**Estrategia Nacional de Ciberseguridad 2019**

|  |
| --- |
| **Enlaces** |
| [Enlace a al BOE](https://www.boe.es/buscar/doc.php?id=BOE-A-2019-6347)  [Texto Consolidado](https://www.boe.es/buscar/act.php?id=BOE-A-2019-6347)  [Enlace1](https://www.dsn.gob.es/es/file/2988/download?token=K4T9k3hV)  [dsn.gob.es](https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019)  [Capitulo a Capitulo](https://www.lisainstitute.com/blogs/blog/estrategia-nacional-ciberseguridad-espana-2019) |
| **Videos** |
| Video1  Video1  Video1 |
| **Apuntes** |
| [Resumen chatGPT](#_Resumen_chatGPT)  [Resumen CAP1 chatGPT](#_Resumen_CAP1_chatGPT) |

## Resumen chatGPT

La Estrategia de Ciberseguridad 2019 es un plan integral diseñado para abordar los desafíos y riesgos en materia de ciberseguridad en España. Esta estrategia tiene como objetivo principal fortalecer la seguridad digital y proteger los sistemas de información del país. Aquí tienes un resumen de sus principales aspectos:

1. **Marco de actuación**: La estrategia establece un marco general de actuación en el ámbito de la ciberseguridad, que incluye la coordinación entre diferentes organismos públicos y la colaboración con el sector privado.
2. **Principales áreas de actuación**:
   * **Prevención y concienciación**: Promoción de la concienciación sobre la importancia de la ciberseguridad, tanto en el ámbito público como privado.
   * **Protección y resiliencia**: Refuerzo de la protección de infraestructuras críticas y mejora de la capacidad de respuesta ante ciberataques.
   * **Normativa y regulación**: Desarrollo y actualización de la normativa relacionada con la ciberseguridad para adaptarse a las nuevas amenazas y tecnologías.
   * **Cooperación internacional**: Colaboración con otros países y organizaciones internacionales para compartir información y buenas prácticas en materia de ciberseguridad.
   * **Innovación y desarrollo tecnológico**: Impulso de la investigación, desarrollo e innovación en ciberseguridad para mantenerse al día con las últimas tecnologías y tendencias.
3. **Medidas específicas**: La estrategia incluye medidas concretas para fortalecer la ciberseguridad, como la creación de equipos de respuesta a incidentes, la promoción de la formación especializada en ciberseguridad y el desarrollo de sistemas de alerta temprana.
4. **Participación del sector privado y la sociedad civil**: Reconoce la importancia de la colaboración con el sector privado y la sociedad civil para mejorar la ciberseguridad, fomentando la participación activa de estos actores en la implementación de la estrategia.

En resumen, la Estrategia de Ciberseguridad 2019 en España es un plan integral que aborda diversos aspectos para fortalecer la seguridad digital del país, incluyendo la prevención, protección, normativa, cooperación internacional y la participación del sector privado y la sociedad civil.

## Resumen Capitulo a capitulo.

La Estrategia Nacional de Ciberseguridad capítulo a capítulo.

**El capítulo 1** “El ciberespacio como espacio común global” presenta las oportunidades y desafíos del ciberespacio y la infraestructura digital, expone el carácter internacional de la aproximación a su seguridad y describe los principales rasgos de la nueva concepción de la ciberseguridad en España.

**En el capítulo 2** “Las amenazas y desafíos en el ciberespacio” se examinan las principales amenazas y desafíos del ciberespacio a los que se enfrenta España. Estas amenazas y desafíos se clasifican en dos categorías:

1. Las que amenazan a activos que forman parte del ciberespacio;
2. Aquellas que usan el ciberespacio como medio para realizar actividades maliciosas e ilícitas de todo tipo.

Dentro de esas **acciones maliciosas** que usan el ciberespacio están:

* **Ciberespionaje**: Este método es mucho más rápido y con menores riesgos que el espionaje tradicional debido al fácil anonimato. Se realiza principalmente por **organismos de inteligencia y militares** que poseen sofisticados recursos e infraestructuras y amplios conocimientos. En el documento se advierte que están aumentando las llamadas **amenazas híbridas** que constituyen un ataque a las vulnerabilidades de las instituciones y estados democráticos a través de distintos medios como acciones militares tradicionales, ciberataques, [**operaciones de manipulación de la información**](https://www.lisainstitute.com/blogs/blog/ataques-desinformacion-que-son-como-evitarlos), o elementos de presión económica.
* **Cibercriminalidad**: Aquí hablamos de ciberterrorismo, ciberdelitos o hacktivismo.
  + Los ciberdelincuentes actúan bajo esquemas de crimen organizado y pretenden usar técnicas para crear modelos de negocio lucrativo y de bajo riesgo, por la difícil localización de sus acciones.
  + Los grupos terroristas usan las debilidades del ciberespacio para realizar ciberataques o efectuar acciones de radicalización de personas y grupos, divulgación de técnicas y herramientas para la comisión de atentados, y de reclutamiento, adiestramiento o propaganda. [**Para saber más de la propaganda yihadista haz clic aquí.**](https://www.lisainstitute.com/blogs/blog/terrorismo-yihadista-propaganda-internet-radicalizacion)
  + Los grupos hacktivistas realizan ciberataques por motivos ideológicos y pretenden efectuar ataques con un gran impacto social o mediático.

**En el capítulo 3** “Propósito, principios y objetivos para la ciberseguridad” se establece el propósito y los principios por los que se rige la Estrategia (unidad de acción, anticipación, eficiencia y resiliencia), así como los objetivos, uno general y cinco específicos que resultan transversales a todos los ámbitos.

Los 4 principios por los que se rige la Estrategia Nacional de Ciberseguridad.

1. **Unidad de acción:**Toda respuesta ante un incidente en el ámbito de la ciberseguridad que pueda implicar a distintos agentes del Estado se verá reforzada si es coherente, coordinada y se resuelve de manera rápida y eficaz, cualidades alcanzables a través de la adecuada preparación y articulación de la unidad de acción del Estado.
2. **Anticipación:**Priman las actuaciones preventivas sobre las reactivas. Disponer de sistemas eficaces, con información compartida lo más próximo al tiempo real, permite alcanzar un adecuado conocimiento de la situación. Dicho factor resulta imprescindible para minimizar el tiempo de respuesta, lo que puede resultar crítico para reducir los efectos de las amenazas.
3. **Eficiencia:**La ciberseguridad precisa del empleo de sistemas multipropósito de gran valor y elevado nivel tecnológico, que llevan asociadas unas necesidades muy exigentes y un alto coste derivado de su desarrollo, adquisición y operación. A lo anterior se suma la necesidad de una planificación anticipada y una elevada complejidad en su sostenimiento.
4. **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.

Objetivos de la Estrategia Nacional de Ciberseguridad.

**Objetivo general:** 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**:

1. **Seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales a fin de crear servicios más eficientes y seguros.** Para ello es necesario aplicar medidas de seguridad que mejoren la capacidad de prevención, detección y respuesta ante un ciberataque, mediante un refuerzo de la coordinación y adaptación de la legislación. [**Si quieres aprender a gestionar mejor la Ciberseguridad, haz clic aquí.**](https://www.lisainstitute.com/collections/cursos/products/curso-gestion-ciberseguridad)
2. **Uso seguro y fiable del ciberespacio frente a su uso ilícito o malicioso.** Para ello, es importante reforzar la cooperación judicial y policial, nacional e internacional, y proporcionar formación y suficientes recursos a los organismos competentes para investigar el cibercrimen. También es esencial la colaboración ciudadana en este ámbito.
3. **Protección del ecosistema empresarial y social y de los ciudadanos para garantizar el derecho que tienen todas las organizaciones y ciudadanos a usar el ciberespacio de forma segura.** Más allá de las medidas de seguridad que implanten los profesionales y empresas para garantizar la protección de la información que manejan, es necesario que el Estado establezca unas medidas generales de ciberseguridad que serán de obligado cumplimiento. Por su parte, los ciudadanos deben también hacer un uso responsable de la red.
4. **Cultura y compromiso con la ciberseguridad y potenciación de las capacidades humanas y tecnológicas.** Para ello, debe fomentarse una cultura de la ciberseguridad mediante acciones de comunicación en los medios y de formación e información a ciudadanos y empresas. Es importante que exista una adecuada oferta formativa para profesionales en ciberseguridad ya que es uno de los perfiles más demandados actualmente por las empresas. [**Si estás planteándote mejorar tu perfil profesional, valora formarte en ciberseguridad como especialización o complemento a tu experiencia y conocimientos**](https://www.lisainstitute.com/collections/cursos/ciberseguridad).
5. **Seguridad del ciberespacio en el ámbito internacional. Se pretende crear un marco para la cooperación y la prevención internacional de ciberdelitos con el que se creará un ciberespacio más seguro, plural y fiable.** A través de la colaboración internacional se aumentará la confianza en Internet, en el desarrollo de nuevas tecnologías y en la transformación digital. Con ello se pretende llegar al mercado único digital. [**Si quieres aplicar tus conocimientos en Ciberinteligencia, te recomendamos este curso.**](https://www.lisainstitute.com/products/curso-experto-en-ciberinteligencia)

**En el capítulo 4**“Líneas de acción y medidas” se establecen las líneas de acción dirigidas a la consecución de los objetivos establecidos.

1. **Reforzar las capacidades** ante las amenazas provenientes del ciberespacio.
2. **Garantizar la seguridad y resiliencia de los activos estratégicos** para España. Incluye entre sus medidas las siguientes: “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; y "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.”
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.
4. **Impulsar la ciberseguridad de ciudadanos y empresas.**
5. **Potenciar la industria española de ciberseguridad**, y la generación y retención de talento, para el fortalecimiento de la autonomía digital.
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.
7. **Desarrollar una cultura de ciberseguridad**.

**En el capítulo 5** “La ciberseguridad en el Sistema de Seguridad Nacional” define la arquitectura orgánica de la ciberseguridad, integrándola en el actual **Sistema de Seguridad Nacional** con 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.