TEMA 127. CIBERSEGURIDAD. LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

Actualizado a 11/01/2022

Contenido

1. CIBERSEGURIDAD, CIBERDEFENSA Y CIBERESPACIO 3
2. ESTRATEGIA NACIONAL DE CIBERSEGURIDAD 2019 3
   2.1. EL CIBERESPACIO: MÁS ALLÁ DE UN ESPACIO COMÚN GLOBAL 3
   2.2. LAS AMENAZAS Y DESAFÍOS EN EL CIBERESPACIO 4
   2.3. PROPÓSITO, PRINCIPIOS Y OBJETIVOS PARA LA CIBERSEGURIDAD 5
   2.4. LÍNEAS DE ACCIÓN Y MEDIDAS 6
   2.5. LA CIBERSEGURIDAD EN EL SISTEMA DE SEGURIDAD NACIONAL 11
      2.5.1. CONSEJO DE SEGURIDAD NACIONAL 11
      2.5.2. COMITÉ DE SITUACIÓN 11
      2.5.3. CONSEJO NACIONAL DE CIBERSEGURIDAD 12
      2.5.4. LA COMISIÓN PERMANENTE DE CIBERSEGURIDAD 13
      2.5.5. FORO NACIONAL DE CIBERSEGURIDAD 13
      2.5.6. AUTORIDADES PÚBLICAS COMPETENTES Y LOS CSIRT DE REFERENCIA NACIONALES 13
3. MARCO JURÍDICO RELEVANTE 13

1. CIBERSEGURIDAD, CIBERDEFENSA Y CIBERESPACIO

El ciberespacio 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 a la seguridad.

La Ciberseguridad se define como el conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan. La **seguridad en el ciberespacio** es un objetivo prioritario en las agendas de los gobiernos con el fin de garantizar su Seguridad Nacional y una competencia del Estado para crear una sociedad digital en la que la confianza es un elemento fundamental.

La nueva **Ciberseguridad** se extiende más allá del campo meramente de la protección del patrimonio tecnológico para adentrarse en las esferas política, económica y social. La ciberseguridad se especifica de una manera más amplia, como un derecho en el artículo 82 de la LO 3/2018 LOPDGDD: "Derecho a la seguridad digital", y específicamente en la Carta de Derechos Digitales española, en su sexto apartado.

La Ciberdefensa, además de prevenir los ataques como hace la Ciberseguridad, da respuesta a los mismos con nuevos ataques con fin de salvaguardar la seguridad.

Según el Global Cybersecurity Index publicado el mes de abril de 2021 por la UIT, España figura en cuarto lugar en el ámbito global y en tercer lugar en el Europeo (segundo tras Estonia en el marco de la UE). España ha mejorado posiciones desde la anterior publicación del índice. Se trata de un índice compuesto para medir el compromiso de los Estados Miembros de la UIT, 194, con la ciberseguridad (ver documento en carpeta). Se recomienda revisar antes del examen si han publicado actualización, ya que está a punto de renovarse: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Otro término destacable es la **ciberdiplomacia**, que consiste en fomentar el comportamiento responsable por parte de los Estados en relación al ciberespacio teniendo en cuenta qué puede hacer la comunidad internacional para mitigar las posibles amenazas, teniendo en cuenta aspectos políticos, legales y técnicos.

2. ESTRATEGIA NACIONAL DE CIBERSEGURIDAD 2019

En 2013 se aprobó la primera Estrategia Nacional de Ciberseguridad en España. La estrategia diseñaba el modelo de gobernanza para la ciberseguridad nacional.

La nueva Estrategia Nacional de Seguridad 2019 fue aprobada en el Consejo de Seguridad Nacional el 12 de Abril de 2019.

Se estructura en los siguientes 5 capítulos:

2.1 EL CIBERESPACIO: MÁS ALLÁ DE UN ESPACIO COMÚN GLOBAL

- **Nueva concepción del Ciberespacio:** es fundamental preservar la defensa de los valores y principios constitucionales y democráticos, así como los derechos fundamentales de los ciudadanos en el ciberespacio, especialmente en la **protección de sus datos personales, su privacidad, su libertad de expresión y el acceso a una información veraz y de calidad.**
- Transición de un modelo de ciberseguridad de **carácter preventivo y defensivo** hacia un esquema que incorpore elementos de **mayor fuerza disuasoria** obedece a un contexto global de mayor competencia geopolítica. **La disuasión** en ciberseguridad requiere la obtención y potenciación de capacidades de **ciberdefensa**, como elemento fundamental de la acción del Estado.
- Necesidad de una **mayor implicación de toda la sociedad** mediante el fomento de una **cultura de ciberseguridad**: el entendimiento de que el **ciudadano es corresponsable** de la ciberseguridad nacional.

2.2 LAS AMENAZAS Y DESAFÍOS EN EL CIBERESPACIO

- Las **ciberamenazas** son todas aquellas disrupciones o manipulaciones maliciosas que afectan a elementos tecnológicos. Afectan a la práctica totalidad de los ámbitos de la Seguridad Nacional, como la Defensa Nacional, la seguridad económica o la protección de las infraestructuras críticas, entre otros, y no distinguen fronteras.
- Las **acciones** que usan el ciberespacio para fines maliciosos pueden afectar a la estabilidad y al ejercicio de derechos y libertades, presentando sustanciales amenazas y desafíos para la Seguridad Nacional. Aprovechan las facilidades que concede el anonimato, la suplantación y la amplificación. Incluyen las relacionadas con **el ciberespionaje** y **la cibercriminalidad**.
    - El **Ciberespionaje** es un método relativamente económico, rápido y con menos riesgos que el espionaje tradicional, dada la dificultad de atribución de la autoría. Actores estatales. APT.
    - **Cibercriminalidad**, hace referencia al conjunto de actividades ilícitas cometidas en el ciberespacio que tienen por objeto los elementos, sistemas informáticos o cualesquiera otros bienes jurídicos, siempre que resulte determinante la utilización de herramientas tecnológicas; en función de la naturaleza del hecho punible en sí, de la autoría, de su motivación, o de los daños infligidos, se podrá hablar así de **ciberterrorismo**, de **ciberdelito**, o en su caso, de **hacktivismo**.
- Se constata una tendencia creciente de las denominadas **amenazas híbridas**, acciones coordinadas y sincronizadas dirigidas a atacar de manera deliberada las vulnerabilidades sistémicas de los estados democráticos y las instituciones. Explotan las facilidades que ofrece Internet para la **desinformación y propaganda**.
- El **empleo malintencionado de datos personales** y las **campañas de desinformación** tienen un alto potencial desestabilizador en la sociedad, y la explotación de brechas en los datos personales supone una violación a la seguridad de dichos datos, que afecta a la **privacidad de las personas** y a **la integridad** y **confidencialidad** de sus datos.
- **Campañas de desinformación**: elementos como las noticias falsas para influir en la opinión pública. Internet y las redes sociales amplifican el efecto y alcance de la información transmitida, en contra de objetivos como organizaciones internacionales, Estados, iniciativas políticas o personajes públicos o incluso a **procesos electorales democráticos.**

2.3 PROPÓSITO, PRINCIPIOS Y OBJETIVOS PARA LA CIBERSEGURIDAD

Propósito de la Estrategia Nacional de Ciberseguridad 2019: Fijar las directrices generales del ámbito de la ciberseguridad de manera que se alcancen los objetivos previstos en la Estrategia de Seguridad Nacional de 2017. Para ello:

- **Refuerzo de capacidades** para hacer frente a las ciberamenazas y el uso malicioso del ciberespacio.
- Fomento de la **cultura de ciberseguridad** a fin de contar con una sociedad más conocedora de las amenazas y desafíos.
- **Apoyo e impulso de la industria** española de ciberseguridad, la promoción de un entorno que favorezca la investigación, el desarrollo y la innovación, y la participación del mundo académico.
- Alcanzar y mantener los **conocimientos, habilidades**, experiencia y capacidades tecnológicas y profesionales.
- Cooperación y cumplimiento del Derecho internacional, y máximo respeto a los principios recogidos en la Constitución y en la Carta de Naciones Unidas.

La Estrategia de Ciberseguridad 2019 se sustenta y se inspira en los **principios rectores** de la Seguridad Nacional:

1. **Unidad de acción**
2. **Anticipación**
3. **Eficiencia**
4. **Resiliencia**

OBJETIVO GENERAL

> *"En línea con la Estrategia de Seguridad Nacional de 2017 y ampliando el objetivo para la ciberseguridad previsto en la misma, España garantizará el **uso seguro y fiable del ciberespacio**, **protegiendo** los **derechos** y las **libertades** de los ciudadanos y promoviendo el **progreso socio económico**"*

Objetivos específicos

Se fijan una serie de objetivos específicos que orientan la acción del Estado en este ámbito:

- **Ob 1: Seguridad y resiliencia** de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales.
- **Ob 2: Uso seguro y fiable** del ciberespacio frente a su uso ilícito o malicioso.
- **Ob 3: Protección del ecosistema** empresarial y social y de los ciudadanos.
- **Ob 4: Cultura y compromiso** con la ciberseguridad y potenciación de las capacidades humanas y tecnológicas.
- **Ob 5: Seguridad** del ciberespacio en el ámbito **internacional**.

2.4 LÍNEAS DE ACCIÓN Y MEDIDAS

La Estrategia de Ciberseguridad 2019 define una serie de líneas de acción y medidas por cada objetivo específico. Así:

- **Ob1: Seguridad y resiliencia** de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales.
  Con respecto a las líneas de acción 1 y 2, se ha publicado el Real Decreto 43/2021 por el que se desarrolla el Real Decreto-ley 12/2018, de seguridad y sistemas de información. Este Real Decreto define, entre otras cuestiones, la cooperación y coordinación de los CSIRT de referencia: CCN-CERT, MCCE e INCIBE-CERT, así como las tareas y apoyo de los CSIRT de referencia a los operadores críticos, operadores de servicios esenciales, proveedores de servicios digitales, las autoridades competentes, la Oficina de Coordinación de Ciberseguridad, entre otros, creando para ello, la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes y la red de CSIRT.
    - **Línea 1:** ***Reforzar las capacidades ante las amenazas provenientes del ciberespacio***
      - 1. Ampliar y mejorar las capacidades de detección y análisis de las ciberamenazas de manera que se permita la identificación de procedimientos y orígenes de ataque, así como la elaboración de la inteligencia necesaria para una protección, atribución y defensa más eficaz.
      - 2. Potenciar la colaboración de los centros de excelencia e investigación en la lucha contra las ciberamenazas.
      - 3. Potenciar la creación, difusión y aplicación de mejores prácticas, y la adopción de estándares en materia de ciberseguridad.
      - 4. Asegurar la coordinación técnica y operacional de los organismos con responsabilidades en ciberseguridad, las empresas y la sociedad.
      - 5. Desarrollar y mantener actualizadas las normas, procedimientos e instrucciones de respuesta frente a incidentes de ciberseguridad, asegurando su integración en el Sistema de Seguridad Nacional.
      - 6. Potenciar las capacidades de ciberdefensa y de ciberinteligencia.
      - 7. Promover la participación de las empresas en plataformas sectoriales para el intercambio y análisis de información, así como para la medida del riesgo sectorial y la propuesta de acciones que lo mitiguen, acompañadas de requerimientos legales que las regulen.
      - 8. Potenciar y apoyar los desarrollos realizados en la red de CSIRT española.
      - 9. Impulsar el desarrollo de plataformas de notificación, intercambio de información y coordinación para la mejora de la ciberseguridad sectorial.
      - 10. Desarrollar instrumentos de prevención, detección, respuesta, retorno a la normalidad y evaluación enfocados a la gestión de crisis para el ámbito de la ciberseguridad en el marco de la Seguridad Nacional.
      - 11. Garantizar la coordinación, la cooperación y el intercambio de información sobre ciberincidentes e inteligencia de ciberamenazas entre el sector público, el sector privado y los organismos internacionales competentes, fomentando la prevención y la alerta temprana.

- 12. Implantar medidas de ciberdefensa activa en el sector público con el objetivo de mejorar las capacidades de respuesta.

- **Línea 2:** ***Garantizar la seguridad y resiliencia de los activos estratégicos para España.***
  - 1. Ampliar y fortalecer las capacidades de prevención, detección, respuesta, recuperación y resiliencia a los ciberataques dirigidos al sector público, a los servicios esenciales y a empresas de interés estratégico.
  - 2. Potenciar el desarrollo de la normativa sobre protección de infraestructuras críticas, reforzando la seguridad de las redes y sistemas de información que las soportan.
  - 3. Asegurar 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, con un enfoque prioritario basado en el riesgo.
  - 4. Potenciar, en el marco de sus competencias, la progresiva implicación y creación de infraestructuras de ciberseguridad en las Comunidades Autónomas, las Ciudades Autónomas, las Entidades Locales y en sus organismos vinculados o dependientes que cooperarán y se coordinarán con las estructuras nacionales en pro de la mejora de la ciberseguridad nacional.
  - 5. Desarrollar el Centro de Operaciones de Ciberseguridad de la Administración General del Estado que mejore las capacidades de prevención, detección y respuesta, e impulsar el desarrollo de centros de operaciones de ciberseguridad en el ámbito autonómico y local.
  - 6. Reforzar la implantación de infraestructuras y servicios de telecomunicaciones y sistemas de información horizontales comunes, y compartidos por las Administraciones Públicas, potenciando su uso y sus capacidades de seguridad y resiliencia, asegurando a la par, la coordinación con los primeros en aquellos casos que no se utilicen las infraestructuras y servicios comunes.
  - 7. Impulsar el desarrollo de un sistema de métricas de las principales variables de ciberseguridad que permita a las autoridades competentes determinar el nivel de seguridad y su evolución.
  - 8. Comprometer al sector público y al privado en la gestión de los riesgos de la cadena de suministro, especialmente en aquellos que afecte a la provisión de servicios esenciales.
  - 9. Desarrollar catálogos de productos y servicios cualificados y certificados, para su empleo en los procesos de contratación del sector público y de los servicios esenciales.
  - 10. Reforzar las estructuras de seguridad y la capacidad de vigilancia de los sistemas de información que manejan información clasificada.
  - 11. Promover la realización de ciberejercicios y evaluaciones de ciberseguridad, especialmente en áreas que puedan afectar a la Seguridad Nacional, la Administración pública, los servicios esenciales y las empresas cotizadas.
  - 12. Asegurar la protección de las Infraestructuras Científico-Técnicas Singulares y los centros de referencia de I+D+i.

- **Ob2:** Uso **seguro y fiable** del ciberespacio frente a su uso ilícito o malicioso.

- **Línea 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.***

    - 1. Reforzar el marco jurídico para responder eficazmente a la cibercriminalidad, tanto en lo relativo a la definición de tipos penales como en la regulación de adecuadas medidas de investigación.
    - 2. Fomentar la colaboración y participación ciudadana, articulando instrumentos de intercambio y transmisión de información de interés policial, y promoviendo el desarrollo de campañas de prevención de la cibercriminalidad orientadas a ciudadanos y empresas.
    - 3. Reforzar las acciones encaminadas a potenciar las capacidades de investigación, atribución, persecución y, en su caso, la actuación penal, frente a la cibercriminalidad.
    - 4. Fomentar el traslado a los organismos competentes de la jurisdicción penal de la información relativa a incidentes de seguridad que presenten caracteres de delito, y especialmente de aquellos que afecten o puedan afectar a la provisión de los servicios esenciales y a las infraestructuras críticas.
    - 5. Procurar a los operadores jurídicos el acceso a información y recursos materiales que aseguren una mejor aplicación del marco jurídico y técnico relacionado con la lucha contra la cibercriminalidad, y que les dote de mayores capacidades para la investigación y enjuiciamiento de los hechos ilícitos que correspondan.
    - 6. Fomentar el intercambio de información, experiencia y conocimientos, entre el personal con responsabilidades en la investigación y persecución de la cibercriminalidad.
    - 7. Asegurar a los profesionales del Derecho y a las Fuerzas y Cuerpos de Seguridad del Estado el acceso a los recursos humanos y materiales que les proporcionen el nivel necesario de conocimientos para la mejor aplicación del marco legal y técnico asociado.
    - 8. Impulsar la coordinación de las investigaciones sobre cibercriminalidad y otros usos ilícitos del ciberespacio entre los distintos órganos y unidades con competencia en esta materia.
    - 9. Fortalecer la cooperación judicial y policial internacional.

- **Ob3: Protección del ecosistema** empresarial y social y de los ciudadanos.
    - **Línea 4:** ***Impulsar la ciberseguridad de ciudadanos y empresas.***
        - 1. Ofrecer a los ciudadanos y al sector privado un servicio público de ciberseguridad integrado, de calidad y de fácil acceso, y que sea un estímulo a la demanda de los servicios que ofrece el sector empresarial de la ciberseguridad.
        - 2. Impulsar la ciberseguridad en las pymes, micropymes y autónomos mediante la articulación de políticas públicas en ciberseguridad, y especialmente con actuaciones dirigidas al fomento de la resiliencia.
        - 3. Promover la ciberseguridad para garantizar la privacidad y protección de datos personales dentro del marco de los derechos digitales del ciudadano acorde con el ordenamiento jurídico, promoviendo la protección de la “identidad digital”.
        - 4. Crear mecanismos ágiles y seguros de denuncia para el sector privado y ciudadanos.

- 5. Estimular la cooperación entre actores públicos y privados, en particular promoviendo el compromiso de los Proveedores de Servicios de Internet y de Servicios Digitales para mejorar la ciberseguridad. Se impulsará la regulación nacional en este sentido y se implantarán medidas de ciberdefensa activa de ciudadanos y pymes.
- 6. Desarrollar mecanismos para la medida agregada del riesgo y su evolución, tanto de ciudadanos como de empresas, para priorizar medidas de ciberseguridad e informar adecuadamente a la sociedad.
- 7. Impulsar en el sector empresarial la implantación de estándares reconocidos de ciberseguridad. Estimular, junto con las entidades de normalización nacional e internacional, la creación, difusión y aplicación de mejores prácticas sectoriales en materia de ciberseguridad, incluidos diferentes esquemas de certificación.
- 8. Impulsar la implantación de sistemas fiables de identificación electrónica y servicios electrónicos de confianza.
- 9. 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.

- **Ob4: Cultura y compromiso** con la ciberseguridad y potenciación de las capacidades humanas y tecnológicas.
  - **Línea 5:** ***Potenciar la industria española de ciberseguridad, y la generación y retención de talento, para el fortalecimiento de la autonomía digital.***
    - 1. Impulsar programas de apoyo a la I+D+i en seguridad digital y ciberseguridad en pymes, empresas, universidades y centros de investigación, facilitando el acceso a programas de incentivos nacionales e internacionales y mediante programas de compra pública innovadora.
    - 2. Dinamizar el sector industrial y de servicios de ciberseguridad, incentivando medidas de apoyo a la innovación, a la inversión, a la internacionalización y a la transferencia tecnológica en especial en el caso de micropymes y pymes.
    - 3. Incrementar las actividades nacionales para el desarrollo de productos, servicios y sistemas de ciberseguridad, y la seguridad desde el diseño, apoyando específicamente aquellas que sustenten necesidades de interés nacional para fortalecer la autonomía digital, y la propiedad intelectual e industrial.
    - 4. Promover las actividades de normalización y la exigencia de requisitos ciberseguridad en los productos y servicios de Tecnologías de la Información y de las Comunicaciones, facilitar el acceso a productos y servicios que respondan a estos requisitos, promoviendo la evaluación de la conformidad y la certificación, y apoyando la elaboración de catálogos.
    - 5. Actualizar, o en su caso desarrollar marcos de competencias en ciberseguridad, que respondan a las necesidades del mercado laboral.
    - 6. Identificar las necesidades de capacidades profesionales de ciberseguridad, fomentando la colaboración con las instituciones educativas y formativas impulsando la

formación continua, la formación para el empleo y universitaria, promoviendo sistemas de acreditación y certificación profesional.

- 7. Impulsar la inclusión de perfiles profesionales de ciberseguridad en las relaciones de puestos de trabajo del sector público.
- 8. Detectar, fomentar y retener el talento en ciberseguridad, con especial atención al campo de la investigación.
- 9. Impulsar programas específicos de I+D+i en ciberseguridad y ciberdefensa.

- **Ob5:** Seguridad del ciberespacio en el ámbito internacional.
  - **Línea 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.***
    - 1. Potenciar y reforzar la presencia de España en las organizaciones, conferencias y foros regionales e internacionales y a los que pertenece y en los que la ciberseguridad forma parte sustancial de sus agendas, y apoyar y participar de manera activa en las diferentes iniciativas, coordinando la posición de los diferentes agentes nacionales implicados.
    - 2. Promover en el ámbito de Naciones Unidas la búsqueda de consensos para el pleno respeto a la Carta de Naciones Unidas y la aplicación y puesta en práctica del Derecho Internacional y las normas para el comportamiento responsable de los Estados. Y del mismo modo avanzar en la adopción e implementación de Medidas para el Fomento de la Confianza en el ciberespacio.
    - 3. Participar activamente en la Unión Europea en el desarrollo de un ecosistema europeo seguro que favorezca el avance y la consolidación del mercado único, y la seguridad y autonomía estratégica de Europa, buscando las complementariedades y la cooperación entre la Unión Europea y la OTAN.
    - 4. Fomentar el diálogo bilateral, la cooperación y los sistemas de intercambio de información, alerta temprana y de experiencias para desarrollar un enfoque coordinado en la lucha contra las ciberamenazas con otros países, promoviendo la negociación y firma de acuerdos internacionales.
    - 5. Promover el desarrollo de capacidades tecnológicas y el acceso a internet en terceros países para contribuir con ello al cumplimiento de los Objetivos de Desarrollo Sostenible.
    - 6. Desarrollar con los países de nuestro entorno una mayor conciencia sobre las Amenazas Híbridas, limitando su impacto sobre la soberanía e integridad de nuestros países.

  - **Línea 7:** ***Desarrollar una cultura de ciberseguridad.***
    - 1. Incrementar las campañas de concienciación a ciudadanos y empresas, y poner a su disposición información útil adaptada a cada perfil, especialmente en el ámbito de los autónomos, pequeñas y medianas empresas.
    - 2. Potenciar actuaciones encaminadas al incremento de la corresponsabilidad y obligaciones de la sociedad en la ciberseguridad nacional.
    - 3. Impulsar iniciativas y planes de alfabetización digital en ciberseguridad.

- 4. Promover la difusión de la cultura de la ciberseguridad como una buena práctica empresarial, y reconocer la implicación de las empresas en la mejora de la ciberseguridad colectiva como responsabilidad social corporativa.
- 5. Promover un espíritu crítico en favor de una información veraz y de calidad y que contribuya a la identificación de las noticias falsas y la desinformación.
- 6. Concienciar a directivos de organizaciones, a los efectos de que habiliten los recursos necesarios y promuevan los proyectos de ciberseguridad que sus entidades puedan necesitar.
- 7. Promover la concienciación y formación en ciberseguridad en los centros de enseñanza, adaptada a todos los niveles formativos y especialidades.
- 8. Buscar y reconocer la colaboración y participación de medios de comunicación, para lograr un mayor alcance en las campañas dirigidas a ciudadanos y, en especial, a menores de edad.

2.5 LA CIBERSEGURIDAD EN EL SISTEMA DE SEGURIDAD NACIONAL

La Estrategia de 2019 impulsa iniciativas que complementan los nuevos avances en el modelo de gobernanza nacional con las políticas europeas. La estructura de la ciberseguridad en el marco del Sistema de Seguridad Nacional está constituida por los siguientes componentes:

1. El Consejo de Seguridad Nacional.
2. El Comité de Situación, único para el conjunto del Sistema de Seguridad Nacional ante situaciones de crisis.
3. El Consejo Nacional de Ciberseguridad.
4. La Comisión Permanente de Ciberseguridad.
5. El Foro Nacional de Ciberseguridad.
6. Las Autoridades públicas competentes y los CSIRT de referencia nacionales.

2.5.1 CONSEJO DE SEGURIDAD NACIONAL

El Consejo de Seguridad Nacional, 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.

El Consejo de Seguridad Nacional actúa, a través del Departamento de Seguridad Nacional como punto de **contacto** único para ejercer una función de enlace y garantizar la cooperación transfronteriza con otros países de la **Unión Europea**.

2.5.2 COMITÉ DE SITUACIÓN

El Comité de Situación tiene carácter único para el conjunto del Sistema de Seguridad Nacional y actuará, apoyado por el Departamento de Seguridad Nacional, de acuerdo con las directrices político-estratégicas dictadas por el Consejo de Seguridad Nacional en materia de **gestión de crisis**.

2.5.3 CONSEJO NACIONAL DE CIBERSEGURIDAD

El Consejo Nacional de Ciberseguridad es un órgano colegiado de apoyo al Consejo de Seguridad Nacional. El Consejo refuerza 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 facilitará la toma de decisiones del propio Consejo mediante el análisis, estudio y propuesta de iniciativas tanto en el ámbito nacional como en el internacional.

El Consejo Nacional de Ciberseguridad se crea por Acuerdo del Consejo de Seguridad Nacional del 5 de diciembre de 2013.

El Consejo Nacional de Ciberseguridad ejercerá las siguientes funciones:

- 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

2.5.4 LA COMISIÓN PERMANENTE DE CIBERSEGURIDAD

La Comisión Permanente de Ciberseguridad se establece con objeto de facilitar la **coordinación interministerial a nivel operacional** en el ámbito de la ciberseguridad. Presidida por el Departamento de Seguridad Nacional, se compone de aquellos órganos y organismos representados en el Consejo Nacional de Ciberseguridad con responsabilidades operativas. Es el órgano al que corresponde asistir al Consejo Nacional de Ciberseguridad sobre aspectos relativos a la valoración técnica y operativa de los riesgos y amenazas a la ciberseguridad.

2.5.5 FORO NACIONAL DE CIBERSEGURIDAD

Es elemento novedoso de colaboración público privada, que actuará en la potenciación y creación de sinergias público privadas, particularmente en la generación de conocimiento sobre las oportunidades y los desafíos y amenazas a la seguridad en el ciberespacio.

La puesta en marcha del foro Nacional de Ciberseguridad, y la armonización de su funcionamiento con los órganos existentes, se realizará mediante la aprobación de las disposiciones normativas necesarias, con el objetivo de alcanzar el funcionamiento coordinado y eficiente de estos componentes en el Sistema de Seguridad Nacional.

2.5.6 AUTORIDADES PÚBLICAS COMPETENTES Y LOS CSIRT DE REFERENCIA NACIONALES

El marco estratégico e institucional de la ciberseguridad se complementa con las autoridades públicas competentes en materia de seguridad de las redes y sistemas de información y los CSIRT de referencia nacional que se recogen en el marco jurídico nacional.

Asimismo, los CSIRT de las Comunidades Autónomas, de las Ciudades Autónomas, de las Entidades Locales y sus organismos vinculados o dependientes, los de las entidades privadas, la red de CSIRT.es y otros servicios de ciberseguridad relevantes deberán estar coordinados con los anteriores en función de las competencias de cada uno de ellos. De igual modo, desde los CSIRT nacionales, en colaboración con los CSIRT autonómicos y privados, se fomentará la puesta en marcha de iniciativas que contribuyan a la consecución de los objetivos de la estrategia nacional.

3. MARCO JURÍDICO RELEVANTE

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que transpone al ordenamiento jurídico español la Directiva (UE) 2016/1148 (conocida como Directiva NIS)
- Real Decreto 43/2021, de 26 de Enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Ley 36/2015, de 28 de septiembre, de Seguridad Nacional (contempla la ciberseguridad como ámbito de especial interés).

- Real Decreto 1150/2021, de 28 de Diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021.
- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

Otros:

- 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»).
- Estrategia Europea de Ciberseguridad (52013JC0001), Comunicación conjunta al Parlamento europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones.
- EJE nº 3 CIBERSEGURIDAD del programa ESPAÑA DIGITAL 2026 (medidas 9-12).