uc3m | Universidad Carlos III de Madrid

OpenCourseWare

DERECHO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

Coordinadora Curso: **-Profª (PhD) María Nieves de la Serna Bilbao**

Titular de Derecho Administrativo UC3M// Departamento de Derecho Público

Co-directora del Máster Universitario en Derecho Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información// Instituto Pascual Madoz

LECCIÓN 10: CIBERSEGURIDAD Y AMENAZAS HÍBRIDAS

II. EL CONSEJO DE CIBERSEGURIDAD NACIONAL Y LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD.

Elaborado por Profs. Dr. Carlos Galán Pascual (PhD) y Carlos Galán Cordero

Profesores Área Derecho Administrativo// Departamento de Derecho Público

Profesores Máster Universitario en Derecho Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información// Instituto Pascual Madoz

Universidad Carlos III de Madrid

SUMARIO:

II. EL CONSEJO DE CIBERSEGURIDAD NACIONAL Y LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD.

II. EL CONSEJO DE CIBERSEGURIDAD NACIONAL Y LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD.

Desde el punto de vista de la gobernanza de la ciberseguridad en nuestro país debemos fijar nuestra atención en dos elementos esenciales: el órgano y su producto; es decir: el Consejo de Ciberseguridad Nacional y la Estrategia Nacional de Ciberseguridad.

El **Consejo Nacional de Ciberseguridad** es el órgano colegiado de apoyo al Consejo de Seguridad Nacional en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, en el marco de la Ley 50/1997, de 27 de noviembre, del Gobierno, creándose por Acuerdo del Consejo de Seguridad Nacional del 5 de diciembre de 2013, estando presidido por la Secretaria de Estado Directora del Centro Nacional de Inteligencia (CNI) y Directora del Centro Criptológico Nacional (CCN).

Como se señala en la página web del Departamento de Seguridad Nacional (DSN), Secretaría Técnica y órgano de trabajo permanente del Consejo, su composición refleja el espectro de los ámbitos de los departamentos, organismos y agencias del sector público con competencias en materia de ciberseguridad, para coordinar aquellas actuaciones que deban abordarse de forma conjunta, pudiendo requerir la presencia de otros actores cuya intervención para alguna sesión concreta se considere necesaria.

Forman el Consejo Nacional de Ciberseguridad:

- Secretaria de Estado Directora del Centro Nacional de Inteligencia (Presidencia).
- Director del Departamento de Seguridad Nacional (Vicepresidencia).
- Departamento de Seguridad Nacional (Secretaría).
- Ministerio de Asuntos Exteriores, Unión Europea y Cooperación.
- Ministerio de Defensa.
- Ministerio del Interior.
- Ministerio de Industria, Comercio y Turismo.
- Ministerio de Política Territorial.
- Ministerio de Ciencia e Innovación.
- Centro Nacional de Inteligencia.
- Ministerio de Derechos Sociales y Agenda 2030.
- Ministerio de Sanidad.
- Ministerio de Transformación Digital y para la Función Pública.

- Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática.
- Ministerio de Transportes, Movilidad y Agenda Urbana.
- Ministerio de Hacienda, y
- Ministerio de Justicia.

Sus **funciones** son las siguientes:

- Apoyar la toma de decisiones del Consejo de Seguridad Nacional en materia de ciberseguridad mediante el análisis, estudio y propuesta de iniciativas tanto en el ámbito nacional como en el internacional.
- Reforzar las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias relacionadas con el ámbito de la ciberseguridad, así como entre los sectores público y privado.
- Contribuir a la elaboración de propuestas normativas en el ámbito de la ciberseguridad para su consideración por el Consejo de Seguridad Nacional.
- Prestar apoyo al Consejo de Seguridad Nacional en su función de verificar el grado de cumplimiento de la Estrategia de Seguridad Nacional en lo relacionado con la ciberseguridad y promover e impulsar sus revisiones.
- Verificar el grado de cumplimiento de la Estrategia de Ciberseguridad Nacional e informar al Consejo de Seguridad Nacional.
- Realizar la valoración de los riesgos y amenazas, analizar los posibles escenarios de crisis, estudiar su posible evolución, elaborar y mantener actualizados los planes de respuesta y formular directrices para la realización de ejercicios de gestión de crisis en el ámbito de la ciberseguridad y evaluar los resultados de su ejecución, todo ello en coordinación con los órganos y autoridades directamente competentes.
- Contribuir a la disponibilidad de los recursos existentes y realizar los estudios y análisis sobre los medios y capacidades de las distintas Administraciones Públicas y Agencias implicadas con la finalidad de catalogar las medidas de respuesta eficaz en consonancia con los medios disponibles y las misiones a realizar, todo ello en coordinación con los órganos y autoridades directamente competentes y de acuerdo con las competencias de las diferentes Administraciones Públicas implicadas en el ámbito de la ciberseguridad.
- Facilitar la coordinación operativa entre los órganos y autoridades competentes cuando las situaciones que afecten a la Ciberseguridad lo precisen y mientras no actúe el Comité Especializado de Situación.

- Todas aquellas otras funciones que le encomiende el Consejo de Seguridad Nacional.

Como se desprende de la lista anterior, el Consejo Nacional de Ciberseguridad se centra en 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, facilitando la toma de decisiones mediante el análisis, estudio y propuesta de iniciativas tanto en los ámbitos nacional e internacional.

Uno de los resultados derivados de la función de este Consejo es la redacción y aprobación de las diferentes Estrategias Nacionales.

Por lo que toca a la ciberseguridad, la más reciente es la regulada por 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[1], y en cuya redacción participaron todos los miembros del Consejo Nacional de Ciberseguridad, además de un Comité de Expertos de asociaciones profesionales, empresas y del mundo académico.

Esta Estrategia Nacional de Ciberseguridad desarrolla las previsiones de la Estrategia de Seguridad Nacional de 2017 en el ámbito de la ciberseguridad, considerando los objetivos generales, el objetivo del ámbito y las líneas de acción establecidas para conseguirlo. Así, tras señalar la importancia del ciberespacio como espacio común global y esbozar sus amenazas y riesgos, la Estrategia, siguiendo el modelo iniciado por su antecedente de 2013, determina los objetivos de ciberseguridad nacional y las líneas de acción para alcanzarlos.

El cuadro siguiente muestra dichos **objetivos** y **líneas de acción**:

OBJETIVOS	LÍNEAS DE ACCIÓN[2]

[1] La primera Estrategia Nacional de Ciberseguridad, publicada en 2013, determinó los objetivos de ciberseguridad como Estado y las líneas de acción a desarrollar para alcanzarlos, sentando el modelo que se ha replicado en la estrategia vigente, alineando a nuestro país en la órbita de los países occidentales más avanzados en la materia. Galán Pascual ha tenido el privilegio de formar parte del equipo de redacción de ambas estrategias nacionales.
[2] Cada una de las Líneas de Acción contempla un conjunto de medidas concretas que, por su extensión, no reproducimos aquí.

OB.1 – Seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público.	LA.1 - Reforzar las capacidades ante las amenazas provenientes del ciberespacio.
	LA.2 – Garantizar la seguridad y resiliencia de los activos estratégicos para España.
OB.2 – Uso seguro y fiable del ciberespacio frente a un uso ilícito o malicioso.	LA.3 – 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.
OB.3 – Protección del ecosistema empresarial y social de los ciudadanos.	LA.4 – Impulsar la ciberseguridad de ciudadanos y empresas.
OB.4 – Cultura y compromiso con la ciberseguridad y protección de las capacidades humanas y tecnológicas.	LA.5 – Potenciar la industria española de ciberseguridad y la generación y retención de talento, para el fortalecimiento de la autonomía digital.
	LA.7 – Desarrollar una cultura de ciberseguridad.
OB.5 – Seguridad del ciberespacio en el ámbito internacional.	LA.6 – Contribuir a la seguridad del ciberespacio en el ámbito internacional, promoviendo un ciberespacio abierto, plural, seguro y confiable, en apoyo de los intereses nacionales.