ESTRATEGIA DE CIBERSEGURIDAD NACIONAL

2013

NIPO 002-13-042-8

GOBIERNO DE ESPAÑA

PRESIDENCIA DEL GOBIERNO

ESTRATEGIA DE CIBERSEGURIDAD NACIONAL

El uso de las Tecnologías de la Información y de la Comunicación se ha incorporado de forma general a la vida cotidiana de nuestra nación. Este nuevo escenario facilita un desarrollo sin precedentes en el intercambio de información y comunicaciones, pero, al mismo tiempo, conlleva serios riesgos y amenazas que pueden afectar a la Seguridad Nacional.

Varios son los factores que contribuyen a la proliferación de acciones delictivas en el ciberespacio. La rentabilidad que ofrece su explotación en términos económicos, políticos o de otro tipo, la facilidad y el bajo coste de empleo de las herramientas utilizadas para la consecución de ataques, y la facilidad de ocultación del atacante hacen posible que estas actividades se lleven a cabo de forma anónima y desde cualquier lugar del mundo, con impactos transversales sobre los sectores público y privado y los propios ciudadanos.

Los distintos perfiles de atacantes que explotan las vulnerabilidades tecnológicas con el objeto de recabar información, sustraer activos de gran valor y amenazar los servicios básicos, pueden afectar al normal funcionamiento de nuestro país. El disfrute pacífico de ciertos derechos fundamentales consagrados en nuestra Constitución y en el ordenamiento jurídico internacional puede verse seriamente comprometido como consecuencia de este tipo de acciones.

Plenamente consciente de la importancia de la cuestión y comprometido con el desarrollo de la Sociedad Digital, el Consejo de Seguridad Nacional ha impulsado la elaboración de la Estrategia de Ciberseguridad Nacional con el fin de dar respuesta al enorme desafío que supone la preservación del ciberespacio de los riesgos y amenazas que se ciernen sobre él.

La Estrategia de Ciberseguridad Nacional se adopta al amparo y alineada con la Estrategia de Seguridad Nacional de 2013, que contempla la ciberseguridad dentro de sus doce ámbitos de actuación.

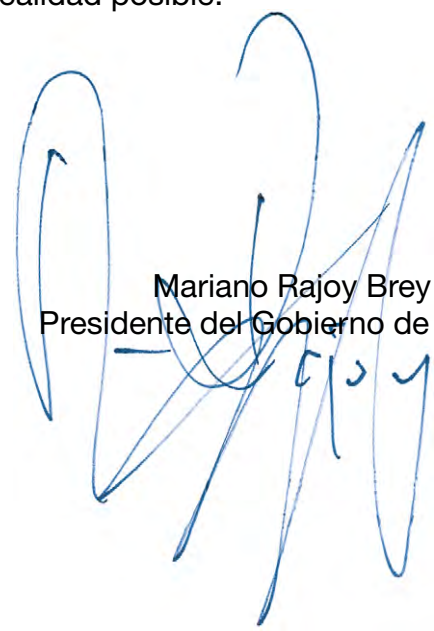
La aprobación del presente documento de carácter estratégico pone de manifiesto las capacidades colectivas y el compromiso de una nación que apuesta en firme por garantizar su seguridad en el ciberespacio. Para España, los

avances en el ámbito de la ciberseguridad contribuyen además a incrementar nuestro potencial económico, ya que promueven un entorno más seguro para la inversión, la generación de empleo y la competitividad.

La Estrategia de Ciberseguridad 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. Asimismo, dado el carácter transnacional de la ciberseguridad, la cooperación con la Unión Europea y con otros organismos de ámbito internacional o regional con competencias en la materia, forma parte esencial de este modelo.

Para el logro de sus objetivos, la Estrategia crea una estructura orgánica que se integra en el marco del Sistema de Seguridad Nacional. Esta estructura servirá para articular la acción única del Estado conforme a unos principios compartidos por los actores concernidos y en un marco institucional adecuado.

Esta dependencia del ciberespacio nos obliga a dedicar todos los medios necesarios a la hora de poner nuestras capacidades al servicio de la ciberseguridad. El entorno es dinámico y son muchas las incertidumbres y retos que afrontamos. Únicamente si nos comprometemos de forma decidida con la seguridad del ciberespacio, la competitividad de nuestra economía y la prosperidad de España serán una realidad posible.



Mariano Rajoy Brey
Presidente del Gobierno de España

Sumario

Resumen Ejecutivo

Resumen Ejecutivo

Resumen Ejecutivo

La **Estrategia de Ciberseguridad Nacional** es el documento estratégico que sirve de fundamento al Gobierno de España para desarrollar las previsiones de la Estrategia de Seguridad Nacional en materia de protección del ciberespacio con el fin de implantar de forma coherente y estructurada acciones de prevención, defensa, detección y respuesta frente a las ciberamenazas.

La Estrategia consta de **cinco capítulos. El primero,** bajo el título *El ciberespacio y su seguridad,* presenta las características que definen el ciberespacio, las oportunidades que ofrece y las implicaciones que posee la dependencia de éste, desde el punto de vista de la seguridad. Este capítulo pone de manifiesto cómo las particularidades que son comunes a las ciberamenazas, la elevada dependencia de la economía y los servicios esenciales del ciberespacio, conllevan a en un incremento de riesgos y amenazas con un impacto potencialmente grave a la Seguridad Nacional.

El **segundo capítulo** establece el *Propósito y los principios rectores de la ciberseguridad en España.* En cuanto a la primera cuestión, se establece como finalidad la fijación de las directrices generales del uso seguro del ciberespacio, mediante una visión integradora que implique la coordinación de Administraciones Públicas, el sector privado y los ciudadanos y que canalice las iniciativas internacionales en la materia, dentro del respeto al ordenamiento jurídico interno e internacional, y en línea con otros documentos estratégicos nacionales e internacionales.

Por lo que se refiere a los *principios rectores* de la ciberseguridad, se recogen el *liderazgo nacional y la coordinación de esfuerzos; la responsabilidad compartida; la proporcionalidad, racionalidad y eficacia; y la cooperación internacional* como extensión de los principios informadores de la Estrategia de Seguridad Nacional. Estos principios subrayan la necesaria planificación de desarrollo del contexto actual haciendo especial hincapié en la protección de los valores constitucionales como elemento común a los cuatro principios.

En el **tercer capítulo,** la Estrategia aborda, con un nivel creciente de detalle, *los*

Objetivos de la ciberseguridad. Como objetivo global se establece lograr que España haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección, análisis, investigación, recuperación y respuesta a los ciberataques. A este fin debe servir la Política de Ciberseguridad Nacional

Seguidamente, la Estrategia fija **seis objetivos específicos:** 1) *para las Administraciones Públicas*, garantizar que los Sistemas de Información y Telecomunicaciones utilizadas por estas poseen el adecuado nivel de seguridad y resiliencia; 2) *para las empresas y las infraestructuras críticas*, impulsar la seguridad y la resiliencia de las redes y los sistemas de información usados por el sector empresarial en general y los operadores de infraestructuras críticas en particular; 3) *en el ámbito judicial y policial*, potenciar las capacidades de prevención, detección, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio; 4) *en materia de sensibilización*, concienciar a los ciudadanos, profesionales, empresas y Administraciones Públicas españolas de los riesgos derivados del ciberespacio; 5) *en capacitación*, alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de la ciberseguridad; *y* 6) *en lo que se refiere a la colaboración internacional*, contribuir en la mejora de la ciberseguridad, apoyando el desarrollo de una política de ciberseguridad coordinada en la Unión Europea y en las organizaciones internacionales, así como colaborar en la capacitación de Estados que lo necesiten a través de la política de cooperación al desarrollo.

El **capítulo cuarto** recoge las *Líneas de Acción de la Ciberseguridad* Nacional, que con carácter interdependiente y vinculadas a los objetivos establecidos en el capítulo precedente, orienta la acción dirigida a alcanzar los objetivos expuestos.

El **quinto y último capítulo** está dedicado a *La ciberseguridad en el Sistema de Seguridad Nacional* y establece la estructura orgánica al servicio de la ciberseguridad. Bajo la dirección del Presidente del Gobierno, la estructura se compone de tres órganos: uno ya existente, el Consejo de Seguridad Nacional, como Comisión Delegada del Gobierno para la Seguridad Nacional; y dos nuevos: el Comité Especializado de Ciberseguridad, que dará apoyo al Consejo de Seguridad Nacional prestando asistencia a la dirección y coordinación de la Política de Seguridad Nacional en materia de ciberseguridad, así como fomentando la coordinación, cooperación y colaboración entre Administraciones Públicas y entre éstas y el sector privado y el Comité Especializado de Situación, que, con apoyo del Centro de Situación del Departamento de Seguridad Nacional, gestionará las situaciones de crisis de ciberseguridad que, por su transversalidad o su dimensión, desborden las capaci-

dades de respuesta de los mecanismos habituales. Los dos Comités Especializados actuarán de forma complementaria.

El ciberespacio y su seguridad

Capítulo 1
El ciberespacio y su seguridad

Capítulo 1
El ciberespacio y su seguridad

El desarrollo de las Tecnologías de Información y Comunicación (TIC) ha generado un nuevo espacio de relación en el que la rapidez y facilidad de los intercambios de información y comunicaciones han eliminado las barreras de distancia y tiempo. El ciberespacio, nombre por el que se designa al dominio global y dinámico compuesto por las infraestructuras de tecnología de la información –incluida Internet–, las redes y los sistemas de información y de telecomunicaciones, han venido a difuminar fronteras, haciendo partícipes a sus usuarios de una globalización sin precedentes que propicia nuevas oportunidades, a la vez que comporta nuevos retos, riesgos y amenazas.

El grado de dependencia de nuestra sociedad respecto de las TIC y el ciberespacio crece día a día. Conocer sus amenazas, gestionar los riesgos y articular una adecuada capacidad de prevención, defensa, detección, análisis, investigación, recuperación y respuesta constituyen elementos esenciales de la Política de Ciberseguridad Nacional.

"El desarrollo de las TIC ha generado un nuevo espacio de relación en el que la rapidez y facilidad de los intercambios de información y comunicaciones han eliminado las barreras de distancia y tiempo"

Los ataques derivados de estas amenazas, denominados ciberataques, comparten generalmente una serie de características que les son comunes:

Características de los ciberataques

Bajo Coste

- muchas de las herramientas utilizadas por los atacantes pueden obtenerse de forma gratuita o a un coste muy reducido.

Ubicuidad y fácil ejecución

- la ejecución de los ataques es independiente de la localización de los agresores, no siendo imprescindible, en muchos casos, grandes conocimientos técnicos.

Efectividad e impacto

- si el ataque está bien diseñado, es posible que alcance los objetivos perseguidos. La ausencia de políticas de ciberseguridad, la insuficiencia de recursos y la falta de sensibilización y formación pueden facilitar este adverso resultado.

Reducido riesgo para el atacante

- la facilidad de ocultación hace que no sea fácil atribuir la comisión de un ciberataque a su verdadero autor o autores, lo que, unido a un marco legal dispar o inexistente, dificulta la persecución de la acción.

La multiplicidad de potenciales atacantes incrementa los riesgos y amenazas que pueden poner en graves dificultades los servicios prestados por las Administraciones Públicas, las Infraestructuras Críticas o las actividades de las empresas y ciudadanos. Además, existen evidencias de que determinados países disponen de capacidades militares y de inteligencia para realizar ciberataques que ponen en riesgo la Seguridad Nacional.

"La ciberseguridad es una necesidad de nuestra sociedad y de nuestro modelo económico"

La ciberseguridad es una necesidad de nuestra sociedad y de nuestro modelo económico. Dada la influencia de los Sistemas de Informa-

ción y Telecomunicaciones en la economía y en los servicios públicos, la estabilidad y prosperidad de España depende en buena medida de la seguridad y confiabilidad del ciberespacio, cualidades que pueden verse comprometidas por causas técnicas, fenómenos naturales o agresiones deliberadas.

Riesgos y Amenazas a la Ciberseguridad Nacional

Propósito y principios rectores ciberseguridad España

Capítulo 2

Propósito y principios rectores de la ciberseguridad en España

Capítulo 2
Propósito y principios rectores de la ciberseguridad en España

España precisa de Sistemas de Información y Telecomunicaciones seguros y confiables, tanto en su infraestructura física (equipos y redes), como en su vertiente inmaterial (programas informáticos, modelos o procedimientos). Estos sistemas, al tiempo que posibilitan el acceso de los ciudadanos y empresas al ciberespacio, albergan información valiosa y sustentan servicios estratégicos para nuestra nación, esenciales para el correcto funcionamiento de nuestra sociedad.

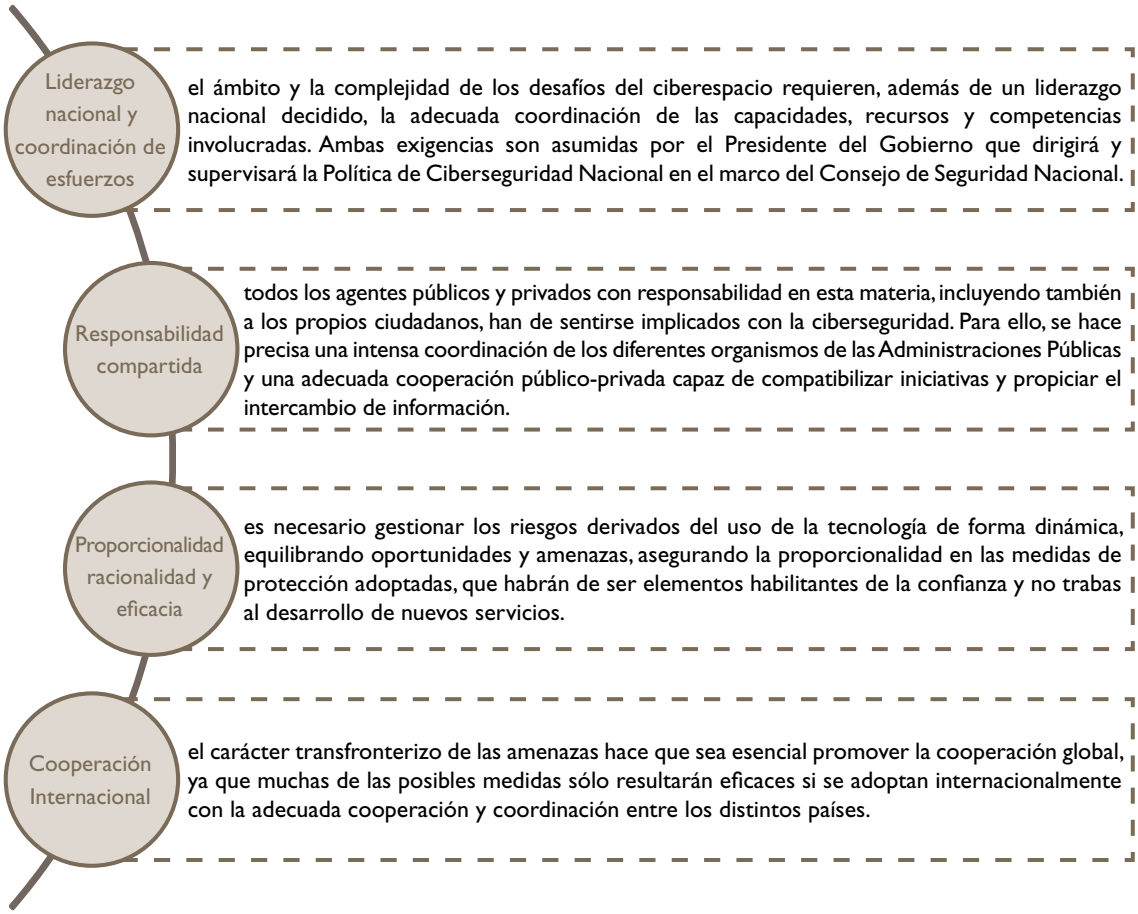
El propósito de la **Estrategia de Ciberseguridad Nacional**, promovida por el **Consejo de Seguridad Nacional** es fijar las directrices generales del uso seguro del ciberespacio, impulsando una visión integradora cuya aplicación ayude a garantizar a nuestra nación su seguridad y progreso, a través de la adecuada coordinación y cooperación de todas las Administraciones Públicas entre ellas, con el sector privado y con los ciudadanos. Todo ello dentro del máximo respeto a los principios recogidos en la Constitución; en las disposiciones de la Carta de Naciones Unidas, relativas al mantenimiento de la paz y seguridad internacional; en coherencia con la Estrategia de Seguridad Nacional y con iniciativas desarrolladas en el marco europeo, internacional y regional.

> ***"El propósito de la Estrategia de Ciberseguridad Nacional, promovida por el Consejo de Seguridad Nacional es fijar las directrices del uso seguro del ciberespacio"***

Igualmente, alienta la presencia de España en los organismos y foros de carácter internacional canalizando las iniciativas y los esfuerzos internacionales en defensa del ciberespacio.

Principios Rectores

La **Estrategia de Ciberseguridad Nacional**, en sintonía con los principios informadores de la Estrategia de Seguridad Nacional, y como extensión de éstos, se sustenta e inspira en los siguientes Principios Rectores:



Y todos ellos, respetando y fortaleciendo la protección y el pleno disfrute de los derechos fundamentales consagrados en nuestra Constitución y en instrumentos internacionales de la importancia de la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos o el Convenio Europeo para la protección de los Derechos Humanos y las Libertades Fundamentales. El Gobierno de España se compromete a desarrollar políticas que, mejorando la seguridad de los Sistemas de Información y Telecomunicaciones que emplean los ciudadanos, profesionales y empresas, preserven los derechos fundamentales de todos ellos, especialmente en los sectores más desprotegidos.

Objetivos de la ciberseguridad

Capítulo 3

Objetivos de la ciberseguridad

Capítulo 3
Objetivos de la ciberseguridad

OBJETIVO GLOBAL

Lograr que España haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección, y respuesta a los ciberataques.

Para alcanzar la seguridad del ciberespacio, se promoverá una Política de Ciberseguridad Nacional mediante el desarrollo del adecuado marco normativo y el impulso de una Estructura que aglutine y coordine a todas las instituciones y agentes con responsabilidad en la materia. Esta Estructura se articulará bajo el principio de eficiencia y sostenibilidad en el uso de los recursos, garantizando unas óptimas capacidades de prevención, defensa, detección, análisis, investigación, recuperación y respuesta de los Sistemas de Información y Telecomunicaciones ante posibles ciberataques.

"Para alcanzar la seguridad del ciberespacio, se promoverá una Política de Ciberseguridad Nacional mediante el desarrollo del adecuado marco normativo y el impulso de una Estructura que aglutine y coordine a todas las instituciones y agentes con responsabilidad en la materia"

El fortalecimiento de la ciberseguridad proporcionará a las Administraciones Públicas, al tejido industrial y empresarial, a la comunidad científica y a los ciudadanos en general, una mayor **confianza** en el uso de las TIC. Para ello, los organismos públicos responsables trabajarán en coordinación con el sector privado y con los propios ciudadanos, para garantizar la seguridad y la confiabilidad de los sistemas que sustentan la llamada Sociedad de la Información.

Asimismo, en defensa del interés nacional, la Política de Ciberseguridad Nacional estará alineada con iniciativas similares a las de los países de nuestro entorno, así como con las organizaciones europeas e internacionales competentes, en particular, con la Estrategia de Ciberseguridad de la Unión Europea.

Finalmente, de cara a garantizar la protección de los sistemas y la resiliencia de los servicios de las Administraciones Públicas y las Infraestructuras Críticas, así como la disponibilidad de productos confiables, será necesario potenciar, impulsar y reforzar las capacidades nacionales de investigación y desarrollo en ciberseguridad de las TIC.

En este sentido, España, manteniendo su política de diversificación y neutralidad tecnológica, velará por la utilización de componentes que estén certificados conforme a normas internacionalmente reconocidas.

Las consideraciones hechas en este objetivo global se aplicarán al resto de los objetivos.

OBJETIVO I

Garantizar que los Sistemas de Información y Telecomunicaciones que utilizan las Administraciones Públicas poseen el adecuado nivel de ciberseguridad y resiliencia

Buena parte de los sistemas TIC de las Administraciones Públicas españolas, la información contenida en ellos y los servicios que prestan, constituyen activos nacionales estratégicos.

Resulta imprescindible potenciar la implantación de un marco nacional, coherente e integrado, de políticas, procedimientos y normas técnicas que ayuden a garantizar la protección de la información pública, sus sistemas y servicios, así como de las redes que los soportan. Este marco será clave para desarrollar e implantar servicios, cada vez más seguros.

"Resulta imprescindible potenciar la implantación de un marco nacional, coherente e integrado, de políticas, procedimientos y normas técnicas que ayuden a garantizar la protección de la información pública"

La adaptación de los sistemas de las Administraciones Públicas a esta realidad pasa por implantar servicios de seguridad en las mismas,

mejorando y ejercitando su capacidad de prevención, detección y respuesta ante incidentes, desarrollando nuevas herramientas y manteniendo actualizado el ordenamiento jurídico.

Asimismo, además de mejorar las capacidades de los sistemas militares de Defensa y de inteligencia es necesario reforzar la seguridad de los Sistemas de Información y Comunicación estratégicos, adaptándolos a los nuevos riesgos y amenazas del ciberespacio.

Las Administraciones Públicas se involucrarán activamente en un proceso de mejora continua respecto de la protección de sus sistemas TIC. Los poderes públicos están obligados a ser ejemplares en la gestión de la ciberseguridad.

OBJETIVO II

Impulsar la seguridad y resiliencia de los Sistemas de Información y Telecomunicaciones usados por el sector empresarial en general y los operadores de Infraestructuras Críticas en particular

En aplicación del principio de responsabilidad compartida, las Administraciones Públicas deben mantener estrechas relaciones con las empresas que gestionan los Sistemas de Información y Telecomunicaciones relevantes para los intereses nacionales, intercambiando el conocimiento que permita una adecuada coordinación entre ambos y la mutua comprensión del entorno de la ciberseguridad.

"Se debe asegurar la Protección del Patrimonio Tecnológico de España"

En este sentido, merece especial mención las acciones para asegurar la Protección del Patrimonio Tecnológico de España, entendido como aquellos activos materiales o inmateriales que sustentan la propiedad intelectual e industrial del sector empresarial, que conforman nuestro presente y condicionan el desarrollo futuro.

Es de interés también determinar el impacto que para España puede tener una potencial interrupción o destrucción de las redes y sistemas que proporcionan servicios esenciales a la sociedad. Puesto que el sector privado posee la titularidad de buena parte de estos sistemas, las medidas que se adopten en materia de ciberseguridad deberán estar alineadas con los requisitos expresados en la normativa reguladora de Protección de Infraestructuras Críticas, para alcanzar un conjunto integrado de medidas de aplicación a los sectores afectados.

OBJETIVO III

Potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio

"Es imprescindible el fortalecimiento de la cooperación judicial y policial internacional, articulando los instrumentos adecuados de colaboración e intercambio de información y la armonización de las legislaciones nacionales"

Las TIC constituyen un medio, un fin o una combinación de ambos, utilizado tanto por las organizaciones terroristas como por las delictivas para lograr sus objetivos. A esto debe unirse la posibilidad, cada vez mayor, de utilizar el ciberespacio como un objetivo en sí mismo para la perpetración de ataques contra servicios esenciales o Infraestructuras Críticas. En ambos casos deben potenciarse los mecanismos de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación en torno a estas formas de criminalidad.

La actuación policial y judicial del Estado en materia de ciberseguridad deberá adecuarse a los patrones de conducta y a las modalidades delictivas de los terroristas y delincuentes en el ciberespacio, cuyos objetivos suelen ser coincidentes con los tradicionales, pero no su metodología.

Para afrontar adecuadamente estas amenazas, que traspasan en muchos casos las fronteras de los Estados, es imprescindible el fortalecimiento de la cooperación judicial y policial internacional, articulando los instrumentos adecuados de colaboración e intercambio de información y la armonización de las legislaciones nacionales, con el desarrollo y mantenimiento de una regulación sólida y eficaz.

Igualmente, se hace necesario fomentar la colaboración ciudadana, facilitando los procedimientos de acceso y transmisión de la información de interés policial.

El éxito en la lucha contra el terrorismo y la delincuencia en el ciberespacio exige la articulación de los mecanismos necesarios que mejoren las capacidades de las instituciones policiales y los organismos judiciales competentes.

OBJETIVO IV

Sensibilizar a los ciudadanos, profesionales, empresas y Administraciones Públicas españolas de los riesgos derivados del ciberespacio

El Gobierno de España, reconociendo la importancia de construir y mantener la confianza en los Sistemas de Información y Telecomunicaciones que usan los ciudadanos, profesionales, empresas y organismos del sector público, acometerá las acciones de información y sensibilización necesarias para asegurar que todos conocen los riesgos de operar en el ciberespacio y poseen los conocimientos y el acceso a las herramientas que posibilitan su protección.

"Las empresas deben ser conscientes de la responsabilidad en la seguridad de sus sistemas, la protección de la información de sus clientes y proveedores y la confiabilidad de los servicios que prestan"

Al mismo tiempo, las empresas deben ser conscientes de la responsabilidad en la seguridad de sus sistemas, la protección de la información de sus clientes y proveedores y la confiabilidad de los servicios que prestan. Mantener la confianza del consumidor es fundamental para el éxito de la economía digital. Lo mismo cabe decir de las Administraciones Públicas y de sus relaciones con los ciudadanos.

Por tanto, una función esencial es promover una sólida cultura de ciberseguridad, que proporcione a todos los actores la conciencia y la confianza necesarias para maximizar los beneficios de la Sociedad de la Información y reducir al mínimo su exposición a los riesgos del ciberespacio, mediante la adopción de medidas razonables que garanticen la protección de sus datos, así como la conexión segura de sus sistemas y equipos.

La gestión eficaz de los riesgos derivados del ciberespacio debe edificarse sobre una sólida cultura de ciberseguridad. Ello requiere de los usuarios una sensibilización respecto de los riesgos que entraña operar en este medio, así como el conocimiento de las herramientas para la protección de su información, sistemas y servicios.

OBJETIVO V

Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de ciberseguridad

Dada la importancia estratégica de la seguridad en el ciberespacio, es absolutamente prioritario disponer del personal cualificado a todos los niveles: órganos de gobierno, directivo, operativo, técnico y judicial.

"Se requiere fomentar y mantener una actividad de I+D+i en materia de ciberseguridad de manera efectiva"

Es importante, además, fomentar y potenciar las capacidades tecnológicas precisas para disponer de soluciones nacionales confiables que permitan proteger adecuadamente los sistemas frente a las diferentes amenazas.

Para alcanzar esta confianza, se requiere fomentar y mantener una actividad de I+D+i en materia de ciberseguridad de manera efectiva. Para ello será necesaria una adecuada coordinación del conjunto de agentes implicados en las TIC, facilitando la colaboración entre empresas y organismos públicos de investigación e impulsando proyectos de evaluación y certificación de la seguridad.

La cualificación del personal encargado de la dirección, gestión e implantación de la ciberseguridad se erige en un objetivo fundamental, especialmente en las Administraciones Públicas y las Infraestructuras Estratégicas y Críticas de interés nacional. Además, la utilización de productos con la seguridad verificada constituye un elemento adicional relevante de protección.

OBJETIVO VI

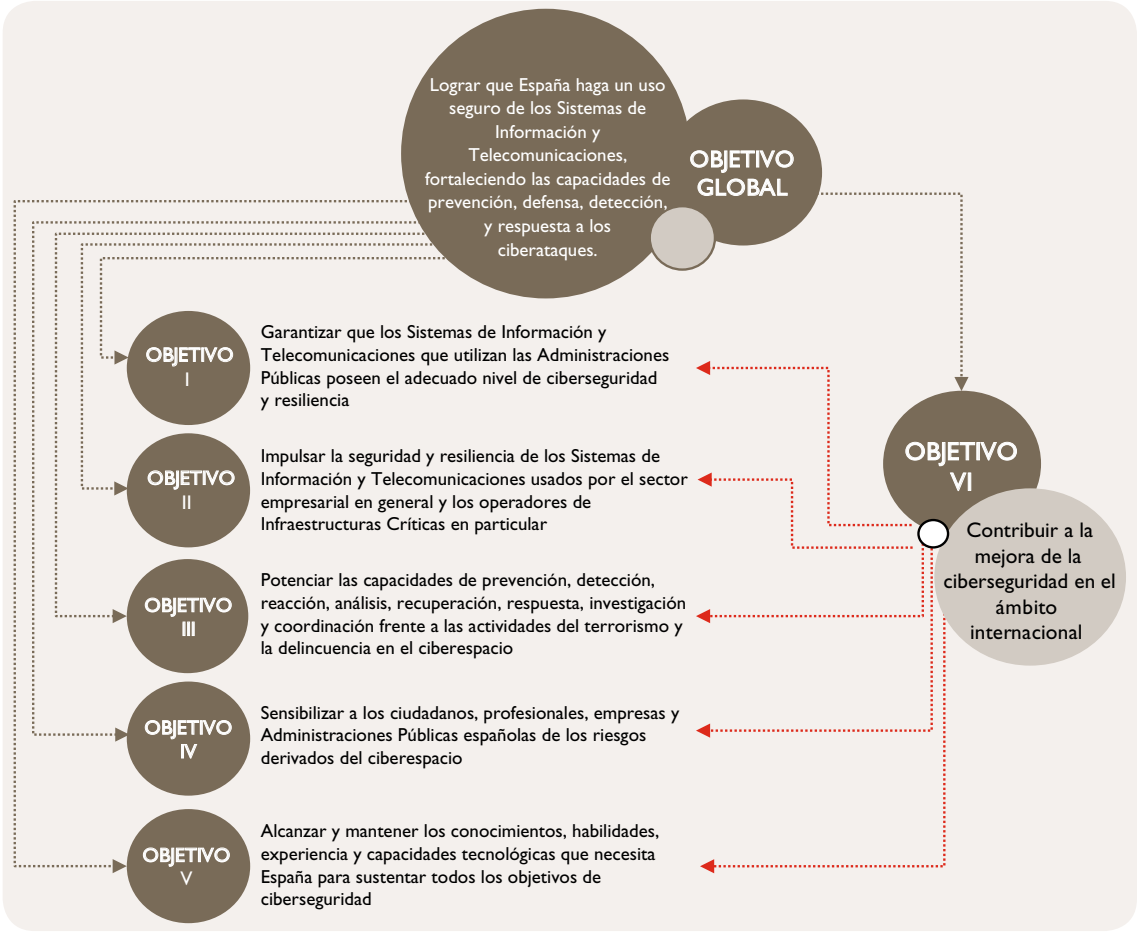
Contribuir a la mejora de la ciberseguridad en el ámbito internacional

Se promoverá y apoyará el desarrollo de una política de ciberseguridad coordinada en la Unión Europea y en las organizaciones internacionales de Seguridad y Defensa en las que participa España, y se colaborará en la capacitación de Estados que lo necesiten, mediante la política de cooperación al desarrollo, ayudándoles a implantar una cultura de la ciberseguridad.

Se fomentará la cooperación en el marco de la UE y con organizaciones internacionales y regionales como, la Agencia Europea de Defensa (EDA), la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), el Centro Europeo de Ciberdelincuencia, adscrito a Europol, la Organización de Naciones Unidas (ONU), la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Organización del Tratado del Atlántico Norte (OTAN) y la Organización para la Cooperación y Desarrollo Económicos (OCDE), entre otras.

"Se promoverá y apoyará el desarrollo de una política de ciberseguridad coordinada en la Unión Europea y en las organizaciones internacionales de Seguridad y Defensa"

Junto a los países de nuestro entorno estratégico, se promoverán los esfuerzos dirigidos a conseguir un ciberespacio seguro y fiable, mediante el refuerzo de la colaboración internacional, creando relaciones de confianza para el intercambio de información y datos esenciales en materia de ciberseguridad, y el desarrollo de iniciativas propias de cooperación y desarrollo. Asimismo se llevarán a cabo actuaciones orientadas a impulsar la adopción de estándares internacionales de ciberseguridad y su elevación progresiva.


Lograr que España haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección, y respuesta a los ciberataques.
OBJETIVO GLOBAL
OBJETIVO I
Garantizar que los Sistemas de Información y Telecomunicaciones que utilizan las Administraciones Públicas poseen el adecuado nivel de ciberseguridad y resiliencia
OBJETIVO II
Impulsar la seguridad y resiliencia de los Sistemas de Información y Telecomunicaciones usados por el sector empresarial en general y los operadores de Infraestructuras Críticas en particular
OBJETIVO III
Potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio
OBJETIVO IV
Sensibilizar a los ciudadanos, profesionales, empresas y Administraciones Públicas españolas de los riesgos derivados del ciberespacio
OBJETIVO V
Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de ciberseguridad
OBJETIVO VI
Contribuir a la mejora de la ciberseguridad en el ámbito internacional

Líneas de acción de la ciberseguridad nacional

Capítulo 4

Líneas de acción de la ciberseguridad nacional

Capítulo 4: Líneas de acción de la ciberseguridad nacional

Para alcanzar los objetivos señalados, la **Estrategia de Ciberseguridad Nacional** se articula a través de las siguientes Líneas de Acción:

LÍNEA DE ACCIÓN 1

Capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas

Incrementar las capacidades de prevención, defensa, detección, análisis, respuesta, recuperación y coordinación ante las ciberamenazas, haciendo énfasis en las Administraciones Públicas, las Infraestructuras Críticas, las capacidades militares y de Defensa y otros sistemas de interés nacional.

En esta línea de acción, el Gobierno de España adoptará las medidas correspondientes, entre ellas:

- Ampliar y mejorar las capacidades de detección y análisis de ciberamenazas que permitan la identificación de procedimientos y orígenes de ataque, y la elaboración de la inteligencia necesaria para una defensa y protección más eficaz de las redes nacionales.
- Ampliar y fortalecer las capacidades de detección y respuesta ante ciberataques dirigidos contra objetivos de carácter nacional, regional o sectorial, incluyendo a ciudadanos y empresas.
- Garantizar la coordinación, la cooperación y el intercambio de información entre la Administración General del Estado, las Comunidades Autónomas, las Entidades Locales, el sector privado y los organismos competentes de la UE e internacionales para asegurar la permanente concienciación, formación y capacidad de respuesta a través del Sistema de Intercambio de Información y Comunicación de Incidentes.

- Asegurar la cooperación de los organismos con responsabilidades en ciberseguridad, en especial entre el CERT de la Administración Pública del Centro Criptológico Nacional (CCN-CERT), el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (MCCD) y el CERT de Seguridad e Industria. Los CERT de las Comunidades Autónomas, los de las entidades privadas y otros servicios de ciberseguridad relevantes deberán estar coordinados con los anteriores en función de las competencias de cada uno de ellos, articulando los instrumentos adecuados a tal efecto.

- Desarrollar y mantener actualizadas las instrucciones de prevención y detección, incluyendo procedimientos de respuesta frente a situaciones de crisis y planes de contingencia específicos ante incidentes de ciberseguridad de ámbito nacional, asegurando su integración en el Sistema de Seguridad Nacional.

- Desarrollar y ejecutar un Programa de Ejercicios de Simulación de Incidentes de Ciberseguridad, para evaluar y perfeccionar las acciones llevadas a cabo en este ámbito.

- Ampliar y mejorar permanentemente las capacidades de Ciberdefensa de las Fuerzas Armadas que permitan una adecuada protección de sus Redes y Sistemas de Información y Telecomunicaciones, así como de otros sistemas que afecten a la Defensa Nacional. Se consolidará la implantación del Mando Conjunto de Ciberdefensa y se potenciará su cooperación con los diferentes órganos con capacidad de respuesta ante incidentes cibernéticos en aspectos de común interés.

- Potenciar las capacidades militares y de inteligencia para ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional.

LÍNEA DE ACCIÓN 2

Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas

Garantizar la implantación del Esquema Nacional de Seguridad, reforzar las capacidades de detección y mejorar la defensa de los sistemas clasificados.

Esta línea de acción abarca las iniciativas necesarias para proteger los Sistemas de Información de la Administración General del Estado, las Comunidades Autónomas, las Entidades Locales y sus organismos vinculados o dependientes, así como los Sistemas de Información y Telecomunicaciones e infraestructuras comunes a todas ellas.

Para ello, el Gobierno de España adoptará, entre otras, las siguientes medidas:

- Asegurar la plena implantación del Esquema Nacional de Seguridad y articular los procedimientos necesarios para conocer regularmente el estado de las principales variables de seguridad de los sistemas afectados.
- Ampliar y mejorar las capacidades del CERT de las Administraciones Públicas-CCN-CERT- y particularmente de sus Sistemas de Detección y de Alerta Temprana.
- Reforzar las estructuras de seguridad y la capacidad de vigilancia de los Sistemas de Información, en particular los que manejan información clasificada.
- Optimizar el modelo de interconexión de los organismos de las Administraciones Públicas españolas a las redes públicas de voz y datos, maximizando su eficacia, disponibilidad y seguridad.
- Reforzar la implantación y seguridad de la infraestructura común y segura en la Administración Pública española (Red SARA), potenciando su uso y sus capacidades de seguridad y resiliencia.
- Desarrollar nuevos servicios horizontales seguros, de acuerdo con directrices de la Dirección de Tecnologías de la Información y de las Comunicaciones de la Administración General del Estado, organismo responsable de la coordinación, dirección y racionalización del uso de las TIC en la Administración General del Estado.
- Incrementar las actividades nacionales para el desarrollo y evaluación de productos, servicios y sistemas a fin de obtener su certificación apoyando específicamente aquellas que sustenten necesidades de interés nacional.
- Potenciar la creación, difusión y aplicación de las Mejores Prácticas en materia de Ciberseguridad en el ámbito de las Administraciones Públicas.

LÍNEA DE ACCIÓN 3

Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Infraestructuras Críticas

Impulsar la implantación de la normativa sobre Protección de Infraestructuras Críticas y de las capacidades necesarias para la protección de los servicios esenciales.

Es necesario incrementar la resiliencia de las Infraestructuras Críticas españolas para evitar una potencial alteración del normal funcionamiento de los servicios esenciales que podrían afectar a la actividad diaria de los españoles.

En este ámbito, el Gobierno de España adoptará, entre otras, las siguientes medidas:

- Asegurar la implantación de la normativa sobre Protección de las Infraestructuras Críticas con el fin de conseguir una seguridad que abarque tanto el ámbito físico como el tecnológico. Para ello, se evaluará la inclusión de las medidas de ciberseguridad oportunas en los distintos planes que se establezcan.
- Ampliar y mejorar las capacidades del CERT de Seguridad e Industria, potenciando la colaboración y coordinación con el Centro Nacional para la Protección de Infraestructuras Críticas, con los diferentes órganos con capacidad de respuesta ante incidentes y con las unidades operativas de las Fuerzas y Cuerpos de Seguridad del Estado.
- Impulsar la participación del sector privado en los Programas de Ejercicios de simulación de incidentes de Ciberseguridad.
- Desarrollar modelos de simulación que permitan analizar las dependencias entre las diferentes Infraestructuras Críticas y los riesgos acumulados por éstas.

LÍNEA DE ACCIÓN 4

Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia

Potenciar las capacidades para detectar, investigar y perseguir las actividades terroristas y delictivas en el ciberespacio, sobre la base de un marco jurídico y operativo eficaz.

Esta línea de acción se concentra en combatir el terrorismo y la delincuencia que actúan en el ciberespacio, en su doble vertiente de instrumento facilitador de sus actividades y de objeto directo de su acción. En este concepto se incluyen también las organizaciones que hacen uso de la tecnología para financiarse o lucrarse, posibilitando la comisión de delitos y el blanqueo de capitales.

En esta línea de acción, el Gobierno de España abordará las medidas correspondientes, entre ellas:

- Integrar en el marco legal español las soluciones a los problemas que surjan relacionados con la ciberseguridad para la determinación de los tipos penales y el trabajo de los departamentos competentes.
- Ampliar y mejorar las capacidades de los organismos con competencias en la investigación y persecución del ciberterrorismo y la ciberdelincuencia así como asegurar la coordinación de estas capacidades con las actividades en el campo de la ciberseguridad, a través del intercambio de información e inteligencia por los canales de comunicación adecuados.
- Fortalecer la cooperación policial internacional y fomentar la colaboración ciudadana, articulando los instrumentos de intercambio y transmisión de información de interés policial.
- Asegurar a los profesionales del Derecho el acceso a la información y a los recursos que les proporcionen el nivel necesario de conocimientos en el ámbito judicial para la mejor aplicación del marco legal y técnico asociado. En este sentido, es especialmente importante la cooperación con el Consejo General del Poder Judicial, la Abogacía del Estado, la Fiscalía General del Estado, la Fiscalía Coordinadora de la Criminalidad Informática y el Consejo General de la Abogacía Española.

LÍNEA DE ACCIÓN 5

Seguridad y resiliencia de las TIC en el sector privado

Impulsar la seguridad y la resiliencia de las infraestructuras, redes, productos y servicios empleando instrumentos de cooperación público-privada.

Esta línea de acción tiene como objeto la mejora de la seguridad y la resiliencia de las redes, productos y servicios que emplea el sector industrial en el desarrollo de su actividad reforzando la colaboración público-privada con el sector industrial y en particular con el de la seguridad TIC. Se valorará, entre otros, la participación de los Colegios y Asociaciones profesionales.

El Gobierno desarrollará, entre otras, las siguientes medidas:

- Impulsar la cooperación entre los sectores público y privado, promoviendo el intercambio de información sobre vulnerabilidades, ciberamenazas y sus posibles consecuencias, especialmente en lo relativo a la protección de los sistemas de interés nacional.
- Promover la cooperación con los sectores de la industria y los servicios de la ciberseguridad, con el fin de mejorar conjuntamente las capacidades de detección, prevención, respuesta y recuperación frente a los riesgos de seguridad del ciberespacio, impulsando la participación activa de los proveedores de servicios así como el desarrollo y adopción de códigos de conducta y buenas prácticas.
- Impulsar el desarrollo de estándares en ciberseguridad a través de los organismos y entidades de normalización y certificación nacionales e internacionales, y promover su adopción.

LÍNEA DE ACCIÓN 6

Conocimientos, Competencias e I+D+i

Promover la capacitación de profesionales, impulsar el desarrollo industrial y reforzar el sistema de I+D+i en materia de ciberseguridad.

Esta línea de acción contempla las iniciativas que es necesario acometer para alcanzar y mantener el adecuado nivel de capacitación en ciberseguridad de los profesionales (conocimientos y competencias) e impulsar la industria y la I+D+i españolas. El Gobierno de España procederá a:

- Desarrollar un Marco de Conocimientos de Ciberseguridad en los ámbitos técnico, operativo y jurídico.
- Extender y ampliar los programas de captación de talento, investigación avanzada y capacitación en ciberseguridad en cooperación con Universidades y centros especializados.
- Establecer mecanismos que permitan identificar de forma temprana las prioridades y demandas de los poderes públicos en materia de ciberseguridad para su incorporación a las iniciativas anteriores.
- Fomentar el desarrollo industrial de productos y servicios en materia de ciberseguridad por medio de instrumentos, entre otros, como el Plan Estatal de Investigación Científica y Técnica y de Innovación e iniciativas de apoyo a su internacionalización.
- Impulsar la coordinación nacional y la dinamización del sector industrial y de servicios de ciberseguridad para la mejora de la competitividad, la internacionalización, la identificación de oportunidades, la eliminación de barreras y la orientación normativa, entre otras actividades.
- Impulsar las actividades de certificación de ciberseguridad de acuerdo con las normas y estándares de reconocimiento internacional, incluyendo estos criterios en los procesos de desarrollo y adquisición de productos o sistemas.
- Impulsar modelos y técnicas de análisis de ciberamenazas y medidas de protección de productos, servicios y sistemas, así como su especificación, evaluación y certificación.

LÍNEA DE ACCIÓN 7

Cultura de ciberseguridad

Concienciar a los ciudadanos, profesionales y empresas de la importancia de la ciberseguridad y del uso responsable de las nuevas tecnologías y de los servicios de la Sociedad de la Información.

El Gobierno de España, adecuará, potenciará o desarrollará las medidas correspondientes, entre ellas:

- Impulsar las actividades de sensibilización para asegurar que los ciudadanos y empresas tienen acceso a información relativa a vulnerabilidades, ciberamenazas e información sobre cómo proteger mejor su entorno tecnológico.
- Propiciar el desarrollo de programas de Concienciación en Ciberseguridad, en colaboración con agentes del sector público y privado potenciando, a través de los organismos con competencias en la materia, la necesaria coordinación y racionalización de esfuerzos.
- Fomentar los mecanismos para apoyar a empresas y profesionales en el uso seguro de las TIC, reforzando los conocimientos en materia de seguridad, promoviendo la adopción de herramientas, la difusión de normativa y el uso de buenas prácticas.
- Asesorar y dar soporte al desarrollo de módulos educativos de sensibilización en ciberseguridad, dirigidos a todos los niveles de la enseñanza.

LÍNEA DE ACCIÓN 8

Compromiso Internacional

Promover un ciberespacio internacional seguro y confiable, en apoyo a los intereses nacionales.

La globalización tecnológica, sus oportunidades y sus riesgos obligan a alinear las iniciativas de todos los países que persiguen un ciberespacio seguro y confiable. Estos esfuerzos internacionales han de contemplar la elaboración y adopción de estándares globales, la expansión de la capacidad del sistema jurídico internacional y el desarrollo y la promoción de las mejores prácticas en el conocimiento de la situación, la alerta y la respuesta ante incidentes cibernéticos.

En esta línea de acción, el Gobierno de España desarrollará, entre otras, las siguientes medidas:

- Potenciar la presencia de España en organizaciones y foros internacionales y regionales sobre ciberseguridad apoyando y participando activamente en las diversas iniciativas y coordinando la posición de los agentes nacionales implicados.
- Promover la armonización legislativa y la cooperación judicial y policial internacionales en la lucha contra la ciberdelincuencia y el ciberterrorismo, apoyando la negociación y adopción de convenios internacionales en la materia.
- Propiciar la suscripción de acuerdos en el seno de organizaciones internacionales y con los principales socios y aliados, para fortalecer la cooperación en materia de ciberseguridad y desarrollar un enfoque coordinado de lucha contra las ciberamenazas.
- Impulsar el establecimiento de canales internacionales de información, detección y respuesta.
- Promover la participación coordinada de instituciones públicas y del sector privado en simulacros y ejercicios internacionales.
- En el ámbito de la UE, colaborar en la armonización de legislaciones nacionales, la implantación de la Estrategia de Ciberseguridad de la UE y el impulso de una política internacional en el ciberespacio.
- Fomentar la cooperación con la OTAN en materia de Ciberdefensa, en particular en lo relativo a la respuesta ante incidentes cibernéticos y al intercambio de información técnica sobre amenazas y vulnerabilidades, a la vez que promover dentro de la propia Organización actuaciones que tengan por objeto señalar a la Ciberdefensa como una de sus prioridades.

LÍNEA DE ACCIÓN		CONTENIDO
1	**Capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas**	Incrementar las capacidades de prevención, defensa, detección, análisis, respuesta, recuperación y coordinación ante las ciberamenazas, haciendo énfasis en las Administraciones Públicas, las Infraestructuras Críticas, las capacidades militares y de Defensa y otros sistemas de interés nacional.
2	**Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas**	Garantizar la implantación del Esquema Nacional de Seguridad, reforzar las capacidades de detección y mejorar la defensa de los sistemas clasificados.
3	**Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Infraestructuras Críticas**	Impulsar la implantación de la normativa sobre Protección de Infraestructuras Críticas y de las capacidades necesarias para la protección de los servicios esenciales.
4	**Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia**	Potenciar las capacidades para detectar, investigar y perseguir las actividades terroristas y delictivas en el ciberespacio, sobre la base de un marco jurídico y operativo eficaz.
5	**Seguridad y resiliencia de las TIC del sector privado**	Impulsar la seguridad y la resiliencia de las infraestructuras, redes, productos y servicios empleando instrumentos de cooperación público-privada.
6	**Conocimientos, Competencias e I+D+i**	Promover la capacitación de profesionales, impulsar el desarrollo industrial y reforzar el sistema de I+D+i en materia de ciberseguridad.
7	**Cultura de ciberseguridad**	Concienciar a los ciudadanos, profesionales y empresas de la importancia de la ciberseguridad y del uso responsable de las nuevas tecnologías y de los servicios de la Sociedad de la Información.
8	**Compromiso internacional**	Promover un ciberespacio internacional seguro y confiable, en apoyo a los intereses nacionales.

La ciberseguridad Sistema Seguridad Nacional

Capítulo 5

La ciberseguridad en el Sistema de Seguridad Nacional

Capítulo 5:
La ciberseguridad en el Sistema de Seguridad Nacional

La visión integral de la ciberseguridad plasmada en esta Estrategia, los riesgos y amenazas detectados que le afectan y los objetivos y líneas de acción trazados, para dar respuesta conjunta y adecuada a la preservación de la ciberseguridad bajo los principios que sustentan el Sistema de Seguridad Nacional, explican la necesidad de contar con una estructura orgánica precisa a estos efectos, que estará constituida por los siguientes componentes bajo la dirección del Presidente del Gobierno:

A. el Consejo de Seguridad Nacional;
B. el Comité Especializado de Ciberseguridad;
C. el Comité Especializado de Situación, único para el conjunto del Sistema de Seguridad Nacional.

Estructura orgánica de la ciberseguridad nacional

ESTRUCTURA ORGÁNICA DE LA CIBERSEGURIDAD

a) Consejo de Seguridad Nacional:

El Consejo de Seguridad Nacional configurado como Comisión Delegada del Gobierno para la Seguridad Nacional, asiste al Presidente del Gobierno en la dirección de la Política de Seguridad Nacional.

b) Comité Especializado de Ciberseguridad:

El Comité Especializado de Ciberseguridad dará apoyo al Consejo de Seguridad Nacional para el cumplimiento de sus funciones y, en particular, en la asistencia al Presidente del Gobierno en la dirección y coordinación de la Política de Seguridad Nacional en el ámbito de la ciberseguridad. Además, reforzará 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.

La composición del Comité Especializado de Ciberseguridad reflejará el espectro de los ámbitos de los departamentos, organismos y agencias de las Administraciones Públicas con competencias en materia de ciberseguridad, para coordinar aquellas actuaciones que se deban abordar de forma conjunta con el fin de elevar los niveles de seguridad.

En el Comité podrán participar otros actores relevantes del sector privado y especialistas cuya contribución se considere necesaria.

En el cumplimiento de sus funciones el Comité Especializado de Ciberseguridad será apoyado por el Departamento de Seguridad Nacional en su condición de Secretaría Técnica y órgano de trabajo permanente del Consejo de Seguridad Nacional.

c) Comité Especializado de Situación:

El Comité Especializado de Situación será convocado para llevar a cabo la gestión de las situaciones de crisis en el ámbito de la ciberseguridad que, atendiendo a la acentuada transversalidad o dimensión e impacto de sus efectos, produzcan el desbordamiento de los límites de capacidad de respuesta eficaz por parte de los mecanismos habituales previstos, siempre respetando las competencias asignadas a las distintas Administraciones Públicas y a los efectos de garantizar una respuesta inmediata y eficaz a través de un solo órgano de dirección político-estratégica de la crisis.

El Comité Especializado de Ciberseguridad y el Comité Especializado de Situación actuarán de forma complementaria, cada uno en su ámbito de competencias, pero bajo la misma dirección estratégica y política del Consejo de Seguridad Nacional presidido por el Presidente del Gobierno.

"El Comité Especializado de Ciberseguridad y el Comité Especializado de Situación actuarán de forma complementaria, cada uno en su ámbito de competencias, pero bajo la misma dirección estratégica y política del Consejo de Seguridad Nacional presidido por el Presidente del Gobierno"

El Comité Especializado de Situación será apoyado por el Centro de Situación del Departamento de Seguridad Nacional con el fin de garantizar su interconexión con los centros operativos implicados y dar una respuesta adecuada en situaciones de crisis, facilitando su seguimiento y control y la trasmisión de las decisiones.

Para el cumplimiento eficaz de sus funciones de apoyo al Comité Especializado de Situación, el Centro de Situación del Departamento de Seguridad Nacional podrá ser reforzado por personal especializado proveniente de los departamentos ministeriales u organismos competentes, los cuales conformarán la Célula de Coordinación específica en el ámbito de la Ciberseguridad.

IMPLANTACIÓN

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

www.lamoncloa.gob.es