ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

2019

GOBIERNO DE ESPAÑA
PRESIDENCIA DEL GOBIERNO

Catálogo de publicaciones de la Administración General del Estado
htttp://publicacionesoficiales.boe.es

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA, RELACIONES CON LAS CORTES E IGUALDAD

NIPO (printed edition): 042-19-028-9
NIPO (online edition): 042-19-0129-4
Depósito Legal: M-16844-2019
Edition date: Junio 2019
Printer: imprenta ROAL, S.L.

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

2019

La Estrategia Nacional de Ciberseguridad ha sido aprobada por el Consejo de Seguridad Nacional.

En el proceso de elaboración han participado: Ministerio de Asuntos Exteriores, Unión Europea y Cooperación; Ministerio de Justicia; Ministerio de Defensa; Ministerio de Hacienda; Ministerio del Interior; Ministerio de Fomento; Ministerio de Educación y Formación Profesional; Ministerio de Industria, Comercio y Turismo; Ministerio de la Presidencia, Relaciones con las Cortes e Igualdad; Ministerio de Política Territorial y Función Pública; Ministerio de Economía y Empresa; Ministerio de Sanidad, Consumo y Bienestar Social; Ministerio de Ciencia, Innovación y Universidades; Centro Nacional de Inteligencia; Departamento de Seguridad Nacional, además de un Comité de Expertos de asociaciones profesionales, empresas y del mundo académico.

DSN

La Cuarta Revolución Industrial, la digital, ha convivido durante años con un tiempo de crisis económica y de secuelas sociales y políticas que aún nos atenazan. Por eso, pese a las innegables oportunidades y avances que nos ofrece, son muchos los ciudadanos que ven con aprehensión e incertidumbre todo lo relativo a la disrupción tecnológica digital. Y es ahí, en la lucha por ese cambio de percepción, donde las administraciones públicas debemos trabajar de forma prioritaria. En juego está la confianza social en las instituciones democráticas y en nuestras propias capacidades para afrontar el futuro con garantías de progreso.

En plena era de transformaciones y de incertidumbres, hemos de ofrecer un horizonte moral y material sólido, y para ello es cada día más imprescindible una ciberseguridad acorde a los nuevos tiempos y amenazas. Capaz de atender los distintos retos y hacerlo desde la cooperación público-privada y con el apoyo de una ciudadanía consciente de la realidad cambiante y comprometida con las soluciones a los desafíos.

A ello busca contribuir esta Estrategia Nacional de Ciberseguridad, alineada con la Estrategia de Seguridad Nacional de 2017. Y lo hace con un objetivo claro como norte: hacer de este momento de cambios, no una fuente de malestar cultural y de regresión económica y laboral, sino una oportunidad para incrementar la competitividad de España y el bienestar de los españoles y las españolas junto a la de nuestros socios europeos. Un trabajo que ha tenido en cuenta, además, el momento geopolítico en el que nos hemos adentrado, y que hace más urgente y necesaria construir y reforzar la autonomía estratégica de la Unión.

En todo ello, España tiene mucho que decir y que aportar. Al fin y al cabo, el nuestro es uno de los países más interconectados del mundo. Y un vistazo a las noticias diarias nos informa de la enorme cantidad y peligrosidad de las amenazas cibernéticas a las que nos enfrentamos. Desde las acciones maliciosas de desinformación en redes sociales, hasta el ciberespionaje o la financiación del terrorismo, de forma creciente el espacio digital influye y modela la realidad. Además, otras nuevas tecnologías como la Inteligencia Artificial, la robótica, el Big y el Smart Data o el blockchain están ya implantadas en la actividad diaria de ciudadanos, empresas y Administraciones Públicas. Posibilitan novedosos instrumentos para obtener información, generar conocimiento e intercambiar datos.

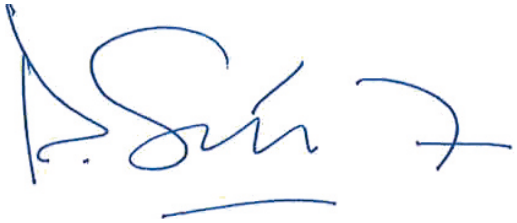
Una influencia que crecerá aún más con la actual implantación del así llamado 5G para la nueva conectividad del "internet de las cosas". Estar más interconectados y ser más dependientes de dichas infraestructuras nos va a ofrecer llegar más lejos en

muchos campos importantes, desde la consecución de los Objetivos de Desarrollo Sostenible de las Naciones Unidas, hasta la lucha contra los efectos del cambio climático.

Pero también nos hace más vulnerables a acciones hostiles contra dichas nuevas infraestructuras, y también desde ellas. Las amenazas son cada vez más sofisticadas y complejas, y el ciberespacio es un ámbito sin fronteras ni demarcaciones jurisdiccionales claras, de débil regulación, donde resulta difícil la trazabilidad y la atribución de las acciones delictivas llevadas a cabo por actores estatales y no estatales.

El reto es enorme y multidisciplinar. Nuestros profesionales en los diversos campos implicados en la ciberseguridad tienen un merecido prestigio y sabrán estar a la altura. Pero la ciberseguridad requiere del compromiso de todos. A las Administraciones Públicas nos corresponde liderarla y ofrecer un marco que aporte certidumbre a unas empresas y unos ciudadanos que deben también comprometerse con ella. Insisto, no sólo para sortear sus peligros y amenazas, sino para aprovechar sus muchas oportunidades en beneficio de todos.

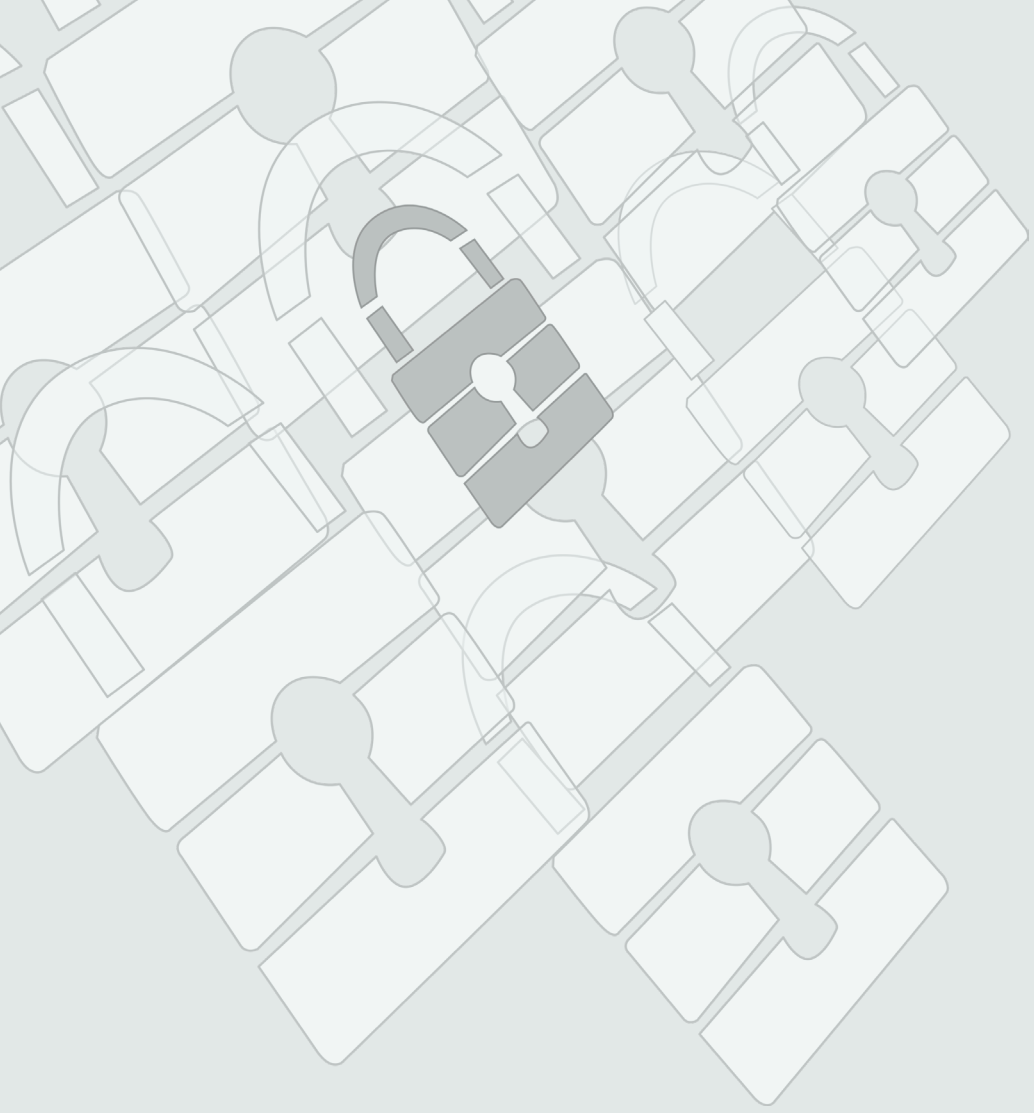
La ciberseguridad protege activos, pero también valores esenciales para una sociedad libre como la que somos. Principios a los que no vamos a renunciar en esta era de transformaciones globales. El desafío técnico que plantea la ciberseguridad es variado y complejo, pero nos jugamos algo más. Algo que atañe a aspectos morales y culturales relacionados con nuestra forma de entender y mirar el mundo, con aquello que más y mejor nos define. De nuestro acierto al diseñar una buena Estrategia de Ciberseguridad depende, en definitiva, la libertad, el bienestar y la democracia. Estoy convencido de que, con este documento, hemos dado un paso clave para encarar con éxito unos años inciertos pero también fascinantes.



Pedro Sánchez

Presidente del Gobierno de España

SUMARIO



Resumen ejecutivo

Resumen ejecutivo

La Estrategia Nacional de Ciberseguridad desarrolla las previsiones de la Estrategia de Seguridad Nacional de 2017 en el ámbito de la ciberseguridad, considerando los objetivos generales, el objetivo del ámbito y las líneas de acción establecidas para conseguirlo.

El documento se estructura en cinco capítulos. El primero, titulado "El ciberespacio, más allá de un espacio común global", proporciona una visión de conjunto del ámbito de la ciberseguridad, los avances realizados en materia de ciberseguridad desde la aprobación de la Estrategia de 2013, las razones que afianzan la elaboración de la Estrategia Nacional de Ciberseguridad 2019, así como las principales características que impulsan su desarrollo.

Las actividades que se desarrollan en el ciberespacio son fundamentales para la sociedad actual. La tecnología e infraestructuras que forman parte del ciberespacio son elementos estratégicos, transversales a todos los ámbitos de actividad, siendo la vulnerabilidad del ciberespacio uno de los principales riesgos para nuestro desarrollo como nación.

Por ello, 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.

Contribuir a la promoción de un ciberespacio seguro y fiable, desde un enfoque multidisciplinar abarcando aspectos más allá de los puramente técnicos, es una tarea que debe partir del conocimiento y comprensión de las amenazas a las que nos podemos enfrentar, incluyendo nuevas y emergentes.

El **segundo capítulo**, titulado "Las amenazas y desafíos en el ciberespacio" determina las principales amenazas del ciberespacio, que derivan de su condición de espacio global común, de la elevada tecnificación y de la gran conectividad, que posibilita la amplificación del impacto ante cualquier ataque. Clasifica estas amenazas y desafíos en dos categorías: por un lado, las que amenazan a activos que forman parte del ciberespacio; y por otro, aquellos que usan el ciberespacio como medio para realizar actividades maliciosas e ilícitas de todo tipo.

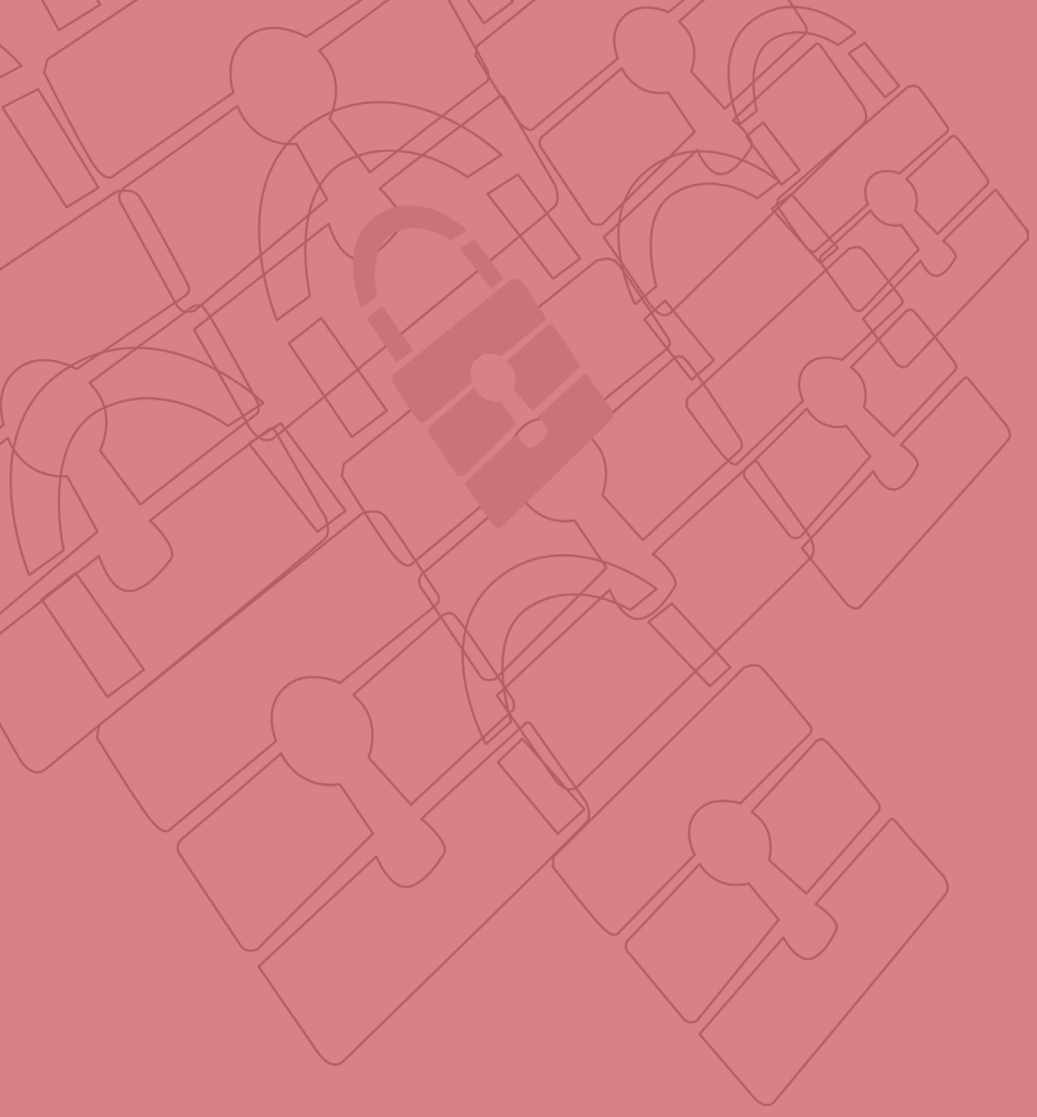
El **tercer capítulo**, titulado "Propósito, principios y objetivos para la ciberseguridad" aplica los principios rectores de la Estrategia de Seguridad Nacional 2017 (Unidad de acción, Anticipación, Eficiencia y Resiliencia) a cinco objetivos específicos que se identifican para la ciberseguridad nacional. Su desarrollo se plasma en el **cuarto capítulo,** titulado "Líneas de acción y medidas", donde se establecen siete líneas de acción, y se identifican las medidas para el desarrollo de cada una de ellas.

Dichas líneas de acción se dirigen a: reforzar las capacidades ante las amenazas provenientes del ciberespacio; garantizar la seguridad y resiliencia de los activos estratégicos para España; impulsar la ciberseguridad de ciudadanos y empresas; 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; impulsar la ciberseguridad de ciudadanos y empresas; potenciar la industria española de ciberseguridad, y la generación y retención de talento, para el fortalecimiento de la autonomía digital; contribuir a la seguridad del ciberespacio en el ámbito internacional, promoviendo un ciberespacio abierto, plural, seguro y confiable, en apoyo de los intereses nacionales y desarrollar una cultura de ciberseguridad de manera que se contribuya al Plan Integral de Cultura de Seguridad Nacional.

El **quinto capítulo**, titulado "La ciberseguridad en el Sistema de Seguridad Nacional" define la estructura orgánica de la ciberseguridad. Bajo la dirección del Presidente del Gobierno, la estructura se compone de tres órganos: el **Consejo de Seguridad Nacional,** como Comisión Delegada del Gobierno para la Seguridad Nacional; el **Consejo Nacional de Ciberseguridad,** que apoya al Consejo de Seguridad Nacional y asiste al Presidente del Gobierno en la dirección y coordinación de la política de Seguridad Nacional en el ámbito de la ciberseguridad, y fomenta las relaciones de coordinación, colaboración y cooperación entre Administraciones Públicas y entre estas y el sector privado, y el **Comité de Situación** que, con el apoyo del Departamento de Seguridad Nacional, gestionará las situaciones de crisis en cualquier ámbito, que por su transversalidad o dimensión, desborden las capacidades de respuesta de los mecanismos habituales.

Se complementa este sistema con la **Comisión Permanente de Ciberseguridad,** que facilita la coordinación interministerial a nivel operacional en el ámbito de la ciberseguridad, siendo el órgano que asistirá al Consejo Nacional de Ciberseguridad sobre aspectos relativos a la valoración técnica y operativa de los riesgos y amenazas a la ciberseguridad; las autoridades públicas competentes y CSIRT (Computer Security Incident Response Team) de referencia nacional, y se incorpora la creación de un elemento novedoso de colaboración público privada, el **foro Nacional de Ciberseguridad**.

Asimismo, en este último capítulo, se exponen a modo de conclusión, unas consideraciones finales y se concretan los mecanismos para la actualización y evaluación de la Estrategia.



Introducción

Introducción

La Estrategia Nacional de Ciberseguridad 2019 establece la posición de España ante una nueva concepción de la ciberseguridad en el marco de la Política de Seguridad Nacional.

En 2013 se aprobó la primera Estrategia Nacional de Ciberseguridad en España. El documento fijaba las directrices y líneas generales de actuación para hacer frente al desafío que supone para el país la vulnerabilidad del ciberespacio. Además, la estrategia diseñaba el modelo de gobernanza para la ciberseguridad nacional. Igualmente, en estos años, España ha seguido avanzando en sus esfuerzos por contribuir a la promoción de un ciberespacio seguro y fiable.

Uno de sus pilares, creado en el año 2014, es el Consejo Nacional de Ciberseguridad, órgano de apoyo del Consejo de Seguridad Nacional. Desde su primera reunión, el Consejo Nacional de Ciberseguridad ha asumido la tarea de coordinar los organismos con competencia en la materia a nivel nacional y el desarrollo del Plan Nacional de Ciberseguridad y sus planes derivados. Así, hoy España cuenta con organismos

especializados en ciberseguridad y una posición destacada a nivel europeo e internacional.

El marco jurídico también ha experimentado una notable adaptación. En respuesta a su evolución y a la experiencia acumulada en estos años, en 2015 se publicó la modificación del Esquema Nacional de Seguridad para garantizar la seguridad de los sistemas del Sector Público. Por otro lado, la entrada en vigor del 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), ha supuesto un importante hito en la mejora de la ciberseguridad en nuestro país, extendiendo el alcance de esta Directiva con el objetivo de mejorar la ciberseguridad de todos los sectores estratégicos.

La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional se promulgó con vocación de dar impulso a uno de los proyectos de mayor responsabilidad para un gobierno, la Seguridad Nacional. En este sentido, la Ley de Seguridad Nacional contempla la ciberseguridad como ámbito de especial interés.

Se puede afirmar, sin lugar a dudas, que la ciberseguridad ha modernizado la Seguridad Nacional, tratándose de uno de los ámbitos de mayor avance hasta la fecha. Esta dinámica debe continuar su camino.

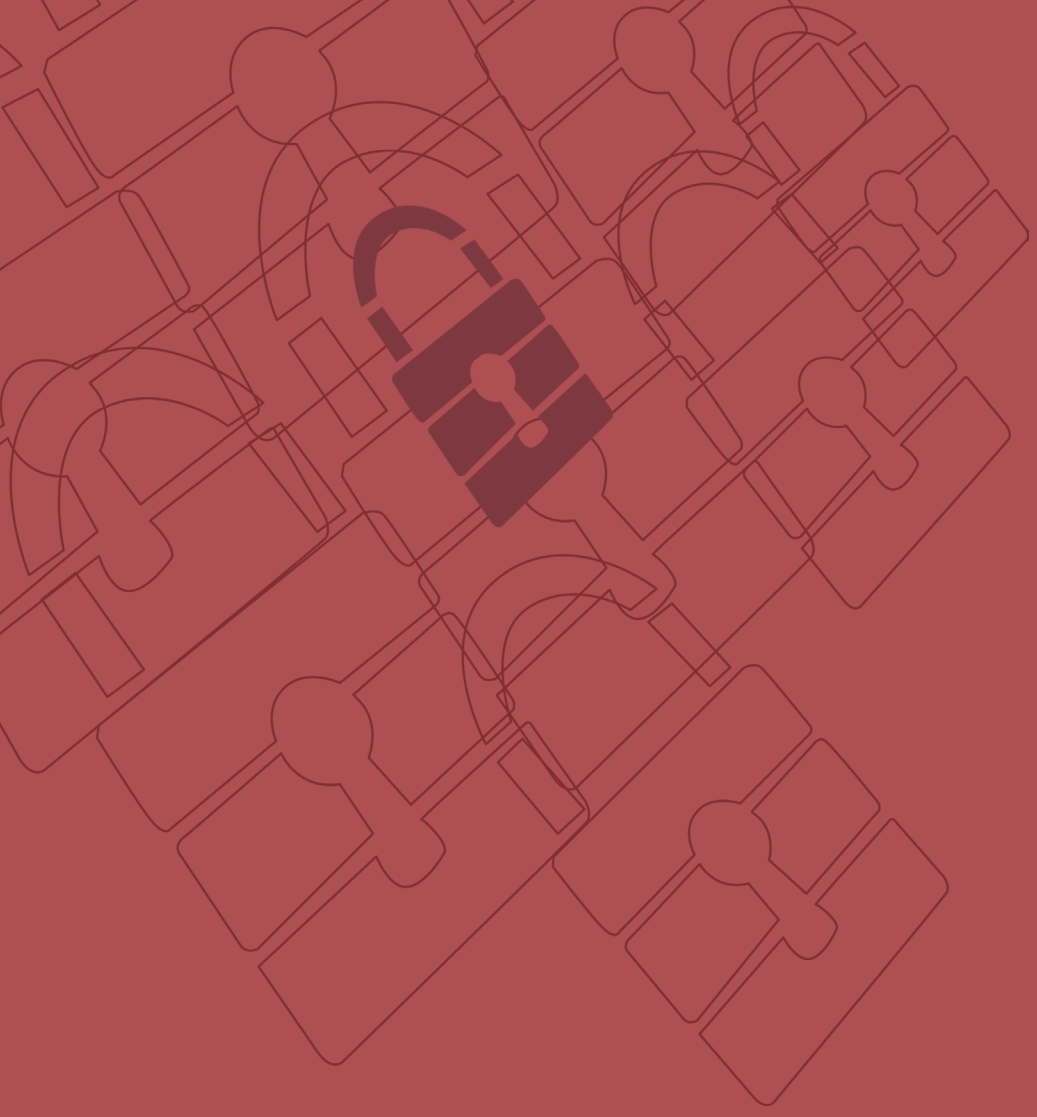
La Estrategia de Seguridad Nacional 2017 marca un punto de inflexión en el pensamiento estratégico nacional, donde la ciberseguridad debe ocupar un espacio propio y diferencial.

Una de las tendencias globales identificadas en la Estrategia, la digitalización, se muestra como motor del cambio con implicaciones para la seguridad. La Estrategia establece un esquema novedoso, con cinco objetivos generales que resultan transversales a todos los ámbitos. La gestión de crisis, la cultura de Seguridad Nacional, los espacios comunes globales, el desarrollo tecnológico y la proyección internacional de España conforman una matriz estratégica donde la ciberseguridad está llamada a abrir nuevas vías hacia el modelo de presente y futuro de la ciberseguridad en España.

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.

Además de las acciones para causar efectos en los sistemas digitales, se debe tener en cuenta la concepción del ciberespacio como un vector de comunicación estratégica, que puede ser utilizado para influir en la opinión pública y en la forma de pensar de las personas a través de la manipulación de la información, las campañas de desinformación o las acciones de carácter híbrido. Su potencial aplicación en situaciones muy diversas, donde se incluyen los procesos electorales, genera un elevado grado de complejidad.

Ante esta visión renovada de un ámbito que se entiende extendido funcionalmente, y para el que la colaboración público-privada es un elemento clave, resulta necesaria una nueva aproximación, una nueva estrategia nacional de ciberseguridad.



Capítulo 1

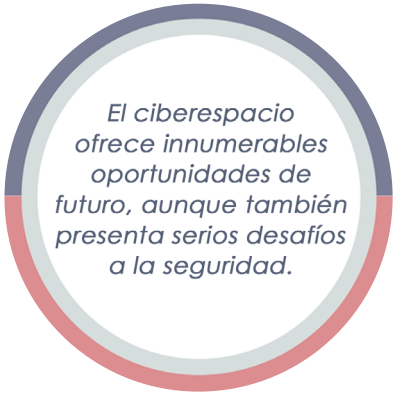
El ciberespacio como espacio común global

El ciberespacio como espacio común global

Este capítulo presenta las oportunidades y desafíos del ciberespacio y la infraestructura digital, expone el carácter inherentemente internacional de la aproximación a su seguridad y describe los principales rasgos de la nueva concepción de la ciberseguridad en España.

El ciberespacio: oportunidades y desafíos

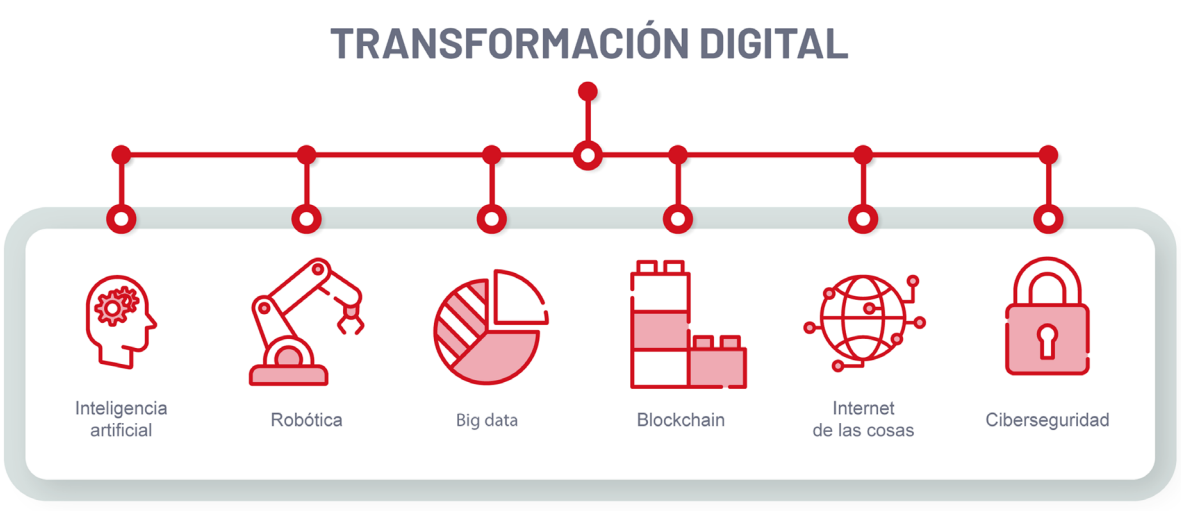
El ciberespacio es un espacio común global caracterizado por su apertura funcional y su dinamismo. La ausencia de soberanía, su débil jurisdicción, la facilidad de acceso y la dificultad de atribución de las acciones que en él se desarrollan definen un escenario que ofrece innumerables oportunidades



de futuro, aunque también presenta serios desafíos a la seguridad.

Por una parte, el ciberespacio posibilita la conectividad universal y facilita el libre flujo de información, servicios e ideas. Se constituye así en un ámbito que estimula el emprendimiento, potencia el progreso socioeconómico y ofrece cada día nuevas posibilidades en todos los sectores de actividad. El cambio que la transformación digital provoca en los procesos productivos se manifiesta a escala global y a un ritmo sin precedentes. La inteligencia artificial, la robótica, el big data, el blockchain y el internet de las cosas son ya una realidad, si bien el verdadero potencial transformador está todavía por descubrir. Sus implicaciones van más allá de la dimensión tecnológica, se extienden hacia nuevos modelos sociales y se adentran en el campo de las relaciones personales y la ética.

Por otra parte, la digitalización transforma la seguridad y presenta serios desafíos. El ciberespacio se configura como campo de batalla donde la información y la privacidad de los datos son activos de alto valor en un entorno de mayor competición geopolítica, reordenación del poder y empoderamiento del individuo. Así, la creciente conectividad y la mayor dependencia de las redes y sistemas, así como de componentes, objetos y dispositivos digitales, generan vulnerabilidades y dificultan la adecuada protección de la información.



Infraestructura digital

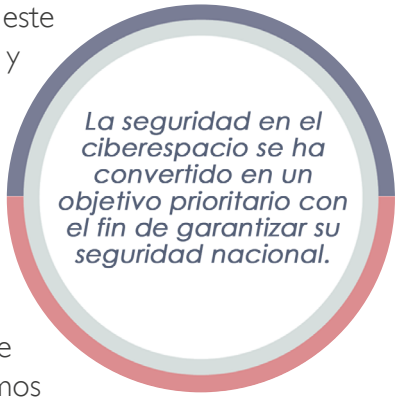
Además de su naturaleza virtual, el ciberespacio se sustenta en elementos físicos y lógicos. Los dispositivos, componentes y sistemas que constituyen las redes y sistemas de información y comunicaciones están expuestos a disfunciones que alteran su correcto funcionamiento y a acciones deliberadas con fines malintencionados, que ponen en riesgo el funcionamiento de las infraestructuras críticas y de los servicios esenciales que dependen de los sistemas y redes digitales asociadas.

Este riesgo se ve amplificado por la prevalencia de criterios comerciales frente a los de seguridad en el diseño de los productos hardware y software, así como de los sistemas y de los servicios, algo que dificulta los procesos de certificación y puede comprometer la cadena de suministro.

Todos estos elementos, unidos a la creciente interconectividad entre sistemas pueden originar efectos en cascada con resultados impredecibles.

Plano internacional: seguridad en el ciberespacio

La seguridad en el ciberespacio se ha convertido en un objetivo prioritario en las agendas de los gobiernos con el fin de garantizar su seguridad nacional y de crear una sociedad digital basada en la confianza. En este contexto, España defiende su visión e intereses como nación y contribuye al esfuerzo conjunto de la comunidad internacional en su apuesta por un ciberespacio abierto, plural y seguro.



España continúa participando activamente en todas las instituciones en las que la ciberseguridad ocupa un lugar destacado, en especial en el marco de la Unión Europea, la Alianza Atlántica y de Naciones Unidas, demostrando así el compromiso con sus socios y aliados. Asimismo, se mantienen vínculos con terceros Estados mediante mecanismos de cooperación bilateral que facilitan elementos de entendimiento y confianza mutua basados en las relaciones fluidas en el ámbito de la ciberseguridad y orientados hacia la construcción de capacidades.

Consciente de la importancia del multilateralismo, además del Derecho Internacional y las normas no vinculantes de comportamiento responsable de los Estados, se destaca el papel de La Carta de Naciones Unidas como principio de referencia para la prevención de conflictos, la cooperación y la estabilidad en el ciberespacio. La construcción de consensos y las medidas de fomento de confianza constituyen la base para su aplicación y puesta en práctica, así como los Tratados y Convenios Internacionales en los que España es parte.

Una nueva concepción del ciberespacio

Es una dimensión fundamental para la estabilidad el 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.

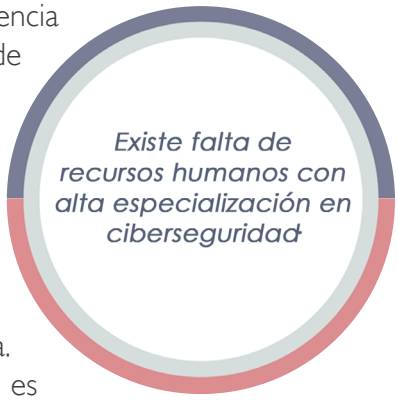
El buen entendimiento de este planteamiento, exige trabajar con un enfoque multidisciplinar, que abarque aspectos más allá de los puramente técnicos, bajo el principio de dirección centralizada y ejecución coordinada, con la afectación de la ciberseguridad a la Seguridad Nacional como competencia del Estado.

En primer lugar, el sector privado juega un papel relevante como uno de los gestores y propietarios de los activos digitales de España, por lo que las capacidades de ciberseguridad del país residen en gran medida en las de sus empresas. Es por tanto necesario el apoyo, la promoción y la inversión en ciberseguridad para impulsar la competitividad y el crecimiento económico, a la vez que proporcionar un entorno digital seguro y fiable.

Por otra parte, se debe aspirar a incrementar la autonomía tecnológica mediante el fomento de una base industrial nacional de ciberseguridad, la I+D+i y la gestión del talento tecnológico.

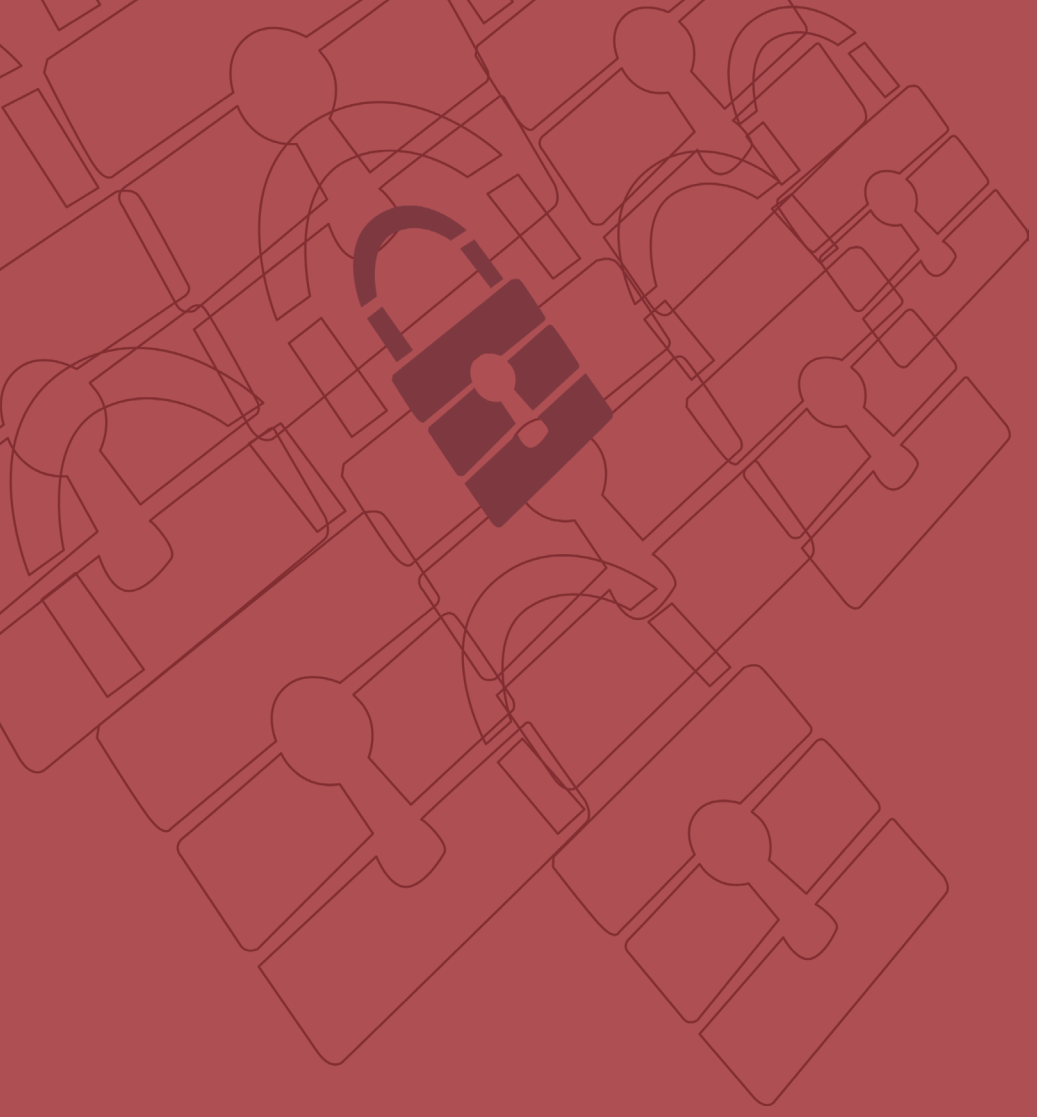
En efecto, el recurso humano continúa siendo un factor crítico. Existe una diferencia importante entre el número de puestos de trabajo para los que es necesaria una alta especialización en las tecnologías de la información, en concreto en ciberseguridad, y las personas disponibles con el nivel de conocimiento o de formación requerida.

En segundo lugar, la 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. El empleo del ciberespacio como dominio de confrontación, de forma independiente o como parte de una acción híbrida, es un rasgo ampliamente reconocido. La disuasión en ciberseguridad requiere la obtención y potenciación de capacidades de ciberdefensa, como elemento fundamental de la acción del Estado.



En tercer lugar, la rápida evolución de las ciberamenazas aconseja una aproximación más proactiva de la ciberinteligencia. Su integración en el esquema conjunto de la ciberseguridad es un elemento clave para el conocimiento de la situación y la necesaria alerta temprana que permita anticiparse a las acciones de los potenciales adversarios a través del conocimiento de sus capacidades, técnicas, tácticas e intenciones. Así mismo, es necesario fomentar el empleo de mecanismos y medios que permitan una oportuna investigación y persecución de los autores para incrementar las posibilidades de atribución.

A todo lo anterior se une la necesidad de una mayor implicación de toda la sociedad mediante el fomento de una cultura de ciberseguridad, para evolucionar desde la concienciación al compromiso, en el entendimiento de que el ciudadano es corresponsable de la ciberseguridad nacional.



Capítulo 2
Las amenazas y desafíos en el ciberespacio

Las amenazas y desafíos en el ciberespacio

En este capítulo se examinan las principales amenazas y desafíos del ciberespacio a los que se enfrenta España.

La promoción de un entorno seguro y fiable es una tarea que debe partir del conocimiento y la comprensión de los desafíos y las amenazas, incluyendo las nuevas y emergentes que afectan al ciberespacio. La Estrategia de Seguridad Nacional de 2017 diferencia entre las ciberamenazas y las acciones que usan el ciberespacio como medio para realizar actividades maliciosas o ilícitas.

Ciberamenazas

Las ciberamenazas son todas aquellas disrupciones o manipulaciones maliciosas que afectan a elementos tecnológicos. Abarcan un amplio abanico de acciones. Las ciberamenazas se caracterizan por su diversidad tanto en lo que concierne a capacidades como a motivaciones. Afectan a la práctica totalidad de los ámbitos de

la Seguridad Nacional, como son la Defensa Nacional, la seguridad económica o la protección de las infraestructuras críticas, entre otros, y no distinguen fronteras.

Su carácter transversal exige que la ciberseguridad sea afrontada con una perspectiva integral que comprenda a las Administraciones Públicas, al sector público y privado y a la sociedad en su conjunto, en tanto puede tener implicaciones simultáneas en aspectos tan diversos como la soberanía, los derechos fundamentales, la defensa, la economía y el desarrollo tecnológico.

El carácter transversal de la ciberseguridad exige que sea afrontado por la sociedad en su conjunto.

En este escenario las defensas deben evolucionar continuamente, para ir adaptándose a una amenaza que lleva la iniciativa y que se multiplica por el efecto llamada que genera su alto grado de impunidad. Todo ello, mientras la superficie a defender se incrementa y complica cada día.

La seguridad de las redes y sistemas de información requiere potenciar las medidas de prevención, detección y respuesta, fomentando la seguridad por diseño y por defecto, que debe estar incorporada tanto en el desarrollo de productos y servicios tecnológicos, como en su actualización o manera de utilización.

Acciones que usan el ciberespacio para fines maliciosos

Las tecnologías digitales dan entrada a nuevas actividades y formas de negocio que requieren ser debidamente reguladas, pues pueden afectar a la estabilidad y al ejercicio de derechos y libertades, presentando sustanciales amenazas y desafíos para la Seguridad Nacional. Igualmente, las mismas cualidades que hacen del ciberespacio un motor del progreso, pueden ser explotadas con fines perniciosos al sumarse a las excepcionales facilidades que concede para el anonimato, la suplantación y la amplificación.

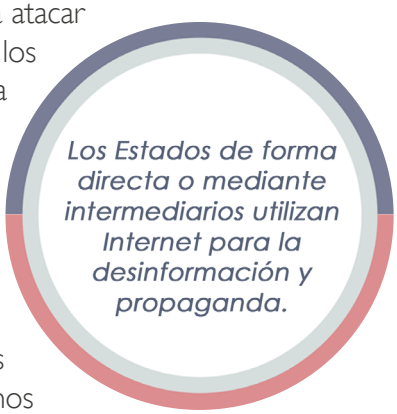
Internet ha hecho que, Estados, grupos organizados, colectivos y hasta individuos aislados pueden alcanzar un nivel de poder y una capacidad de influir impensable en otros tiempos.

Debido a la revolución de Internet, Estados, grupos organizados, colectivos y hasta individuos aislados pueden alcanzar un nivel de poder y una capacidad de influir impensable en otros tiempos. La conectividad digital por una parte lleva a que los movimientos sociales globales tengan una importancia estratégica hasta hace poco subestimada.

Las acciones que usan el ciberespacio como medio para realizar actividades maliciosas o ilícitas 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. Las mayores capacidades corresponden principalmente a actores estatales (organismos de inteligencia o militares), que fundamentalmente operan a través de las denominadas Amenazas Persistentes Avanzadas, un tipo de amenaza en la que el adversario posee sofisticados niveles de conocimiento y de recursos e infraestructuras para, mediante múltiples tipos de ataques, interactuar sobre sus objetivos por un extenso periodo de tiempo, adaptarse a los esfuerzos del defensor para resistir, así como mantener el nivel de interacción con el objetivo para ejecutar sus objetivos.

Asimismo, se constata una tendencia creciente de las denominadas amenazas híbridas. Se trata de acciones coordinadas y sincronizadas dirigidas a atacar de manera deliberada las vulnerabilidades sistémicas de los estados democráticos y las instituciones, a través de una amplia gama de medios, tales como acciones militares tradicionales, ciberataques, operaciones de manipulación de la información, o elementos de presión económica. Actores estatales y no estatales, bien de forma directa o a través de intermediarios, explotan las facilidades que ofrece internet para la desinformación y propaganda y un interés generalizado en la obtención y desarrollo de capacidades militares para operar en el ciberespacio, incluyendo en muchos casos capacidades ofensivas.



La cibercriminalidad, por su parte, es un problema de seguridad ciudadana de primer orden, representando una de las amenazas más extendidas y generalizadas, que se materializa de forma continua y que victimiza cada vez de manera más importante a miles de instituciones, empresas y ciudadanos. El término 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 en su planificación, desarrollo y ejecución 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.

El empleo de nuevas modalidades de transacción financiera y económica, como las criptomonedas, para el tráfico y el comercio de bienes y prestación de servicios ilícitos o la extorsión, el fraude y la falsificación de medios de pago no monetarios, constituyen un serio desafío a la seguridad por su sofisticación y complejidad. Estos pueden ser utilizados en el blanqueo de capitales y la evasión de impuestos y representan una fuente de ingresos para el crimen organizado y por lo tanto son facilitadores de otras actividades como la financiación del terrorismo, que toma provecho de la dificultad de seguimiento que estas nuevas técnicas ofrecen.

Los ciberdelincuentes operan bajo esquemas de crimen organizado.

Los ciberdelincuentes operan bajo esquemas de crimen organizado y continúan explorando de manera incesante técnicas sobre las que construir modelos de negocio lucrativo y de bajo riesgo, amparados por la difícil trazabilidad de sus acciones.

Los grupos terroristas tratan de aprovechar las vulnerabilidades del ciberespacio para realizar ciberataques o para actividades de radicalización de individuos y colectivos, financiación, divulgación de técnicas y herramientas para la comisión de atentados, y de reclutamiento, adiestramiento o propaganda. Íntimamente relacionado con ello, se halla la amenaza contra las infraestructuras críticas, con la posibilidad cierta de causar un colapso a través de las redes mediante una caída en cadena de los servicios esenciales.

Los grupos hacktivistas realizan ciberataques por razones ideológicas y, aprovechándose en ocasiones de productos, servicios y herramientas disponibles en el ciberespacio, buscan desarrollar ataques con un gran impacto mediático o social.

Tampoco se puede menospreciar la amenaza que entraña el incremento continuado de la contratación de servicios de cibercriminales, las organizaciones que buscan causar daño a sus competidores y los recursos tecnológicos y humanos internos que puedan resultar dañinos para las organizaciones, sin olvidar todas aquellas amenazas emergentes y las acciones resultantes de la falta de cultura de ciberseguridad.

La información digital se ha convertido en un activo de alto valor añadido. El empleo malintencionado de datos personales y las campañas de desinformación tienen un alto potencial desestabilizador en la sociedad.

Por otra parte, la información digital se ha convertido en un activo de alto valor añadido. El análisis de los datos personales que circulan en la red se aprovecha para múltiples fines que abarca

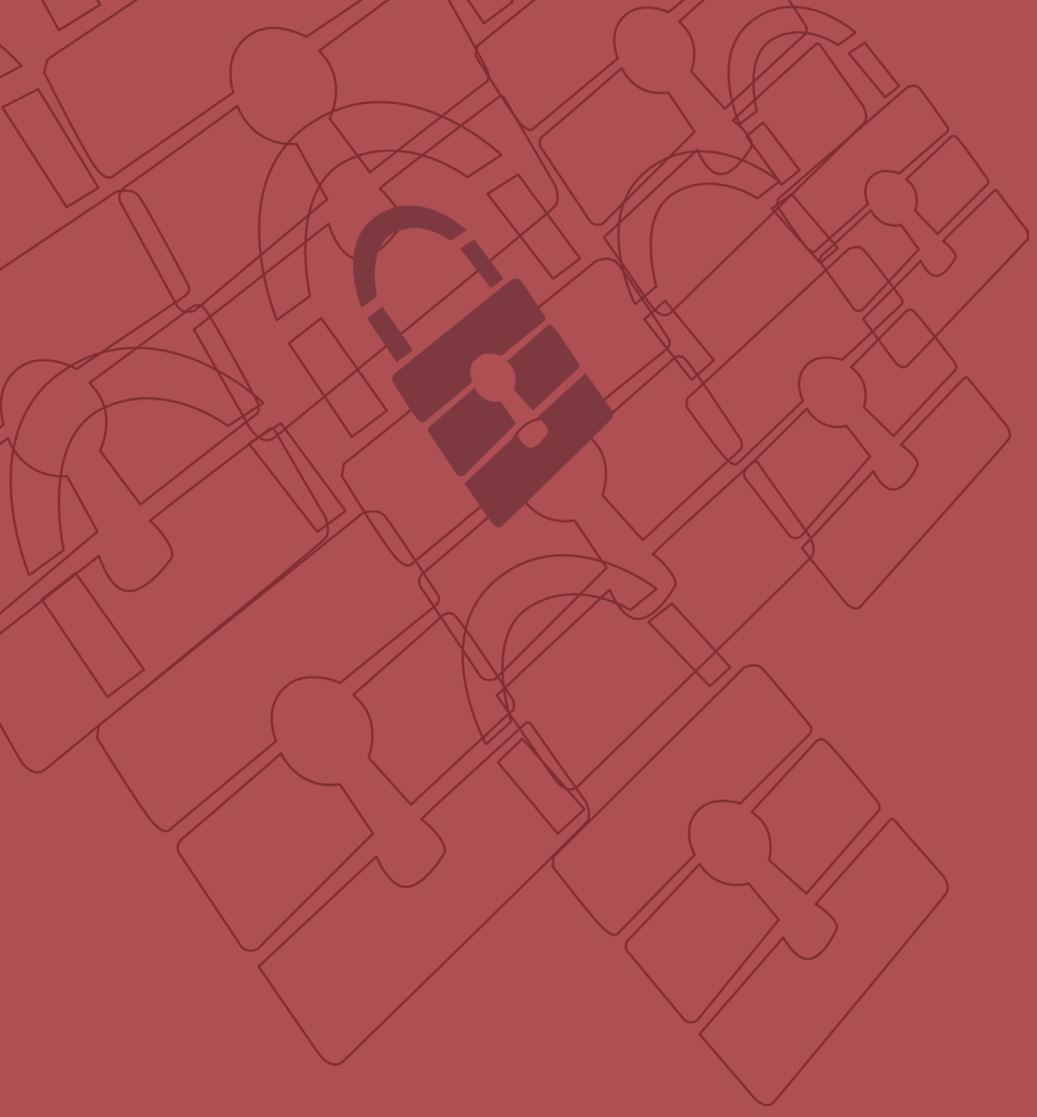
desde estudios sociológicos hasta campañas comerciales. El empleo malintencionado de datos personales y las campañas de desinformación tienen un alto potencial desestabilizador en la sociedad, y la explotación de brechas de seguridad en los datos personales supone una violación a la seguridad de dichos datos, que afecta a la privacidad de las personas y a la integridad y confidencialidad de sus datos.

En cuanto a las campañas de desinformación, hacen uso de 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, con potencial aplicación en contra de objetivos como por ejemplo organizaciones internacionales, Estados, iniciativas políticas o personajes públicos o incluso a procesos electorales democráticos.

CIBERAMENAZAS Y ACCIONES QUE USAN EL CIBERESPACIO CON FINES MALICIOSOS

Disrupciones o manipulaciones maliciosas que afectan a elementos tecnológicos.
La acciones que usan el ciberespacio como medio para realizar actividades maliciosas o ilícitas.

CIBERESPIONAJE	AMENAZAS HÍBRIDAS	CIBERCRIMEN	HACKTIVISMO
Amenazas Persistentes Avanzadas	Acciones militares Ciberataques Manipulación de la información	Ciberterrorismo Ciberdelito	Ciberataques



Capítulo 3

Propósito, principios y objetivos para la ciberseguridad

Propósito, principios y objetivos para la ciberseguridad

En este capítulo se establece el propósito y los principios por los que se rige la Estrategia, así como los objetivos: uno general y cinco específicos.

Propósito

España precisa, tal y como establece la Estrategia de Seguridad Nacional de 2017, garantizar un uso seguro y responsable de las redes y los sistemas de información y comunicaciones a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques potenciando y adoptando medidas específicas para contribuir a la promoción de un ciberespacio seguro y fiable.

Por tanto, el propósito de la Estrategia Nacional de Ciberseguridad 2019, es 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, España ha de seguir avanzando en el **refuerzo de capacidades** para hacer frente a las ciberamenazas y el uso malicioso del ciberespacio. En consecuencia, se

seguirán promoviendo medidas que ayuden a garantizar a nuestra nación su seguridad, con especial atención al sector público y los servicios esenciales, en un marco más coordinado y con estructuras de cooperación mejoradas.

Por otra parte, el fomento de la **cultura de ciberseguridad** ha de ser uno de los ejes centrales a desarrollar a fin de contar con una sociedad más conocedora de las amenazas y desafíos a las que se enfrenta. El derecho a hacer un uso seguro y fiable del ciberespacio y el contribuir a que así sea, es una responsabilidad compartida.

España sigue avanzando en el refuerzo de capacidades para garantizar la seguridad del sector público y los servicios esenciales.

Asimismo, la ciberseguridad es progreso, por lo que el **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 tiene un carácter singular.
Por otro lado, es un objetivo prioritario en nuestra sociedad alcanzar y mantener los **conocimientos, habilidades**, experiencia y capacidades tecnológicas y profesionales, ya que solo mediante su promoción se podrá responder a los grandes retos de la ciberseguridad.

La transversalidad y globalidad del ciberespacio, requiere además de la cooperación y del cumplimiento del Derecho internacional, del máximo respeto a los principios recogidos en la Constitución y en la Carta de Naciones Unidas; en coherencia con la Estrategia de Seguridad Nacional y con las iniciativas desarrolladas en el marco europeo, regional e internacional, prevaleciendo en todo momento los intereses nacionales.

Principios Rectores

La Estrategia Nacional de Ciberseguridad, se sustenta y se inspira en los principios rectores de la Seguridad Nacional: unidad de acción, anticipación, eficiencia y resiliencia.

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.

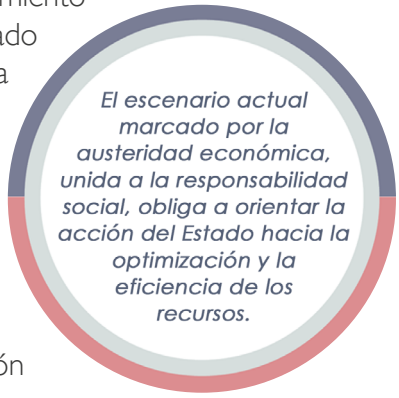
Una gestión centralizada de las crisis que afecten al ciberespacio, permite mantener una visión completa de la situación de la amenaza y posibilita el empleo de los recursos disponibles de forma más rápida, eficiente, coherente e integral.

2. **Anticipación**: La especificidad del ciberespacio y de los actores implicados demanda que existan mecanismos de anticipación en organismos especializados, que orienten la Acción del Estado en situaciones de crisis, y en la que igualmente debe participar el sector privado.

   La anticipación prima 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.

   Además, el escenario actual y futuro está marcado por la austeridad económica, que unida a la responsabilidad social de obtener el máximo rendimiento de los recursos disponibles, obliga a orientar la acción del Estado hacia la optimización y la eficiencia de los dedicados a la ciberseguridad, por lo que resultarán indispensables la unidad de acción, compartición de información e integración de estos recursos para alcanzar la eficiencia deseada.



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. Especial mención merece el refuerzo que requieren las redes de información y comunicaciones frente a actividades de las ciberamenazas o al uso ilícito del ciberespacio.

PRINCIPIOS RECTORES

Objetivo general

Los nuevos retos de la ciberseguridad han requerido la adaptación de su objetivo general de manera que se muestre más integrador, inclusivo y menos tecnificado.

> 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.

Basados en este objetivo general, a continuación, se fijan una serie de objetivos específicos que orientan la acción del Estado en este ámbito.

Objetivo 1

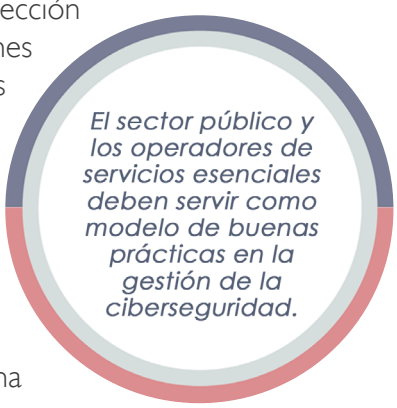
> Seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales.

Es necesario consolidar un marco nacional coherente e integrado que ayude a garantizar la protección de la información manejada por el sector público y por los servicios esenciales, sus sistemas y servicios, así como de las redes que los soportan. Este marco permitirá desarrollar e implantar servicios cada vez más seguros y eficientes.

Para ello, es necesario implantar medidas de seguridad enfocadas a mejorar las capacidades de prevención, detección y respuesta ante incidentes, desarrollando nuevas soluciones, reforzando la coordinación y adaptando en consecuencia el ordenamiento jurídico.

En particular, las acciones contra el ciberespionaje merecen especial mención 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.

El sector público y los operadores de servicios esenciales se deben involucrar activamente en un proceso de mejora continua respecto de la protección de sus sistemas de Tecnologías de la Información y las Comunicaciones basados en una vigilancia permanente de su exposición a las amenazas. Estos agentes deben servir como modelo de **buenas prácticas en la gestión de la ciberseguridad.**



En aplicación del principio de responsabilidad compartida, el sector público debe mantener estrechas relaciones con las empresas que gestionan los Sistemas de Tecnologías de la información y las comunicaciones relevantes para los intereses nacionales, intercambiando el conocimiento que permita una adecuada coordinación entre ambos y una cooperación efectiva que genere una sinergia apropiada dentro del entorno de la ciberseguridad.

El fortalecimiento de la ciberseguridad requiere un conocimiento sistemático sobre el impacto de una potencial interrupción o destrucción de las redes y sistemas que proporcionan servicios esenciales, así como métricas del nivel de seguridad de estos sistemas que permitan la oportuna toma de decisiones según su grado de exposición.

Objetivo II

Uso seguro y fiable del ciberespacio frente a su uso ilícito o malicioso.

El ciberespacio juega un papel cada vez más importante tanto en la comisión de hechos ilícitos o maliciosos, como en su investigación para promover la confianza de los ciudadanos. Es necesario garantizar una adecuada persecución de los fenómenos criminales que en él se desarrollen.

Son tres los ámbitos en los que se desenvuelve la lucha contra la cibercriminalidad: (i) el ciberespacio como objetivo directo de los hechos delictivos, o de la amenaza; (ii) el ciberespacio como medio clave para la su comisión; y (iii) el ciberespacio como medio u objeto directo de investigación de cualquier tipo de hecho ilícito.

Sobre la base de una regulación sólida y eficaz que refuerce y garantice la lucha contra la cibercriminalidad, es necesario el fortalecimiento de la cooperación judicial y policial, tanto nacional como internacional, así como la asignación de recursos suficientes a los órganos competentes en la materia y la capacitación de los profesionales que trabajan en este ámbito.

Del mismo modo, es fundamental fomentar la colaboración y participación ciudadana, facilitando los procedimientos de acceso y transmisión de la información de interés judicial y policial e identificando aspectos que requieran de una mejora en las capacidades de las instituciones policiales y de los organismos judiciales competentes.

Objetivo III

Protección del ecosistema empresarial y social y de los ciudadanos.

Todas las personas y organizaciones tienen derecho a hacer un uso seguro del ciberespacio. Es por ello responsabilidad del Estado promover e impulsar las medidas para alcanzar y mantener un nivel suficiente de ciberseguridad, que proteja especialmente a los más vulnerables y que permita el adecuado desarrollo socioeconómico de España.

La ciberseguridad es una responsabilidad compartida con los actores privados que, por acción u omisión, puedan afectarla; y no es posible conseguirla sin su participación. Por tanto, entre las medidas a impulsar deben estar aquellas que conduzcan a la necesaria cooperación para la seguridad común.

La ciberseguridad es una responsabilidad compartida entre el Estado y los actores privados, precisando un intercambio permanente de conocimiento.

La defensa de ciudadanos, autónomos y empresas debe ir más allá de las medidas de autoprotección que ellos puedan tomar, por lo que es conveniente implantar medidas para su ciberdefensa activa. A la vez todos los usuarios del ciberespacio deben hacer un uso responsable de la tecnología a su alcance.

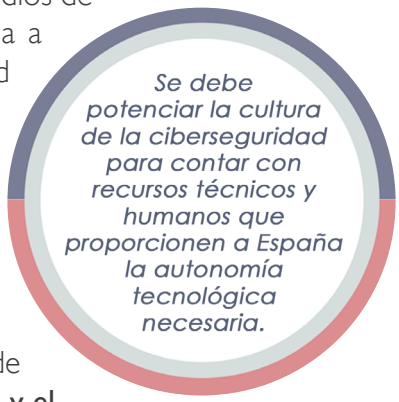
La acelerada adopción por la sociedad de tecnologías emergentes provoca que los riesgos evolucionen. Por ello, el intercambio permanente de conocimiento con los diferentes actores y el establecimiento de mecanismos de monitorización para la protección del ecosistema empresarial y social y de los ciudadanos serán instrumentos que permitirán al Gobierno estar informado y tomar las decisiones oportunas para actualizar y adecuar las acciones resultado de la presente estrategia.

Objetivo IV

Cultura y compromiso con la ciberseguridad y potenciación de las capacidades humanas y tecnológicas.

Para afrontar los desafíos que plantea la ciberseguridad, España debe contar con recursos técnicos y humanos que le proporcionen la autonomía tecnológica necesaria y la capacitación adecuada para el uso seguro del ciberespacio, situando a la ciberseguridad como habilitador clave para una nación emprendedora.

Para ello debe mejorar la ciberseguridad colectiva difundiendo la cultura de la ciberseguridad con la ayuda de organismos públicos y privados y medios de comunicación, potenciando mecanismos de información y asistencia a los ciudadanos y fomentando espacios de encuentro entre la sociedad civil, administraciones y empresas.



Se debe también contribuir al uso seguro y responsable de las Tecnologías de la Información y de las Comunicaciones promoviendo la capacitación en ciberseguridad de los profesionales adecuada a la demanda del mercado laboral, estimulando el desarrollo de los profesionales con habilidades propias, impulsando la formación y cualificación especializada, así como las capacidades de generación de conocimiento, **el desarrollo actividades de I+D+i en ciberseguridad y el fomento del uso de productos y servicios certificados**.

Asimismo, merece especial atención la protección del patrimonio tecnológico y de la propiedad industrial e intelectual. Para promover la soberanía tecnológica y aprovechar las oportunidades que ofrece la transformación digital, se fomentará e impulsará la industria española de ciberseguridad y las mejores prácticas en el desarrollo e implantación de sistemas de información y comunicaciones.

Objetivo V

Seguridad del ciberespacio en el ámbito internacional.

España promoverá un ciberespacio abierto, plural, seguro y confiable tanto en sus relaciones bilaterales como en las organizaciones multilaterales, regionales e internacionales, y en los foros y conferencias, donde la ciberseguridad ocupa un lugar destacado.

Abogará por la creación de un marco internacional para la prevención de conflictos, la cooperación y la estabilidad en el ciberespacio, en el que se apliquen los principios de La Carta de Naciones Unidas en su totalidad, el Derecho Internacional, los Derechos Humanos y el Derecho Humanitario Bélico, así como las normas no vinculantes sobre el comportamiento responsable de los Estados.

Consciente de la importancia del multilateralismo, considera relevante el papel de Naciones Unidas para avanzar en la construcción de consensos, que, junto a la adopción y puesta en marcha de medidas de fomento de la confianza, la colaboración y participación de todos los actores implicados (Estados, sector privado, sociedad civil, usuarios y academia), constituyen la base para lograr seguridad y estabilidad en el ciberespacio y avanzar hacia su regulación.

En línea con nuestros socios europeos, reforzará la confianza en Internet, en la transformación digital y en el desarrollo de las nuevas tecnologías, contribuyendo a consolidar un ecosistema cibernético europeo seguro que permita avances hacia el mercado único digital. Para ello defenderá un internet interoperativo, neutral, abierto y diverso, reflejo de la pluralidad cultural y lingüística internacional, basado en un sistema de gobernanza democrático representativo e inclusivo, resultado de la concertación y el consenso. Ademas, un acceso a internet global y generalizado, contribuyendo con ello al cumplimiento de los Objetivos de Desarrollo Sostenible.

Del mismo modo, nuestra pertenencia a la Unión Europea, nos obliga a fortalecer la seguridad y la autonomía estratégica europea mediante la búsqueda de sinergias, la cooperación técnica, operativa, estratégica y política; a reforzar nuestra resiliencia,

nuestra capacidad de respuesta ante las crisis y las complementariedades entre los ámbitos civiles y militares como socios UE y aliados OTAN.

Sobre la base de lo anterior, España continuará participando activamente en la Unión Europea y la Organización del Tratado del Atlántico Norte (OTAN); en Naciones Unidas, y en sus foros derivados como el Foro de Gobernanza de Internet (IGF); en la Organización para la Seguridad y la Cooperación en Europa (OSCE), en el desarrollo e implementación de las Medidas de Fomento de la Confianza; en la Organización de Estados Americanos (OEA). Así como con el Foro Global del Expertos en Ciberseguridad (GFCE) y la Coalición por la Libertad en Internet (FOC), sin olvidar nuestra presencia en el Centro Europeo de Excelencia para contrarrestar las Amenazas Híbridas (Hybrid CoE), así como en el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCD CoE).

Además, reforzará la cooperación internacional bilateral en materia de ciberseguridad, promoverá relaciones fluidas y de confianza en este ámbito, colaborará en la construcción de capacidades en terceros Estados, prestando especial atención a las mujeres y los jóvenes y fomentará la creación de canales de información e intercambio de experiencias, impulsando, para todo ello, la adopción de acuerdos bilaterales y multilaterales en este ámbito.

OBJETIVOS DE LA ESTRATEGIA

OBJETIVO GENERAL

En línea con la Estrategia de Seguridad Nacional, España garantizará el uso seguro y fiable del ciberespacio, protegiendo los derechos y las libertades de los ciudadanos y promoviendo el progreso socio económico.

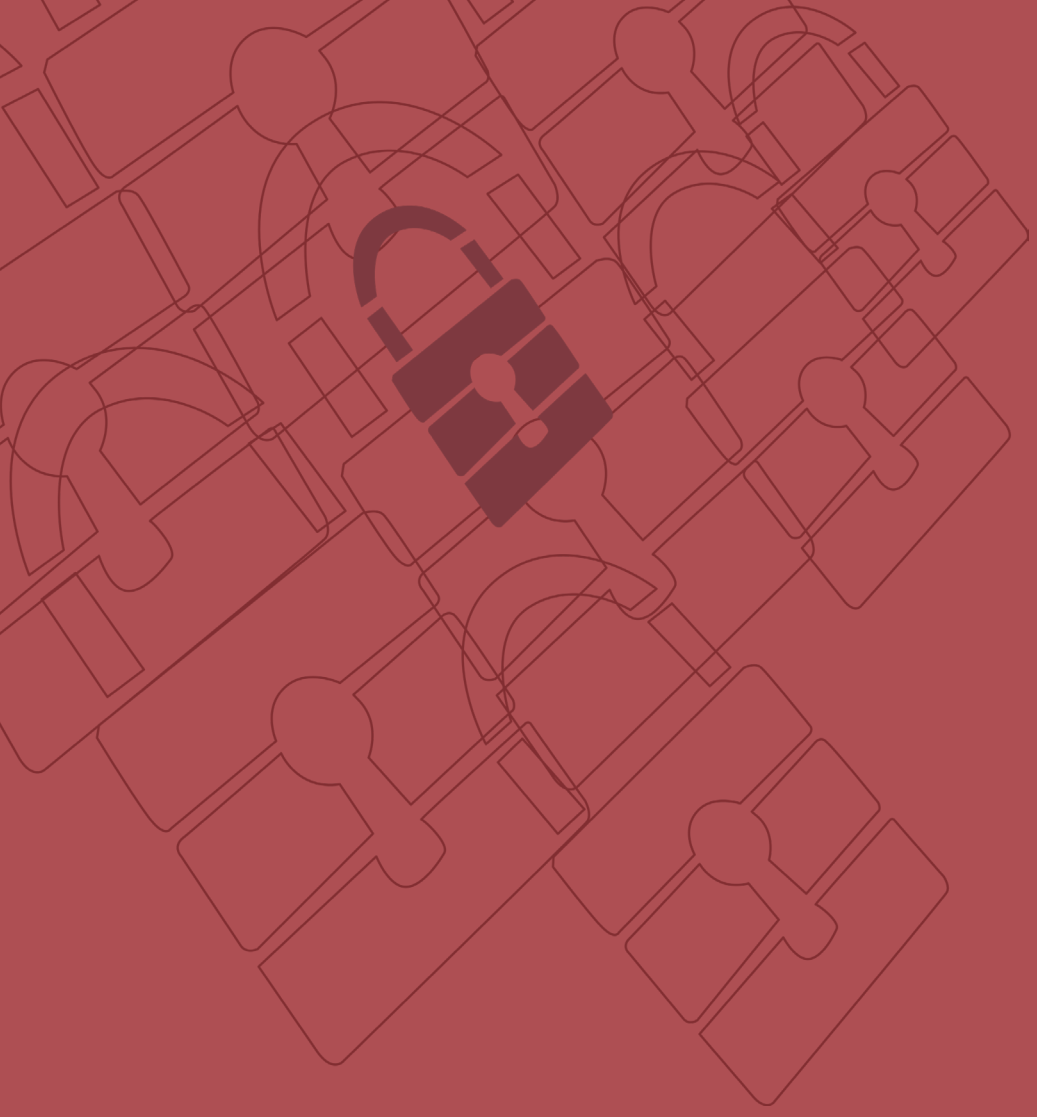
Objetivo **01** Seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales.

Objetivo **02** Uso seguro y fiable del ciberespacio frente a un uso ilícito o malicioso.

Objetivo **03** Protección del ecosistema empresarial y social de los ciudadanos.

Objetivo **04** Cultura y compromiso con la ciberseguridad y protección de las capacidades humanas y tecnológicas.

Objetivo **05** Seguridad del ciberespacio en el ámbito internacional.



Capítulo 4

Líneas de acción y medidas

Líneas de acción y medidas

En este capítulo se establecen las líneas de acción dirigidas a la consecución de los objetivos establecidos.

LÍNEA DE ACCIÓN 1

Reforzar las capacidades ante las amenazas provenientes del ciberespacio.

Esta línea de acción responde al Objetivo 1 de la Estrategia.

MEDIDAS

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 DE ACCIÓN 2

Garantizar la seguridad y resiliencia de los activos estratégicos para España.

Esta línea de acción responde al Objetivo I de la Estrategia.

MEDIDAS

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.

LÍNEA DE ACCIÓN 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.

Esta línea de acción responde al Objetivo II de la Estrategia.

MEDIDAS

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.

LÍNEA DE ACCIÓN 4

Impulsar la ciberseguridad de ciudadanos y empresas.

Esta línea de acción responde al Objetivo III de la Estrategia.

MEDIDAS

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.

LÍNEA DE ACCIÓN 5

Potenciar la industria española de ciberseguridad, y la generación y retención de talento, para el fortalecimiento de la autonomía digital.

Esta línea de acción responde al Objetivo IV de la Estrategia.

MEDIDAS

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.

LÍNEA DE ACCIÓN 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.

Esta línea de acción responde al Objetivo V de la Estrategia.

MEDIDAS

1. Potenciar y reforzar la presencia de España en las organizaciones, conferencias y foros regionales e internacionales 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 DE ACCIÓN 7

Desarrollar una cultura de ciberseguridad.

Las medidas incluidas en esta Línea de Acción contribuirán al Plan de Cultura de Seguridad Nacional y responde al objetivo IV de la Estrategia.

MEDIDAS

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.

LÍNEAS DE ACCIÓN

Objetivo I

LÍNEA DE ACCIÓN I - II

Reforzar las capacidades ante las amenazas provenientes del ciberespacio.

Garantizar la seguridad y resiliencia de los activos estratégicos para España.

Objetivo II

LÍNEA DE ACCIÓN III

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.

Objetivo III

LÍNEA DE ACCIÓN IV

Impulsar la ciberseguridad de ciudadanos y empresas.

Objetivo IV

LÍNEA DE ACCIÓN V

Potenciar la industria española de ciberseguridad, y la generación y retención de talento, para el fortalecimiento de la autonomía digital.

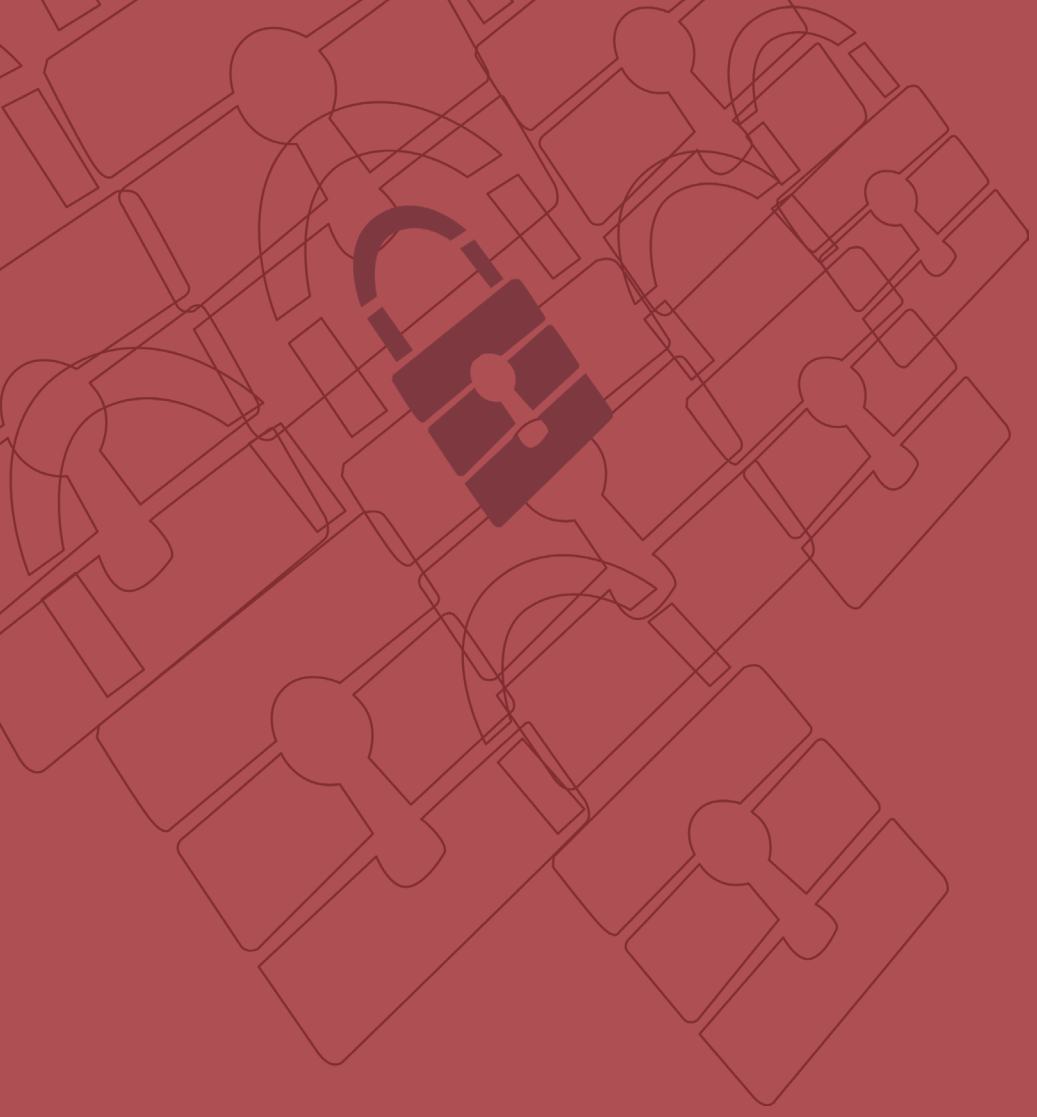
LÍNEA DE ACCIÓN VII

Desarrollar una cultura de ciberseguridad.

Objetivo V

LÍNEA DE ACCIÓN VI

Contribuir a la seguridad del ciberespacio en el ámbito internacional, promoviendo un ciberespacio abierto, plural, seguro y confiable, en apoyo de los intereses nacionales.



Capítulo 5

La ciberseguridad en el Sistema de Seguridad Nacional

La ciberseguridad en el Sistema de Seguridad Nacional

En este capítulo se contempla la integración de la ciberseguridad en el actual Sistema de Seguridad Nacional.

La Estrategia de Ciberseguridad Nacional de 2013 y la posterior aprobación de la Ley de Seguridad Nacional de 2015 establecen una estructura orgánica específica para la ciberseguridad. En la presente Estrategia de 2019 se impulsan 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.

El 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.

El 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.

El Consejo Nacional de Ciberseguridad

El Consejo Nacional de Ciberseguridad da 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.

Entre sus funciones se encuentran reforzar las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias en materia de ciberseguridad, así como entre los sectores público y privado, y facilitar la toma de decisiones del propio Consejo mediante el análisis, estudio y propuesta de iniciativas tanto en el ámbito nacional como en el internacional, así como 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.

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.

El funcionamiento de la Comisión se enmarca en el procedimiento de gestión de crisis en el ámbito de la ciberseguridad. Dicho procedimiento establece sus funciones dirigidas a detectar y valorar los riesgos y amenazas; facilitar el proceso de toma de decisiones y asegurar una respuesta óptima y coordinada de los recursos del Estado. Además, incluye los diferentes niveles de activación del Sistema de Seguridad Nacional, e instrucciones para la gestión de la comunicación pública.

A fin de responder de manera oportuna y porporcionada a situaciones de especial relevancia en el desarrollo de sus funciones, se progresará en la definición de sus capacidades y responsabilidades.

Foro Nacional de Ciberseguridad

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.

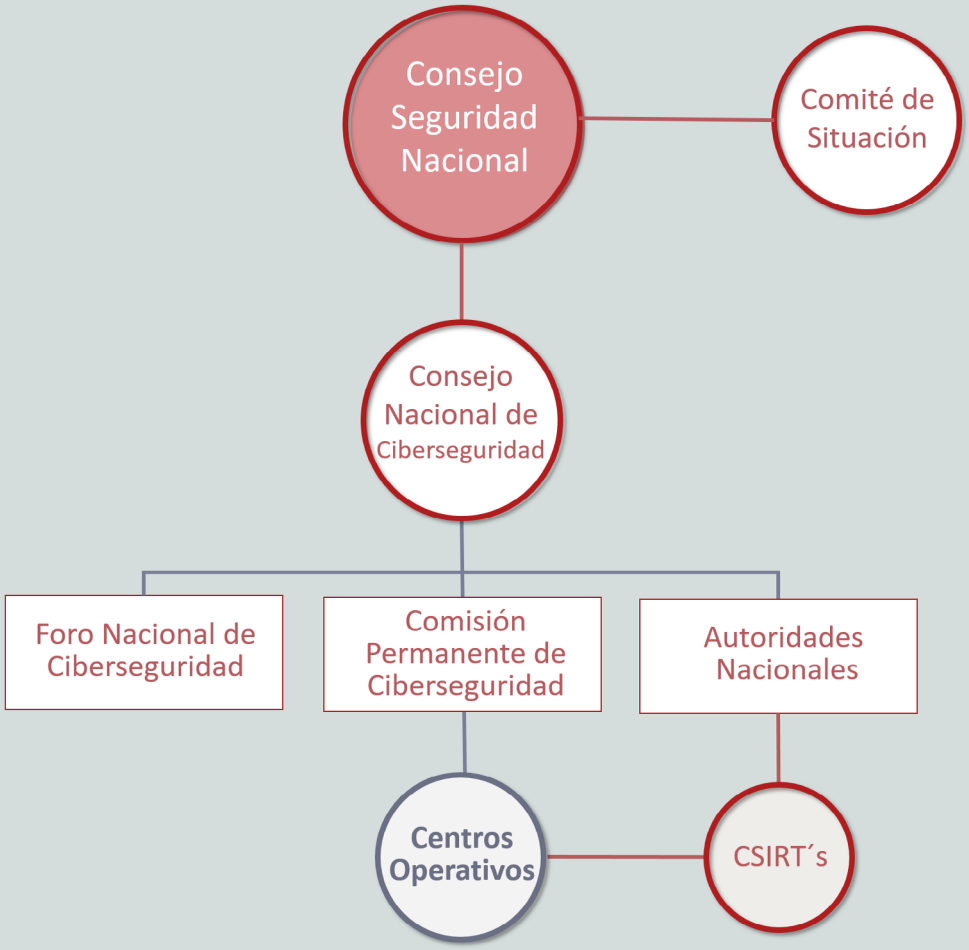
La puesta en marcha del **foro Nacional de Ciberseguridad**, y la armonización de su funcionamiento con los órganos existentes, se realizará mediante la aprobación de las disposiciones normativas necesarias, con el objetivo de alcanzar el funcionamiento coordinado y eficiente de estos componentes en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

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.

ESTRUCTURA DE LA CIBERSEGURIDAD EN EL SISTEMA DE SEGURIDAD NACIONAL



Consideraciones finales y evaluación

La experiencia adquirida desde la Estrategia de Ciberseguridad Nacional de 2013, ha permitido plasmar en el presente documento una actualización de las amenazas y los desafíos a las que nos enfrentamos siempre en continua evolución. Para adecuarse a este nuevo escenario cambiante, se proponen un conjunto de Líneas de Acción y medidas más dinámicas que permitan, si fuese necesario, una rápida adaptación del ecosistema de ciberseguridad nacional, basadas en un modelo de gobernanza con una considerable madurez, donde debe participar activamente el sector privado y el resto de la sociedad civil.

En este sentido, la Estrategia se concibe como un documento vivo que ha de adaptarse a la evolución de la ciberseguridad, por lo que deberá ser objeto de revisión continua, como también los planes específicos y sectoriales que de ella se deriven. Por otro lado se elaborará un informe anual de evaluación de la Estrategia donde figurará el grado de ejecución y cumplimiento de sus objetivos.

A la vista del incremento de las amenazas y desafíos a la ciberseguridad y como los enfrontan países de nuestro entorno, resulta cada vez más urgente dotarse de recursos económicos, humanos y materiales para hacer frente a los mismas. Una de las acciones especialmente relevantes en este marco es que el Centro de Operaciones de Ciberseguridad de la Administración General del Estado se encuentre adecuadamente dotado.

DSN

www.dsn.gob.es