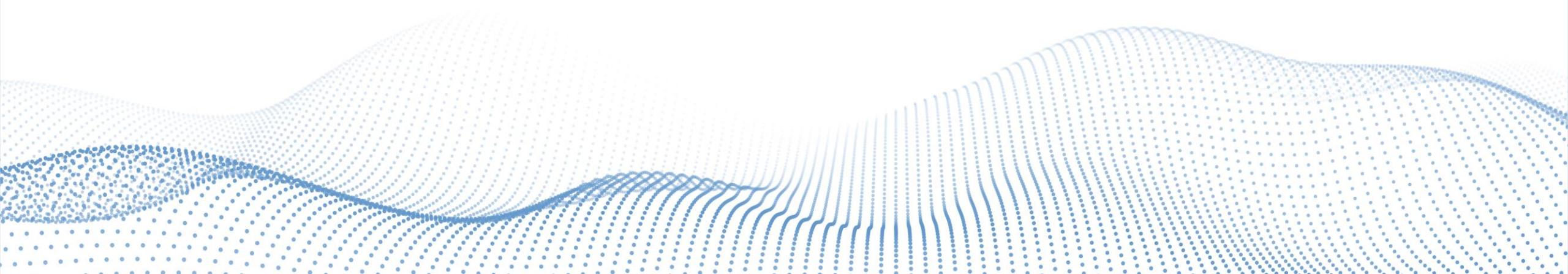


# Curso Superior en Ciberseguridade

Marco estratéxico e normativo de ciberseguridade

# Curso Superior en Ciberseguridade

Marco estratéxico e normativo de ciberseguridade



## Presentación



Fernando Suárez Lorenzo

-  <https://www.linkedin.com/in/fsuarezl/>
-  <https://twitter.com/fsuarezl>



## Reflexión inicial

- Preocupación creciente en ciberseguridad
- Necesidad de cooperación
- Ciberseguridad como problema global
- Tensión económica entre potencias
- Papel UE



# Jerarquía normativa

- Constitución de 1978: es la norma suprema que regula la estructura jurídica y la interrelación de normas.
- Tratados internacionales y Derecho de la Unión Europea.
- Leyes promulgadas por las Cortes Generales (Parlamento y Senado):
  - Leyes orgánicas.
  - Leyes ordinarias.
- Normas reglamentarias con rango de Ley como el Real Decreto Ley y el Real Decreto Legislativo.
- Reglamentos: Órdenes ministeriales, Ordenes de las Comisiones Delegadas del Gobierno...
- Leyes y Reglamentos de las Comunidades Autónomas.

## Pirámide de Kelsen

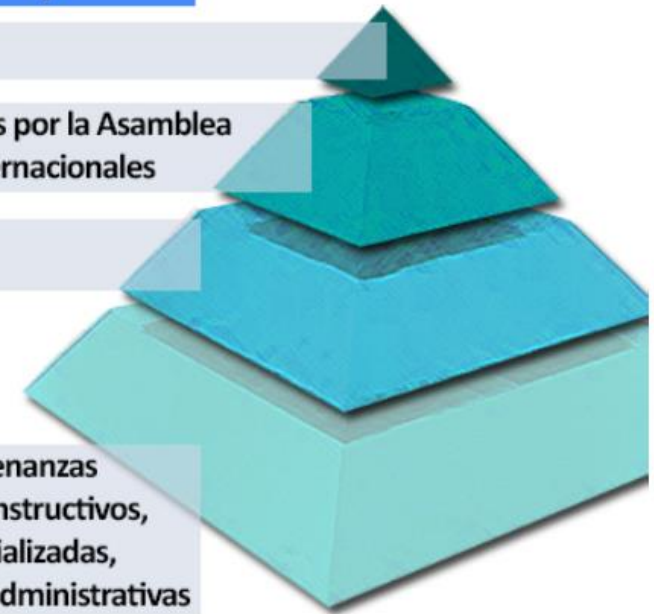
### Esquema de prevalencia de las normas jurídicas

1 Constitución

2 Leyes emitidas por la Asamblea y tratados internacionales

3 Reglamentos

4 Decretos, ordenanzas municipales, instructivos, normas especializadas, resoluciones administrativas



## Jerarquía normativa

- **Reglamento.** Los reglamentos son actos legislativos vinculantes. Deben aplicarse en su integridad en toda la UE
- **Directiva.** Las directivas son actos legislativos en los cuales se establecen objetivos que todos los países de la UE deben cumplir.
- **Decisiones.** Las decisiones son vinculantes para aquellos a quienes se dirigen (un país de la UE o una empresa concreta) y son directamente aplicables.
- **Recomendaciones.** Las recomendaciones no son vinculantes
- **Dictámenes.** Los dictámenes son instrumentos que permiten a las instituciones hacer declaraciones de manera no vinculante, es decir, sin imponer obligaciones legales a quienes se dirigen





# Ciberseguridade Europa

- La UE tiene su origen en el mercado único (libre circulación de personas y productos)
- La ciberseguridad empieza a tener protagonismo a raíz de los ataques en Estonia (2007) y Stuxnet.
- La ciberseguridad es una prioridad **política** en la UE y en todos los países.



Iniciativas legislativas máis importantes

## Directiva NIS

- Establece obligaciones para todos los Estados miembros en busca de adoptar una estrategia nacional sobre la seguridad de redes y sistemas de información.
- Crear un grupo de cooperación estratégica e intercambio de información entre los Estados miembros.
- Crear una red de Equipos de Respuesta a Incidentes de Seguridad Informática (red CSIRT), para contribuir en la rapidez y eficacia de la cooperación operativa.
- Establecer y notificar los requisitos de seguridad para operadores de servicios esenciales (como el energético, financiero, salud, etc.) y proveedores de servicios digitales (como motores de búsqueda, comercio electrónico o cómputo en la nube).
- Determinar obligaciones para las autoridades nacionales competentes de cada Estado miembro.





Iniciativas legislativas máis importantes

## Estrategia de Mercado Único Digital

- Regulamento General de Protección de Datos
- Regulamento sobre la privacidad: respeto a la vida privada y la protección de datos personales en las comunicaciones electrónicas
- Revisión iniciativa ciberseguridad e impulso de nuevas propuestas



## Autoridades más relevantes

- CERT EU
- ENISA. European Union Agency for Cybersecurity
- EDA. European Defense Agency
- EUROPOL-Cybercrime Center
- EUISS-European Union Institute for Security Studies
- JRC H2020 on Cybersecurity



## Tallín 2017 - Estrategia de Ciberseguridad para Europa

- Nuevo mandato para ENISA
- Marco de certificación de ciberseguridad
- Implementación completa de directiva NIS en 2018
- Fondo de respuesta de emergencias a cibercrisis
- Centro de competencias en ciberseguridad
- Acceso transfronterizo a evidencias electrónicas ante ciberataques
- Campañas de concienciación
- Mayor cooperación con la OTAN
- Grupo de expertos sobre fake news



## Estrategia de Ciberseguridad para Europa

La estrategia describe cómo la UE puede aprovechar y fortalecer todas sus herramientas y recursos para ser tecnológicamente soberana

La nueva estrategia tiene como objetivo garantizar una Internet global y abierta con fuertes salvaguardas donde existan riesgos para la seguridad y los derechos fundamentales de las personas en Europa. Siguiendo los avances logrados en las estrategias anteriores, contiene propuestas concretas para el despliegue de tres instrumentos principales:

- resiliencia, soberanía tecnológica y liderazgo;
- capacidad operativa para prevenir, disuadir y responder;
- cooperación para promover un ciberespacio global y abierto



# Ley de Servicios Digitales (2022)

La Ley de Servicios Digitales mejora significativamente los mecanismos de eliminación de contenidos ilícitos y protección efectiva de los derechos fundamentales de los usuarios, incluida la libertad de expresión:

- medidas para luchar contra los bienes, servicios o contenidos ilícitos online
- nuevas obligaciones sobre trazabilidad de las empresas usuarias
- garantías eficaces para los usuarios
- prohibición de determinado tipo de anuncios selectivos
- medidas de transparencia
- obligación para las plataformas online de muy gran tamaño
- acceso de los investigadores
- estructura de supervisión adecuada al ciberespacio



## Para los ciudadanos

- Mejor protección de los derechos fundamentales.
- Más opciones, precios más bajos.
- Menor exposición a contenidos ilícitos.



## Para los proveedores de servicios digitales

- Seguridad jurídica y armonización de las normas.
- Puesta en marcha y expansión más fáciles en Europa.



## Para las empresas usuarias de servicios digitales

- Más opciones, precios más bajos.
- Acceso a los mercados de la UE a través de las plataformas.
- Igualdad de condiciones frente a los proveedores de contenidos ilícitos.



## Para la sociedad en general

- Mayor control democrático y supervisión de las plataformas sistémicas.
- Atenuación de riesgos sistémicos tales como la manipulación o la desinformación.



# La ciberseguridad en la Seguridad Nacional

- Sistema de Seguridad Nacional con sus componentes principales desde el punto de vista de la ciberseguridad y sus componentes (Consejo de Seguridad Nacional, Consejo Nacional de Ciberseguridad, Comité Especializado de Situación)
- Estrategias (Estrategia de Seguridad Nacional 2017 y Estrategia Nacional de Ciberseguridad 2019)
- Claves de la Protección de Infraestructuras Críticas
- Seguridad de las redes y sistemas de información.

## AMENAZAS Y DESAFÍOS PARA LA SEGURIDAD NACIONAL



### LEYENDA

- AMENAZAS
- AMENAZAS Y DESAFÍOS EN LOS ESPACIOS COMUNES GLOBALES
- AMENAZAS SOBRE LAS INFRAESTRUCTURAS CRÍTICAS
- DESAFÍOS

## El Sistema de Seguridad Nacional

- El **Consejo de Seguridad Nacional**, Comisión Delegada del Gobierno para la Seguridad Nacional que asiste al Presidente del Gobierno en la dirección de la Política de Seguridad Nacional.
- El **Comité Especializado de Situación**, único para el conjunto del Sistema de Seguridad Nacional.
- El **Consejo Nacional de Ciberseguridad**, comité especializado que da apoyo al Consejo de Seguridad Nacional en el ámbito de la ciberseguridad.
- La **Comisión Permanente de Ciberseguridad** persigue facilitar la coordinación interministerial a nivel operacional en el ámbito de la ciberseguridad.
- El **Foro Nacional de Ciberseguridad** actuará en la potenciación y creación de sinergias público privadas.
- Las **Autoridades públicas competentes en materia de seguridad de las redes y sistemas de información y los CSIRT de referencia nacionales**.

## Sistema de Seguridad Nacional



### Consejo Nacional de Ciberseguridad

- Constituido el 25 de febrero de 2014.
- Lo preside el Secretario de Estado Director del CNI
- Órgano de apoyo del Consejo de Seguridad Nacional
- Refuerza las relaciones de coordinación, colaboración y cooperación entre las entidades de la Administración con competencias en materia de ciberseguridad, así como entre los sectores público y privado



## Estrategia de Seguridad Nacional

La Estrategia de Seguridad Nacional 2021 se estructura en cinco capítulos.

- Seguridad Global y Vectores de Transformación, analiza el contexto internacional de seguridad
- Una España Segura y Resiliente, traza un perfil de España y su seguridad.
- El tercer capítulo recoge los riesgos y las amenazas a la Seguridad Nacional, cuyas principales características son su interrelación y dinamismo.
- Un Planeamiento Estratégico Integrado, establece tres objetivos, que marcan las prioridades de la Seguridad Nacional para este ciclo estratégico.
- El quinto capítulo está dedicado a la gestión de crisis en el marco del Sistema de Seguridad Nacional.



## Estrategia Nacional de Ciberseguridad

### 5 objetivos específicos:

- Objetivo I: Seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales.
- Objetivo II: Uso seguro y fiable del ciberespacio frente a su uso ilícito o malicioso.
- Objetivo III: Protección del ecosistema empresarial y social y de los ciudadanos.
- Objetivo IV: Cultura y compromiso con la ciberseguridad y potenciación de las capacidades humanas y tecnológicas.
- Objetivo V: Seguridad del ciberespacio en el ámbito internacional





## Estrategia Nacional de Ciberseguridad

### 7 líneas de acción :

- Línea de Acción 1. Reforzar las capacidades ante las amenazas provenientes del ciberespacio.
- Línea de Acción 2. Garantizar la seguridad y resiliencia de los activos estratégicos para España.
- Línea de Acción 3. Reforzar las capacidades de investigación y persecución de la cibercriminalidad.
- Línea de Acción 4. Impulsar la ciberseguridad de ciudadanos y empresas
- Línea de Acción 5. Potenciar la industria española de ciberseguridad.
- Línea de Acción 6. Contribuir a la seguridad del ciberespacio en el ámbito internacional.
- Línea de Acción 7. Desarrollar una cultura de ciberseguridad.



## Protección de Infraestructuras Críticas

Infraestructura crítica: *Las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.*

12 sectores estratégicos para la identificación de infraestructuras críticas: Administración, Agua, Alimentación, Energía, Espacio, Industria Química, Industria Nuclear, Instalaciones de Investigación, Salud, Sistema Financiero y Tributario, Tecnologías de la Información y las Comunicaciones (TIC) y Transporte.

La Ley 8/2011 establece el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) como órgano de asistencia al Secretario de Estado de Seguridad en la ejecución de las funciones que se le encomiendan a éste como órgano responsable del sistema.



### Protección de Infraestructuras Críticas

Comisión Nacional PIC: órgano colegiado adscrito a la Secretaría de Estado de Seguridad, que desarrolla las funciones que le encomiendan la Ley 8/2011 y su reglamento de desarrollo, el Real Decreto 704/2011.

Entre sus funciones figuran:

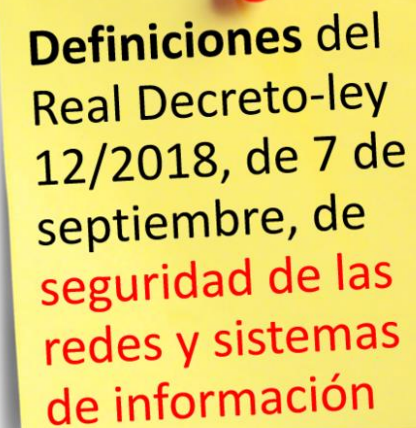
- Aprobar los Planes Estratégicos Sectoriales (PES).
- Designar a los operadores críticos.
- Aprobar la creación, modificación o supresión de grupos de trabajo sectoriales o de carácter técnico.
- Identificar los servicios esenciales.
- Designar los operadores de los servicios esenciales.



## Seguridad de las Redes y Sistemas de Información

El Real Decreto-Ley 12/2018 tiene por 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”, a la vez que “establece un marco institucional para la coordinación entre autoridades competentes y con los órganos de cooperación relevantes en el ámbito comunitario”

Es de aplicación a la prestación de los servicios esenciales dependientes de las redes y sistemas de información comprendidos en los sectores estratégicos y de los servicios digitales considerados “servicios de la sociedad de la información”



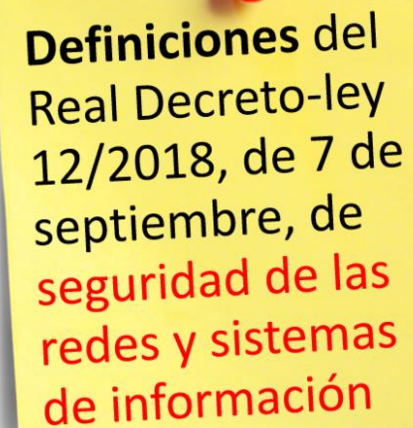
**Definiciones del  
Real Decreto-ley  
12/2018, de 7 de  
septiembre, de  
seguridad de las  
redes y sistemas  
de información**

sept. 2018

#### Seguridad de las Redes y Sistemas de Información

El artículo 11 del Real Decreto-Ley recoge los tres CSIRT de referencia que se coordinarán entre sí y con el resto de equipos nacionales e internacionales en la respuesta a incidentes y gestión de riesgos. Para el Sector público, el CSIRT de referencia es el CCN-CERT, del Centro Criptológico Nacional.

Los otros dos CSIRT son el INCIBE-CERT para la comunidad que no pertenezca al CCN-CERT, ciudadanos y entidades de derecho y el ESPDEF-CERT, del Mando Conjunto de Ciberdefensa, que cooperará con los otros dos CSIRT en aquellas situaciones que éstos requieran en apoyo de los operadores de servicios esenciales y, necesariamente, en aquellos que tengan incidencia en la Defensa Nacional.



**Definiciones del  
Real Decreto-ley  
12/2018, de 7 de  
septiembre, de  
seguridad de las  
redes y sistemas  
de información**

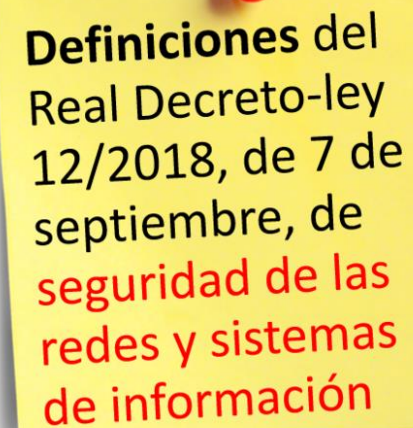
sept. 2018



## Seguridad de las Redes y Sistemas de Información

En relación con las obligaciones se establece que los operadores de servicios esenciales y los proveedores de servicios digitales deberán adoptar medidas técnicas y de organización, adecuadas y proporcionadas, para gestionar los riesgos.

Del mismo modo, se establece la obligación de los operadores de servicios esenciales y de los proveedores de servicios digitales de notificar a la autoridad competente, a través del correspondiente CSIRT de referencia, los incidentes que puedan tener efectos perturbadores significativos en dichos servicios



**Definiciones del  
Real Decreto-ley  
12/2018, de 7 de  
septiembre, de  
seguridad de las  
redes y sistemas  
de información**

sept. 2018

# Plan Nacional de Ciberseguridad

Aprobado en Consejo de Ministros el 29 de marzo de 2022 cumpliendo el mandato emitido por el Consejo de Seguridad Nacional y desarrolla la Estrategia Nacional de Ciberseguridad 2019.

El plan, coordinado por el Departamento de Seguridad Nacional de la Presidencia del Gobierno, prevé cerca de 150 iniciativas para los próximos tres años.

- Creación de la plataforma nacional de notificación y seguimiento de ciberincidentes.
- Impulsar el Centro de Operaciones de Ciberseguridad de la Administración General del Estado.
- Sistema integrado de indicadores de ciberseguridad a nivel nacional.
- Creación de infraestructuras de ciberseguridad.
- Impulsar la ciberseguridad de pymes, micropymes y autónomos.
- Promover un mayor nivel de cultura de ciberseguridad.



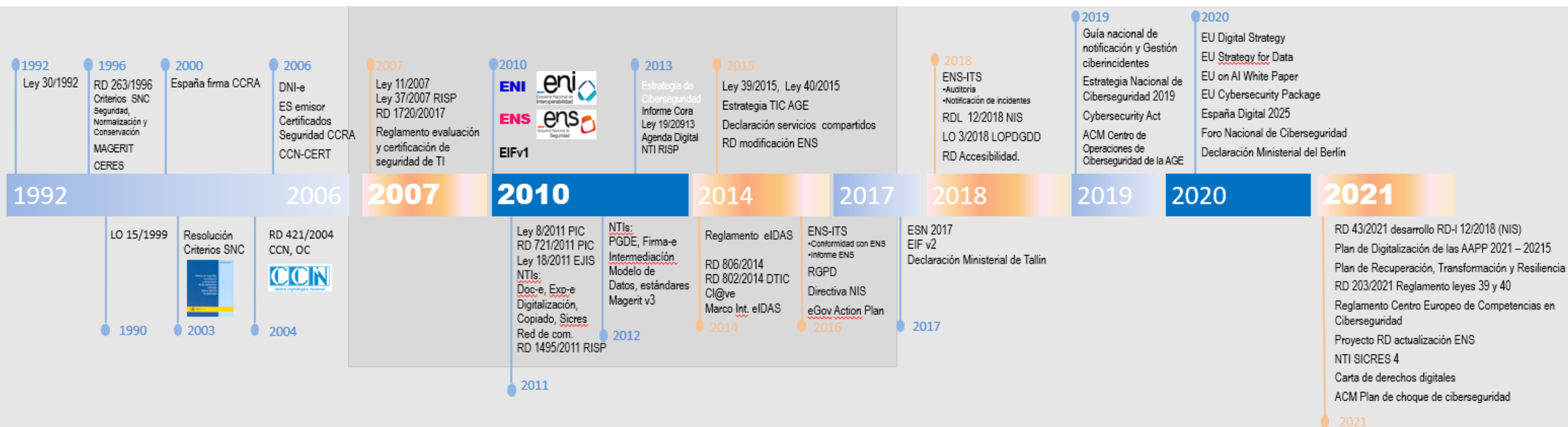
# El Esquema Nacional de Seguridad

Surge para dar respuesta a:

- La «Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas» recoge entre los derechos de las personas en sus relaciones con las Administraciones Públicas el relativo “a la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas”.
- La «Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público», por su parte, incluye a la seguridad entre los principios de actuación de las administraciones públicas, así como la garantía de la protección de los datos personales



# Diagrama de tiempo ciberseguridad en administración digital



# Código de Derecho de la Ciberseguridad

Herramienta donde se puedan encontrar, actualizadas, las normas que afecten directamente a la ciberseguridad



Última modificación: **4 de mayo de 2022.**



[Descargar PDF](#) (7.239 KB)



[Descargar ePUB](#) (2.626 KB)



[Comprar edición en papel](#)



[Vídeo tutorial: Códigos electrónicos](#)



# Who is Who

Entidad	Base legal	Competencias principales
<b>Secretaría de Estado de Digitalización e Inteligencia Artificial</b>		
<b>SGAD</b>	RD 3/2010 RD 403/2020	<p>2.d) La elaboración, desarrollo, implantación y gestión del <b>Catálogo de Medios y Servicios Comunes, incluidos los Compartidos</b>.</p> <p>2.u) El <b>diseño, provisión y explotación de las infraestructuras tecnológicas y de los servicios de seguridad</b> necesarios para la prestación de servicios comunes, incluidos los declarados compartidos, que correspondan a la Secretaría General de Administración Digital.</p> <p>5.a) La <b>dirección técnica y estratégica del Centro de Operaciones de Ciberseguridad</b> de la Administración General del Estado (AGE) y sus organismos. De forma especial, asumirá la coordinación en la respuesta a incidentes.</p> <p>5.b) <b>El desarrollo y aplicación de lo dispuesto en el Real Decreto 3/2010</b> (Esquema Nacional de Seguridad) y sus Instrucciones Técnicas de Seguridad. En especial, la definición de estándares, de directrices técnicas y de gobierno TIC, de normas de seguridad de aplicación a las AA.PP. y la realización de propuestas e interlocución con el Centro Criptológico Nacional (CCN) en el desarrollo de guías de seguridad.</p>
<b>INCIBE</b>	Estatutos (Medio propio)	<p>La Sociedad tendrá como objeto social la gestión, asesoramiento, promoción y difusión de proyectos tecnológicos en el marco de la Sociedad de la Información.</p> <p>La Sociedad, como <b>medio propio personificado y servicio técnico de la AGE</b> y sus organismos públicos...</p>
<b>INCIBE-CERT</b>	Estatutos (Medio propio) RD-I 12/2018	<p>El INCIBE-CERT, del INCIBE, al que corresponde la <b>comunidad de referencia constituida por aquellas entidades no incluidas en el ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre</b>.</p> <p>Es el <b>centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado</b> en España operado por el INCIBE.</p> <p>El INCIBE-CERT será operado conjuntamente por el INCIBE y el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC) en todo lo que se refiera a la gestión de incidentes que afecten a los <b>operadores críticos</b>.</p>
<b>Red.es</b>	Estatutos (Medio Propio)	<p>Entidad pública adscrita al Ministerio de Asuntos Económicos y Transformación Digital a través de la SEDIA.</p> <p><b>Trabaja, además, por la seguridad en Internet de la mano de INCIBE.</b></p>

# Who is Who

Centro Nacional de Inteligencia (CNI)		
Centro Criptológico Nacional (CCN)	RD 421/2004	<p><b>Elaborar y difundir normas, instrucciones, guías y recomendaciones</b> para garantizar la seguridad de los sistemas TIC (las guías en cuestión se conocen como "Guías CCN-STIC" –Seguridad de las tecnologías de la información y las comunicaciones-).</p> <p><b>Formar al personal del Sector Público especialista</b> en el campo de la seguridad.</p> <p>Velar por el cumplimiento de la normativa relativa a la <b>protección de la información clasificada</b> en su ámbito de competencia.</p> <p>Coordinar la promoción, desarrollo, obtención, adquisición y puesta en explotación y uso de <b>tecnologías de seguridad</b>.</p> <p><b>Valorar y acreditar la capacidad de los productos de cifra</b> y de los sistemas para manejar información de forma segura.</p> <p><b>Constituir el Organismo de Certificación (OC)</b> del Esquema Nacional de Evaluación y Certificación de la Seguridad, de aplicación a productos y sistemas en su ámbito.</p> <p>Contribuir a la mejora de la ciberseguridad española, a través del <b>CCN-CERT</b>, afrontando de forma activa las amenazas que afecten a sistemas del Sector Público, a empresas y organizaciones de interés estratégico para el país, en coordinación con el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) y a cualquier sistema TIC que procese información clasificada.</p> <p>Establecer las necesarias relaciones y firmar los <b>acuerdos pertinentes con organizaciones similares de otros países</b>, para el desarrollo de las funciones mencionadas.</p>
CCN-CERT	RD 421/2004 RD 3/2010 RD-I 12/2018	<p>El CCN-CERT, del Centro Criptológico Nacional (CCN), al que corresponde la <b>comunidad de referencia constituida por las entidades del ámbito subjetivo de aplicación de la Ley 40/2015</b>, de 1 de octubre.</p> <p>En los <b>supuestos de especial gravedad</b> que reglamentariamente se determinen y que requieran un nivel de coordinación superior al necesario en situaciones ordinarias, <b>el CCN-CERT ejercerá la coordinación nacional de la respuesta técnica de los CSIRT</b> (equipos de respuesta a incidentes de seguridad informática - <i>Computer Security Incident Response Team</i>).</p> <p><b>Coordinación nacional de la respuesta técnica de los equipos de respuesta</b> a incidentes de seguridad informática (CSIRT) en materia de seguridad de las redes y sistemas de información del sector público comprendido en la Ley 39/2015 y en la Ley 40/2015.</p> <p><b>Ejercerá la función de enlace para garantizar la cooperación transfronteriza de los CSIRT de las AA.PP. con los CSIRT internacionales</b>, en la respuesta a los incidentes y gestión de riesgos de seguridad que les correspondan.</p>
Organismo de Certificación (OC)	RD 421/2004	<p>La <b>evaluación y certificación de un producto de seguridad TIC</b> está asignada al CCN a través del RD 421/2004 en sus artículos 1 y 2.1, el cual establece la de "constituir el organismo de certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las TI, de aplicación a productos y sistemas en su ámbito".</p>

# Who is Who

Presidencia del Gobierno		
Departamento de Seguridad Nacional (DSN)	RD 1119/2012	<b>Secretaría Técnica y órgano de trabajo permanente del Consejo de Seguridad Nacional (CSN)</b> y órganos de apoyo, Comités Especializados, como el <b>Consejo Nacional de Ciberseguridad (CNCS)</b> que ejercen funciones en ámbitos de actuación previstos en la Estrategia de Seguridad Nacional y la <b>Estrategia Nacional de Ciberseguridad 2019 (ENCS 2019)</b> .
Consejo Nacional de Ciberseguridad CNCS	Orden PRA/33/2018, de 22 de enero	<p><b>Órgano de apoyo del Consejo de Seguridad Nacional</b> de los previstos en el artículo 20.3 de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, al que corresponde ejercer las <b>funciones asignadas por aquél en el ámbito de la ciberseguridad</b> y en el marco del Sistema de Seguridad Nacional.</p> <p><b>Refuerza las relaciones de coordinación, colaboración y cooperación</b> entre las entidades de la Administración con competencias en materia de ciberseguridad, así como entre los sectores público y privado, y facilita la toma de decisiones del Consejo de Seguridad Nacional mediante el análisis, estudio y propuesta de iniciativas en el ámbito de la ciberseguridad.</p> <p>Cuenta como apoyo con la <b>Comisión Permanente de Ciberseguridad (CPCS)</b>.</p>
Foro Nacional de Ciberseguridad	Estrategia Nacional de Ciberseguridad 2019 (ENCS 2019)	La Estrategia Nacional de Ciberseguridad 2019 (ENCS 2019) en su línea de Acción 4. <i>Impulsar la ciberseguridad de ciudadanos y empresas</i> incluye la medida "9. <i>Promover la creación del foro Nacional de Ciberseguridad, que integre a representantes de la sociedad civil, expertos independientes, sector privado, la academia, asociaciones, organismos sin ánimo de lucro, entre otros, con el objetivo de potenciar y crear sinergias público privadas, particularmente en la generación de conocimiento sobre las oportunidades y amenazas para la seguridad en el ciberespacio.</i> "

# Who is Who

Secretaría de Estado de Seguridad		
<b>Centro Nacional de Protección de Infraestructuras y Críticas (CNPIC)</b>	Ley 8/2011 RD 704/2011 RD 770/2017 RD-I 12/2018	Actividades en relación con la <b>protección de las infraestructuras críticas</b> en el territorio nacional, en colaboración con otros departamentos ministeriales.  <b>Cuando las actividades que desarrollen puedan afectar de alguna manera a un operador crítico</b> , los CSIRT de referencia se coordinarán con el Ministerio del Interior, a través de la Oficina de Coordinación Cibernética (OCC) del CNPIC, de la forma que reglamentariamente se determine.
<b>Oficina de Coordinación Cibernética (OCC)</b>	RD 770/2017 RD-I 12/2018	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, y 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, desempeñando la <b>coordinación técnica en materia de ciberseguridad entre dicha Secretaría de Estado y sus organismos dependientes</b> , sin perjuicio de las competencias atribuidas a otros Ministerios
<b>Comisión Nacional PIC</b>	Ley 8/2011 RD 704/2011	Órgano colegiado adscrito a la Secretaría de Estado de Seguridad, que desarrolla las funciones que le encomiendan la Ley 8/2011 y su reglamento de desarrollo, el Real Decreto 704/2011.
<b>Unidad Central de Ciberdelincuencia de la Policía Nacional</b>		Policía Nacional
<b>Departamento de Delitos Telemáticos de la Guardia Civil (GDT)</b>		El Grupo de Delitos Telemáticos (GDT) fue creado para investigar, dentro de la Unidad Central Operativa de la Guardia Civil, todos aquellos delitos que se cometen a través de Internet.

## Who is Who

Ministerio de Defensa		
<b>ESPDEF-CERT</b>	RD-I 12/2018	Cooperará con el CCN-CERT y el INCIBE-CERT en aquellas situaciones que éstos requieran en apoyo de los operadores de servicios esenciales y, necesariamente, en aquellos operadores que tengan incidencia en la Defensa Nacional y que reglamentariamente se determinen.
<b>Mando conjunto de Ciberespacio (MCCE)</b>	Orden Ministerial 10/2013, por la que se crea el Mando Conjunto de Ciberdefensa	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 (FAS) en el ámbito ciberespacial.





## Contacto

---

**Fernando Suárez Lorenzo**

Presidente do CPEIG

[presidente@cpeig.gal](mailto:presidente@cpeig.gal)