración y por último, se analizan los nuevos retos que se habrán de afrontar a medio plazo y largo plazo.

[5] *Directiva (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 en la Unión. Art. 1*

2 ESTADO DEL ARTE

El desarrollo de la ciberseguridad ha ido aparejado al desarrollo y creciente uso de las tecnologías de la información y la comunicación.

La creciente necesidad de proteger los sistemas de información ha motivado que se implanten **innumerables modelos de certificación en seguridad** promovidos por el sector privado, como por ejemplo el *Certified Security Systems Professional (CISSP)*, que es el certificado más reconocido a nivel mundial y que garantiza que se poseen las competencias para gestiona la seguridad en los sistemas TIC de una organización, o el *Certified Information Security Manager* (CISM) con una temática parecida, y que son reconocidos por los contratantes, o no, de manera coyuntural.

Entre tanto, las autoridades competentes, nacionales o comunitarias, han ido regulando la ciberseguridad en función de sus necesidades, ya sea a nivel nacional, como por ejemplo el ENS español, vigente desde 2010, o a nivel sectorial, encontrando sectores muy avanzados en regulación como por ejemplo el financiero o las telecomunicaciones, y sectores con menos desarrollo regulatorio como por ejemplo el sector de la alimentación o del agua, lo que ocasiona un verdadero **laberinto regulatorio muy desequilibrado entre los sectores estratégicos.**

Los Estados miembros y después la Comisión Europea, han ido realizando verdaderos **esfuerzos por regular de manera homogénea** el galimatías regulatorio existente. Ejemplos de ello son el *Reglamento eIDAS 910/2014 sobre identificación electrónica y servicios de confianza*, que define un marco jurídico coherente para el uso de la identidad digital y la firma electrónica, o la *Directiva NIS* para adquirir un elevado nivel de seguridad común en los sistemas y redes de comunicación, o la *Ley de Ciberseguridad Europea* para regular todo lo relativo a las certificaciones en ciberseguridad.

Si, además, tenemos en cuenta que la ciberseguridad es un ámbito especialmente dinámico, donde prácticamente cada día se están introduciendo nuevas variables que hay que considerar para su regulación, como por ejemplo las nuevas tecnologías como el *5G*[6], que va a condicionar las telecomunicaciones en los próximos años, o la tecnología *blockchain*[7] que va a revolucionar los procesos adminstrativos y legales futuros, ,el *big data*[8], o el *IoT*, que afectan de manera transversal a nuestra sociedad en múltiples ámbitos, y que requieren una regulación específica, nos encontramos con un panorama en el que existen **contínuos vacíos legislativos**, ya que los **tiempos de implantación de**

[6] Quinta generación de telefonía móvil

[7] Tecnología de cadena de bloques para generar un registro distribuido que registra de manera fehaciente determinados actos

[8] Manejo de grandes volúmenes de datos para uso analítico y prospectivo

las tecnologías van mucho más rápidos que los tiempos necesarios para regular la materia que se trate.

Pero no sólo las tecnologías, sino acontecimientos sobrevenidos, como la pandemia de 2020 ocasionada por el coronavirus, ha impactado en la ciberseguridad, ya que se han tenido que utilizar, como consecuencia de los confinamientos, infinidad de modelos de conexiones remotas y de plataformas de comunicación no suficientemente probadas, lo que ha revelado nuevas demandas de seguridad específicas en estos recursos.

Por último, otro problema añadido es el **aumento y la especialización de la cibercriminalidad**, tanto para acciones terroristas, como para espionaje industrial, como para delincuencia común.

La facilidad para la comisión de delitos a través de las redes, los enormes beneficios que generan, la introducción del modelo *Crime as a Service* donde se contratan servicios para delinquir, está provocando que cada vez suframos en nuestros sistemas informáticos ataques más sofisticados y en mayor número, lo que la lucha contra la cibercriminalidad se ha convertido en un objetivo prioritario para garantizar la ciberseguridad de las infraestructuras críticas españolas.

3 MARCO NORMATIVO

3.1 Leyes europeas

3.1.1 Directiva 2008/114/CE del Consejo de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.

Esta Directiva establece un procedimiento de identificación y designación de infraestructuras criticas europeas («las ICE») y un planteamiento común para evaluar la necesidad de mejorar la protección de dichas infraestructuras, con el fin de contribuir a la protección de la población.

Establece la definición de infraestructura crítica como el elemento, sistema o parte de este 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; y define infraestructura crítica europea como aquella que concierne a dos Estados miembros.

Además, establece un procedimiento de identificación de infraestructuras críticas en base a los siguientes criterios horizontales:

a) el número de víctimas (valorado en función del número potencial de víctimas mortales o de heridos);

b) el impacto económico (valorado en función de la magnitud de las pérdidas económicas o el deterioro de productos o servicios, incluido el posible impacto medioambiental);

c) el impacto público (valorado en función de la incidencia en la confianza de la población, el sufrimiento físico y la alteración de la vida cotidiana, incluida la perdida de servicios esenciales).

Los criterios sectoriales tendrán en cuenta las características de los diferentes sectores de las ICE.

En un primer momento, los sectores que se tendrán en cuenta a efectos de la ejecución de esta Directiva serán los de la energía y el transporte junto con sus correspondientes subsectores.

Se consideran futuras revisiones de la Directiva donde podrán determinarse nuevos sectores dándose prioridad al sector de las TIC.

La Directiva establece un mecanismo de coordinación entre los diferentes Estados miembros y la Comisión para las infraestructuras compartidas.

Una vez identificadas las infraestructuras, la Directiva establece la obligatoriedad de la existencia de Planes de seguridad del operador (PSO) donde se identificarán los elementos infraestructurales

críticos y sus soluciones de seguridad, estableciéndose unos contenidos mínimos que deberá incluir dicho PSO. Será cada Estado miembro quién garantizará la aplicación del citado plan.

Se crea la figura de los responsables de enlace para la seguridad quienes ejercerán la función de punto de contacto para cuestiones de seguridad entre el propietario u operador de ICE y la autoridad competente del Estado miembro, quién aplicará un mecanismo de comunicación adecuado con el objetivo de intercambiar información pertinente sobre los riesgos y amenazas identificados en relación con la ICE de que se trate.

Cada Estado miembro presentará cada dos años a la Comisión datos generales resumidos sobre los tipos de riesgos, amenazas y vulnerabilidades encontrados en cada uno de los sectores en los que se hayan designado ICE. Basándose en estos informes la Comisión y los Estados miembros evaluarán por sectores la necesidad de introducir medidas de protección adicionales a escala comunitaria para las ICE.

La Comisión, además, podrá elaborar, en cooperación con los Estados miembros, directrices metodológicas comunes para la realización de análisis de riesgos de las IC y apoyará, a través de las autoridades del Estado miembro interesado, a los propietarios u operadores de ICE designadas facilitándoles acceso a las mejores prácticas y métodos, y fomentando la formación y los intercambios de información sobre novedades técnicas relacionadas con la protección de infraestructuras críticas.

Cada Estado miembro habrá de designar un punto de contacto para la protección de infraestructuras críticas europeas que coordinará las cuestiones relativas a la protección de infraestructuras críticas europeas en el propio Estado miembro, con los demás Estados miembros y con la Comisión.

3.1.2 Directiva (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 en la Unión.

La Directiva consta de 75 considerandos, siete capítulos y 25 artículos.

El Capítulo I establece unas disposiciones generales, definiendo el objeto de la norma, que es lograr un elevado nivel común de seguridad de las redes y sistemas de información dentro de la Unión a fin de mejorar el funcionamiento del mercado interior.

Para ello establece para todos los Estados miembros la obligación de adoptar una estrategia de seguridad de las redes y sistemas de información. Crea, además, un Grupo de cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y desarrollar la confianza y seguridad entre ellos.

Establece obligaciones y responsabilidades a los Estados miembros para que designen autoridades nacionales competentes, puntos de contacto únicos y centros de respuesta ante incidentes (CSIRT) para apoyo técnico en lo relativo a las medidas de seguridad y los incidentes.

En su articulado da una serie de definiciones, siendo el aspecto más importante que la Directiva considera redes y sistemas de información, no sólo a las redes de comunicación electrónicas, sino a todo dispositivo en el que se realizan el tratamiento automático de datos digitales, incluyendo también los datos en todo su ciclo de vida.

Una cuestión relevante en la norma es la identificación de los operadores de los servicios esenciales recogidos en el ámbito de la norma, que son los siguientes:

- Energía
- Transporte
- Banca
- Infraestructura de los mercados financieros

- Sector sanitario
- Suministro y distribución de agua potable
- Infraestructura digital

Para su identificación, se tendrán en cuenta los siguientes criterios:

- Si la entidad presta un servicio esencial para el mantenimiento de actividades sociales o económicas cruciales
- Si la prestación de dicho servicio depende de las redes e información
- Si un incidente tendría efectos perturbadores significativos9 en la prestación de dicho servicio

Cada Estado miembro tendrá que adoptar una estrategia nacional de seguridad de las redes y sistemas de información que establezca los objetivos estratégicos y las medidas políticas y normativas adecuadas teniendo en cuenta los objetivos y prioridades. Habrán de establecer un marco de gobernanza con las funciones y responsabilidades de las instituciones públicas y demás actores y tendrá en cuenta la identificación de medidas de preparación, respuesta y recuperación, así como programas de formación y concienciación, entre otras cuestiones.

Cada Estado miembro tendrá que designar una o más autoridades nacionales competentes en materia de seguridad de las redes y sistemas de información que cubra al menos los sectores. Dichas autoridades supervisarán la aplicación de la Directiva a escala nacional, así como un punto de contacto único en materia de seguridad de las redes y sistemas de información.

La Directiva contempla la creación de uno o varios equipos de respuesta a incidentes de seguridad informática (CSIRT) que serán responsables de la gestión de incidentes y riesgos, estableciéndose una red de CSIRTs nacionales, en la que se podrá intercambiar información técnica y colaboración en incidentes transfronterizos.

Cabe destacar la creación de un Grupo de cooperación a fin de apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y desarrollar confianza y seguridad que estará formado por representantes de los Estados miembros, la Comisión y la ENISA.

Los requisitos de seguridad para las redes y sistemas de información que la Directiva exige, quedan a cargo de los Estados miembros, quienes velarán por que los operadores de servicios esenciales tomen las medidas técnicas y de organización adecuadas y proporcionadas para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información que utilizan en sus operaciones, para que tomen las medidas adecuadas para prevenir y reducir al mínimo los efectos de los incidentes que afecten la seguridad de las redes y sistemas de información utilizados para la prestación de tales servicios esenciales con el objeto de garantizar su continuidad y para que los operadores de servicios esenciales notifiquen sin dilación indebida a la autoridad competente o al CSIRT los incidentes que tengan efectos significativos[10] en la continuidad de los servicios esenciales que prestan.

A los proveedores de servicios digitales, la Directiva le dedica un capítulo aparte debido a la especificidad y transversalidad del sector. Establece la obligación a los Estados miembros de velar por que dichos proveedores adopten las medidas técnicas y organizativas adecuadas para gestionar los riesgos para la seguridad de las redes y sistemas de información en la misma línea que los operadores de servicios esenciales.

[9] Atendiendo a los siguientes factores: número de usuarios, dependencia de otros sectores, repercusión en las actividades económicas, sociales o en la seguridad pública, cuota de mercado, extensión geográfica y la capacidad para mantener el nivel de servicio.

[10] En base al número de usuarios afectados, la duración del incidente o la extensión geográfica afectada

Para la aplicación y observancia de la norma, se establecen una serie de obligaciones a los operadores y a las autoridades competentes relativas a la información de las medidas de seguridad adoptadas y a la subsanación de posibles incumplimientos.

Debido a la globalización en la provisión de servicios digitales, se hace especial mención a los casos en que un proveedor de servicios se considerará sometido a la jurisdicción de un Estado miembro

- Cuando se encuentre su establecimiento principal.
- Cuando su domicilio social se encuentre en ese Estado miembro.
- Cuando se encuentre establecido su representante.

La Directiva impone un régimen de sanciones aplicables en caso de incumplimiento de las disposiciones nacionales aprobadas, que deberán ser efectivas, proporcionadas y disuasorias. Las autoridades competentes deberán adoptar todas las medidas necesarias para garantizar su aplicación.

La Comisión revisará periódicamente el funcionamiento de la Directiva en base los informes del Grupo de cooperación y de la red de CSIRT sobre la experiencia adquirida a nivel estratégico y operativo.

Por último, se le da de plazo a los Estados para su adopción y publicación, a más tardar el 9 de mayo de 2018.

3.1.3 Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación.

Este reglamento consta de 110 considerandos, 4 títulos y 69 artículos y es obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

El objeto y el ámbito de aplicación de este reglamento se ha redactado con vistas a garantizar el correcto funcionamiento del mercado interior, aspirando al mismo tiempo a alcanzar un nivel elevado de ciberseguridad, ciberresiliencia y confianza dentro de la Unión.

Para ello establece dos líneas de actuación: Por un lado, refuerza a la Agencia de la Unión Europea para la Ciberseguridad (ENISA), redefiniendo sus objetivos, tareas y aspectos organizativos y por otro lado establece un marco para la creación de esquemas europeos de certificación de la ciberseguridad que garanticen un nivel adecuado de ciberseguridad de los productos, servicios y procesos de las TIC en la Unión, así como de evitar la fragmentación del mercado interior respecto a los esquemas de certificación de la ciberseguridad.

El reglamento encomienda a ENISA el apoyo activo a los Estados miembros, a las instituciones, órganos y organismos de la Unión en la mejora de la ciberseguridad. Para ello lo convierte en un centro de conocimientos técnicos sobre ciberseguridad dándole las competencias para la asistencia en ciberseguridad a las instituciones de la Unión, para el apoyo a la creación de capacidades, fomento de la cooperación e intercambio de información y la promoción del uso de la certificación europea de ciberseguridad para evitar la fragmentación del mercado interior.

Además, le encomienda la asistencia en elaboración y ejecución de la política y del Derecho de la Unión en el ámbito de la ciberseguridad, la creación de capacidades para mejorar la prevención, detección, análisis y respuesta ante ciberamenazas e incidentes, el apoyo a la cooperación operativa entre los Estados miembros y las instituciones de la Unión y al mercado, certificación de la

ciberseguridad y normalización, mediante la promoción del desarrollo y la aplicación de la política de la Unión en materia de certificación de la ciberseguridad de productos, servicios y procesos TIC.

Además, se le encomienda el análisis de las tecnologías emergentes y los análisis estratégicos de las ciberamenazas e incidentes, entre otros. Colaborará en la sensibilización y educación de ciudadanos, organizaciones y empresas, a participará en tareas de investigación e innovación.

Por último, le es encomendada la tarea de contribuir a los esfuerzos de la Unión para cooperar con terceros países y organizaciones internacionales en materia de ciberseguridad.

El Capítulo III lo dedica el reglamento a la organización de ENISA, que estará integrado por un Consejo de Administración, un Comité Ejecutivo, un director ejecutivo, un Grupo Consultivo y una red de funcionarios de enlace nacionales para facilitar el intercambio de información entre ENISA y los Estados miembros.

Para llevar a cabo sus operaciones, ENISA redactará un documento único de programación anual y plurianual con sus actividades previstas.

La segunda línea de actuación que es establecer un Marco de Certificación de la Ciberseguridad, viene recogida en el Título III, donde se crea el marco europeo de certificación de la ciberseguridad con el fin de mejorar las condiciones de funcionamiento del mercado interior incrementando el nivel de ciberseguridad dentro de la Unión y haciendo posible un planteamiento armonizado a nivel de la Unión de esquemas europeos de certificación de la ciberseguridad, con el objetivo de crear un mercado único digital para los productos, servicios y procesos de las TIC, definiendo un mecanismo destinado a instaurar esquemas europeos de certificación de la ciberseguridad y a confirmar que los productos, servicios y procesos de TIC que hayan sido evaluados con arreglo a dichos esquemas cumplan los requisitos de seguridad especificados con el objetivo de proteger la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o procesados o las funciones o servicios que ofrecen, o a los que permiten acceder, dichos productos, servicios y procesos durante todo su ciclo de vida.

Para ello, la Comisión publicará un programa de trabajo evolutivo que definirá las prioridades estratégicas de los futuros esquemas europeas de certificación que serán priorizados en base a la disponibilidad y el desarrollo de esquemas nacionales de certificación, el Derecho o las políticas aplicables, la demanda del mercado, la evolución de las amenazas.

Además, la Comisión podrá solicitar a ENISA una propuesta de esquema de certificación basándose en el programa de trabajo evolutivo o fuera del mismo si se hace de manera justificada.

ENISA mantendrá un sitio web para ofrecer información sobre los esquemas europeos de certificación de la ciberseguridad, donde relacionará aquellos esquemas nacionales de certificación de la ciberseguridad que hayan sido sustituidos por un esquema europeo de certificación de la ciberseguridad.

El reglamento establece los objetivos de seguridad de los esquemas europeos de certificación de la ciberseguridad que se establezcan, que deberán diseñarse para cumplir, al menos los siguientes objetivos de seguridad: proteger los datos en todo su ciclo de vida, proteger el acceso a la información, detectar vulnerabilidades, efectuar registros de actividad, mantener una política de backup, la seguridad por diseño y las actualizaciones.

En otro orden de cosas, se da la posibilidad a los esquemas de certificación de establecer uno o mas niveles de garantía de los tres disponibles: básico, sustancial y elevado, donde se reflejará el nivel de riesgo asociado al uso.

Un certificado europeo de ciberseguridad o una declaración de la conformidad de la UE de nivel básico cumple con los requisitos de seguridad necesarios para minimizar los riesgos básicos conocidos de ciberincidentes y ciberataques. Las actividades de evaluación a efectuar incluirán al menos una revisión de la documentación técnica.

El certificado de nivel de garantía «sustancial» ofrece garantías de que se cumplen los requisitos de seguridad, para minimizar los riesgos relacionados con la ciberseguridad conocidos, los riesgos de incidentes y los ciberataques cometidos por agentes con capacidades y recursos limitados. Se incluirá al menos un análisis de vulnerabilidades y la comprobación de que se aplican correctamente las funcionalidades de seguridad necesarias en el uso.

Un certificado de nivel de garantía «elevado» ofrece garantías de que los productos, servicios y procesos de TIC para los cuales se expide dicho certificado cumplen los correspondientes requisitos de seguridad y de que se han evaluado hasta un nivel permite minimizar el riesgo de ciberataques sofisticados cometidos por agentes con capacidades y recursos considerables.

La norma deja la posibilidad al fabricante o proveedor de realizar una autoevaluación de conformidad bajo su exclusiva responsabilidad para el nivel de garantía básico.

La certificación de la ciberseguridad será voluntaria salvo que se disponga otra cosa en el Derecho de la Unión o de los Estados miembros, y se entenderán conformes con los requisitos de dicho esquema.

Los certificados europeos de ciberseguridad, que serán reconocidos en todos los Estados miembros, se expedirán por el período previsto en el esquema europeo de certificación de la ciberseguridad y podrán renovarse siempre y cuando sigan cumpliéndose los requisitos correspondientes.

Los esquemas nacionales de certificación de ciberseguridad y los procedimientos correspondientes para los productos, servicios y procesos de TIC cubiertos por un esquema europeo de certificación de la ciberseguridad dejarán de surtir efectos a partir de la fecha establecida en el acto de ejecución de este reglamento. A partir de ahí, los Estados miembros no podrán introducir nuevos esquemas de certificación cubiertos por un esquema de certificación europeo. Cualquier intención de un Estado miembro de crear un esquema nacional de certificación, deberá ser comunicado a la Comisión.

Cada Estado miembro designará a una o más autoridades nacionales de certificación de la ciberseguridad en su territorio para que se encarguen de las tareas relativas a la supervisión de la aplicación de las normas recogidas en los esquemas.

Se establece un procedimiento de revisión interpares para alcanzar normas equivalentes en toda la Unión en lo que respecta a la aplicación de los criterios de los certificados y las declaraciones de conformidad.

Por último, cabe destacar que se crea el Grupo Europeo de Certificación de la Ciberseguridad que estará integrado por representantes de las autoridades nacionales de certificación de la ciberseguridad o por representantes de otras autoridades nacionales pertinentes, para asesoramiento y asistencia a la Comisión y a ENISA en esta materia.

Se encomienda a los Estados miembros que establezcan un régimen de sanciones aplicables a los incumplimientos de los esquemas europeos de certificación de la ciberseguridad y adopten las medidas necesarias para garantizar su aplicación.

3.2 Leyes españolas

3.2.1 Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

Esta ley, nacida de la transposición de la *Directiva 2008/114/CE consta de 3 títulos y 18 artículos,* tiene por objeto establecer el marco legal y organizativo para mejorar la prevención, preparación y

respuesta del Estado frente a atentados terroristas u otras amenazas que afecten a infraestructuras críticas, previa identificación y designación de las mismas.

Para ello, establece determinadas obligaciones que deben asumir tanto las Administraciones Públicas como los operadores de aquellas infraestructuras que se determinen como infraestructuras críticas.

Comienza con una serie de definiciones, como **servicio esencial**, que considera es 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.

Establece la definición de **sector estratégico**, siendo este 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.

Cabe reseñar la definición de **infraestructuras estratégicas y críticas,** definida la primera como aquellas instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales; y definiendo la segunda como aquella infraestructura estratégica cuyo funcionamiento es indispensable y **no permite soluciones alternativas**, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

Por último, otro concepto importante es el de **criterios horizontales de criticidad** que son los parámetros en función de los cuales se determina la criticidad, la gravedad y las consecuencias de la perturbación o destrucción de una infraestructura crítica, en base al potencial de víctimas mortales o heridos con lesiones graves y las consecuencias para la salud pública, el impacto económico en función de la magnitud de las pérdidas económicas y el deterioro de productos y servicios, el impacto medioambiental, y por último, el impacto público y social, que va relacionado con la confianza del ciudadano en sus Instituciones Públicas, el sufrimiento físico o la alteración de la vida cotidiana por el grave deterioro de servicios esenciales.

El Ministerio del Interior, será el responsable de la elaboración de un **Catálogo Nacional de Infraestructuras Estratégicas** que contendrá toda la información y valoración de las infraestructuras estratégicas del país, entre las que se hallarán incluidas aquellas clasificadas como críticas o críticas europeas, en las condiciones que se determinen en el Reglamento que desarrolle la presente Ley, siendo además el competente para clasificar una infraestructura como estratégica, y en su caso, como infraestructura crítica.

El siguiente título trata sobre la organización del **Sistema de Protección de Infraestructuras Críticas** compuesto por una serie de instituciones, órganos y empresas, procedentes públicas o privadas con responsabilidades en el correcto funcionamiento de los servicios esenciales.

Esta ley, con vocación de colaboración público-privada, involucra a los siguientes agentes:

- La Secretaría de Estado de Seguridad del Ministerio del Interior.
- El Centro Nacional para la Protección de las Infraestructuras Críticas.
- Los Ministerios
- Las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía.
- Las Delegaciones del Gobierno
- Las Corporaciones Locales
- La Comisión Nacional para la Protección de las Infraestructuras Críticas.
- El Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.
- Los operadores críticos del sector público y privado.

La **Secretaría de Estado de Seguridad** es nombrada responsable del Sistema de Protección de las infraestructuras críticas nacionales y es la encargada de dirigir la estrategia nacional de protección de infraestructuras críticas y aprobar los planes de seguridad.

Se crea el **Centro Nacional para la Protección de las Infraestructuras Críticas** (en adelante CNPIC) encargado del impulso, la coordinación y supervisión de todas las actividades que tiene encomendadas la Secretaría de Estado de Seguridad en relación con la protección de las Infraestructuras Críticas en el territorio nacional, además corresponderá la realización de altas, bajas y modificaciones de infraestructuras en el Catálogo, así como la determinación de la criticidad de las infraestructuras estratégicas incluidas en el mismo.

Por cada sector estratégico, se designará, al menos, un **ministerio, organismo, entidad u órgano de la Administración General del Estado** integrado en el Sistema, que será el encargado de impulsar, en el ámbito de sus competencias, las políticas de seguridad del Gobierno sobre los distintos sectores estratégicos nacionales y de velar por su aplicación, actuando igualmente como puntos de contacto especializados en la materia.

Las **Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades intervendrán**, a través de las Fuerzas y Cuerpos de Seguridad en la implantación de los diferentes planes de las infraestructuras críticas de su demarcación

Para las **Comunidades Autónomas y Ciudades con Estatuto de Autonomía** que ostenten competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público participarán en la implantación de los planes a través de sus respectivos cuerpos policiales, y serán miembros de la Comisión Nacional para la Protección de las Infraestructuras Críticas. Las Comunidades Autónomas no incluidas en los apartados anteriores participarán en el Sistema de Protección de Infraestructuras Críticas y en los Órganos previstos en esta Ley, de acuerdo con las competencias que les reconozcan sus respectivos Estatutos de Autonomía.

Otro órgano de nueva creación es la **Comisión Nacional para la Protección de las Infraestructuras Críticas**, que es un órgano colegiado competente para aprobar los diferentes Planes Estratégicos Sectoriales así como para designar a los operadores críticos a propuesta del **Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas,** al que le corresponderá la elaboración de los diferentes Planes Estratégicos Sectoriales y la propuesta a la Comisión de la designación de los operadores críticos por cada uno de los sectores estratégicos definidos.

Especial atención merecen la figura de **operadores críticos** que son los encargados de proveer un servicio esencial a través de sus infraestructuras críticas.

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 y deberán, entre otras obligaciones, elaborar el **Plan de Seguridad del Operador** y un **Plan de Protección Específico** por cada una de las infraestructuras consideradas como críticas en el Catálogo, así como designar a un **Responsable de Seguridad y Enlace**, que será el interlocutor con el CNPIC en esta materia, y a un **Delegado de Seguridad** por cada una de sus infraestructuras consideradas Críticas.

Incluidos los planes comentados en el párrafo anterior, el sistema de planificación de esta norma comprende los siguientes planes:

El **Plan Nacional de Protección de las Infraestructuras Críticas,** elaborado por la Secretaría de Estado de Seguridad, es un documento para dirigir y coordinar las actuaciones en esta materia en la lucha contra el terrorismo.

Los **Planes Estratégicos Sectoriales**, elaborados por el Grupo de Trabajo Interdepartamental, que incluyen por sectores los criterios de las medidas a adoptar frente a una situación de riesgo.

Los **Planes de Seguridad del Operador** son documentos de alto nivel que contemplan aspectos relativos a la seguridad organizativa y procedimental del operador crítico. Deberán contener, al menos,

aspectos relacionados con la política de seguridad del operador, marco de gobierno de la seguridad, identificación y estudio de los servicios esenciales que presta, la metodología de análisis de riesgos empleada, los criterios de aplicación de las medidas de seguridad empleadas y documentación complementaria.

Los **Planes de Protección Específicos** son documentos de seguridad de cada una de las infraestructuras críticas, donde se establecen las medidas de seguridad adoptadas por los operadores críticos para su protección.

Los **Planes de Apoyo Operativo** son planes de carácter táctico, elaborados por el Cuerpo Policial con competencia en la demarcación, para cada una de las infraestructuras críticas, que deberán contener, al menos, los aspectos organizativos de la seguridad de la infraestructura, la descripción de la misma, un análisis de riesgos y un plan de acción con las medidas de seguridad a implementar.

3.2.2 Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Desarrollo reglamentario pendiente de publicación.

Esta norma consta de 7 títulos y 42 artículos y tiene como objeto regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales, y establecer un sistema de notificación de incidentes. Para ello, establece un marco institucional donde se definen los roles y responsabilidades de los distintos actores implicados.

La utilización del **instrumento jurídico del real decreto-ley** fue motivado por el retraso en la transposición de la Directiva, ya que el plazo para su transposición se encontraba vencido desde el 9 de mayo de 2018.

Cabe resaltar que, en el **ámbito de aplicación** se incluyen, además de los servicios digitales que sean mercados en línea, motores de búsqueda en línea y servicios de computación en nube, los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y no solo los sectores establecidos en la Directiva.

En la siguiente figura 3-1 se muestra la comparativa entre sectores estratégicos de la *Ley 8/2011* (PIC) y sectores estratégicos de la *Directiva (UE) 2016/1148* (NIS)

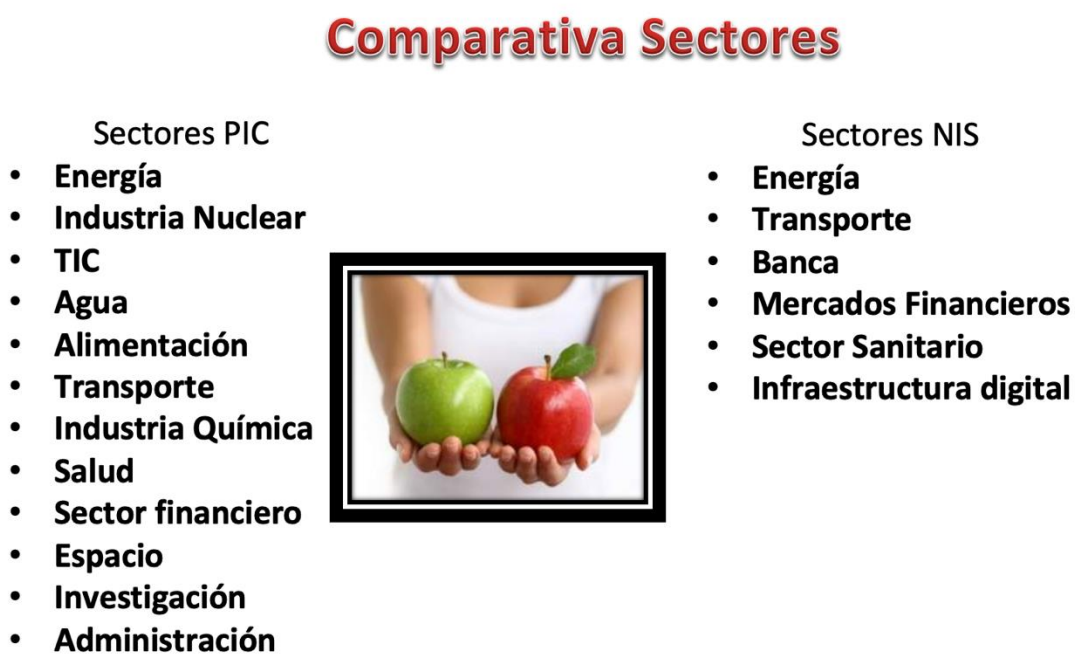

Figura 3-1 Comparativa sectores PIC vs. NIS. (fuente: composición del autor)

Otra novedad importante es la **competencia por territorialidad**, que viene a solucionar el problema de la globalización de las empresas, sobre todo de los grandes proveedores de servicios digitales, determinando que para los **operadores de servicios esenciales**, se entenderá establecidos en España, y por tanto les será de aplicación esta norma, cuando su residencia o domicilio social se encuentren en territorio español, y sea el lugar donde se centraliza la gestión administrativa y la dirección de sus actividades, además, los establecidos en otro país, si tienen en España un establecimiento permanente. En el caso de los **proveedores de servicios digitales**, será de aplicación para los que tengan su sede social en España y constituya su establecimiento principal en la Unión Europea, así como los que, no estando establecidos en la Unión Europea, designen en España a su representante en la Unión para el cumplimiento de la Directiva NIS.

En lo que respecta a la **identificación de los servicios esenciales y a los operadores de los mismos**, la norma vincula la relación de los servicios esenciales y de los operadores de dichos servicios a los identificados como operadores críticos, siempre y cuando tengan dependencia de las redes y sistemas de información para la provisión del servicio esencial que presta.

Solo en el caso de que dichos operadores no sean críticos, se identificarán por los efectos perturbadores significativos que pudiesen acarrear la degradación del servicio esencial que prestan, y que están relacionados con la **importancia del servicio prestado**, atendiendo a la disponibilidad de alternativas y a la valoración del impacto, y en relación al **número de afectados.**

Igualmente, para la revisión de los planes estratégicos, se vinculan a los planes estratégicos sectoriales de la Ley 8/2011, marcando una **estrecha dependencia entre ambas normativas**.

La norma queda alineada con la **Estrategia de Ciberseguridad Nacional** al enmarcar los objetivos y medidas al amparo de esta.

El modelo de determinación de las **Autoridades competentes**, cuyas funciones básicas serán de supervisión, control y ejercer la potestad sancionadora, asigna la competencia a la Secretaría de Estado de Seguridad del Ministerio del Interior para aquellos operadores de servicios esenciales que también sean operadores críticos conforme a la Ley 8/2011, siendo las Autoridades competentes para

el resto las sectoriales que se determinen reglamentariamente y que serán definidas en el reglamento de desarrollo próximo a publicarse.

Si los operadores de servicios esenciales pertenecen a la Administración Pública y no están incluidos en el catálogo de operadores críticos, la Autoridad será ejercida por el Ministerio de Defensa a través del Centro Criptológico Nacional.

Para los proveedores de servicios digitales, serán el Ministerio de Economía y Empresa, a través de la Secretaría de Estado de Avance Digital, quién ejerza de Autoridad competente.

Se establece al Departamento de Seguridad Nacional como **punto de contacto único** para la cooperación transfronteriza.

La norma recoge tres **CSIRT de referencia**, siendo para el Sector público el **CCN-CERT**, del Centro Criptológico Nacional, que, además, ejercerá la coordinación nacional de la respuesta técnica de los CSIRT en los supuestos de especial gravedad y que requieran un nivel de coordinación superior al necesario en situaciones ordinarias.

El **INCIBE-CERT** será el de referencia para entidades de derecho privado y, en los casos que afecten a operadores críticos, será operado conjuntamente con el CNPIC.

Por último, el **ESPDEF-CERT**, del Mando Conjunto del Ciberespacio, que cooperará con los otros dos CSIRT en aquellas situaciones que tengan incidencia en la Defensa Nacional.

Es importante destacar la obligación de los operadores de servicios esenciales y los proveedores de servicios digitales de **notificar a la autoridad competente**, a través del CSIRT de referencia, los incidentes que puedan tener efectos perturbadores significativos[11] en los servicios que proveen además de aquellas incidencias que presenten una situación potencial de peligro.

El texto también señala que las autoridades competentes y los CSIRT de referencia utilizarán una plataforma común para facilitar y automatizar los procesos de notificación, que actualmente se encuentra en fase de desarrollo.

La norma considera de especial interés la comunicación de incidentes, llegando incluso a proteger a los empleados y al personal que notifique dichos incidentes que no podrá sufrir consecuencias adversas en su puesto de trabajo o con la empresa.

Los operadores de servicios esenciales y los proveedores de servicios digitales tienen la obligación de resolver sus incidentes de seguridad, si bien podrán solicitar ayuda especializada, incluida la del CSIRT de referencia, cuando no los puedan resolver por sí mismos.

En cuanto a las **obligaciones de seguridad**, se establece que los afectados por esta norma deberán adoptar las medidas técnicas y de organización adecuadas para gestionar los riesgos que se planteen en el ámbito de sus responsabilidades, debiendo adoptar las medidas adecuadas para reducir al mínimo el impacto de los incidentes.

Será en el desarrollo reglamentario donde se especificarán las medidas mínimas de seguridad que han de establecerse, y que tendrán como base las recogidas en el Esquema Nacional de Seguridad, u otros esquemas específicos, sin perjuicio de que se tengan en consideración determinados estándares de seguridad de la información.

Para la interlocución entre los operadores de servicios esenciales y la Autoridad competente, se crea la figura del **Responsable de Seguridad de la Información.**

Para los proveedores de servicios digitales, las medidas son menos tasadas, abarcando los aspectos generales que han de abordar, como son la seguridad de los sistemas, la gestión de incidentes o la continuidad de negocio, entre otros.

Cabe hacer mención especial que este Real Decreto-Ley incluye un régimen sancionador que puede llevar multas de hasta un millón de euros para las faltas muy graves.

[11] En España esta cuestión se resolvió publicando la Guía Nacional de Comunicación y Gestión de Incidentes, donde existe un catálogo de incidentes que han de ser comunicados.

3.2.3 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.

Pese a que su importancia dentro de la protección de infraestructuras críticas es relativa, ese esquema ha sido de las primeras normas de ciberseguridad publicadas en España y se ha revelado como inspiradora de la normativa que se ha ido elaborando en nuestro país en los años siguientes.

El *Esquema Nacional de Seguridad* consta de 10 títulos y 44 artículos y tiene por objeto dar cumplimiento a lo establecido en el *artículo 42 de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos*, y determinar la política de seguridad que se ha de aplicar en la utilización de dichos medios electrónicos en el ámbito de la Administración Electrónica, para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

Los elementos principales del esquema son **seis principios básicos**, **15 requisitos mínimos** y **75 controles** (agrupados en organizativas, operacionales y de protección).

Los principios **básicos** que han de inspirar las actuaciones en materia de seguridad en los sistemas de información utilizados, como son la seguridad integral, la gestión de riesgos, la prevención, reacción y recuperación, las líneas de defensa, la reevaluación periódica y la función diferenciada.

Dichos principios básicos, han sido las bases de lo que será todo el entramado normativo posterior, por lo que merece la pena tratarlos someramente:

La norma entiende la **seguridad integral** como un proceso constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, prestando especial intención a la **concienciación** de todas las personas implicadas.

Establece la obligación de establecer una metodología de análisis y gestión de riesgos, adoptando MAGERIT como la metodología a emplear para dicha gestión.

MAGERIT es una metodología de análisis y gestión de riesgos elaborada por el antiguo Consejo Superior de Administración Electrónica (actualmente Comisión de Estrategia TIC), que responde a la necesidad de la Administración, de conocer y gestionar los riesgos de los, cada vea más numerosos sistemas de información utilizados para el cumplimiento de sus funciones, mediante una aproximación metódica que evite la improvisación y las valoraciones subjetivas de los analistas.

La metodología proviene de una adaptación del estándar internacional ISO *3001* donde se desarrolla un marco de trabajo para la gestión de riesgos. En la siguiente figura 3-2 se muestra el encaje de la metodología MAGERIT dentro del estándar.

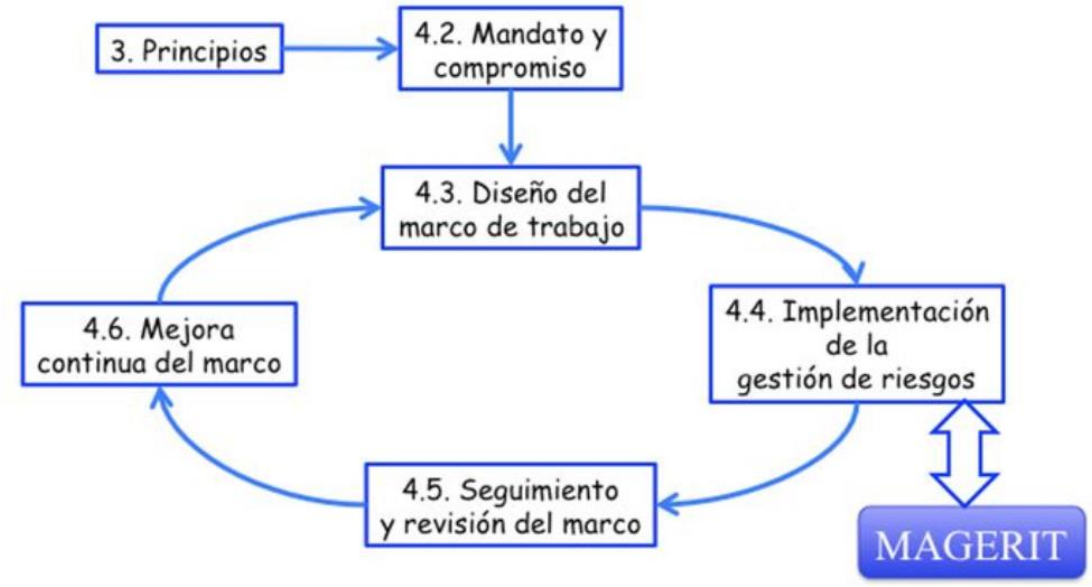

Figura 3-2 ISO 3001. Marco de trabajo para la gestión de riesgos. (fuente: www.administración electrónica. Gob.es)

Las **medidas de prevención, reacción y recuperación**, se valoran como un todo, relacionadas entre si para reforzar la seguridad, así, las medidas de prevención deberán reducir la posibilidad de que una amenaza se materialice, enlazándolas con las de reacción en el caso de que las primeras no hayan surtido efecto.

Por último, las medidas de recuperación permitirán la restauración de la información y los servicios en el menor tiempo posible, garantizándose la información, en cualquier caso.

La seguridad de los sistemas se encuentra articulada en múltiples líneas de defensa de carácter organizativo, físico y lógico, constituyéndose una **defensa en profundidad** que reduzca la probabilidad de que un ataque comprometa a todo el conjunto.

El sistema de seguridad se **reevaluará** y actualizará periódicamente, adecuándose a la constante evolución de los riesgos y a los sistemas de protección.

La seguridad se entenderá como una **función diferenciada** entre la responsabilidad de la información, la prestación de los servicios técnicos y la seguridad, contemplándose distintos roles como el responsable de la información, el responsable del servicio y el responsable de la seguridad.

El esquema establece unos **requisitos mínimos de seguridad** que emanan de una **política de seguridad** que han de poseer todos los órganos superiores de las Administraciones públicas y que han de estar aprobadas por su titular.

En dicha política, se habrán de recoger, como mínimo, los siguientes aspectos:

- Se deberá contar con una **organización de seguridad**, donde se identifique claramente a los responsables de la seguridad y sus funciones. Los procedimientos y las normas de seguridad han de ser conocidos por todos los miembros de la organización.
- Cada organización realizará su **propia gestión de riesgos** a los que se encuentran expuestos sus sistemas mediante una **metodología reconocida** internacionalmente y deberá existir una proporcionalidad entre las medidas adoptadas y los riesgos existentes.

- En cuanto a la **gestión de personal**, todo el personal relacionado con los sistemas de información deberá ser formado e informado de sus obligaciones en materia de seguridad y sus actuaciones deberán ser supervisadas para verificar que se siguen los procedimientos establecidos.
- De la seguridad de los sistemas de información, se deberán encargar **profesionales** que garanticen la misma desde su instalación, mantenimiento, gestión de incidencias y desmantelamiento.
- El **acceso a los sistemas** de información deberá ser controlado limitando el acceso de los usuarios a las funciones permitidas.
- Se deben **proteger las instalaciones** donde se encuentran los sistemas de información, mediante áreas separadas y cerradas con un control de acceso.
- El esquema valora positivamente la instalación de **productos certificados** en seguridad en base a las normas y estándares de mayor reconocimiento internacional, en los sistemas de información de la Administración.
- El diseño y la configuración de los sistemas atenderán al principio de **seguridad por defecto** los cuales proporcionarán la mínima funcionalidad requerida sin ninguna funcionalidad adicional deshabilitando desde su configuración las funciones que no sean utilizadas.
- Para mantener **íntegros y actualizados los sistemas**, todo elemento físico o lógico que vaya a instalarse, deberá ser autorizado previamente. El responsable de seguridad deberá ser consciente en todo momento del estado de seguridad de los sistemas, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten.
- Se debe proteger en todo momento la información en **tránsito** por entornos inseguros, así como a la **información almacenada** asegurando la recuperación y conservación a largo plazo.
- El sistema ha de proteger su perímetro, en particular, si existe **interconexión a redes** públicas.
- Se deben **registrar las actividades** de los usuarios, reteniendo la información necesaria que permita identificar en cada momento a la persona que actúa.
- Se registrarán los **incidentes de seguridad** que se produzcan y las acciones de tratamiento que se sigan para la mejora continua de la seguridad del sistema.
- Los sistemas establecerán los mecanismos necesarios para garantizar la **continuidad de las operaciones** en caso de un incidente que imposibilite la prestación normal del servicio.
- El proceso de seguridad implantado deberá estar inspirado en el proceso de **mejora de continua** de los sistemas de gestión de seguridad de la información.
- Para el **cumplimiento de los requisitos mínimos** se aplicarán las medidas de seguridad indicadas en este esquema, teniendo en cuenta los activos del sistema, su categoría y la gestión de los riesgos.
- Se contempla la utilización de **infraestructuras y servicios comunes** que habrán de cumplir los requisitos mínimos de esta norma.
- El Centro Criptológico Nacional, publicará distintas **guías de seguridad** de las tecnologías de la información y las comunicaciones.
- Las Administraciones públicas podrán determinar aquellos sistemas de información a los que **no les sea de aplicación** por tratarse de sistemas no relacionados con el objeto de este esquema.

En otro orden de cosas, el real decreto contempla la **auditoría bianual** ordinaria para comprobar el cumplimiento del esquema, y con carácter extraordinario cuando se produzcan cambios sustanciales en los sistemas.

Se contempla la elaboración regular de un **informe de seguridad de los sistemas**, que permita conocer el estado de seguridad de los mismos.

Se faculta al **Centro Criptológico Nacional**, a través del CCN-CERT para la respuesta ante incidentes de seguridad de la administración pública, además de para la divulgación de una serie de documentos de mejores prácticas de seguridad. Además, se le encomienda la formación destinada a los especialistas en ciberseguridad de la Administración, y a la emisión de alertas sobre vulnerabilidades o nuevas amenazas.

La **conformidad con el ENS** será publicitada a través de las correspondientes sedes electrónicas y a los distintivos de seguridad obtenidos en base a su cumplimiento.

Para modular el equilibrio entre las medidas de seguridad que se han de implantar y la importancia de la información que contienen los sistemas o del servicio que prestan, una vez analizados en cada una de las dimensiones de seguridad[12], se establecen tres **categorías.**

i. Se categorizará **nivel bajo**, cuando las consecuencias de un incidente supongan un **perjuicio limitado** sobre la organización o sobre los individuos afectados, como, por ejemplo, una reducción apreciable en la prestación del servicio, daños menores en los activos, el incumplimiento de alguna norma, que tenga carácter subsanable o un perjuicio menor reparable a un individuo.

ii. Un sistema será clasificado con **nivel medio** cuando las consecuencias de un incidente de seguridad supongan un **perjuicio grave** para la organización o sobre los individuos afectados. Ejemplos de perjuicio grave, serian una reducción significativa en la prestación del servicio, un daño significativo en los activos, el incumplimiento de una norma que no pueda ser subsanable o un perjuicio significativo a una persona de difícil reparación.

iii. Por último, será de **nivel alto** cuando las consecuencias supongan un perjuicio **muy grave** para la organización o sobre los individuos afectados. Un perjuicio grave sería, por ejemplo, la pérdida total del servicio, el daño muy grave o irreparable de activos de la organización, el incumplimiento grave de alguna ley o regulación, o causar a una persona un perjuicio grave de difícil o imposible reparación.

Para determinar la categoría de un sistema se hará en base al estudio de cada una de sus dimensiones de seguridad, clasificándose de **categoría alta** cuando alguna de sus dimensiones alcance el **nivel alto.** El mismo criterio se seguirá para los de nivel medio y nivel bajo con sus correspondientes niveles.

Cuando un sistema contenga informaciones de diferente nivel, se establecerá el nivel mayor.

En el Anexo II del real decreto, se establecen las medidas de seguridad a adoptar que habrán de ser **proporcionales a las dimensiones de seguridad y a la categoría del sistema** de información a proteger.

Las medidas de seguridad pueden ser de tres tipos: las relacionadas al **marco organizativo**, que contempla la organización estratégica, las relativas al **marco operacional**, relativa a procesos y procedimientos de seguridad, y por último las **medidas de protección** específicas para activos concretos.

[12] El ENS establece cinco dimensiones de seguridad: Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad. Éstas dos últimas no están reconocidas en ningún otro sistema de gestión de seguridad de la información, al entenderse que van implícitas en las anteriores.

Dicho anexo, se complementa con una serie de tablas donde se detallan cada una de las medidas de seguridad del catálogo que han de ser implementadas en base a la categoría del sistema.

A continuación, tabla 3-1 presenta las principales diferencias entre ambos esquemas de seguridad de la información.

ISO 27001	ENS
Estándar internacional sin rango legal	Norma legal española derivada de la ley 11/2007
Carácter voluntario	Obligación legal
Auditoría con interpretación flexible	Auditoría con interpretación rígida
Para todos los sistemas de información	Para los sistemas de la Administración Pública
Certificación de cumplimiento bianual	Declaración de conformidad bianual

Tabla 3-1. Comparativa de los esquemas ENS e ISO 27001(fuente: elaboración propia)

3.3 Normativa sectorial

Debido a la especificidad de cada uno de los doce sectores estratégicos que comprenden la normativa de protección de infraestructuras críticas, se muestra especialmente compleja su armonización.

Sectores con un alto desarrollo en las tecnologías de la información y la comunicación, como los del transporte o el sector financiero, tienen muy poco que ver con sectores de entorno más industrial, como el sector químico, o sectores con poco desarrollo tecnológico como el sector alimentario o el del agua.

A continuación, se hace un repaso a los sectores o subsectores más significativos en cuanto a su especificidad.

3.3.1 Sector financiero

El sistema financiero es clave en el desarrollo de un país. Un buen funcionamiento de los mercados e instituciones financieras, conlleva su mayor crecimiento ya que permite el desarrollo enconómico y garantiza las inversiones y los pagos, proporcionando un entorno seguro para los negocios.

La función principal del sistema financiero es la intermediación entre los agentes económicos que quieran prestar o invertir sus fondos disponibles y aquellos que necesitan dichos fondos para adquirir bienes u otros fines, que se realiza a través de entidades bancarias o del mercado de valores.

El sistema financiero español ha sufrido un proceso de transformación en las ultimas décadas que lo han convertido en un sistema internacionalizado, interconectado y complejo.

Las entidades financieras más importantes para la financiación de la economía española son las entidades de crédito, concretamente los bancos y las cajas de ahorros. Entre las funciones que realizan en la economía están la concesión de préstamos y créditos, los servicios de pagos, la emisión y gestión de otros medios de pago, la intermediación en los mercados interbancarios, así como el asesoramiento

y prestación de servicios a empresas en materia de estructura de capital, estrategia empresarial, adquisiciones y fusiones.

El Banco de España, como supervisor del sistema bancario, opera bajo el paraguas del Banco Central Europeo (BCE), que junto con los bancos centrales de los países de la Unión constituyen el Euro sistema, el cual define y ejecuta la política monetaria única.

Dentro del sistema financiero español cabe mencionar las bolsas de valores. Estos mercados canalizan importantes volúmenes de inversión, desde donde se dirigen y gestionan los mercados de valores y sistemas financieros en España, y se coordina los mercados de renta variable y fija, derivados y sistemas de compensación y liquidación.

En la figura 3-3 se muestra la complejidad del sector y la interrelación entre los distintos elementos que lo componen.

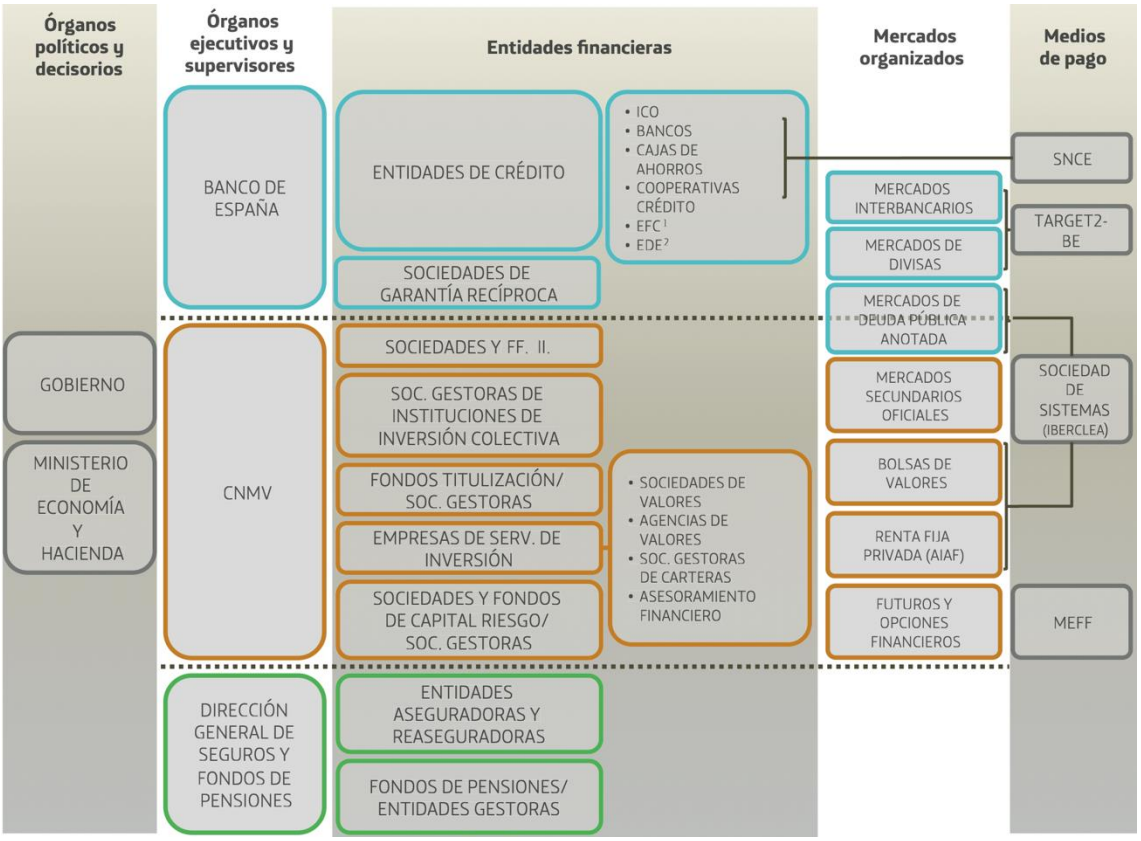

Figura 3-3. Estructura del sistema financiero español. (fuente Afi)

El desarrollo del sistema financiero está íntimamente ligado a la evolución de las TIC, pasándose del negocio de manejo de dinero al negocio de la gestión y procesamiento de información, donde las TIC se revelan como una parte indisoluble y esencial del negocio financiero.

El modelo de negocio, el aumento de la competencia, la adecuación al mercado único, así como el impulso de la innovación productiva y tecnológica, se basa en el uso intensivo de estas tecnologías.

La seguridad de este tipo de infraestructuras está muy focalizada en garantizar la seguridad de la información de sus sistemas tecnológicos, ya que un compromiso de los mismos, no sólo acarrearía grandes pérdidas económicas, sino que además supondría una merma en la confianza de un modelo de negocio basado en las transacciones económicas digitales, ya sea en la bolsa, en el mercado de valores, en la banca on-line, o mediante el uso de tarjetas bancarias o terminales TPV.

Según las estadísticas de Cibercriminalidad de 2019 del Ministerio del Interior, más del 80% de los ciberdelitos que se comenten en nuestro país, son estafas económicas en sus distintos ámbitos.

En la figura 3-4 se recogen distintos hitos tecnológicos del sector financiero donde se observa la temprana adopción de las TIC en este sector y lsu utilización de manera general en todo su modelo de negocio y en sus procesos.

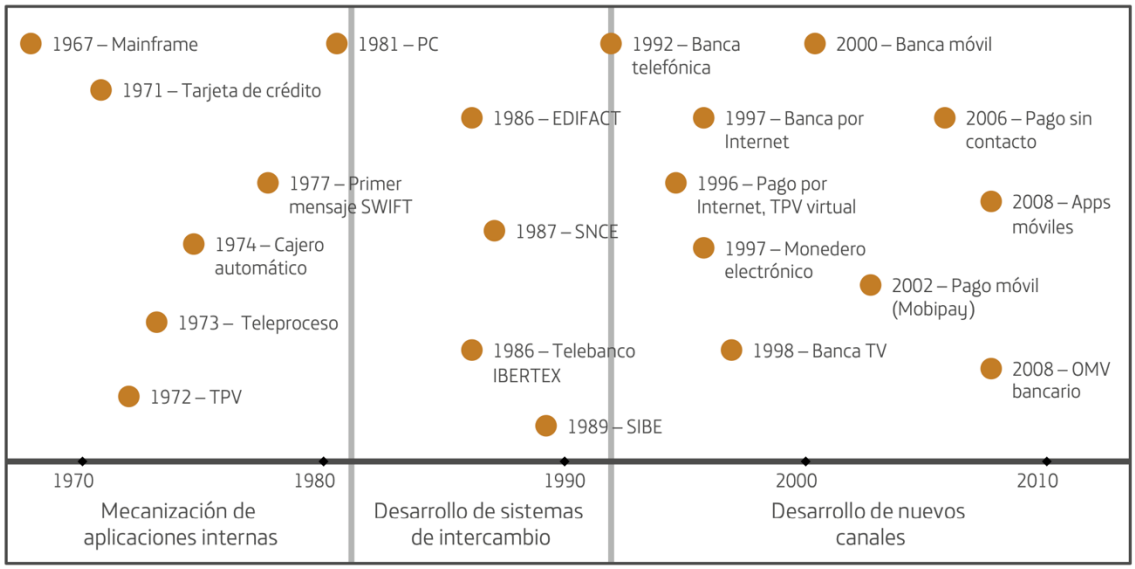

Figura 3-4. Hitos tecnológicos del sector financiero (fuente Afi)

3.3.2 Sector transportes. Subsector aéreo

El subsector de transporte aéreo es especialmente complejo, porque no sólo comprende los sistemas de control del tráfico o de la navegación aérea, sino además el control de pasajeros y mercancías en los aeropuertos y la seguridad de todo el conjunto, motivado por los distintos ataques terroristas que a lo largo del tiempo se han ido produciendo no sólo en aeropuertos sino en el interior de las aeronaves, ya sea mediante secuestros o colocación de artefactos explosivos o interceptación en vuelo buscando la enorme repercusión que estos incidentes producen en el mundo.

Sirvan como recordatorio un breve resumen de ataques a este sector:

- El primer atentado terrorista en un avión que se conoce se remonta a 1933. Se trataba concretamente de un vuelo de *United Airlines*, que partió de Newark con destino a Chicago. Las pruebas demostraron que fue una bomba compuesta de nitroglicerina la que estalló en el interior del aparato.
- En diciembre de 1988 se produjo la tragedia de Lockerbie, cuando, unos minutos después de despegar de Londres el vuelo 103 de Pan Am, explotó una bomba instalada en el interior de una grabadora dentro de una maleta. Los 259 pasajeros y 11 personas en tierra en Lockerbie (Escocia) murieron.
- En septiembre de 2001 dos aviones secuestrados por miembros de Al Qaeda se estrellaron contra la Torres Gemelas.
- En agosto de 2004 se cometió un doble atentado en Rusia donde dos aeronaves fueron destruidas en pleno vuelo por el estallido de dos artefactos explosivos cuya colocación fue atribuida por los servicios de seguridad rusos a activistas chechenos.

Este tipo de ataques, ha hecho que el enfoque en la seguridad se base en la seguridad física, sobre todo en el control de personas y materiales en los aeropuertos.

La Agencia Estatal de Seguridad Aérea (AESA), es la encargada de proveer la seguridad en todos los ámbitos de la navegación aérea, trabajado conjuntamente con el Centro Nacional de Protección de Infraestructuras Críticas y la Oficina de Coordinación de Ciberseguridad del Ministerio del Interior para la protección los servicios esenciales y de las infraestructuras críticas de este sector.

AESA ha elaborado distintas guías de seguridad operacional, donde se encuentran muy desarrolladas las medidas de seguridad físicas, pero no tanto las de seguridad lógica.

Desde la Agencia Europea de Seguridad Aérea (EASA), como consecuencia de la entrada en vigor de la Directiva NIS, se ha instado a la Autoridad española a la modificación de los reglamentos de navegación aérea para incorporar medidas de seguridad lógica en los sistemas de información que conforman todos los ámbitos del transporte aéreo y que están llamados a complementar los elaborados procedimientos de seguridad física.

Dicha modificación afectaría a los siguientes servicios:

i. El **servicio de control de tráfico aéreo** (ATC) prestado por controladores aéreos, que aplican separaciones entre los aviones y emiten autorizaciones de control a petición de los pilotos en función de las condiciones del tránsito y del entorno. Integra todos los centros de control de ruta, aproximación y aeródromo españoles, de forma que la gestión se realiza sobre datos coherentes y de una manera coordinada.

ii. Los **servicios de navegación aérea** que permiten pilotar eficientemente una aeronave a su lugar de destino, asegurando la integridad de los tripulantes, pasajeros, y de los que están en tierra, basada en la observación del cielo, del terreno, y de los datos aportados por los instrumentos de vuelo.

La navegación aérea, en algunos casos, necesita de instalaciones exteriores para poder realizar el vuelo, ya que por sí sola la aeronave no es capaz de navegar. Las radioayudas, de las estaciones de superficie o la navegación por satélite, necesitan de la protección de sus sistemas lógicos para evitar compromisos de seguridad.

iii. El **control de personas y mercancías en los aeropuertos**, se apoyan en medidas de seguridad soportadas por tecnologías de la información y comunicación. Ya sea para la gestión del equipaje, los controles de pasajeros, los circuitos cerrados de televisión, los controles de acceso a las instalaciones, son necesarios sistemas de información eficientes que garanticen la seguridad sin que provoquen retrasos en un sector tan estratégico para España debido no solo al incremento del número de pasajeros a lo largo del año, sino a la afluencia masiva en determinadas épocas del año como consecuencia del turismo.

3.3.3 Sector industria nuclear

Otro ejemplo muy significativo de la propia idiosincrasia de los sectores en el mundo de las infraestructuras críticas, la podemos encontrar en el sector de la industria nuclear.

Este sector, no sólo se basa en la producción eléctrica de las centrales nucleares, sino en el transporte y almacenamiento del material radioactivo, así como en el transporte y uso de dicho material en otros ámbitos, como por ejemplo en el ámbito sanitario.

La seguridad nuclear aborda los potenciales riesgos radiológicos de las instalaciones nucleares derivados de la manipulación y el almacenamiento de sustancias nucleares o del uso de la energía nuclear para la obtención de energía eléctrica, tanto en circunstancias normales como en caso de incidentes, con el fin de lograr la adecuada protección de los trabajadores, el público y el medio ambiente.

El Consejo de Seguridad Nuclear (CSN) es el órgano competente en la materia y establece la normativa que regula la seguridad nuclear en todas las fases de la vida de las instalaciones nucleares.

La regulación de la seguridad nuclear se centra especialmente en los aspectos físicos como el emplazamiento, diseño, construcción, operación y desmantelamiento de todas las instalaciones nucleares y se basa en la interposición de un conjunto de barreras físicas y administrativas contra los riesgos radiológicos potenciales. Para alcanzar y mantener un adecuado nivel de seguridad nuclear, el CSN exige además a los titulares de las instalaciones personal debidamente cualificado, un enfoque adecuado en materia de seguridad física y el establecimiento de una cultura de seguridad efectiva.

Este enfoque a la seguridad física a lo largo de los años, ha motivado el desarrollo de unos procedimientos muy elaborados y una enorme lista de normativa, no solo nacional sino también internacional, que regulan dichos aspectos de una manera muy completa.

No obstante, este enfoque partía de la premisa que eran instalaciones aisladas sin contacto con el exterior, por lo que no se contemplaba de manera específica el uso de las tecnologías de la información y la comunicación.

Esto no significa que no dispongan de sistemas informáticos, ya que la operación de las centrales nucleares se basa en sistemas informáticos de operación industrial (OT). Dichos sistemas de operación, permiten la producción automatizada y el control de los procesos de las centrales nucleares.

El **enfoque de la seguridad** en los sistemas OT, en un entorno de trabajo con máquinas y dispositivos, la importancia de la seguridad se ha centrado en la protección del medio ambiente, las personas y las infraestructuras ante posibles fallos en la continuidad de la actividad que desarrollan.

Sin embargo, en los sistemas con tecnologías de la información (IT), la seguridad se basa en proteger la información con respecto a cualquier tipo de riesgo ya sea personal, técnico, de origen natural etc.

Si bien ambos enfoques de seguridad buscan proteger la Confidencialidad, Integridad y Disponibilidad de la información de los sistemas en sus entornos se persiguen los objetivos de manera diferente. Mientras que en los entornos IT la confidencialidad de la información es el aspecto más importante a proteger, en los entornos OT es la disponibilidad el aspecto con mayor importancia, ya que una parada de servicio en sus sistemas puede ocasionar un impacto económico muy importante.

En la figura 3-5 se pueden observar gráficamente estos conceptos.

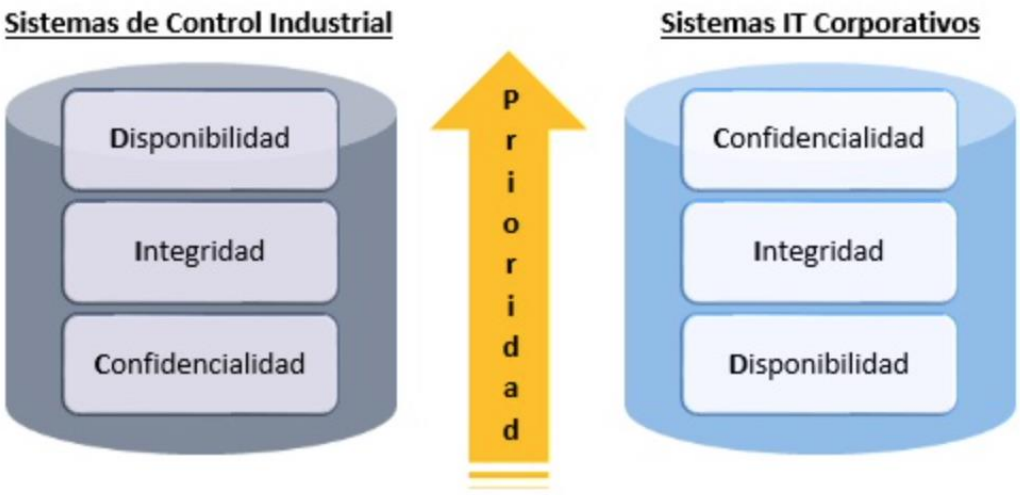

Figura 3-5. Comparativa OT vs IT (fuente INCIBE)

Consecuentemente, el problema que presentan estos sistemas, es que en su diseño no se pensó en la seguridad, ya que tradicionalmente su uso ha sido en entornos muy cerrados y controlados.

Tampoco están diseñados para una actualización de parches de seguridad permanente, y que las paradas de producción son especialmente costosas o directamente inasumibles.

La integración con sistemas de información y la telecomunicación es cada vez mayor, por lo que se están revelando carencias de seguridad de unos con respecto de otros a la hora de interconectar ambos entornos.

Si además consideramos que los sistemas OT han sido diseñados para un uso continuado de entre 20 a 30 años debido a las importantes inversiones que son necesarias para su renovación, nos encontramos con un importante problema de seguridad que ha de ser mitigado con medidas compensatorias que minimicen los riesgos a las vulnerabilidades presentadas.

3.3.4 Sector energía. Subsector eléctrico

Si existe un sector crítico por excelencia, es el sector de la energía, y especialmente el subsector de la energía eléctrica. Esto es así porque el resto de servicios esenciales no podría proveerse sin una fuente continuada y estable de energía eléctrica, mostrándose como un sector con el que tienen interdependencias el resto de los servicios esenciales.

La generación y distribución de energía eléctrica son dos aspectos que guardan un delicado equilibrio, ya que una generación de energía superior a lo que las redes de distribución pueden gestionar generaría una sobretensión en la misma, que podría ocasionar la caída del sistema.

Por otro lado, una generación de energía insuficiente, provocaría fallos en la distribución o directamente la indisponibilidad de abastecimiento.

La interconexión de redes entre países todavía ha acentuado más la complejidad de la gestión del suministro eléctrico.

Para una correcta gestión existen las **redes de distribución inteligentes** o *smarts grids*, que utiliza la tecnología informática para optimizar la producción y la distribución de electricidad, con el fin de equilibrar mejor la oferta y la demanda entre productores y consumidores, incluyendo las energías alternativas. Esto convierte a estos sistemas en objetivo de especial atención para ataques cibernéticos.

Conscientes de su importancia, buena parte de los esfuerzos realizados en el ámbito de la ciberseguridad están centrados en los sistemas de distribución de energía y especialmente en las redes de distribución inteligentes.

La directiva del Consejo de la Unión Europea (2008/114/EC) ya sugería la importancia protección de las redes eléctricas.

En este sentido, la Comisión Europea constituyó en 2009 el *Smart Grid Task Force (SGTF).* Este organismo ha publicado recomendaciones relativos a la estandarización de los sistemas eléctricos y la seguridad y privacidad de los usuarios.

Entre los documentos generados por la *SGTF* destacan los siguientes:

- *Smart Grid Reference Architecture.*
- *Smart Grid Information Security.*
- *Inventory of EU Smart Grid projects.*

El *Joint Research Center* de la Comisión Europea que es un grupo que trabaja para mejorar la seguridad de las redes de distribución inteligentes cuyo objetivo principal es proporcionar el conocimiento técnico y el asesoramiento científico necesarios para implantar las distintas políticas establecidas por la Unión Europea sobre el sector eléctrico.

Su actividad gira en torno a la obtención y proceso de datos sobre redes de energía, asesoramiento sobre aspectos relacionados con las *smart grids* y la difusión y cooperación con los principales actores.

Tres años después, ENISA publicó un informe de recomendaciones para los Estados Miembros de la Unión Europea sobre la seguridad en *smart grids*, donde se detalla el estado actual de las redes inteligentes de distribución europeas y realiza una serie de propuestas como la mejora del marco regulatorio, la promoción de la colaboración público-privada en materia de seguridad, la promoción de

la concienciación y la formación, promover investigaciones para la mejora de la seguridad o implicar a los CERTs europeos para apoyo y asesoramiento, entre otras.

Dentro del ámbito de la Directiva NIS, el Grupo de Cooperación, cuyo objetivo es proponer la dirección estratégica para la implantación de la directiva, ha creado un grupo de trabajo para proponer mejoras en la seguridad de las redes y sistemas de información del sector de la energía, con propuestas alineadas con las del informe de ENISA del párrafo anterior.

3.4 Estándares internacionales

3.4.1 La ISO/IEC 27001. Sistema de gestión de seguridad de la información

La *Norma ISO/IEC 27001* es una norma desarrollada por la Organización Internacional de Normalización (ISO) como metodología la implementación de un sistema de gestión de la Seguridad de la Información en una organización, resultado de la adaptación de la norma de estandarización británica BS 7799-2.

Actualmente a nivel mundial la norma ISO 27001 es la norma de referencia para certificar la seguridad de la información en las organizaciones. En España el número de certificaciones rondan las 800, ascendiendo a un total de más de 33.000 los certificados a nivel mundial.

Este estándar sirve de guía para establecer de manera coordinada la comunicación entre las partes de una organización relacionadas con la seguridad de los sistemas, a crear una cultura de seguridad en la organización y optimiza la gestión de la seguridad a través de la **evaluación y la mejora continua** como se muestra en la figura 3-6, mediante la realización de auditorías internas, acciones correctivas y preventivas y auditorías de cumplimiento.

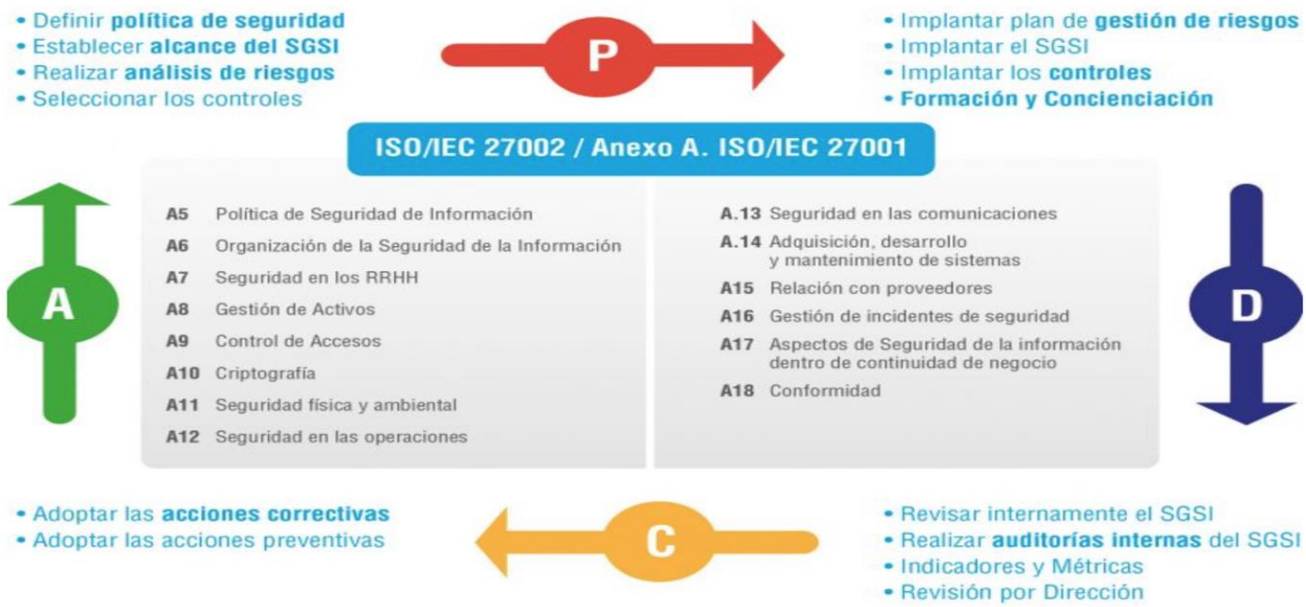

Figura 3-6. Ciclo de mejora continua. (fuente www.aenor.com)

La demostración de su cumplimiento, ante una entidad acreditada, da lugar a una **certificación** qué se ha de renovar bianualmente.

La norma consta de un catálogo de **114 controles de seguridad,** recogidos en la norma *ISO 27002*, que la organización deberá seleccionar de acuerdo con su **documento de aplicabilidad**, dónde se ha de hacer constar que controles no aplican y el motivo.

Dichos controles se estructuran en los siguientes **dominios**:

- **Política de seguridad.** Como pilar del sistema de gestión se ha de publicar un documento de alto nivel donde la dirección se comprometa a la consecución de unos objetivos globales y el alcance de la misma, entre otras cuestiones.
- **Organización de la seguridad**. Aquí se establece la necesidad de dotar a la organización de una estructura de seguridad con roles y responsabilidades perfectamente definidas y que involucre a todas las áreas de la misma.
- **Administración de Activos**. En este apartado se dan pautas para el control de los activos de información, asignando responsables para cada uno de ellos, de tal forma que la organización tenga un control exhaustivo de dónde se encuentra la información y quién es responsable de la misma.
- **Seguridad de los Recursos Humanos**. En este dominio se establecen los requisitos para garantizar la seguridad entre las personas de la organización desde el momento de su contratación y su etapa productiva, hasta el de su cese de actividad.
- **Seguridad Física y Ambiental**. En este aparatado se consideran los factores físicos y ambientales relacionados con los sistemas de información de la organización, como son la temperatura y humedad que podrían afectar a la electrónica de los activos o la seguridad física del centro de proceso de datos dónde se alojan, introduciendo el concepto de perímetro de seguridad física.
- **Gestión de Comunicaciones y Operaciones.** En este apartado se establecen procedimientos y responsabilidades para una correcta gestión en la comunicación organizacional que permitan la comunicación y la operación de todos los recursos de tratamiento de la información con garantías.
- **Sistema de Control de Accesos.** Los controles de este dominio dan una serie de orientaciones sobre la manera en la que se ha de controlar el acceso a los sistemas, partiendo del principio de la *necesidad de conocer* para garantizar la confidencialidad, pero atendiendo de manera equilibrada a los requisitos de seguridad y de negocio.
- **Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.** En este dominio se reflejan las buenas prácticas que se han de observar para la adquisición de elementos *software* o *hardware* previo análisis de los requisitos de seguridad, el desarrollo de software inspirado en el principio de la *seguridad por diseño* y el mantenimiento de los sistemas de información.
- **Administración de Incidentes de Seguridad de la Información**. Este dominio marca las pautas a seguir para que la organización pueda gestionar de manera correcta los eventos e incidentes de seguridad y además pueda establecer mecanismos de lecciones aprendidas que faciliten la resolución de incidentes futuros.
- **Plan de Continuidad del Negocio.** En este apartado se exige a la organización la elaboración de un plan que permita la continuidad de la actividad en caso de un incidente de seguridad que imposibilite el funcionamiento normal de los servicios.
- **Cumplimiento normativo.** Este último apartado busca evitar los incumplimientos de cualquier norma civil o penal, o cualquier otra regulación u obligación contractual, incluidas las medidas de seguridad.

3.4.2 La serie NIST 800

El Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST) tiene como misión la promoción de la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida.

En el ámbito de sus competencias, el NIST tiene publicada la serie *NIST 800*, que es un conjunto de documentos que describen las políticas, procedimientos y directrices de seguridad informática del gobierno federal de los Estados Unidos. Los documentos están disponibles de forma gratuita y pueden ser útiles para las empresas e instituciones educativas, así como para las agencias gubernamentales.

Las publicaciones de la serie *NIST 800* han ido evolucionando como resultado de la investigación de métodos viables y eficaces en función de los costes para optimizar la seguridad de los sistemas y redes de tecnología de la información. Las publicaciones abarcan todos los procedimientos y criterios recomendados por la NIST para evaluar y documentar las amenazas y vulnerabilidades y para aplicar medidas de seguridad a fin de reducir al mínimo el riesgo de incidentes. Las publicaciones pueden ser útiles como directrices para la aplicación de las normas de seguridad y como referencias jurídicas en caso de disputas judiciales relacionadas con cuestiones de seguridad.

Las publicaciones abarcan diferentes cuestiones de la ciberseguridad como, por ejemplo, la guía de seguridad en el correo electrónico (800-45), o la seguridad en *firewalls (800-41)*, la seguridad en servidores WEB (800-44), o la última publicación de requerimientos de seguridad para dispositivos IoT (*Internet of Things*) que es un borrador de fecha de 15 de diciembre de 2020 con número 800-213, entre muchísima documentación que se puede consultar en su página WEB[13].

Además, emite informes con el nombre *NISTIR* de distintas cuestiones de ciberseguridad donde entran al detalle de determinados aspectos, como por ejemplo la *NISTIR 7176* donde se establecen las cuestiones más relevantes sobre la seguridad de los sistemas de control industrial, o la *NISTIR 7628* que aborda la seguridad de las redes inteligentes de distribución de energía eléctrica, no sólo las cuestiones técnicas, sino también la cuestión de la privacidad de los usuarios.

Estas guías de la serie 800, así cómo los infomes que publica, pese a ser fuente de inspiración, no sólo para las certificaciones internacionales en ciberseguridad de carácter privado, sino también para la reglamentación europea en esta materia, **no están demasiado extendidas en nuestro entorno**.

Europa en su conjunto, y los países de manera particular, lo que suelen hacer es un análisis y una interpretación de toda esa normativa para la elaboración de una normativa propia más adaptada a las necesidades y requerimientos europeos.

El volumen de información de una normativa tan prolífica, nos impide entrar en más detalle sobre la misma, ya que el objeto de este trabajo es apuntar las distintas normativas que, de manera directa o indirecta, regulan la ciberseguridad de las infraestructuras críticas en nuestro país.

La figura 3-7 muestra de manera gráfica la interrelación de los elementos de la serie NIST 800, enfocados a los pasos para el establecimiento de un marco para la gestión de riesgos.

[13] https://csrc.nist.gov/publications/sp800

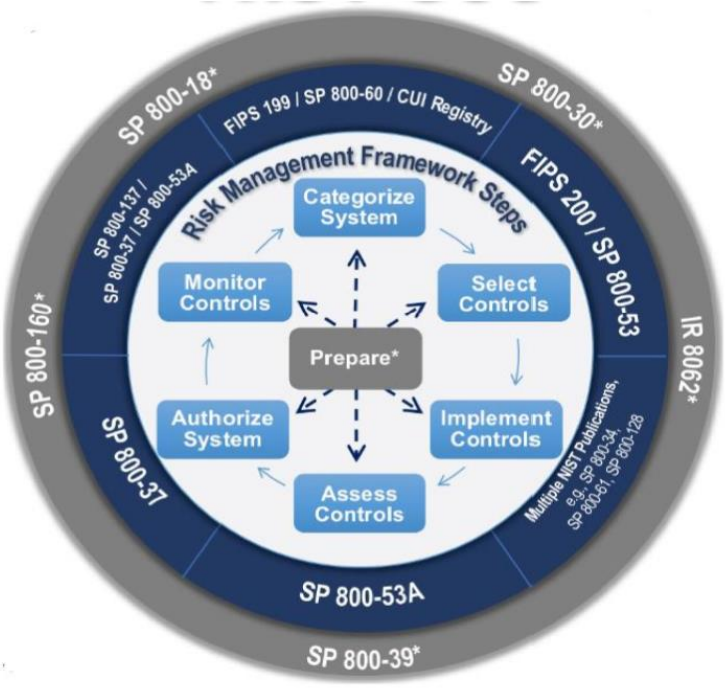

Figura 3-7. Serie NIST 800 (fuente www.nist.gov)

3.4.3 Los Criterios Comunies para la evaluación de la Seguridad de la Tecnología de la Información (Common Criteria)

Los Criterios Comunes para la Evaluación de la Seguridad de la Tecnología de la Información (*Common Criteria*, *CC*) y la Metodología Común para la Evaluación de la Seguridad de la Tecnología de la Información (*Common Methodology for Information Technology Security Evaluation CEM*) que los acompaña, son la base técnica de un acuerdo internacional denominado Acuerdo de Reconocimiento de Criterios Comunes (*Common Criteria Recognition Arrangement*, *CCRA*), que permite garantizar que los productos de seguridad son evaluados por laboratorios competentes e independientes autorizados para determinar el cumplimiento de determinadas propiedades de seguridad.

Para ello, dentro del proceso de certificación de criterios comunes, se elaboran documentos de apoyo que definen cómo se aplican los criterios y los métodos de evaluación a la hora de certificar tecnologías específicas.

La certificación de las propiedades de seguridad de un producto, que se basa en el resultado de su evaluación, han de ser reconocidos por todos los signatarios del CCRA.

Para la adquisición de un producto de seguridad de la TIC que maneje información nacional clasificada en nuestro país, debe ir precedida de un proceso de comprobación de que las medidas de seguridad del producto son adecuadas para proteger esa información. Esta responsabilidad está asignada al Centro Criptológico Nacional (CCN) mediante el *RD 421/2004 de 12 de marzo*.

Este Organismo de Certificación (OC), en relación con la certificación funcional de la seguridad de las tecnologías de la información, se articula mediante el, *Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, aprobado por la Orden PRE/2740/2007de 19 de septiembre*, complementado por una normativa interna propia adaptada a los requisitos necesarios para ser reconocido tanto a nivel nacional, según la norma *UNE-EN ISO/IEC 17065*, como a nivel internacional, según el "*Common Criteria Certificate Recognition Agreement" (CCRA*), como organismo de certificación de la seguridad de las TIC.

En su portal WEB[14] está disponible toda la información sobre la situación de la CCRA, la CC y los planes de certificación, los laboratorios autorizados, los productos certificados y la información, las noticias y los eventos relacionados.

En la figura 3-8 se muestran de manera gráfica los países miembros que están habilitados para autorizar la emisión de certificados a la izquierda y los países que tienen reconocido este estándar a la derecha.

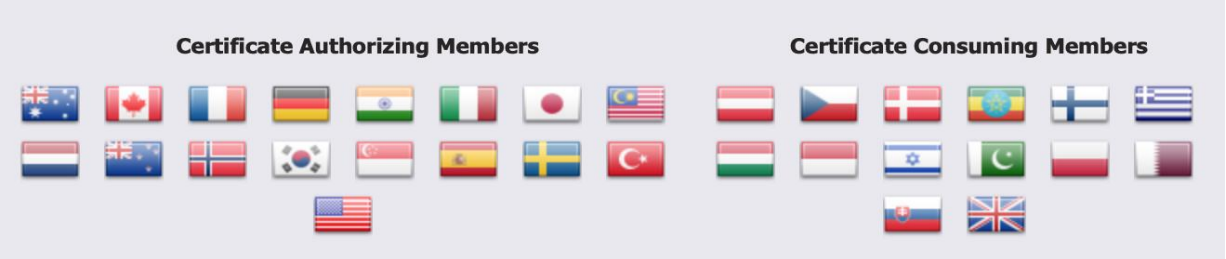

Figura 3-8. Países firmantes y consumidores de Common Criteria (fuente www.commoncriteriaportal.org)

A modo de resumen, se refleja en la figura 3-9 la principal normativa que regula la ciberseguridad de las infraestructuras críticas.

En cuanto a la normativa sectorial es tan extensa y de carácter tan específico, que excede el propósito de este trabajo, por lo que no se ha considerado en el mismo.

LEGISLACIÓN EUROPEA	LEGISLACIÓN ESPAÑOLA	ESTÁNDARES INTERNACIONALES
Directiva 2008/114/CE	Ley 8/2011 y RD 704/2011	ISO/IEC 27001
Directiva (EU) 2016/1148	R.D-L 12/2018 y RD sin publicar	NIST 800
Reglamento (EU) 2019/881	R.D. 3/2010	COMMON CRITERIA

Figura 3-9. Cuadro resumen de principal normativa y estándares para la seguridad en infraestructuras críticas (fuente: elaboración propia)

[14] https://www.commoncriteriaportal.org

4 LA CONVERGENCIA DE LOS SERVICIOS ESENCIALES

La existencia desde 2011 de la *Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas*, así como la *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*, complementada mediante la elaboración por parte del CNPIC de las *Guías de Buenas Prácticas para la elaboración de los Contenidos Mínimos de los Planes de Seguridad del Operador* y *Guías de Buenas Prácticas para la elaboración de los Contenidos Mínimos de los Planes de Protección Específicos*, donde se dan una serie de líneas maestras para la correcta elaboración de los mencionados planes, habían creado una estructura normativa muy robusta para la seguridad de las infraestructuras críticas, que a lo largo de los años ha ido consolidándose y perfeccionándose.

Dicha normativa, además, se encuentra armonizada con el *Plan de Prevención y Protección Antiterrorista (PPPA)* que da las directrices generales para asegurar la detección, seguimiento, análisis y evaluación continuada del riesgo de atentado terrorista, así como la puesta en marcha y la coordinación de los dispositivos preventivos que sean necesarios.

Las medidas del *PPPA* están dirigidas a la protección de instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales, así como a centros y organismos públicos u oficiales, u otros activos, cuya destrucción, ataque o degradación suponga un daño importante a la vida humana, la vulneración de derechos fundamentales, la afectación al normal funcionamiento de las instituciones o de los sectores estratégicos, afectación al orden público o la convivencia, impacto público, social o simbólico y pérdidas económicas o patrimoniales.

En dicho plan se establece el *Nivel de Alerta Antiterrorista* consistente en una escala compuesta por varios niveles cada uno de los cuales se encuentra asociado a un grado de riesgo, en función de la valoración de la amenaza terrorista que se aprecie en cada momento. La clasificación prevista en el Plan de Prevención y Protección Antiterrorista cuenta con cinco niveles de activación siendo el Nivel 1 correspondiente a riesgo bajo, el Nivel 2 a riesgo moderado, el Nivel 3 a riesgo medio, el Nivel 4 a riesgo alto y el Nivel 5 a riesgo muy alto. En el momento de escribir este trabajo (enero de 2021), nos encontramos en el Nivel 4.

Este panorama se ve afectado como consecuencia de la publicación de la entrada en vigor de la *Directiva (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 en la Unión* y de la transposición de la misma a la normativa española mediante la publicación del *Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información*, ya que esta disposición europea legisla sobre determinados aspectos de la normativa española anterior, que continúa plenamente en vigor, como son la mencionada *Ley 8/2011*, la *36/2015, de 28 de septiembre, de Seguridad Nacional, y con el 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*, como normativa especial en materia de seguridad de los sistemas de información del sector público.

Se atribuye al Consejo de Seguridad Nacional la función de actuar como punto de contacto con otros países de la Unión Europea y un papel coordinador de la política de ciberseguridad a través de la Estrategia de Ciberseguridad Nacional donde sienta las prioridades, objetivos y medidas adecuadas para alcanzar y mantener un elevado nivel de seguridad de las redes y sistemas de información.

Por tanto, se hace necesaria la coexistencia de todas estas legislaciones a la hora de su transposición, para salvaguardar por un lado su cumplimiento normativo y por otro, la seguridad jurídica, evitando contradicciones en las normas o la doble exigencia de determinadas obligaciones, teniendo en cuenta que la Directiva NIS concierne sólo a la ciberseguridad, no entrando a valorar los aspectos de seguridad física.

Para asegurar esta coexistencia, la transposición española de la norma, en su **ámbito de aplicación**, no sólo tuvo en cuenta los seis sectores estratégicos comprendidos en el ámbito de la Directiva NIS, sino que asimiló los doce sectores estratégicos de la normativa para la protección de infraestructuras críticas (PIC).

También se apoya en ella para definir el concepto de **servicio esencial,** y se atribuye a sus órganos colegiados la determinación de los servicios esenciales y de los operadores de servicios esenciales sujetos al real decreto-ley de tal forma que, para la **identificación de los servicios esenciales y el nombramiento de los operadores que los prestan (OSE)**, se utilizan los mismos procedimientos y los mismos actores, lo que ha supuesto la equivalencia entre operador crítico y operador de servicios esenciales, facilitando enormemente los procesos de identificación y nombramiento.

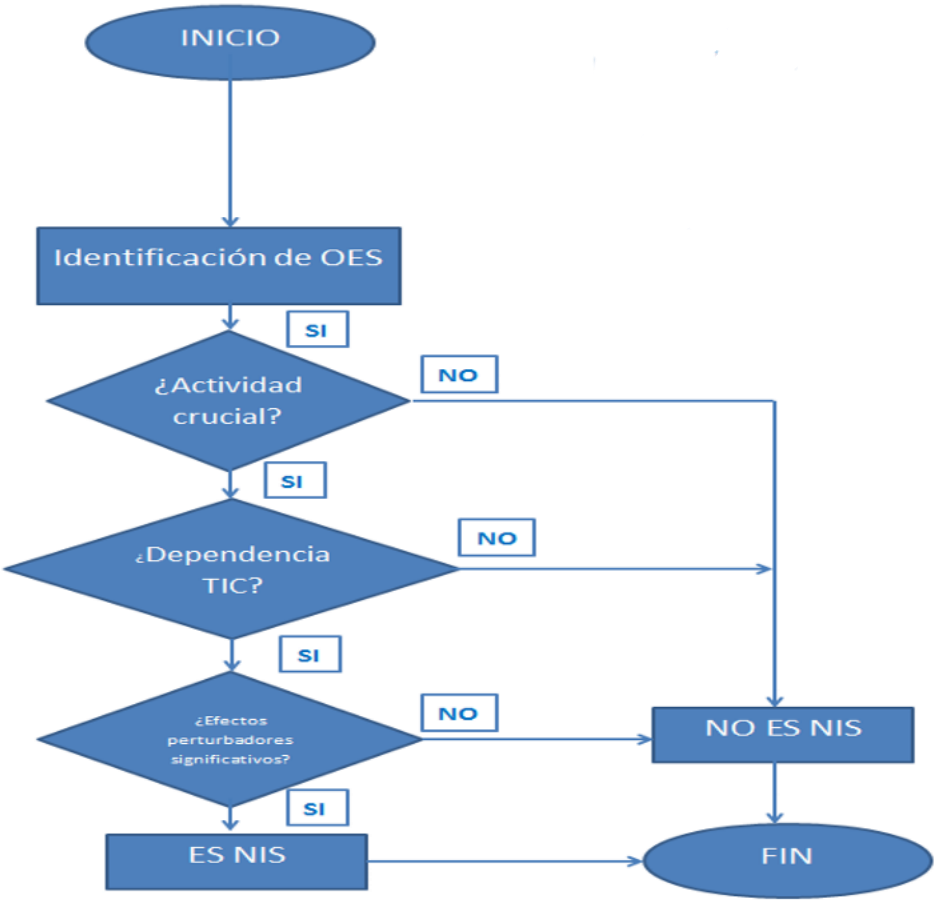

Figura 4-1 Metodología para la identificación de operadores de servicios esenciales (fuente OCC)

Así, las Autoridades competentes siguen siendo sectoriales y es el Grupo de Trabajo Interdepartamental el que se va a encargar de identificar los servicios esenciales, que serán aprobados por la Comisión Nacional para la Protección de Infraestructuras Críticas, que es un órgano colegiado interministerial.

Ambas normativas, la PIC y la NIS, se complementan en distintos aspectos como son la regulación de las **principales figuras responsables de la seguridad**.

La normativa PIC habla del ***Responsable de Seguridad y Enlace (RSE),*** recogido en el *artículo 16 de la Ley PIC,* cuyo nombramiento es obligatorio para los operadores críticos y ha de ser comunicado al Ministerio del Interior, y que debe contar con la habilitación de Director de Seguridad o equivalente, con las funciones recogidas en el *artículo 34 del reglamento PIC* de representación ante la Secretaría de Estado de Seguridad en todas las materias relativas a la seguridad de sus infraestructuras y los diferentes planes de seguridad.

Igualmente, se contempla la designación de un ***Delegado de Seguridad*** por cada una de las infraestructuras críticas identificadas como responsable de la seguridad de la misma.

El artículo 25 del mencionado reglamento, da un enfoque integral de la seguridad para los Planes de Protección Específicos de las Infraestructuras, considerando la seguridad desde su aspecto físico y lógico, lo que hace pensar que estas figuras deberían ser los responsables de ambos aspectos.

No obstante, la realidad es que estos responsables de seguridad han necesitado de personal especialmente cualificado para la seguridad lógica de los sistemas, siendo la figura del CISO[15] la que tradicionalmente se ha encargado de estas cuestiones.

Estas figuras se ven complementadas por la figura del ***Responsable de Seguridad de la Información*** (***RSI)*** recogida en el *artículo 16.3 del R.D-L 12/2018* donde se establece la obligación a los operadores de servicios esenciales de designar y comunicar a la autoridad competente, la persona, unidad y órgano colegiado responsable de la seguridad de la información y que actuará como punto de contacto y de coordinación técnica con la misma.

En el borrador del reglamento de desarrollo del real decreto-ley se recogen las funciones de esta figura que, en esencia, son las **funciones típicas de un CISO,** en un intento de regular normativamente a esta figura.

Por último, caben destacar las diferencias entre ambas normativas que han de ser armonizadas.

Un aspecto a considerar es el **distinto alcance** a la hora de considerar los sistemas de información que han de ser evaluados. Mientras que en la normativa PIC se circunscriben al servicio esencial por el que han sido nombrados operadores críticos, en la normativa NIS, se consideran todos los servicios esenciales que prestan, independientemente de cual sea el servicio esencial por el que fue nombrado crítico. Esto ha ocasionado que, para dar cumplimiento a esta última normativa, se hayan de considerar un mayor número de sistemas a evaluar, lo que supone un esfuerzo adicional a los operadores con el consiguiente coste económico

Para establecer criterios únicos de actuación y limitar los sistemas que han de ser evaluados, el CNPIC editó un Documento de Aplicabilidad de Sistemas que difundió a los operadores de servicios esenciales, donde se identificaban tres grandes grupos de sistemas de información.

Por un lado, se contemplan los sistemas de información que participan activamente en la provisión del servicio esencial. Otro grupo son los sistemas, que, no participando activamente, un compromiso de seguridad podría afectar a la provisión del servicio de manera indirecta. Por último, se considera un tercer grupo de sistemas que no están incluidos en los dos grupos anteriores.

En un primer momento, sólo se consideran los del primer grupo de sistemas, que está compuesto por los sistemas de operación, los de control, los de comunicaciones y los que proveen seguridad a los anteriores.

Las **exigencias de seguridad** también son distintas. Mientras en el ámbito PIC se han de tener diseñados unos planes de seguridad por parte de los operadores, denominados *Planes de Seguridad del Operador y Planes de Protección Específicos,* donde se asume la obligación de estos de colaborar en materia de seguridad, implantando las medidas de seguridad correspondientes, y que vienen reflejadas en las Instrucciones del Secretario de Estado de Seguridad de *Guías de Contenidos Mínimos,* la normativa NIS establece la obligación de la elaboración de un análisis de riesgos, la obligación de la notificación a la Autoridad competente de los incidentes con efectos perturbadores significativos y el cumplimiento de una serie de medidas de seguridad, recogidas en el futuro reglamento de desarrollo del real decreto-ley, y que tendrán como base las del *Esquema Nacional de Seguridad,* o las de otros esquemas de certificación más específicos, sin perjuicio de normas y estándares internacionalmente reconocidos.

En lo que respecta la **notificación de incidentes de ciberseguridad**, para evitar la complejidad en la normativa, se ha editado una *Guía Nacional de Notificación y Gestión de Ciberincidentes*[16] que recoge la taxonomía de los incidentes en el ámbito de la ciberseguridad, su gravedad en base a la

[15] *Chief Information Security Officer*

[16] https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

peligrosidad y el impacto, y los procedimientos para su comunicación a la Autoridad competente. Esta guía ha servido también para normalizar la comunicación de los ciberincidentes en el ámbito PIC.

Por último, cabe destacar que la normativa NIS, a diferencia de la PIC, contempla un **régimen sancionador** para el incumplimiento de las obligaciones de la misma.

En la figura 4-2 podemos encontrar la pirámide normativa para la protección de las infraestructuras críticas, donde en la cúspide se muestra la ley y su desarrollo reglamentario y de forma descendiente y de manera jerarquizada, los distintos planes de seguridad.

Figura 4-2 Pirámide de normativa de seguridad PIC (fuente: CNPI

La tabla 4-1 muestra los ciberincidentes reportados en el 2020 en las infraestructuras estratégicas, clasificados por sector estratégico.

SECTOR ESTRATÉGICO	CIBERATAQUES 2020
Administración	1308
Espacio	1
Industria nuclear	17
Investigación	0
Agua	1724
Energía	72
Salud	6
Industria química	8
TIC	139
Transporte	4440

Alimentación	16
Sistema financiero	2549

Tabla 4-1. Ciberataques a infraestructuras enero-septiembre 2020 (fuente: elaboración propia con datos del Ministerio del Interior)

En la tabla 4-2 podemos observar la clasificación de la peligrosidad de los ciberataques a dichas infraestructuras:

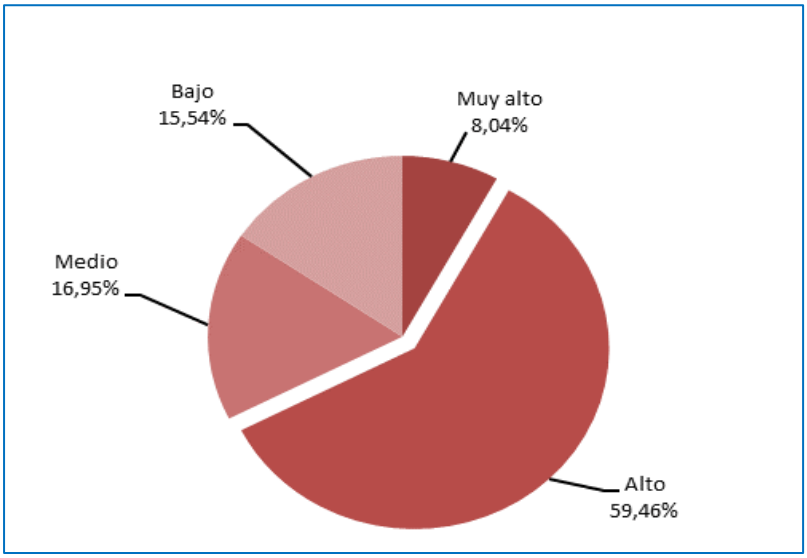

Tabla 4-2. Ciberataques a infraestructuras enero-septiembre 2020 por peligrosidad (fuente: Mº Interior)

5 LA GOBERNANZA DE LA CIBERSEGURIDAD

5.1 La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional

La *Ley de Seguridad Nacional* consta de cinco títulos y veintinueve artículos y tiene por objeto regular los principios básicos y los principales actores de la Seguridad Nacional. Además, crea el Sistema de Seguridad Nacional y establece los criterios para la gestión de una crisis y la contribución de recursos a la Seguridad Nacional.

Define la *Seguridad Nacional* como la acción del Estado dirigida a proteger la libertad, los derechos y bienestar de los ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así´ como a contribuir a la seguridad internacional en el cumplimiento de los compromisos asumidos.

Establece la obligación a las Administraciones Públicas y a los ciudadanos de participar, en base a sus competencias, en la *Política de Seguridad Nacional*, que es una política pública bajo la dirección del presidente del Gobierno y la responsabilidad del Gobierno.

Los *principios básicos* que orientarán la política de Seguridad Nacional son la unidad de acción, anticipación, prevención, eficiencia, sostenibilidad en el uso de los recursos, capacidad de resistencia y recuperación, coordinación y colaboración.

La *Estrategia de Seguridad Nacional* es el marco político estratégico de referencia de la Política de Seguridad Nacional que contiene el análisis del entorno estratégico, concreta los riesgos y amenazas que afectan a la seguridad de España, define las líneas de acción estratégicas en cada ámbito de actuación y promueve la optimización de los recursos existentes. Se revisará cada cinco años o cuando lo aconsejen las circunstancias.

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.

Se consideran **ámbitos de especial interés** de la Seguridad Nacional por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales, **la ciberseguridad**, la seguridad económica y

financiera, la seguridad marítima, la seguridad del espacio aéreo y ultraterrestre, la seguridad energética, la seguridad sanitaria y la preservación del medio ambiente.

La norma define cuales son los órganos competentes en materia de Seguridad Nacional, siendo las Cortes Generales, el Gobierno y su presidente, los ministros, los delegados del Gobierno de Ceuta y Melilla y el **Consejo de Seguridad Nacional**, que, en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, es el órgano al que corresponde asistir al Presidente del Gobierno en la dirección de la política de Seguridad Nacional y del Sistema de Seguridad Nacional, entre otras funciones.

La figura 5-1 muestra gráficamente la composición del Consejo de Seguridad Nacional con los cargos ministeriales que lo componen y sus roles correspondientes.

Figura 5-1. Composición del Consejo de Seguridad Nacional (fuente www.dsn,.gob.es)

Dentro de la estructura del Sistema de Seguridad Nacional, se crea el **Departamento de Seguridad Nacional** que ejercerá las funciones de Secretaría Técnica y órgano de trabajo permanente del Consejo de Seguridad Nacional y de sus órganos de apoyo.

5.2 El Consejo Nacional de Ciberseguridad

El *Consejo de Ciberseguridad Nacional* es el órgano colegiado de apoyo al Consejo de Seguridad Nacional en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional.

Es presidido por el secretario de Estado director del Centro Nacional de Inteligencia y se crea por Acuerdo del Consejo de Seguridad Nacional del 5 de diciembre de 2013.

Este consejo es el encargado de reforzar las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias en materia de ciberseguridad, así como entre los sectores públicos y privados, y facilita la toma de decisiones del propio Consejo mediante el análisis, estudio y propuesta de iniciativas tanto en el ámbito nacional como en el internacional.

Se reúne a iniciativa de su presidente como mínimo con carácter bimestral o cuantas veces lo considere necesario atendiendo a las circunstancias que afecten a la Ciberseguridad.

La figura 5-2 muestra la composición del Consejo Nacional de Ciberseguridad, los órganos que tienen vocalía en el mismo, además del resto de roles definidos para su funcionamiento.

Figura 5-2. Composición del Consejo Nacional de Ciberseguridad. (fuente www.dsn.gob.es)

5.3 La Estrategia Nacional de Ciberseguridad

La *Estrategia Nacional de Ciberseguridad 2019* publicada en la *Orden PCI/487/2019, de 26 de abril,* aprobada por el Consejo de Seguridad Nacional, es el marco de referencia de un modelo integrado basado en la implicación, coordinación y armonización de todos los actores y recursos del Estado, en la colaboración público-privada, y en la participación de la ciudadanía con la que se pretende garantizar la seguridad, las infraestructuras y la tecnología que integran el ciberespacio.

Este documento es una actualización de la primera Estrategia de Ciberseguridad Nacional de 2013, donde, en base a las lecciones aprendidas y a la situación actual, se han recogido nuevos riesgos y amenazas.

Para adecuarse a este nuevo escenario cambiante, la reciente Estrategia propone un conjunto de **Líneas de Acción y medidas** más dinámicas que permiten una rápida adaptación del ecosistema de ciberseguridad nacional.

En sus primeros apartados, la *estrategia* analiza los principales riesgos y amenazas, diferenciando entre aquellos que amenazan los activos de la información y los que utilizan el ciberespacio para la realización de actividades ilegales o maliciosas.

Entre las **amenazas**, a las que se encuentra expuesto nuestro país, destaca el ciberespionaje por unidades de inteligencia o militares de terceros países, las amenazas híbridas o la manipulación de

información, así como la cibercriminalidad, donde delincuentes comunes, terroristas o hacktivistas, utilizan el ciberespacio para la consecución de sus objetivos.

El documento establece los **principios** por los que se rige la estrategia, que son:

- **Unidad de acción.** Se requiere la adecuada preparación y articulación de la unidad de acción del Estado para dar una respuesta ante un incidente en el ámbito de la ciberseguridad que pueda implicar a distintos agentes del Estado.

- **Anticipación**. Priman las actuaciones preventivas sobre las reactivas. Se apuesta por sistemas eficaces, con información compartida en tiempo real, que permitan un adecuado conocimiento de la situación para la adopción de las medidas preventivas más adecuadas.

- **Eficiencia.** Establece la necesidad de una planificación anticipada para la adquisición de sistemas multipropósito de elevado nivel tecnológico que llevan asociadas unas necesidades muy exigentes y un alto coste derivado de su desarrollo, adquisición y operación.

- **Resiliencia**. La resiliencia es una característica fundamental que deben poseer los sistemas e infraestructuras críticas. El Estado está obligado a asegurar la disponibilidad de los elementos que se consideren esenciales para la nación, mejorando su protección contra las ciberamenazas.

Además, el documento establece varios **objetivos**, uno general y cinco específicos que resultan transversales a todos los ámbitos.

El **Objetivo general** es que España ha de garantizar el uso seguro y fiable del ciberespacio, protegiendo los derechos y las libertades de los ciudadanos y promoviendo el progreso socio económico.

Los **Objetivos específicos** son garantizar la *seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales*, el *uso seguro y fiable del ciberespacio frente a su uso ilícito o malicioso,* la *protección del ecosistema empresarial y social y de los ciudadanos,* la *cultura y compromiso con la ciberseguridad y potenciación de las capacidades humanas y tecnológicas,* y la *seguridad del ciberespacio en el ámbito internacional.*

Por último, para la consecución de los objetivos anteriores, establece las **siete líneas de acción y medidas** siguientes:

- **Reforzar las capacidades ante las amenazas provenientes del ciberespacio**.

- **Garantizar la seguridad y resiliencia de los activos estratégicos para España**, incluyendo medidas como la plena implantación del Esquema Nacional de Seguridad, del Sistema de Protección de las Infraestructuras Críticas, y el cumplimiento y armonización de la normativa sobre protección de infraestructuras críticas y servicios esenciales, o implantar el Centro de Operaciones de Ciberseguridad de la Administración General del Estado para incrementar las capacidades de prevención, detección y respuesta, e impulsar el desarrollo de centros de operaciones de ciberseguridad en el ámbito de la Administración.

- **Reforzar las capacidades de investigación y persecución de la cibercriminalidad**, garantizando la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio.

- **Impulsar la ciberseguridad de ciudadanos y empresas.**

- **Potenciar la industria española de ciberseguridad, y la generación y retención de talento, para el fortalecimiento de la autonomía digital.**

- **Contribuir a la seguridad del ciberespacio en el ámbito internacional**, promoviendo un ciberespacio abierto, plural, seguro y confiable, en apoyo de los intereses nacionales.

- **Desarrollar una cultura de ciberseguridad.**

Por tanto, cualquier actuación en materia de ciberseguridad de la Administración pública, o cualquier iniciativa, deberá estar inspirada en los principios y objetivos de la Estrategia Nacional de Ciberseguridad.

6 CIBERACTORES PRINCIPALES

6.1 Centro Nacional de Protección de Infraestructuras Críticas[17] (CNPIC)

El Centro Nacional para la Protección de las Infraestructuras Críticas fue creado en el año 2007, mediante Acuerdo de Consejo de Ministros de 2 de noviembre, siendo sus competencias reguladas por la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y por el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

Este centro depende del Gabinete de Coordinación y Estudios de la Secretaría de Estado de Seguridad, del Ministerio del Interior, máximo responsable del Sistema de Protección de las Infraestructuras Críticas nacionales, asignándole al CNPIC la dirección y coordinación de cuantas actividades relacionadas con la protección de infraestructuras críticas tenga encomendadas dicha Secretaría, así como el desarrollo de una serie de funciones, para lo cual está estructurado orgánicamente, lo que posibilita el cumplimiento de los cometidos que tiene asignados y la integración de la protección física y cibernética de las infraestructuras frente a cualquier tipo de amenaza, especialmente las procedentes de ataques terroristas u organizaciones criminales.

El CNPIC desempeña, entre otras, las siguientes funciones:

- Asiste al Secretario de Estado de Seguridad en la ejecución de sus funciones en materia de protección de infraestructuras críticas, actuando como órgano de contacto y coordinación con los agentes del Sistema.
- Ejecutar y mantener actualizado el Plan Nacional de Protección de las Infraestructuras Críticas.
- Determinar la criticidad de las infraestructuras estratégicas incluidas en el Catálogo.
- Mantiene operativo y actualizado el Catálogo de Infraestructuras Estratégicas

[17] Anteriormente denominado Centro Nacional de Protección de Infraestructuras y Ciberseguridad, hasta la entrada en vigor del *Real Decreto 734/2020, de 4 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior.*

- Dirige y coordina los análisis de riesgos de los Planes Estratégicos Sectoriales, para su estudio.
- Establece los contenidos mínimos de los Planes de Seguridad de los Operadores, de los Planes de Protección Específicos y de los Planes de Apoyo Operativo
- Analiza los Planes de Protección Específicos facilitados por los operadores críticos respecto a las diferentes infraestructuras críticas que propone, en su caso, para su aprobación, al Secretario de Estado de Seguridad.
- Validar los Planes de Apoyo Operativo diseñados para cada una de las infraestructuras críticas existentes en el territorio nacional por el Cuerpo Policial estatal o, en su caso, autonómico competente.
- Implanta mecanismos permanentes de información, alerta y comunicación con todos los agentes del Sistema.
- Recopilar, analizar, integrar y valorar la información sobre infraestructuras estratégicas procedente de instituciones públicas, servicios policiales, operadores y de los diversos instrumentos de cooperación internacional para su remisión al Centro Nacional de Coordinación Antiterrorista del Ministerio del Interior o a otros organismos autorizados.
- Participar en la realización de ejercicios y simulacros en el ámbito de la protección de las infraestructuras críticas.
- Coordina los trabajos y la participación de expertos en los diferentes grupos de trabajo y reuniones sobre protección de infraestructuras críticas, en los ámbitos nacional e internacional.

La figura 6-1 muestra los doce sectores estratégicos recogidos en la normativa PIC sobre los que se han de elaborar los Planes Estratégicos Sectoriales para identificar los servicios esenciales que prestar así como las infraestructuras críticas que les dan soporte.

Figura 6-1 Sectores Estratégicos PIC (fuente CNPIC)

El **Servicio de Planes y Seguridad** es el responsable de coordinar todos aquellos asuntos relacionados con la seguridad integral de las infraestructuras críticas y estratégicas nacionales, llevando a cabo las labores de implantación del sistema de planificación de la normativa relativa a la protección de infraestructuras críticas.

Además, es el encargado de la custodia, mantenimiento y explotación del Catálogo Nacional de infraestructuras estratégicas que es el registro con la información completa, actualizada y contrastada de todas las infraestructuras estratégicas ubicadas en el territorio nacional, incluyendo las críticas y de la explotación de la herramienta de mensajería instantánea ALERTPIC[18].

El servicio está dividido en tres secciones: Análisis, Estudios sobre Infraestructuras y Centro de Coordinación y Alerta.

Para el desempeño de sus cometidos, se apoya en los servicios transversales siguientes:

Servicio de Coordinación, que tiene como función el auxilio y cooperación con el titular del centro sobre el cumplimiento de sus funciones, asistida por la Sección de Relaciones Internacionales, encargada de las relaciones internacionales, especialmente con la Unión Europea.

[18] ALERTPIC, es una aplicación de mensajería instantánea basada en ALERTCOPS, utilizada como canal alternativo ante situaciones de indisponibilidad de los canales convencionales de comunicación con los operadores críticos.

Servicio de Normativa que tiene como misiones principales las relativas al ámbito normativo en todo lo relacionado con la protección de las infraestructuras críticas y servicios esenciales.

6.2 La Oficina de Coordinación de Ciberseguridad (OCC)

La Oficina de Coordinación de Ciberseguridad se crea mediante la publicación del *Real Decreto 734/2020, de 4 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior* y tiene su origen en la antigua Oficina de Coordinación Cibernética del Centro Nacional de Protección de Infraestructuras Críticas.

Se constituye como el órgano técnico de coordinación en materia de ciberseguridad del Ministerio del Interior y depende del Gabinete de Coordinación y Estudios de la Secretaría de Estado de Seguridad.

Las funciones que la norma le otorga son, por un lado, ser el **punto de contacto nacional de coordinación operativa** para el intercambio de información con la Comisión Europea y los Estados miembros, en el marco de lo establecido por la *Directiva 2013/40/UE de 12 de agosto de 2013,* relativa a los ataques contra los sistemas de información, por otro lado ejercer como **canal específico de comunicación** entre los Centros de Respuesta a Incidentes Cibernéticos (CSIRT) nacionales de referencia y la Secretaría de Estado de Seguridad, y por último, desempeñar la **coordinación técnica en materia de ciberseguridad** entre dicha Secretaría de Estado y sus organismos dependientes.

Se organiza en dos servicios: el **Servicio de Análisis de la Ciberseguridad y la Cibercriminalidad** cuya principal función es la coordinación de la lucha contra la cibercriminalidad, siendo la pieza de encaje en el Ministerio del Interior entre estos dos ámbitos, y el **Servicio de Operación** cuya función está relacionada con la resolución de incidentes de ciberseguridad de operadores de servicios esenciales, realización de ciberejercicios, búsqueda de vulnerabilidades y elaborar inteligencia para la ciberseguridad dentro de su ámbito.

En la actualidad se encuentra implicada en la elaboración del Plan Estratégico contra la Cibercriminalidad 2020.

6.3 El Centro Criptológico Nacional (CCN)

El *Centro Criptológico Nacional* (CCN) se crea mediante la *Ley 11/2002, 6 de mayo, reguladora del Centro Nacional de Inteligencia* (CNI), que incluye al Centro Criptológico Nacional como uno de sus órganos.

Dos años más tarde, se publica el *Real Decreto 421/2004, 12 de marzo, que regula y define el ámbito y funciones del CCN.*

Entre las funciones asignadas, se encuentra la responsabilidad de la respuesta ante ciberataques sobre sistemas clasificados, sistemas del Sector Público y empresas y organizaciones de sectores estratégicos para el país en coordinación con el CNPIC, además de establecerse al CCN-CERT como CERT Gubernamental/Nacional competente con la misión de contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente al Sector Público y a las empresas y organizaciones de sectores estratégicos en coordinación con CNPIC y afrontar de forma activa las nuevas ciberamenazas.

La *Orden del Ministerio de Presidencia PRE/2740/2007, de 19 de septiembre, que regula el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información* fue la precursora del *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*. Esta norma fue modificada por el *RD 951/2015, de 23 de octubre*, en respuesta a la evolución del entorno regulatorio, las tecnologías de la información y experiencia de implantación.

La implantación de dicho Esquema en toda la Administración Pública, es responsabilidad del CCN.

Además, el CCN-CERT se convierte en **CSIRT de referencia para la Administración pública** en el ámbito de la normativa NIS, siendo el CCN Autoridad competente para los operadores de servicios esenciales de la misma cuando estos no hayan sido nombrados por su condición de operadores críticos.

6.4 El Instituto Nacional de Ciberseguridad (INCIBE)

Este instituto tiene como reforzar la ciberseguridad, la confianza y la protección de la información y privacidad en los servicios de la Sociedad de la Información, aportando valor a ciudadanos, empresas, Administración, red académica y de investigación española, sector de las tecnologías de la información y las comunicaciones y sectores estratégicos relacionados con la normativa de protección de infraestructuras críticas.

El Instituto Nacional de Ciberseguridad de España (INCIBE), anteriormente Instituto Nacional de Tecnologías de la Comunicación, es una sociedad dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial y es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos, la red académica y de investigación, los profesionales, las empresas y especialmente para sectores estratégicos.

Como centro de excelencia, INCIBE se convierte en un instrumento del Gobierno para desarrollar la ciberseguridad como motor de transformación social y oportunidad para la innovación. Para ello, realiza una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia.

El INCIBE-CERT es el centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España operado por el Instituto Nacional de Ciberseguridad, dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial.

En el caso de la gestión de incidentes que afecten a operadores críticos del sector privado, INCIBE-CERT **está operado conjuntamente por INCIBE y CNPIC**, Centro Nacional de Protección de Infraestructuras y Ciberseguridad del Ministerio del Interior.

El **INCIBE-CERT** es uno de los equipos de respuesta de referencia ante incidentes que se coordina con el resto de los equipos nacionales e internacionales para mejorar la eficacia en la lucha contra los delitos que involucran a las redes y sistemas de información, reduciendo sus efectos en la seguridad pública, además de ser el **CSIRT de referencia para el sector privado** en el ámbito de la normativa NIS.

6.5 El Mando Conjunto del Ciberespacio (MCCE)

El Mando Conjunto del Ciberespacio (MCCE) es el órgano responsable del planeamiento, la dirección, la coordinación, el control y la ejecución de las acciones conducentes a asegurar la libertad de acción de las Fuerzas Armadas en el ámbito ciberespacial.

Para cumplir su misión, planea, dirige, coordina, controla y ejecuta las operaciones militares en el ciberespacio, de acuerdo con sus planes operativos, realizando las acciones necesarias para garantizar la supervivencia de los elementos físicos, lógicos y virtuales críticos para la Defensa y las Fuerzas Armadas

Además, es responsable de la seguridad de la *Infraestructura Integral de Información para la Defensa (I3D)* en el ámbito operativo y colabora en la transformación digital del Ministerio de Defensa.

También es responsable en colaboración con el EMACON, de la definición de requisitos operativos, seguimiento de la obtención y el sostenimiento de los medios de Ciberdefensa, CIS (Sistemas de Información y Telecomunicaciones) conjuntos de Mando y Control, de Guerra Electrónica y Navegación, Identificación y Sistemas de Observación de la Tierra, velando por la interoperabilidad de estos con los específicos de los Ejércitos y de la Armada. Asimismo, presta apoyo CIS a la estructura del EMAD.

Entre sus **cometidos específicos** se encuentran, entre otros, garantizar el libre acceso al ciberespacio a las Fuerzas Armadas, garantizar la disponibilidad, integridad y confidencialidad de la información y el funcionamiento de los servicios críticos de los sistemas de información y telecomunicaciones de las Fuerzas Armadas en un ambiente degradado debido a incidentes, accidentes o ataques.

Además, el obtener, analizar y explotar la información sobre ciberataques e incidentes en las redes y sistemas de su responsabilidad y ejercer la respuesta oportuna.

En la figura 6-2 se presentan las principales agencias de ciberseguridad estatales, sus dependencias orgánicas y su relación entre ellas.

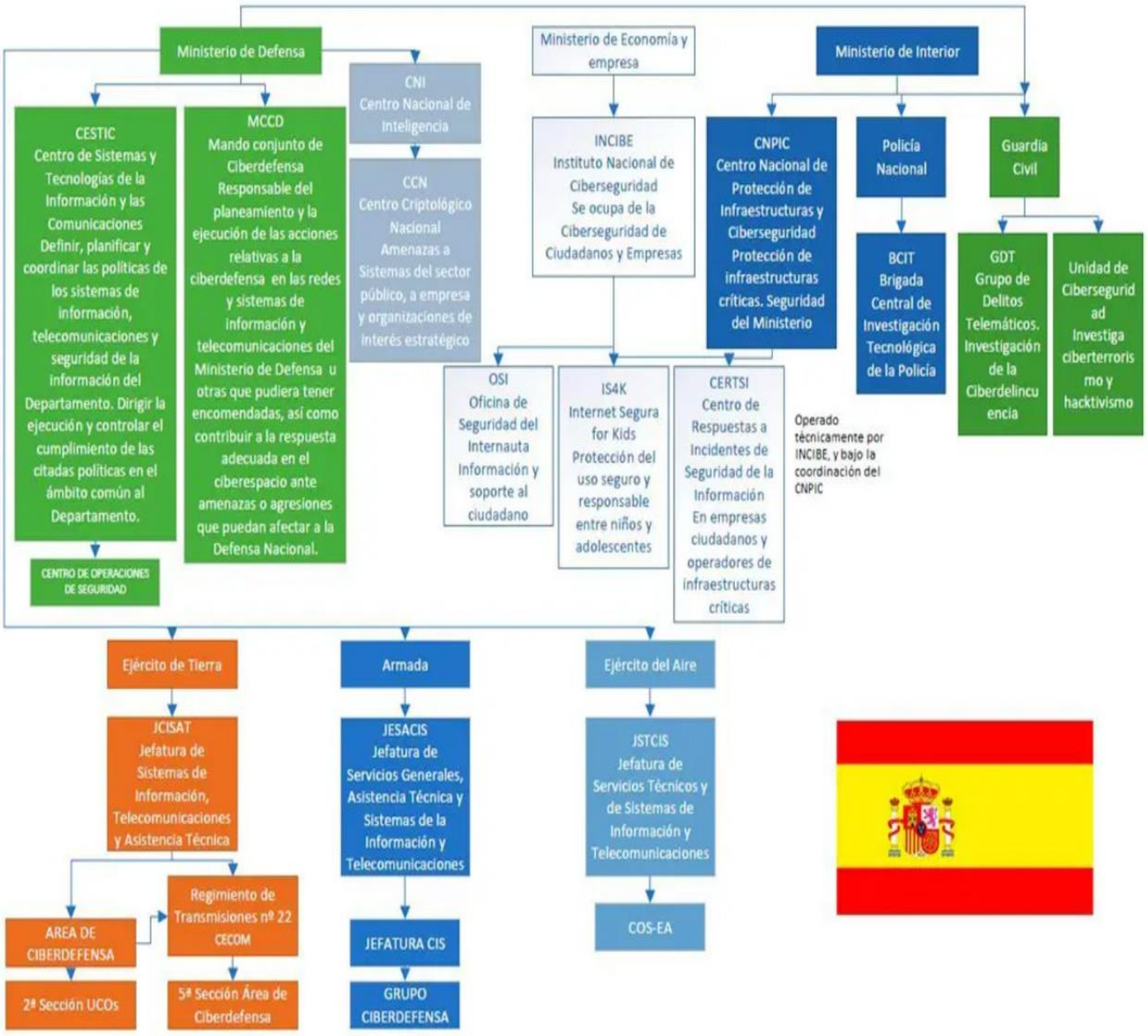

Figura 6-2. Agencias de ciberseguridad estatales (fuente: www.pabloyglesias.com)

7 CONCLUSIONES Y LÍNEAS FUTURAS DE ACTUACIÓN

7.1 Tiempos desacompasados

Los próximos retos en ciberseguridad a los que se tendrán que enfrentar la Unión Europea en su conjunto, y España de manera particular, están caracterizados por un dinamismo y una velocidad que no se ajustan a los tiempos de producción regulatoria para la resolución de los problemas que vayan surgiendo, que son mucho más lentos.

Esto implica que necesariamente la regulación normativa relativa a estos aspectos, necesariamente irá retrasada con la necesidad de solución de los problemas, existiendo una percepción en la ciudadanía de que no se abordan los problemas de manera diligente.

Las Autoridades europeas y españolas, habrán de realizar un esfuerzo para dinamizar los trámites legislativos y acortar los tiempos si quieren reaccionar a las cuestiones de la ciberseguridad en unos tiempos razonables.

7.2 La armonización normativa

La producción normativa en ciberseguridad se ha producido de manera desigual en la Unión Europea.

Países como Reino Unido, Alemania o España, abordaron la legislación en esta materia de manera temprana, lo que les ha permitido tener una normativa muy cohesionada en ciberseguridad. Esto ha ocasionado una colisión con las normas europeas que a posteriori se han publicado, por lo que es necesaria la armonización entre las complejas estructuras normativas de estos países y las primeras.

Dentro del propio seno de la Unión, Autoridades centrales como la del Banco Central Europeo o ENISA, han ido emitiendo numerosas normas sectoriales a lo largo del tiempo para regular el marco de sus competencias. La necesidad de transversalidad de la ciberseguridad y la uniformidad en todos los países, ha provocado la publicación de normas generalistas como la *Directiva NIS*, el *Reglamento de Ciberseguridad Europeo*, o el *Reglamento eIDAS*.

En este momento, se están revelando incoherencias con la normativa sectorial que está motivando que se prioricen estas normas específicas sobre las generalistas, lo que está debilitando el carácter uniformador con el que fueron creadas estas últimas. Ejemplo de ello son las diferentes taxonomías de los incidentes de seguridad entre las distintas autoridades. Esta disfunción permite clasificar de manera distinta un mismo incidente, según lo interprete una autoridad u otra, y consecuentemente, se exige un

distinto tratamiento a la hora de aplicar procedimientos o de cumplimentar tiempos de resolución del incidente, todo ello agravado porque, en la mayoría de los casos, su incumpliemitento conlleva sanciones económicas.

Los Estados miembros de la Unión que carecían de legislación sobre ciberseguridad en el momento de la publicación de las normas europeas, han tenido mucho más fácil la adecuación a dicha normativa.

7.3 La certificación en ciberseguridad

La existencia en los Estados miembros de Unión Europea de innumerables certificaciones en ciberseguridad, ya sea de procesos, esquemas o elementos de software o hardware regulados por las Autoridades competentes locales, sumados a las certificaciones exigidas por las Autoridades de la Unión, mas las distintas certificaciones de organismos privados reconocidos internacionalmente, presentan un panorama muy complicado a la hora de obtener certificaciones por parte de los operadores, ya que para operar en determinados sectores, necesitan según sea la Autoridad competente, varios certificados en ciberseguridad con el consiguiente gasto, y donde además, se exigen los mismos controles.

El Reglamento de Ciberseguridad Europeo de 2019 se publicado en un intento de poner orden en esta materia y crear certificaciones únicas en todo el territorio para simplificar el proceso de certificación.

No obstante, el panorama actual es que los operadores disponen de distintas certificaciones en ciberseguridad, que no son reconocidas por las autoridades y que en el ámbito privado tampoco pueden ser aprovechadas debido a que los niveles de certificación no son homogéneos.

Por parte del sector bancario, uno de los más activos en estas cuestiones, se ha creado un grupo de trabajo para la realización de una matriz de correspondencias entre los distintos certificados de su sector, que permita la racionalización en el uso de los certificados en beneficio de los operadores.

Por último, está el problema de la **re-certificación**. Para la obtención de cualquier certificado en ciberseguridad, se han de realizar determinadas acciones para garantizar que el sistema en cuestión es seguro. Ello pasa necesariamente por estudios de laboratorio si son productos, o por auditorias si son procesos o esquemas. Dichas acciones suponen un coste en dinero y en tiempo.

El problema se presenta cuando, debido al dinamismo propio de la ciberseguridad, se han de actualizar versiones, o rediseñar procesos. Estas acciones que son necesarias para el mantenimiento de los sistemas y para garantizar un determinado nivel de seguridad, provoca que las certificaciones dejen de tener validez por la modificación del alcance objeto de la certificación.

La agilización de los procesos de certificación, su menor coste, así como la flexibilización en el reconocimiento de variación de versiones, es la única manera de que se puedan abordar las recertificaciones como una exigencia en ciberseguridad.

7.1 La lucha contra el Cibercrimen

El uso de las tecnologías de la información y la comunicación se ha hecho presente como un aspecto más de nuestra vida cotidiana. Cualquier actividad va estrechamente ligada de una forma de otra a estas tecnologías.

Como ejemplo, del creciente uso de las TIC en nuestro país, en la tabla 7-1 podemos observar el creciente aumento de las compras por Internet en los últimos años.

% POR GRUPO DE EDAD DE PERSONAS QUE HAN COMPRADO ALGUNA VEZ POR INTERNET										
	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Edad: De 16 a 24 años	19,5	21,5	26,7	26,9	33,2	40,3	44,4	49,2	54,7	56,4
Edad: De 25 a 34 años	26,4	29,4	31,8	35,1	39,6	46,2	49,8	57,2	60,9	67,2
Edad: De 35 a 44 años	22,0	22,8	29,2	30,3	37,1	41,3	46,4	52,2	56,4	59,9
Edad: De 45 a 54 años	14,0	16,2	19,6	20,5	27,2	31,3	34,0	40,6	43,7	46,5
Edad: De 55 a 64 años	7,2	9,4	9,4	11,1	13,8	18,6	19,7	23,3	27,4	32,9
Edad: De 65 a 74 años	3,1	3,4	3,5	3,7	4,5	6,6	7,5	10,6	12,0	13,5

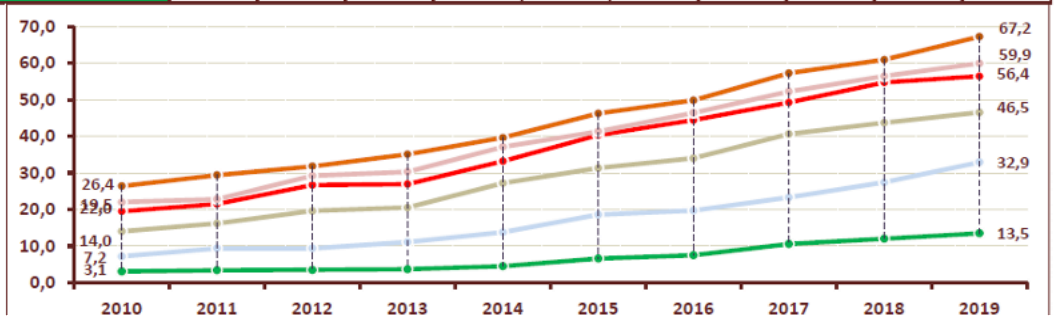

Tabla 7-1. Sociograma de compras por Internet (fuente: Ministerio del Interior)

Esta normalidad tecnológica está siendo aprovechada por la delincuencia para cometer hechos delictivos a través de estas mismas tecnologías debido especialmente a los beneficios que les supone comparados con la comisión de los mismos por los métodos tradicionales, como son la dificultad de atribución, el escaso riesgo y los enormes beneficios que se pueden obtener con su comisión.

La globalización de los movimientos terroristas, ha favorecido su presencia en las redes para publicidad de sus actuaciones y sus postulados, además de para el uso de Internet como una herramienta más para atacar sus objetivos.

Nuevos delitos relacionados con las redes, motivados por prácticas de riesgo como el *sexting*[19], o por actividades delictivas, como por ejemplo el *grooming*[20] o el intercambio de material pedófilo, han sufrido también un importante incremento.

En el Estudio de la cibercriminalidad de 2019[21] publicado por el Ministerio del Interior, se observa como nuestro país ha sufrido un fortísimo incremento de la cibercriminalidad, produciéndose entre los años 2018 a 2019 un incremento del 41%, y un total, desde que se comenzaron estos registros en el año 2015, de un incremento del 210%.

El 10% del total de delitos que se cometen en España son ciberdelitos y la cifra continúa subiendo año tras año.

En la tabla 7-2 se observa el incremento de delitos conocidos en los últimos años clasificados por modalidad delictiva.

[19] Sexting: intercambio de imágenes de contenido sexual por internet

[20] Grooming: acoso sexual a menores a través de internet

[21] http://www.interior.gob.es/documents/10180/9814700/Estudio+sobre+la+Cibercriminalidad+en+España+2019.pdf/24bd3afb-5a8e-4767-9126-c6c3c256982b

HECHOS CONOCIDOS	2016	2017	2018	2019
ACCESO E INTERCEPTACIÓN ILÍCITA	3.243	3.150	3.384	4.004
AMENAZAS Y COACCIONES	12.036	11.812	12.800	12.782
CONTRA EL HONOR	1.546	1.561	1.448	1.422
CONTRA PROPIEDAD INDUST./INTELEC.	129	121	232	197
DELITOS SEXUALES(*)	1.231	1.392	1.581	1.774
FALSIFICACIÓN INFORMÁTICA	3.017	3.280	3.436	4.275
FRAUDE INFORMÁTICO	70.178	94.792	136.656	192.375
INTERFERENCIA DATOS Y EN SISTEMA	1.336	1.291	1.192	1.473
Total HECHOS CONOCIDOS	**92.716**	**117.399**	**160.729**	**218.302**

Tabla 7-2. Número de ciberdelitos denunciados en 2019 por tipología (fuente: Ministerio del Interior)

La *Estrategia Nacional de Ciberseguridad* considera a la cibercriminalidad como una amenaza a la Seguridad Nacional, estableciendo en la Línea de Acción tercera la responsabilidad al Estado de "*Reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio*", mediante el reforzamiento del marco jurídico, el fomento de la colaboración y participación ciudadana, potenciando las capacidades de investigación, reforzando la comunicación con los órganos judiciales y fomentando el intercambio de información entre las unidades policiales de inteligencia tanto nacionales como internacionales.

Para dar cumplimiento a esta línea de acción, el Ministerio del Interior está elaborando el *Plan Estratégico contra la Cibercriminalidad*, donde recoge cada una de las acciones de la *Estrategia Nacional* y las desarrolla en planes de actuación específicos que habrán de ejecutar las Fuerzas y Cuerpos de Seguridad del Estado.

Actualmente existe un encendido debate sobre si la ciberseguridad es la parte preventiva del ciclo de la cibercriminalidad, compuesto por la prevención, la investigación y persecución de los autores y el auxilio a la víctima. El argumento es que, si la ciberseguridad cumple su función de proteger de los ciberataques, no se producirían hechos delictivos.

Por otro lado, están los que opinan que la ciberseguridad es un concepto más amplio que sobrepasa ampliamente el ámbito de la cibercriminalidad.

Una tercera corriente opina que son dos ámbitos diferentes con ciertos elementos comunes como la prevención o los ciberataques y aspectos exclusivos de cada uno de ellos como la investigación de los autores en el ámbito de la cibercriminalidad o las malas *praxis* en el de la ciberseguridad. En cualquier caso, el debate está servido.

En la figura 7-1 se exponen distintos componentes de uno y otro ámbito con los aspectos que les son comunes y de los que todavía los expertos en la materia no se han puesto de acuerdo.

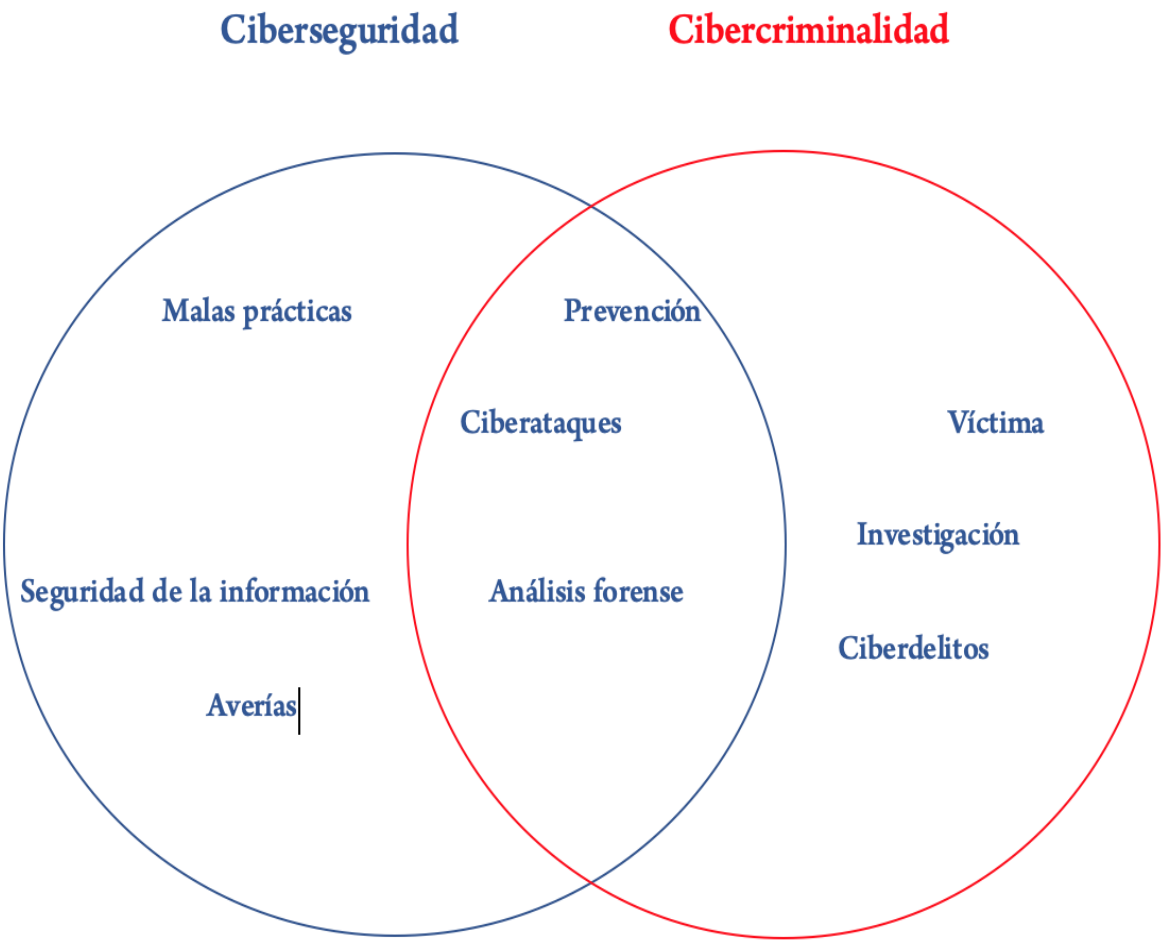

Figura 7-1. Aspectos relacionados entre la ciberseguridad y la cibercriminalidad (fuente: elaboración propia)

La **mejora en la eficacia de lucha contra la criminalidad** pasa por la aplicación de determinadas medidas recogidas en el borrador del *Plan Estratégico contra la Cibercriminalidad 2020* del Ministerio del Interior, como son:

- Fomentar el conocimiento y la información a los usuarios y público en general para incrementar la prevención y la autoprotección
- Incrementar las capacidades operativas y de inteligencia de las unidades policiales y las competencias y habilidades de los agentes que las integran
- Compartir información para generar inteligencia
- Impulsar la coordinación nacional y la cooperación internacional
- Promover un marco jurídico eficaz
- Establecer líneas de colaboración y asociación con la industria, con las Universidades y con demás actores relevantes en este ámbito

8 BIBLIOGRAFÍA

Legislación:

ÁMBITO	NOMBRE DE LA NORMA
Norma europea	Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad en las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) nº. 526/2013 (Reglamento sobre la Ciberseguridad). *Diario Oficial de la Unión Europea*, núm. 151, de 7 de junio de 2019, pp. 15-65
Norma europea	Directiva (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 en la unión. *Diario Oficial de la Unión Europea* L 194/1, 19 de julio de 2016, pp. 1-30
Norma europea	Directiva (CE) 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de mejorar su protección. *Diario Oficial de la Unión Europea* núm. 345, de 23 de diciembre de 2008, pp. 75-82
Norma española	Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. *Boletín Oficial del Estado*, de 29 de abril de 201, núm. 1092, pp. 71548-71586
Norma española	Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. *Boletín Oficial del Estado*, de 23 de junio de 2007, núm. 150, pp. 27150-27166
Norma española	Real Decreto 734/2020, de 4 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior. *Boletín Oficial del Estado*, de 5 de agosto de 2020, núm. 211, pp. 63852-63884
Norma española	Real Decreto 951/2015, de 23 de octubre, de modificación del 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. *Boletín Oficial del Estado*, de 4 de noviembre de 2015, núm. 264, pp. 104246-

104267

Norma española Real Decreto 1308/2011, de 26 de septiembre, sobre protección física de las instalaciones y los materiales nucleares, y de las radiactivas. *Boletín Oficial del Estado,* de 7 de octubre de 2011, núm. 242, pp. 105299-105330

Norma española Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas. *Boletín Oficial del Estado,* de fecha 21 de mayo de 2011, núm. 121, pp. 50808-50826

Norma española 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 *Boletín Oficial del Estado,* de 29 de enero de 2010, núm. 25, pp. 8089-8138

Norma española Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional. *Boletín Oficial del Estado,* de 19 de marzo de 2004, núm. 68, pp. 12203-12204

Norma española Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. *Boletín Oficial del Estado,* de 8 de septiembre de 2018, núm. 218, pp. 87675-87696

Norma española 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. *Boletín Oficial del Estado*, de 18 de septiembre de 2015, núm. 224, pp. 82405-82425

Norma española Acuerdo del Consejo Nacional de Ciberseguridad de 29 de mayo de 2015

Norma española. Instrucción núm. 1/2016, de la Secretaria de Estado de Seguridad, por la que se actualiza el Plan Nacional de Protección las Infraestructuras Críticas

Norma española Instrucción núm. 10/2015 de la Secretaría de Estado de Seguridad, por la que se regula el proceso de implantación del sistema de protección de infraestructuras críticas a nivel territorial

Norma española Instrucción 3/2015 de la Secretaría de Estado de Seguridad por la que se actualiza el Plan de Prevención y Protección Antiterrorista

Norma española Consejo de Seguridad Nacional. Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional. *Boletín Oficial del Estado,* de 30 de abril de 2019, núm. 103, pp. 43437-43455

Norma española Ministerio del Interior. Orden INT/318/2011, de 1 de febrero, sobre personal de seguridad privada. *Boletín Oficial del Estado,* de 18 de febrero de 2011, núm. 42, pp. 18348-18369

Norma española Ministerio del Interior. Orden INT/314/2011, de 1 de febrero, sobre empresas de seguridad privada. *Boletín Oficial del Estado,* de 18 de febrero de 2011, núm. 42, pp. 18287-18308

Norma española CNPIC-CCN-DSN. Guía Nacional de Notificación y Gestión de Ciberincidentes

Norma española CNPIC. Guía de Buenas Prácticas Plan de Seguridad del Operador, de 8 de septiembre de 2015

Norma española CNPIC. Guía de Buenas Prácticas Plan de Protección Específico, de

	8 de septiembre de 2015
Estándar	ISO 27001 Sistema de gestión de seguridad de la información.
Estándar	ISO 27002 Código de prácticas para los controles de seguridad de la informació
Estándar	ISO 17065 Evaluación de la conformidad. Requisitos para organismos que certifican productos, procesos y servicios
Norma EEUU.	NIST SP 800-82 Guía para la Seguridad de los Sistemas de Control Industrial (ICS)

Recursos:

NOMBRE DEL RECURSO	FECHA DE CONSULTA	URL
Asociación de Periodistas Europeos	12/09/2020	http://www.apeuropeos.org/wordpress/wp-content/uploads/2020/09/Conferencia-Paz-Esteban.pdf
Departamento de Seguridad Nacional	24/10/2020	https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-ciberseguridad-nacional
Portal de Administración Electrónica	02/11/2020	https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio-2019/Septiembre/Noticia-2019-09-13-Ley-ciberseguridad-UE-marco-certificacion-ciberseguridad.html#.X_GjfS0rxQJ
Internet Archive	10/10/2020	https://web.archive.org/web/20100830110225/http://www.commoncriteriaportal.org/products.html
Diario Oficial de la Unión Europea	20/11/2020	https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:L:2008:345:FULL&from=PT
Cuadernos de Seguridad	17/11/2020	https://cuadernosdeseguridad.com/2018/09/la-directiva-nis-se-incorpora-al-ordenamiento-juridico-espanol/
Fundación Telefónica	02/12/20	https://www.afi.es/webAfi/descargas/1410874/1448777/las-tic-

		y-el-sector-financiero-del-futuro.pdf
Wikipedia	28/11/2020	https://es.wikipedia.org/wiki/Navegación_aérea
Enaire	03/12/2020	https://www.enaire.es/servicios/atm/sistemas_de_gestion_del_transito_aereo_atm/sacta
La Información.com	05/12/2020	https://www.lainformacion.com/economia-negocios-y-finanzas/los-ataques-terroristas-en-aviones-una-tactica-que-se-remonta-a-1933_rG7bCBF49wobd6ChhDGHR4/
Agencia de Seguridad Aérea	12/10/2020	https://www.seguridadaerea.gob.es
Conejo de Seguridad Nuclear	03/01/2021	https://www.csn.es/seguridad-nuclear
INCIBE	20/12/2020	https://www.incibe-cert.es/blog/diferencias-ti-to
Portal de la Administración Electrónica	26/12/2020	https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html
Centro de Ciberseguridad Industrial	02/11/2020	https://www.cci-es.org/documents/10694/331476/documento+PIC+y+CI.pdf/6f4f7e57-4719-4d85-ad27-7218800ca138
Wikipedia	23/12/2020	https://es.wikipedia.org/wiki/Red_eléctrica_inteligente
normaiso27001.es	13/10/2020	https://normaiso27001.es
National Institute of Standars and Technology USA	27/12/2020	https://csrc.nist.gov/publications/sp800
Common Criteria	04/10/2020	https://www.commoncriteriaportal.org

Centro Criptológico Nacional	04/01/2021	https://www.ccn.cni.es/index.php/en/menu-certification-organism-en
Departamento de Seguridad Nacional	02/12/2020	https://www.dsn.gob.es/es/nivel-alerta-antiterrorista
Lisa Institute	11/11/2020	https://www.lisainstitute.com/blogs/blog/estrategia-nacional-ciberseguridad-espana-2019
Agencia Estatal del Boletín Oficial del Estado	02/12/2020	https://www.boe.es/buscar/doc.php?id=BOE-A-2020-9138
INCIBE	03/01/2021	https://www.incibe.es
Ministerio de Defensa	03/01/2021	https://emad.defensa.gob.es/unidades/mcce/

ANEXO I: LISTADO DE ACRÓNIMOS

ARLI-SI: Análisis de Riesgo Ligero de Seguridad Industrial
CC: *Common Criteria*
CCN: Centro Criptológico Nacional
CCN-CERT: Centro de respuesta a incidentes de seguridad del Centro Criptológico Nacional
CCRA: *Common Criteria Recognition Arrangement*
CEM: *Methodology for Information Technology Security Evaluation*
CERT: *Computer Emergency Response Team*
CIS: Sistemas de Información y Telecomunicaciones
CISM: *Certified Information Security Manager*
CISO: *Chief Information Security Officer*
CISSP: *Certified System Security Systems Professional*
CNPIC: Centro Nacional de Protección de Infraestructuras Críticas
CSIRT: Equipo de respuesta ante incidentes de seguridad
C4V: Construcción de Capacidades en Ciberseguridad de la Cadena de Valor
DSN: Departamento de Seguridad Nacional
EMACON: Estado Mayor Conjunto de la Defensa
EMAD: Estado Mayor de la Defensa
ENS: Esquema Nacional de Seguridad
ENSI: Esquema Nacional de Seguridad Industrial
GTI PIC: Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas
IMC: Indicadores para la Mejora de Ciberresiliencia
INCIBE: Instituto Nacional de Ciberseguridad de España.
INCIBE-CERT: Centro de respuesta a incidentes de seguridad del INCIBE
IoT: *Internet of things*
ISO: *International Organization for Standardization*
IT: *Information technologies*
I3D: Infraestructura Integral de Información para la Defensa
MCCE: Mando Conjunto del Ciberespacio.
NIS: *Security of Network and Information Systems.*
NIST: *National Institute of Standars and Technology*
OCC: Oficina de Coordinación de Ciberseguridad
OT: *Operation technologies*
PAO: Plan de Apoyo Operativo
PES: Plan Estratégico Sectorial
PIC: Protección de Infraestructuras Críticas
PPPA: Plan de Protección y Prevención Antiterrorista
PSO: Plan de Seguridad del Operador
PPE: Plan de Protección Específico
RD: Real Decreto
RDL: Real Decreto-ley
SES: Secretaría de Estado de Seguridad
SGTF: *Smart Grid Task Force*
TIC: Tecnologías de la Información y la Comunnicación
UE: Unión Europea.
URL: Uniform Resource Locator
5G: Quinta generación de telefonía móvil