

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

2019



DSN

Catálogo de publicaciones de la Administración General del Estado
<http://publicacionesoficiales.boe.es>

Edita:



© Editor, 2019

NIPO (edición impresa): 042-19-028-9

NIPO (edición on line): 042-19-029-4

Depósito Legal: 16844-2019

Fecha de edición: Junio 2019

Imprime: imprenta GRAFOX IMPRENTA, S.L.

Los derechos de explotación de esta obra están amparados por la Ley de Propiedad Intelectual. Ninguna de las partes de la misma puede ser reproducida, almacenada ni transmitida en ninguna forma ni por medio alguno, electrónico, mecánico o de grabación, incluido fotocopias, o por cualquier otra forma, sin permiso previo, expreso y por escrito de los titulares del © Copyright.

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

EL PRESIDENTE DEL GOBIERNO

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

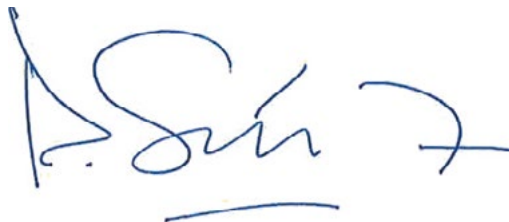
EL PRESIDENTE DEL GOBIERNO

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.....	9
Introducción.....	13
Capítulo 1	
El ciberespacio como espacio común global.....	17
El ciberespacio: oportunidades y desafíos.....	17
Infraestructura digital.....	19
Plano internacional: seguridad en el ciberespacio.....	19
Una nueva concepción del ciberespacio.....	20
Capítulo 2	
Las amenazas y desafíos en el ciberespacio	23
Ciberamenazas	23
Acciones que usan el ciberespacio para fines maliciosos.....	24

Capítulo 3

Propósito, principios y objetivos para la ciberseguridad.....29

Propósito.....	29
Principios Rectores.....	30
Objetivo general.....	34
Objetivo I.....	34
Objetivo II.....	36
Objetivo III.....	37
Objetivo IV.....	38
Objetivo V.....	39

Capítulo 4

Líneas de acción y medidas43

Línea de acción I.....	44
Línea de acción 2.....	46
Línea de acción 3.....	48
Línea de acción 4.....	50
Línea de acción 5.....	52
Línea de acción 6.....	54
Línea de acción 7.....	56

Capítulo 5

La ciberseguridad en el Sistema de Seguridad Nacional.....61

El Consejo de Seguridad Nacional.....	62
El Comité de Situación.....	62
El Consejo Nacional de Ciberseguridad.....	62
La Comisión Permanente de Ciberseguridad.....	63
Foro Nacional de Ciberseguridad.....	64
Autoridades públicas competentes y los CSIRT de referencia nacionales.....	64
Consideraciones finales y evaluación.....	66



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.

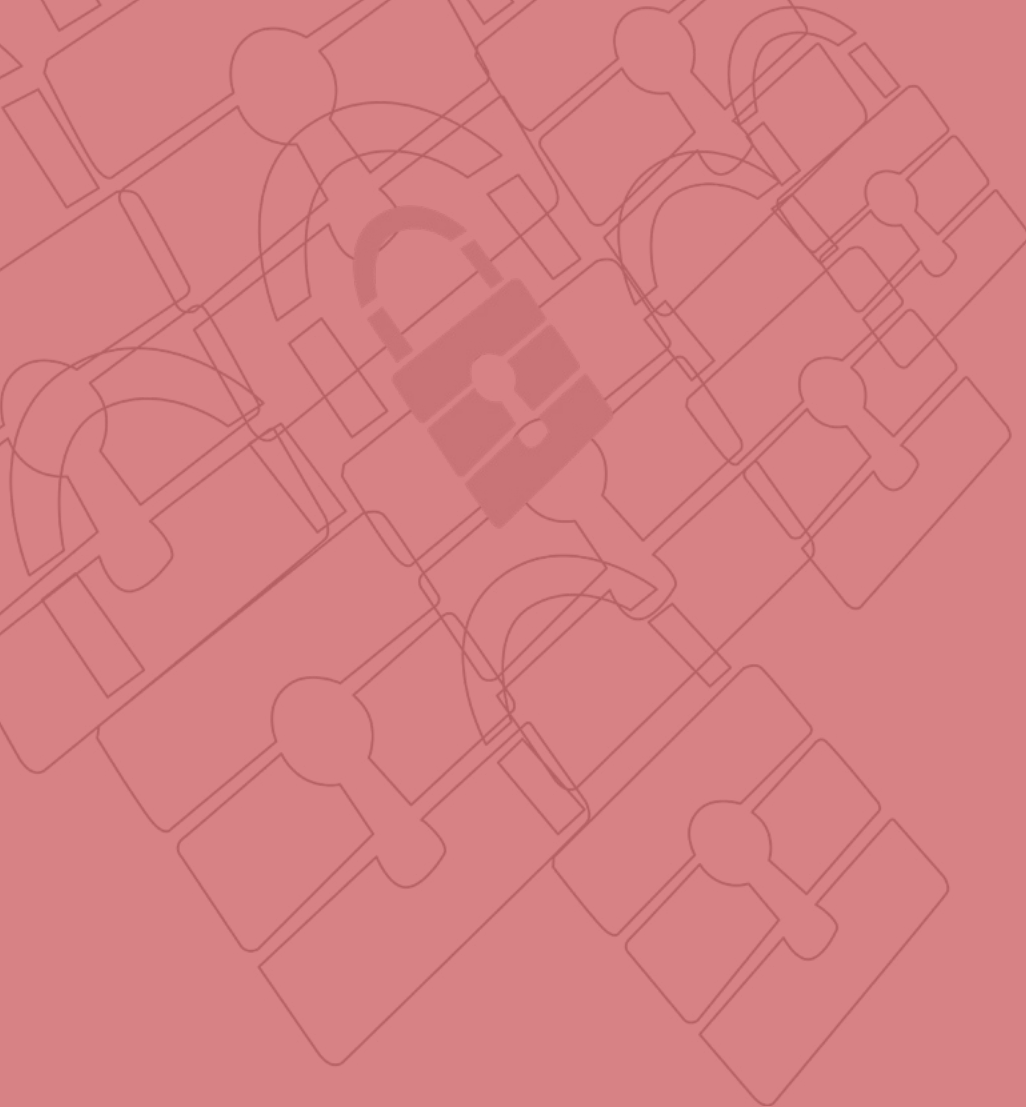
El **tercer capítulo**, titulado “Propósito, principios y objetivos para la ciberseguridad” aplica los principios rectores de la Estrategia de Seguridad Nacional 2017 (Unidad de acción, Anticipación, Eficiencia y Resiliencia) a cinco objetivos específicos que se identifican para la ciberseguridad nacional. 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.

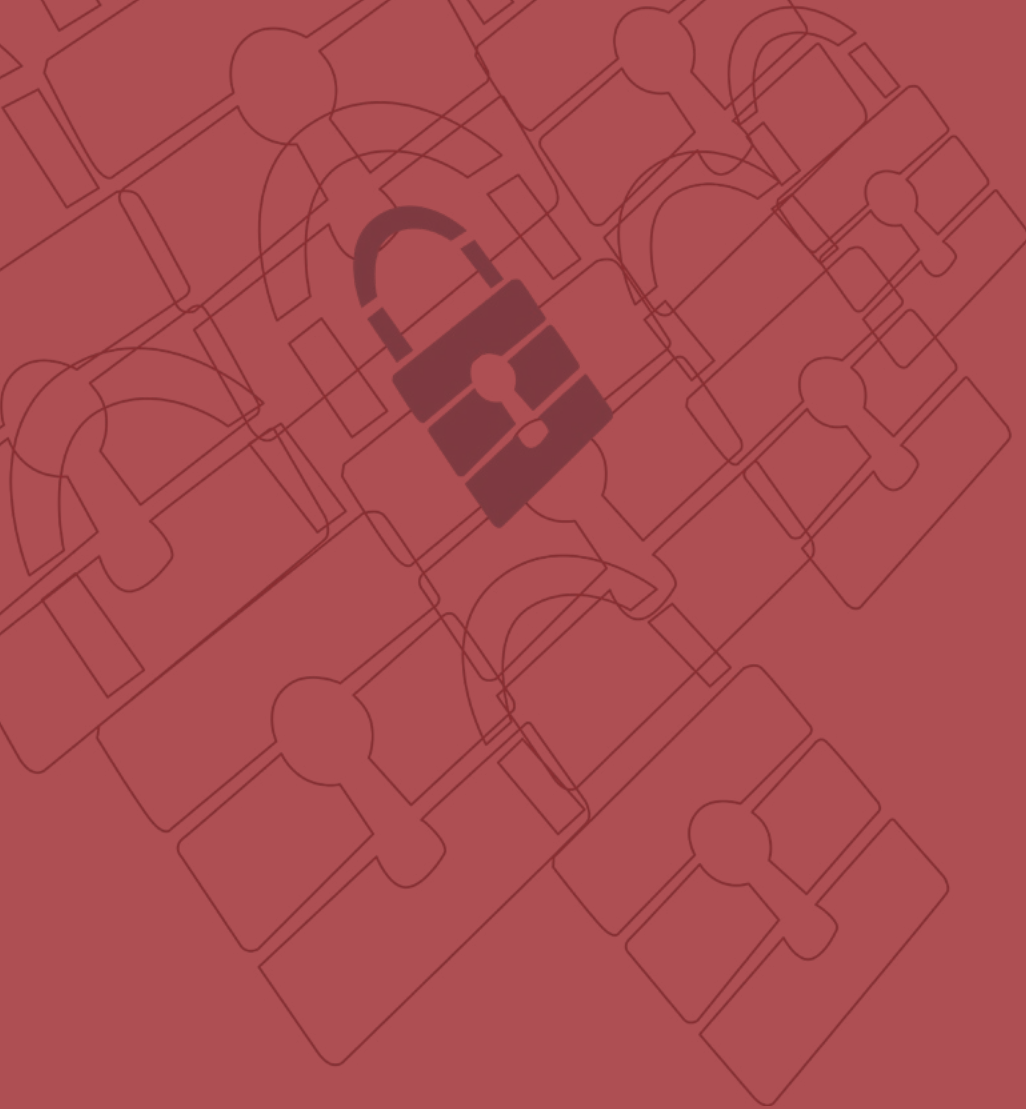
Una de las tendencias globales identificadas en la Estrategia, la digitalización, se muestra como motor del cambio con implicaciones para la seguridad. La Estrategia establece un esquema novedoso, con cinco objetivos generales que resultan transversales a todos los ámbitos. La gestión de crisis, la cultura 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



El ciberespacio ofrece innumerables oportunidades de futuro, aunque también presenta serios desafíos a la seguridad.

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.

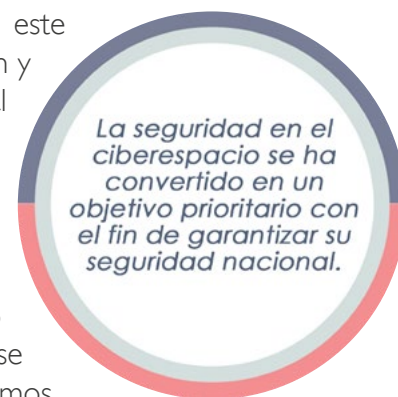
Este riesgo se ve amplificado por la prevalencia de criterios comerciales frente a los de seguridad en el diseño de los productos hardware y software, así como de los sistemas y de los servicios, algo que dificulta los procesos de certificación y puede comprometer la cadena de suministro.

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.



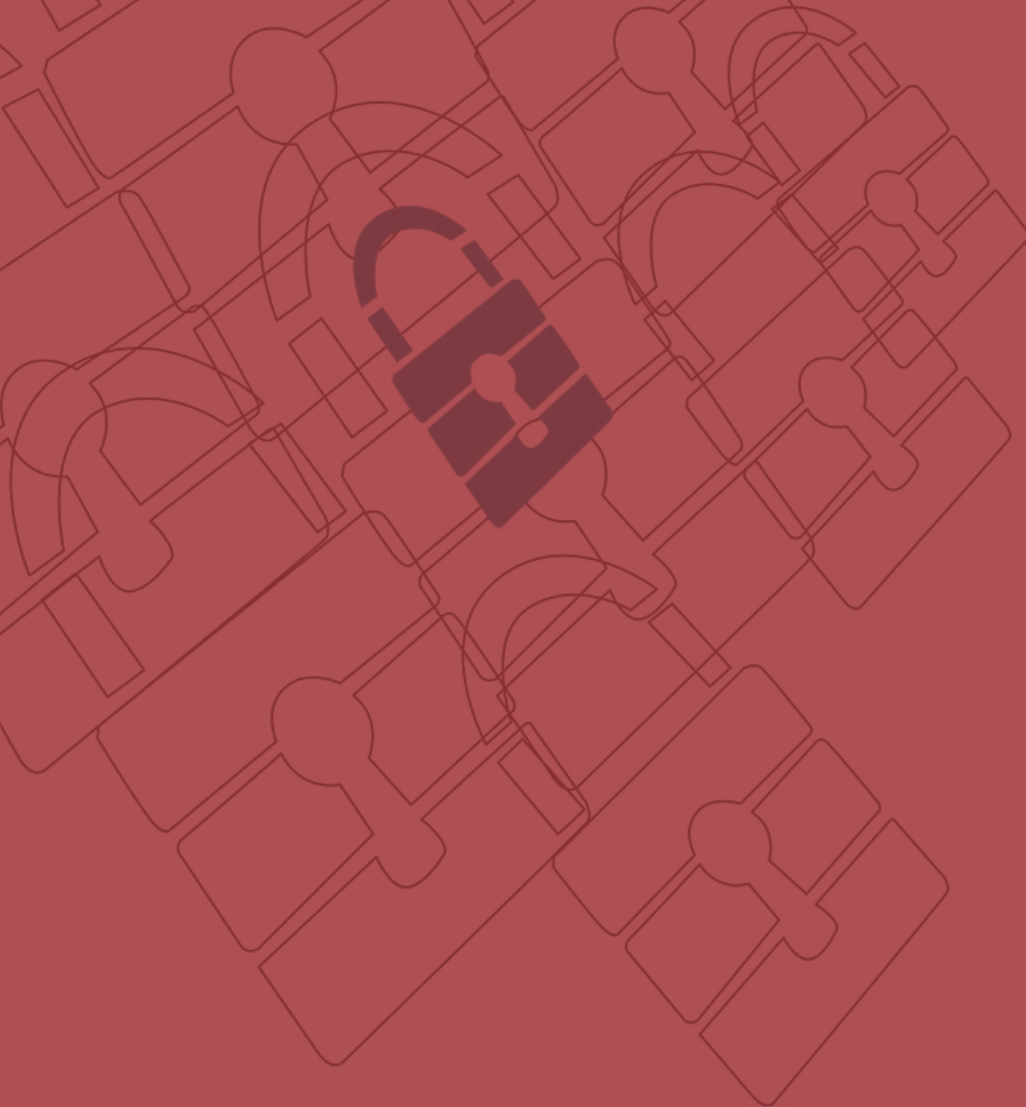
En efecto, el recurso humano continúa siendo un factor crítico. Existe una diferencia importante entre el número de puestos de trabajo para los que es necesaria una alta especialización en las tecnologías de la información, en concreto en ciberseguridad, y las personas disponibles con el nivel de conocimiento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

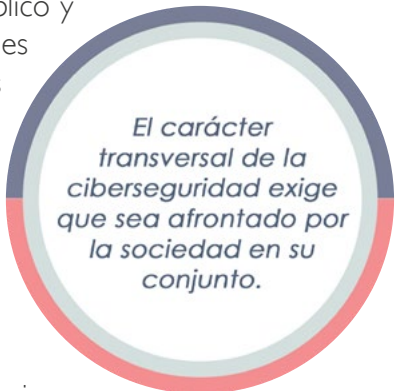
Las ciberamenazas son todas aquellas interrupciones o manipulaciones maliciosas que afectan a elementos tecnológicos. Abarcan un amplio abanico de acciones. Las ciberamenazas se caracterizan por su diversidad tanto en lo que concierne a capacidades como a motivaciones. Afectan a la práctica totalidad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

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.

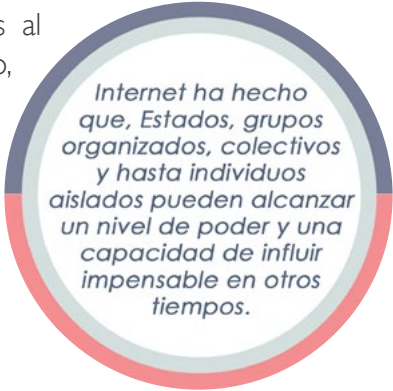


El carácter transversal de la ciberseguridad exige que sea afrontado por la sociedad en su conjunto.

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.

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.

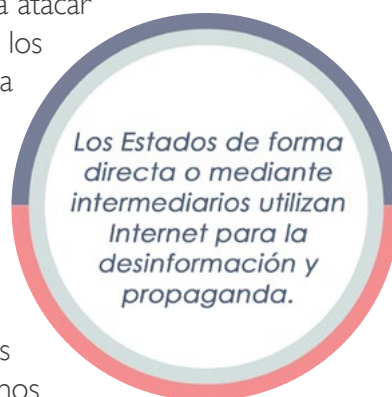


Internet ha hecho que, Estados, grupos organizados, colectivos y hasta individuos aislados pueden alcanzar un nivel de poder y una capacidad de influir impensable en otros tiempos.

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.

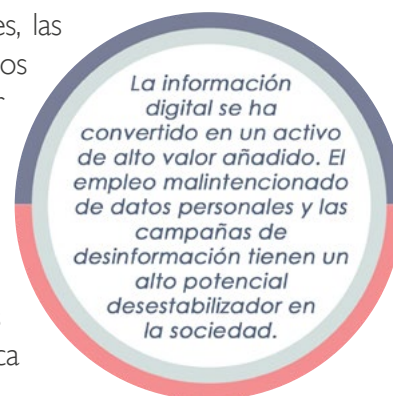


Los ciberdelincuentes operan bajo esquemas de crimen organizado y continúan explorando de manera incesante técnicas sobre las que construir modelos de negocio lucrativo y de bajo riesgo, amparados por la difícil trazabilidad de sus acciones.

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.



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
Persistentes
Avanzadas



AMENAZAS HÍBRIDAS

Acciones militares
Ciberataques
Manipulación de
la información



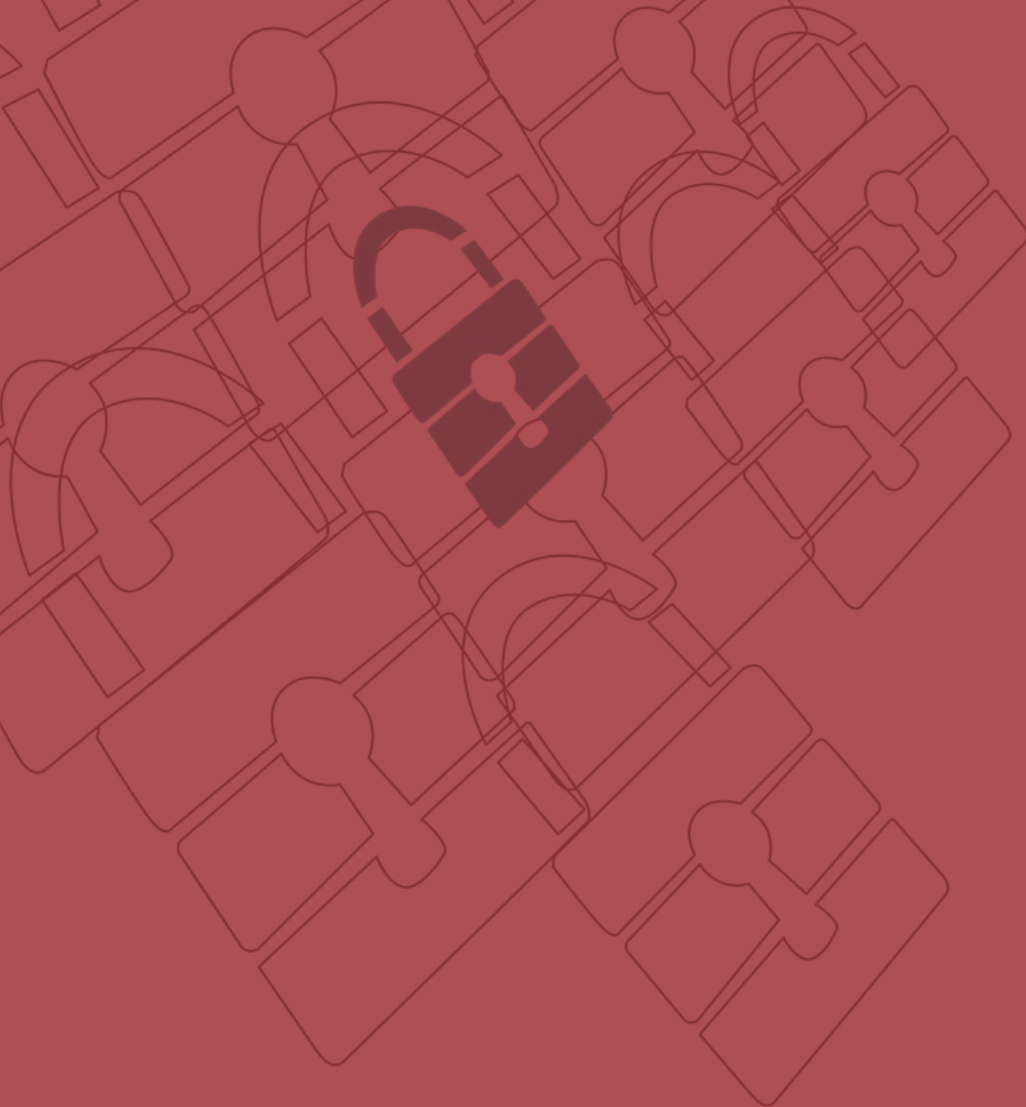
CIBERCRIMEN

Ciberterrorismo
Ciberdelito



HACKTIVISMO

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

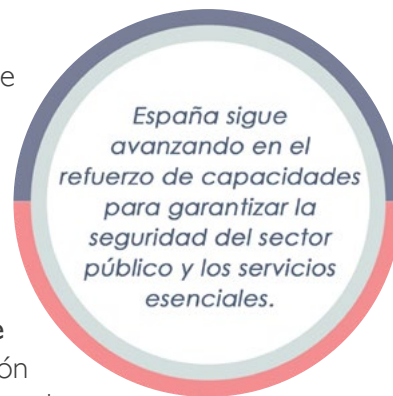
seguirán promoviendo medidas que ayuden a garantizar a nuestra nación su seguridad, con especial atención al sector público y los servicios esenciales, en un marco más coordinado y con estructuras de cooperación mejoradas.

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.

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.

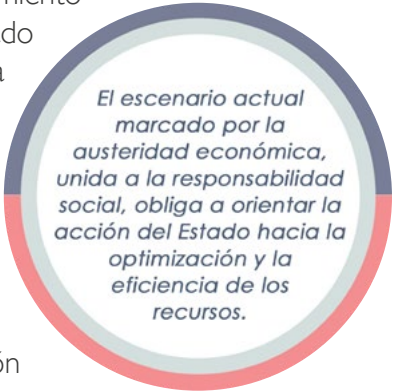
- 2. Anticipación:** La especificidad del ciberespacio y de los actores implicados demanda que existan mecanismos de anticipación en organismos especializados, que orienten la Acción del Estado en situaciones de crisis, y en la que igualmente debe participar el sector privado.

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.



El escenario actual marcado por la austeridad económica, unida a la responsabilidad social, obliga a orientar la acción del Estado hacia la optimización y la eficiencia de los recursos.

PRINCIPIOS RECTORES



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.

01



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.

02

03



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.



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.

04

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 I

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.

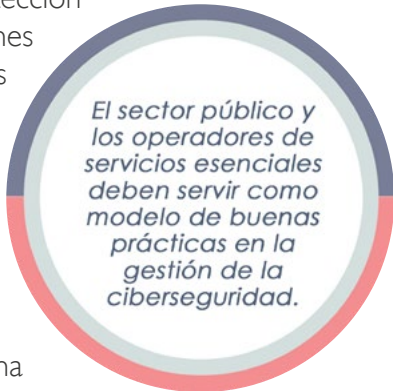
Para ello, es necesario implantar medidas de seguridad enfocadas a mejorar las capacidades de prevención, detección y respuesta ante incidentes, desarrollando nuevas soluciones, reforzando la coordinación y adaptando en consecuencia el ordenamiento jurídico.

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.

A circular graphic with a white center and a multi-colored border (blue, green, red). It contains the text: *El sector público y los operadores de servicios esenciales deben servir como modelo de buenas prácticas en la gestión de la ciberseguridad.*

El sector público y los operadores de servicios esenciales deben servir como modelo de buenas prácticas en la gestión de la ciberseguridad.

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.



Es necesario el fortalecimiento de la cooperación judicial y policial, tanto nacional como internacional, la asignación de recursos suficientes y la colaboración y participación ciudadana.


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 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.



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

Objetivo IV

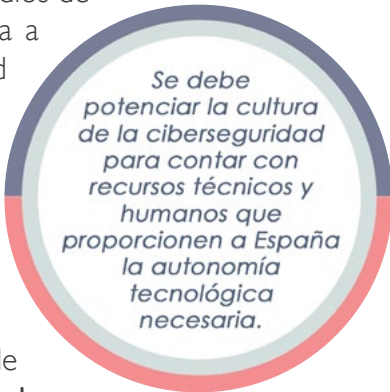
Cultura y compromiso con la ciberseguridad y potenciación de las capacidades humanas y tecnológicas.

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.



Se debe potenciar la cultura de la ciberseguridad para contar con recursos técnicos y humanos que proporcionen a España la autonomía tecnológica necesaria.

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. Además, 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.

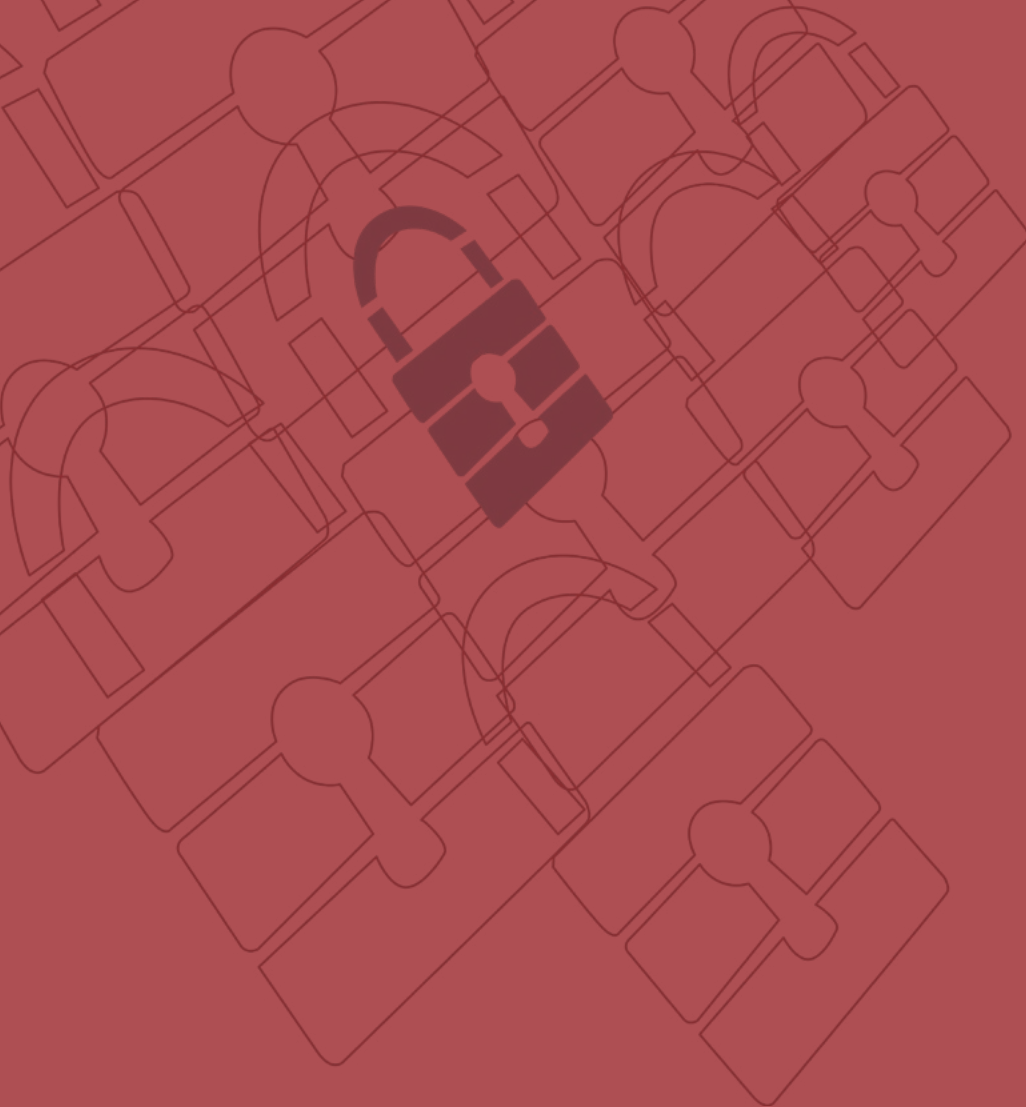


Objetivo

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 I

Reforzar las capacidades ante las amenazas provenientes del ciberespacio.

Esta línea de acción responde al Objetivo I 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

Reforzar las capacidades ante las amenazas provenientes del ciberespacio.

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

LÍNEA DE ACCIÓN I-II

Objetivo II

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.

LÍNEA DE ACCIÓN III

Objetivo III

Impulsar la ciberseguridad de ciudadanos y empresas.

LÍNEA DE ACCIÓN IV

Objetivo IV

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

LÍNEA DE ACCIÓN V

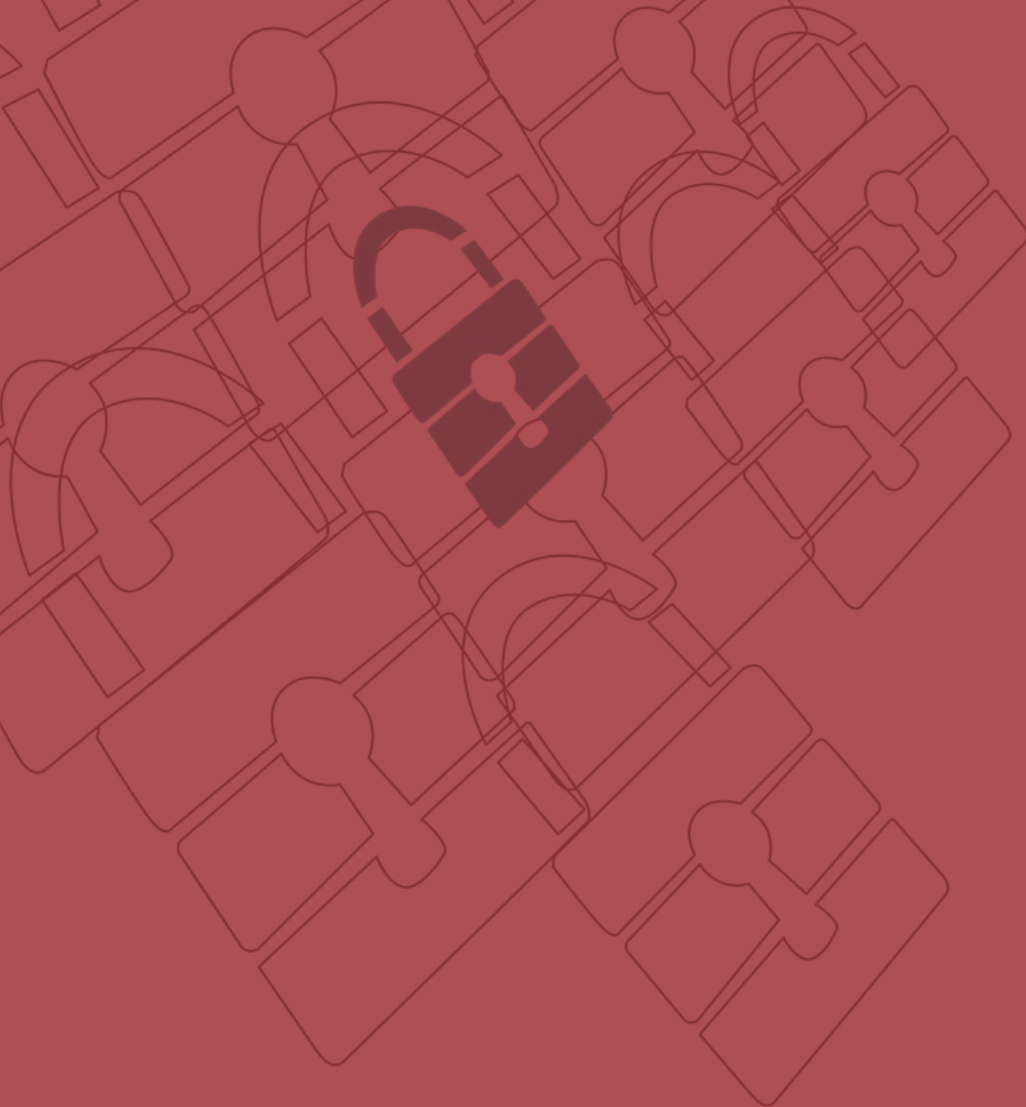
Desarrollar una cultura de ciberseguridad.

LÍNEA DE ACCIÓN VII

Objetivo V

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

LÍNEA DE ACCIÓN VI



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 proporcionada 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.

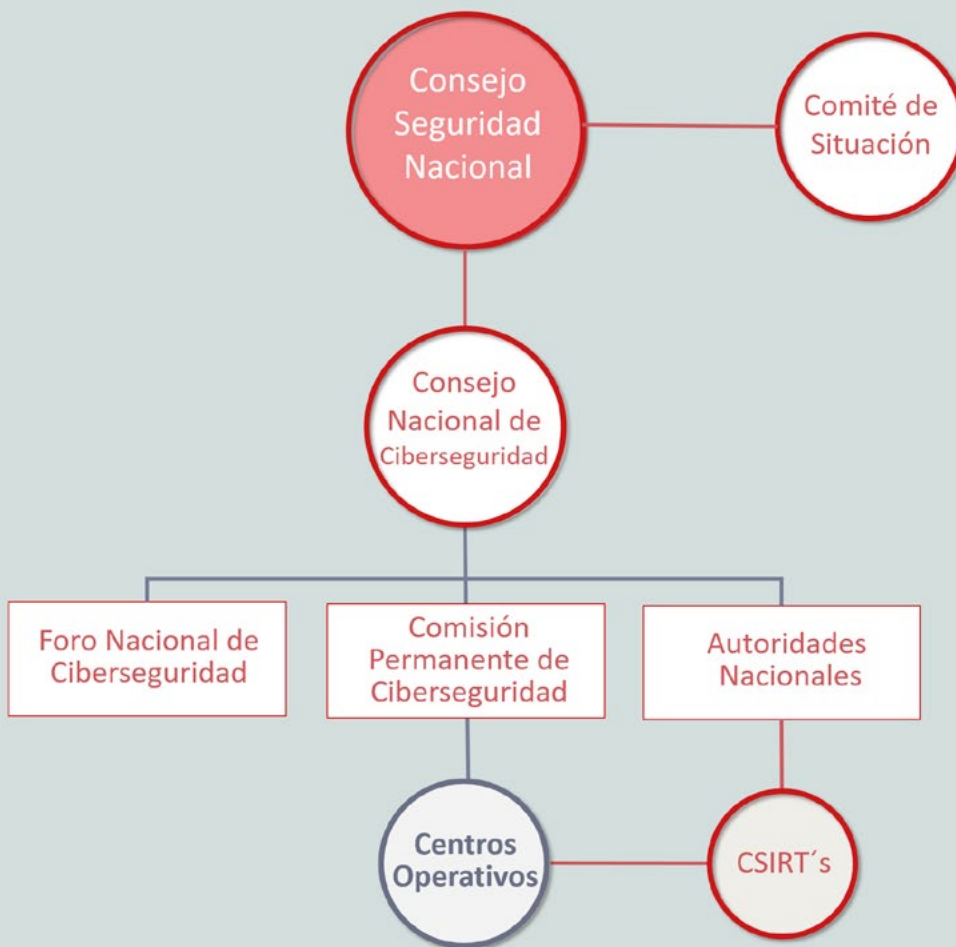
La puesta en marcha del **foro Nacional de Ciberseguridad**, y la armonización de su funcionamiento con los órganos existentes, se realizará mediante la aprobación de las disposiciones normativas necesarias, con el objetivo de alcanzar el funcionamiento coordinado y eficiente de estos componentes en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

NATIONAL CYBERSECURITY STRATEGY

2019



DSN

Catálogo de publicaciones de la Administración General del Estado
<http://publicacionesoficiales.boe.es>

Edita:



© Author and editor, 2019

NIPO (printed edition): 042-19-028-9

NIPO (online edition): 042-19-029-4

Depósito Legal: M-16844-2019

Edition date: June 2019

Printer: GRAFOX IMPRENTA, S.L.

All rights are protected by the Intellectual Property Law. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronically, mechanically, photocopying, recording or otherwise without the prior permission of the © Copyright holder.

NATIONAL CYBERSECURITY STRATEGY

2019

National Cybersecurity Strategy 2019 has been approved by the National Security Council.

The following bodies participated in the process: The Ministry of Foreign Affairs, European Union and Cooperation; the Ministry of Justice; the Ministry of Defence; the Ministry of the Treasury; the Ministry of Home Affairs; the Ministry of Public Works; the Ministry of Education and Vocational Training; the Ministry of Industry, Trade and Tourism; the Ministry of the Presidency, Parliamentary Relations and Equality; the Ministry of Territorial Policy and Public Function; the Ministry of the Economy and Business; the Ministry of Health, Consumption and Social Well-being; the Ministry of Science, Innovation and Universities; the National Intelligence Centre; the National Security Department and a Committee of Experts from professional associations, companies and the academia.



DSN

THE PRESIDENT OF THE GOVERNMENT

The fourth industrial revolution—the digital revolution—has, for years, coexisted with times of economic crises and social and political after-effects from which we are still recovering. Therefore, despite the undeniable opportunities and advances the digital world has to offer, many of our citizens are apprehensive and uncertain about all things related to the digital technological disruption. And it is here, in the fight to change that perception, that we in the public administrations must focus our priority efforts. What is at stake is society's trust in democratic institutions and in our own capacity to face the future in the certainty that we are making progress.

In the midst of an era of transformations and of uncertainties, we must offer a solid moral and material horizon, and to this end, it is increasingly essential to have cybersecurity that is equipped for the new times and the new threats. Cybersecurity that is capable of addressing the different challenges, and of doing so with public-private cooperation and with the support of a citizenry that is aware of the changing reality and committed to the solutions to these challenges.

This National Cybersecurity Strategy, in line with the 2017 National Security Strategy, seeks to contribute to this. And it seeks to do so with a clear goal as its guide: ensuring that these times of changes are not a source of cultural discontent and of economic and labour regression, but, rather, an opportunity to increase Spain's competitiveness and the well-being of Spaniards, as well as that of our European partners. This work has also taken into account our current geopolitical situation, which makes it more urgent and necessary to build and strengthen the European Union's strategic autonomy.

In all of this, Spain has a lot to say and to contribute. After all, ours is one of the most interconnected countries in the world. It only takes a glance at the daily news to realize how common and how dangerous the cyber threats we are facing really are. From fake news on social networks, to cyber espionage or the funding of terrorism—the digital realm is increasingly influencing and shaping reality. Moreover, other new technologies, such as artificial intelligence, robotics, big and smart data, and blockchain are already part of the daily activity of citizens, companies and public administrations. These new technologies have paved the way for ground-breaking instruments to obtain information, generate knowledge, and share data.

This influence will grow even further with the current implementation of what is known as 5G for the new connectivity of the internet of things. Being more interconnected and more dependent on said infrastructures will allow us to advance in many important fields, from achieving the United Nations Sustainable Development Goals, to combating the effects of climate change.

THE PRESIDENT OF THE GOVERNMENT

But it also makes us more vulnerable to hostile actions against—and coming from—said new infrastructures. Threats are becoming increasingly sophisticated and complex, and cyberspace is a weakly regulated area with no clear borders or jurisdictional demarcations, where the traceability of criminal actions, and the identification of state or non-state perpetrators, is difficult.

The challenge is enormous and multidisciplinary. Our professionals in the diverse areas involved in cybersecurity have well-deserved prestige and will be able to rise to the challenge. But cybersecurity requires commitment from us all. It is our responsibility, at the public administrations, to lead this commitment and to offer a framework of certainty to companies and citizens, who must also share this commitment. Once again, this is not only to avert the dangers and threats, but to make the most of the many opportunities to the benefit of all.

Cybersecurity protects assets, but it also protects essential values for a free society such as ours. We are not going to relinquish these principles in this era of global transformation. The technical challenges involved in cybersecurity are varied and complex, but something else is at stake. Something that refers to moral and cultural values related to our way of seeing and understanding the world, to what best defines us. Our freedom, well-being and democracy ultimately depend upon our success in designing an effective Cybersecurity Strategy. I am convinced that, with this document, we have taken a key step towards successfully addressing uncertain, but at the same time fascinating, years.



Pedro Sánchez Castejón

President of the Government of Spain



SUMMARY

Executive Summary.....	77
Introduction	81
Chapter 1	
Cyberspace: beyond a global common space	85
Cyberspace: opportunities and challenges.....	85
Digital infrastructure	87
International plan: security in cyberspace	87
A new conception of cyberspace.....	88
Chapter 2	
Threats and challenges in cyberspace.....	91
Cyberthreats	91
Actions that use cyberspace for malicious purposes.....	92

Chapter 3

Proposal, principles and goals for cybersecurity.....97

Proposal	97
Governing Principles	98
General Goal.....	102
Goal I	102
Goal II	104
Goal III.....	105
Goal IV	106
Goal V	107

Chapter 4

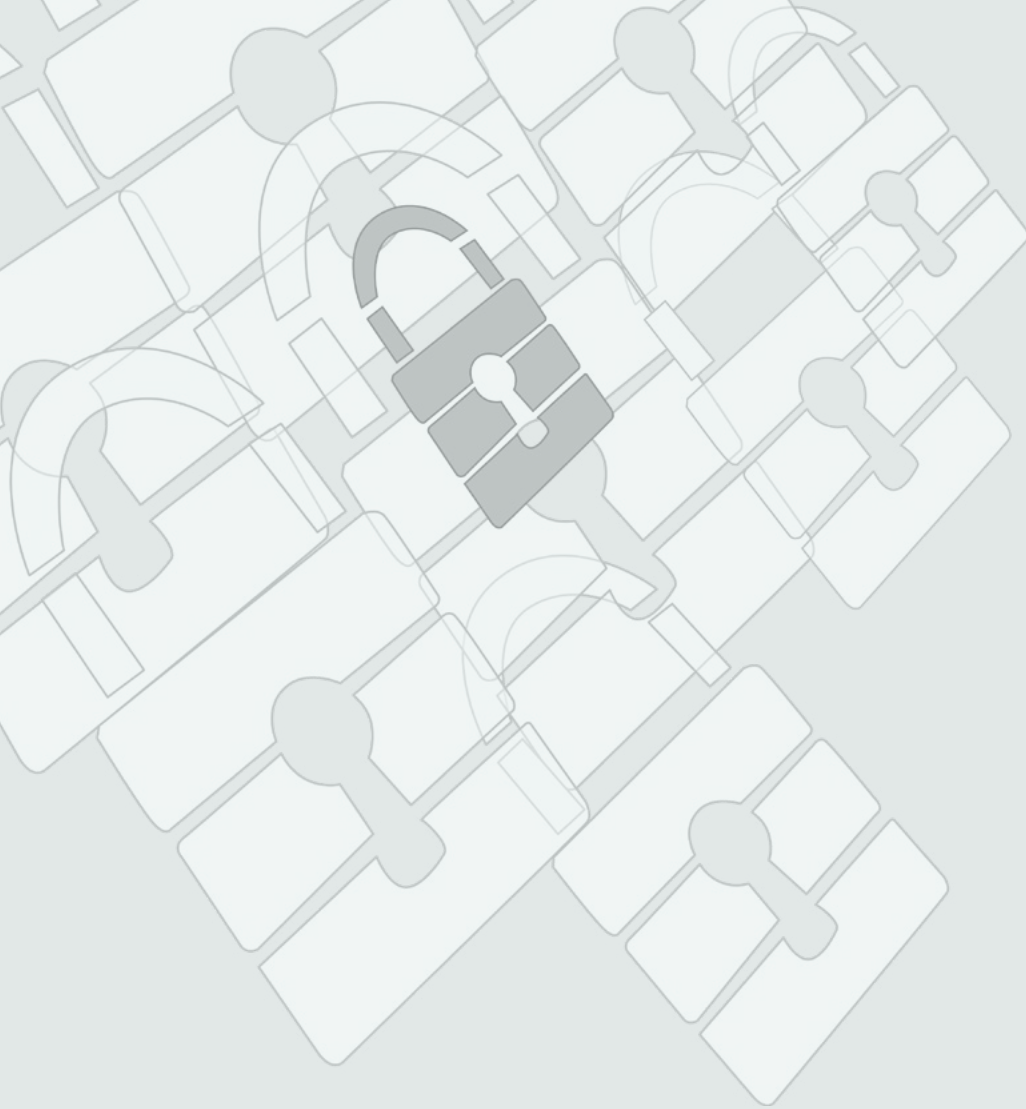
Lines of action and measures.....111

Line of action 1	112
Line of action 2	114
Line of action 3	116
Line of action 4	118
Line of action 5	120
Line of action 6	122
Line of action 7	124

Chapter 5

Cybersecurity in the National Security System129

The National Security Council.....	130
The Situation Committee.....	130
The National Cybersecurity Council	130
The Cybersecurity Standing Committee.....	131
National Cybersecurity Forum.....	131
Competent public authorities and the national reference CSIRT	132
Final considerations and evaluation.....	134



Executive Summary

Executive Summary

The National Cybersecurity Strategy works with forecasts from the 2017 National Security Strategy in the cybersecurity field, considering general goals, the field's specific goal and lines of action laid down to achieve them.

The document is divided into five chapters. The first, entitled “Cyberspace, beyond a common global space”, provides an overall understanding of the cybersecurity field, progress made in it since approving the Strategy in 2013, reasons behind drawing up the 2019 National Cybersecurity Strategy, plus the main features of its development.

Activities in cyberspace are fundamental for current society. Cyberspace technology and infrastructures are strategic elements, running across all fields of activity, making cyberspace vulnerability a major risk for our development as a nation.

For this reason, cyberspace security is a priority goal on government agendas to guarantee National Security and a State competence to create a trust-based digital society.

Helping promote secure and reliable cyberspace, from a multidisciplinary focus, moving beyond purely technical aspects, is a task that should stem from knowing about and understanding any threats we might face, including new and emerging threats.

The **second chapter**, entitled “Threats and challenges in cyberspace” determines the main threats to cyberspace stemming from its definition as a common global space, highly technified and widely connected, that amplifies the impact of any attack. It classifies these threats and challenges in two categories: on the one hand, threats to cyberspace assets; and on the other, threats that use cyberspace to carry out all types of malicious and illicit activities.

The **third chapter**, entitled “Proposal, principles and goals for cybersecurity” applies the governing principles of the 2017 National Security Strategy (Action unit, Anticipation, Efficiency and Resilience) to five specific goals. Its development is mentioned in the **fourth chapter**, entitled “Lines of action and measures”, setting seven lines of action and identifying measures to develop each one.

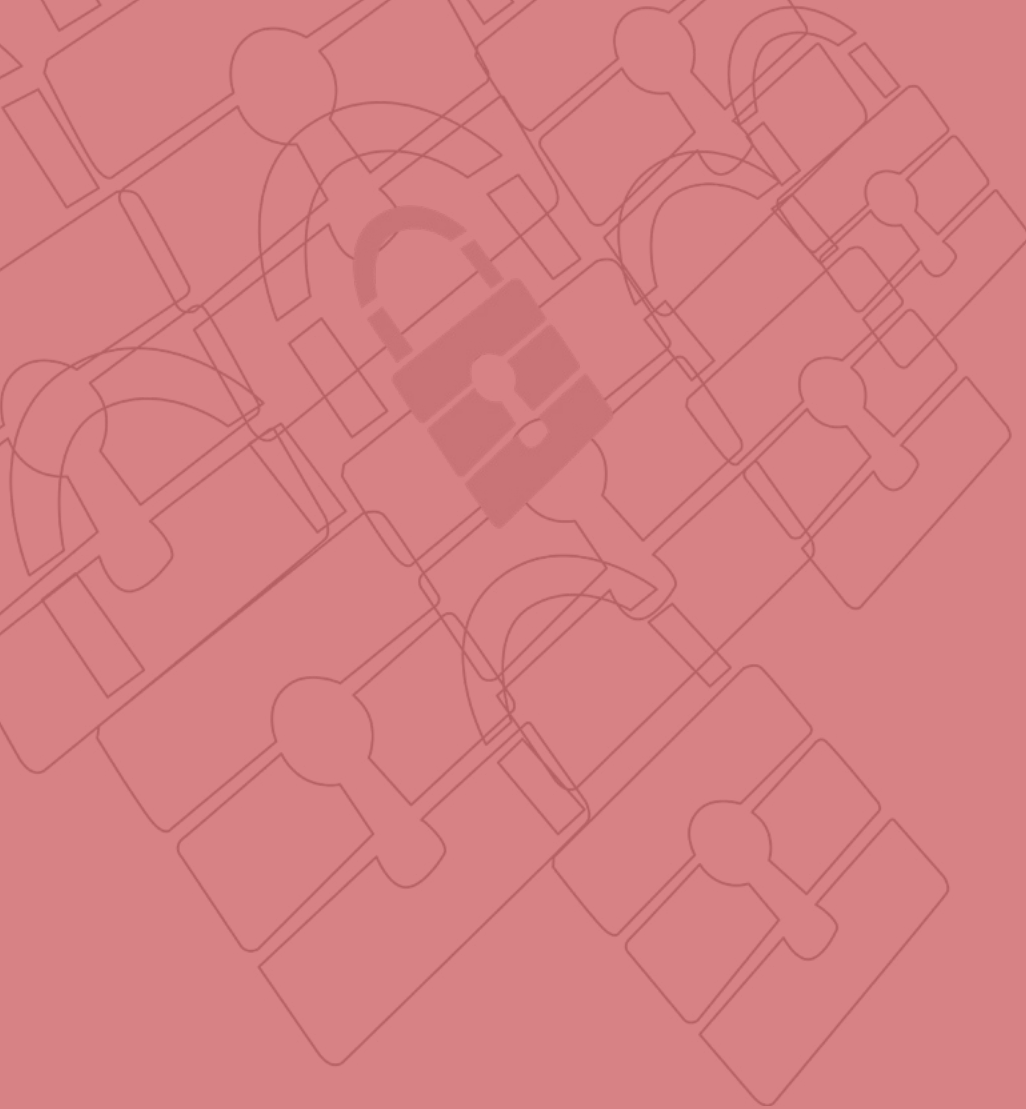
These lines of action aim to: strengthen skills to fight threats from cyberspace; guarantee strategic asset security and resilience for Spain; boost cybersecurity for citizens and companies; strengthen skills to investigate and prosecute cybercrimes, guarantee citizen security and protect rights and freedoms in cyberspace; boost cybersecurity for citizens and companies; bolster the Spanish cybersecurity industry and encourage and retain talent, strengthen digital autonomy; contribute to international cyberspace security, promoting open, plural, secure and reliable cyberspace supporting national interests and developing a cybersecurity culture to contribute to the Comprehensive National Security Culture Plan.

The **fifth chapter**, entitled “Cybersecurity in the National Security System” defines cybersecurity’s organic architecture. Led by Spain’s Prime Minister, the structure is divided into three authorities: the **National Security Council**, as the Government’s Delegate Commission for National Security; the **National Cybersecurity Council**, that supports the National Security Council and helps the Prime Minister manage and coordinate National Security policy on cybersecurity, and promotes coordination, collaboration and cooperation among Public Administrations and between these and

the private sector; and the **Specialised Situation Committee** that, with support from the National Security Department, will support crisis situation management in any field that, because it crosses disciplines or due to its sheer size, might overwhelm the response capabilities of the usual mechanisms.

This system is completed by the **Standing Committee on Cybersecurity**, that eases inter-ministerial coordination at an operational level in the field of cybersecurity, as the authority assisting the National Cybersecurity Council on aspects relating to technical and operational evaluation of risks and threats to cybersecurity; the competent public authorities and the national CSIRT (Computer Security Incident Response Team) and it includes setting up a new public-private joint-project, the **National Cybersecurity Forum**.

In addition, this last chapter makes some final conclusions and outlines mechanisms to update and assess the Strategy.



Introduction

Introduction

The 2019 National Cybersecurity Strategy establishes Spain's position in the light of a new understanding of cybersecurity within the framework of the National Security Policy.

Spain's first National Cybersecurity Strategy was approved in 2013. The document set directives and general lines of action to tackle the challenge that cyberspace vulnerability represented for the country. Furthermore, the strategy designed the governance model for national cybersecurity. In the intervening period, Spain has also continued moving forward in a bid to contribute to secure, reliable cyberspace.

One of its mainstays, dating back to 2014, is the National Cybersecurity Council, an authority supporting the National Security Council. Since its first meeting, the National Cybersecurity Council has assumed the task of coordinating nationally-competent organisations plus developing the National Cybersecurity Plan and its

offshoots. Consequently, Spain today can boast specialist cybersecurity organisations and an outstanding position not only in Europe but throughout the world.

The legal framework has also been considerably adapted. To keep on top of its evolution and use experience accumulated over these last few years, the National Security Framework modification was published in 2015 to guarantee security for Public Sector systems. On the other hand, bringing into force the Royal Decree-law 12/2018 of 7 September, on information network and system security, that transposes Directive (EU) 2016/1148 (known as the NIS Directive) to Spanish legal order, represented an important milestone in our country's cybersecurity improvements, extending the scope of this Directive in an attempt to improve cybersecurity among all strategic sectors.

Law 36/2015, of 28 September, on National Security was extended to boost a project representing one of the government's greatest responsibilities, National Security. The National Security Law considers cybersecurity as a special interest field.

Without the shadow of a doubt, cybersecurity has modernised National Security, as this field has made the greatest progress to date. This dynamic should stay on the same track.

The 2017 National Security Strategy was a turning point in national strategic thinking, giving cybersecurity its own differential space.

One of the global trends identified in the Strategy, digitalisation, is shown to drive change with implications for security. The Strategy sets a new framework, with five general goals running across all fields. Crisis management, National Security Culture, global common spaces, technological development and international projection for Spain shape a strategic grid where cybersecurity is used to open up new paths leading to Spain's present and future security model.

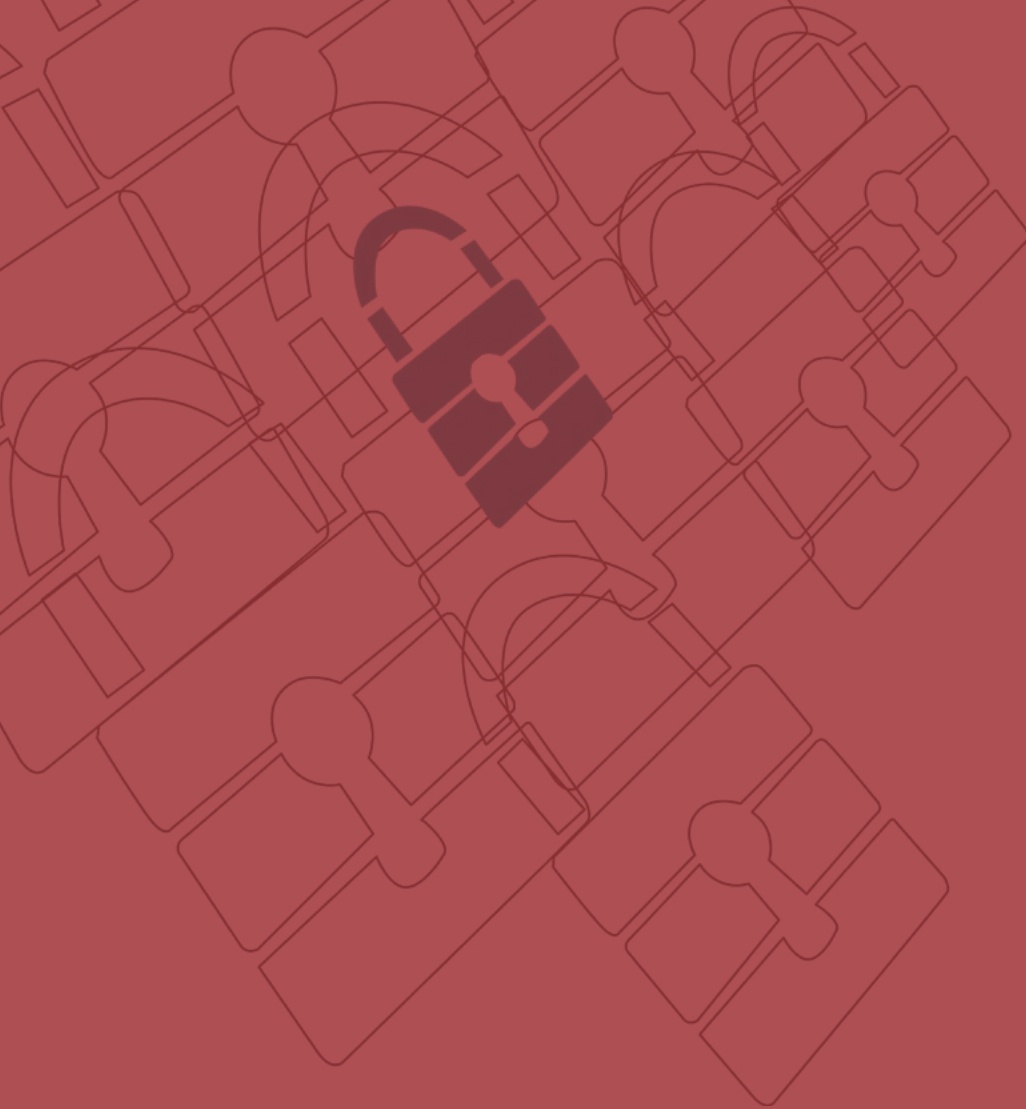


Spain can boast specialist cybersecurity organizations and an outstanding position not only in Europe but throughout the world.

New cybersecurity spreads beyond the mere sphere of protecting technological patrimony and delves into political, economic and social fields.

In addition to actions that affect digital systems, cyberspace should be considered as a strategic communication vector that can be used to influence public opinion and how people think by manipulating information, disinformation campaigns or hybrid actions. Its potential application in a very wide range of situations, including electoral processes, makes it extremely complex.

This renewed outlook in a field that is understood to have spread functionally, and where public-private collaboration is key, calls for a new approach in the form of a new national cybersecurity strategy.



Chapter 1


Cyberspace: beyond a global common space

Cyberspace: beyond a global common space

This chapter presents the opportunities and challenges of cyberspace and digital infrastructure, outlines the inherently international aspect of its security approach and describes the broad strokes of Spain's new understanding of cyberspace.

Cyberspace: opportunities and challenges

Cyberspace is a global common space characterised by its functionality and dynamism. Lack of sovereignty, its weak jurisdiction, ease of access and difficulty to attribute actions within it define a scenario with a wide range of future opportunities while also posing some serious

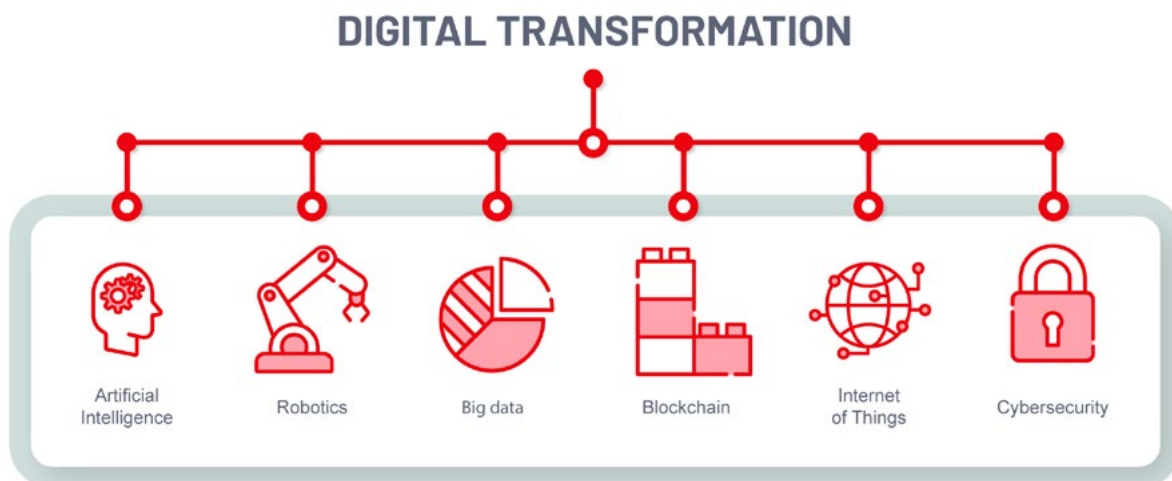


Cyberspace defines a scenario with a wide range of future opportunities while also posing some serious security challenges.

security challenges.

On the one hand, cyberspace makes universal connectivity possible and eases free flow of information, services and ideas. It is thereby a field that stimulates entrepreneurship, strengthens socio-economic progress and creates new opportunities every day in all business sectors. The change caused by digital transformation of production processes is demonstrated globally at an unprecedented rate. Artificial intelligence, robotics, big data, blockchain and the Internet of Things are already with us, although the real transforming power is still to be unleashed. Its implications go beyond technology, extending to new social models and delving into personal relations and ethics.

On the other hand, digitalisation transforms security and lays down some serious challenges. Cyberspace is structured as a battleground where information and data privacy are high-value assets in an environment with greater geopolitical competition, reorganisation of power and individual empowerment. Consequently, booming connectivity and greater dependence on networks and systems, not to mention digital components, objects and devices, create vulnerabilities and make it hard to protect information properly.



Digital infrastructure

Cyberspace is not only virtual, but also sustained by physical and logical elements. Devices, components and systems within information and communication networks and systems can be exposed to malfunctions that stop them working correctly and deliberate actions with malicious intentions that jeopardise correct operation of critical infrastructures and essential services that depend on the associated digital systems and networks.

This risk is amplified by the importance of commercial criteria over security criteria in hardware and software product design, not to mention systems and services, which complicate certification processes and might compromise the supply chain.

All these aspects, along with mounting interconnectivity between systems, can bring about cascade effects with unpredictable results.

International plan: security in cyberspace

Security in cyberspace has become a top priority on government agendas to guarantee national security and create a trust-based digital society. In this context, Spain defends its outlook and interests as a nation and works with the international community by backing open, plural and secure cyberspace.

Spain maintains its active role in all institutions where cybersecurity takes centre-stage, particularly within the European Union, the Atlantic Alliance and the United Nations, thereby proving its commitment to partners and allies. Ties are also maintained with third-party States through bilateral cooperation mechanisms that ease understanding and mutual trust based on fluid relationships in the field of cybersecurity, in an attempt to build on our skills.

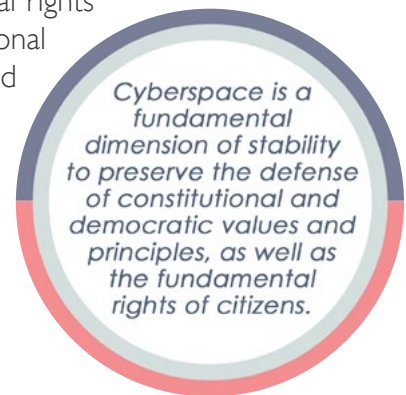


Aware of the importance of a multilateral approach, in addition to International Law and non-binding standards for responsible behaviour among States, we might highlight the role of the United Nations Charter as the reference principle for conflict prevention, cooperation and stability in cyberspace. Forging agreements and trust-building measures are the basis for its application and implementation, as well as International Treaties and Agreements that Spain has joined.

A new conception of cyberspace

A fundamental dimension of stability involves continued defence of constitutional and democratic values and principles plus citizens' fundamental rights in cyberspace, particularly in terms of protecting their personal data, privacy, freedom of expression and access to truthful, good quality information.

Good understanding of this approach requires a multidisciplinary focus, moving beyond purely technical aspects, using centralised management principles and coordinating its performance, assigning cybersecurity to National Security as a State competence.



Firstly, the private sector plays a relevant role as administrator and owner of Spain's digital assets, meaning that the country's cybersecurity skills largely lie in its companies. This thereby means that cybersecurity needs support, promotion and investment to become more competitive and boost economic growth, whilst providing a secure and reliable digital environment.

On the other hand, we should aspire to increasing technological autonomy by encouraging a national industrial base for cybersecurity, R+D+i and technological talent management. Human resources remain a critical factor. A gaping chasm has opened up between the number of highly specialised jobs in information technologies,

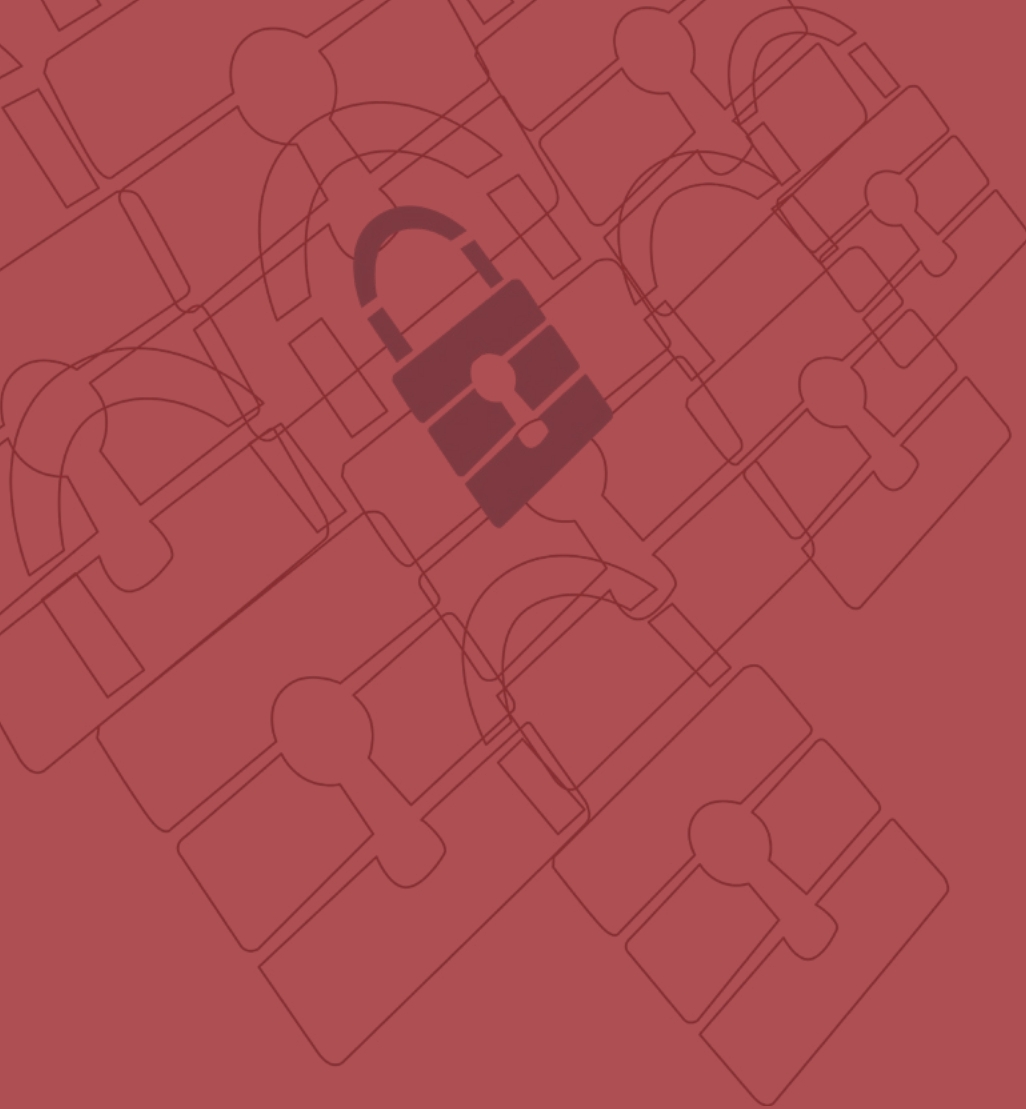
particularly cybersecurity, and availability of workers with the required level of knowledge or training.

Secondly, transition from a preventive and defensive cybersecurity model to a more dissuasive framework falls into line with a global context demonstrating greater geopolitical competence. Use of cyberspace as a field of confrontation, independently or as part of a hybrid action, is widely recognised. Dissuasion in cybersecurity requires obtaining and strengthening cyberdefence skills, as a fundamental element of the State's action.

Thirdly, fast evolving cyberthreats require a more proactive approach from cyberintelligence. Its integration in the overall cybersecurity framework is key to provide knowledge of the situation and the necessary early warning that can anticipate actions from potential opponents through knowledge of their skills, techniques, tactics and intentions. In addition, it is necessary to encourage the use of mechanisms and means that allow appropriate investigation and prosecution of perpetrators to increase possibilities of attribution.

All the above can be added to the need for greater implication from all society by encouraging a cybersecurity culture, to evolve from awareness of the commitment, in the understanding that citizens have joint-responsibility for national cybersecurity.





Chapter 2

Threats and challenges in cyberspace

Threats and challenges in cyberspace

This chapter examines the main threats and challenges that Spain faces in cyberspace.

Promoting a secure, reliable environment is a task that should work from knowledge and understanding of the challenges and threats, including new and emerging aspects, that affect cyberspace. The 2017 National Security Strategy differentiates between cyberthreats and actions that use cyberspace as a medium for malicious or illicit activities.

Cyberthreats

Cyberthreats are malicious disruptions or manipulations that affect technological elements. They encompass a wide range of actions. Cyberthreats are characterised by their diversity in terms of both capacity and motivation. They affect practically all fields of National Security, such as National Defence, economic

security or protection of critical infrastructures, among others, and they do not respect borders.

This transverse nature means that cybersecurity covers a comprehensive perspective that includes Public Administrations, the public and private sector and society as a whole, so there might be simultaneous implications on a wide range of aspects such as sovereignty, fundamental rights, defence, the economy and technological development.



In this scenario, defences can evolve continually to adapt to a dominating threat that is multiplied by the pull effect caused by its high degree of impunity. At the same time, the defence ground is expanding and becoming more complicated every day.

In this respect, providing security in information networks and systems requires improving prevention, detection and response measures, encouraging security through design and by default. It should be incorporated both into developing technological products and services and their updates or how they are used.

Actions that use cyberspace for malicious purposes

Digital technologies open up new activities and ways of doing business that have to be duly regulated as they might affect stability and our rights and freedoms, presenting substantial threats and challenges for National Security. In the same way, the same qualities that help cyberspace drive progress can be exploited for harmful purposes when combined with how exceptionally easy it is to remain anonymous, steal identities and amplify effects.



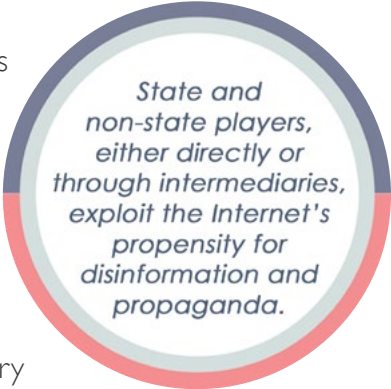
Thanks to the Internet revolution, States, organised groups, collectives and even isolated individuals can attain a so-far unprecedented level of power and capability to influence. Digital connectivity means that

global social movements take on strategic importance that has been underestimated until now.

The actions that cyberspace uses to carry out malicious or illicit activities include cyberespionage and cybercrime.

Cyberespionage is a relatively cheap, fast method with fewer risks than traditional espionage, given the difficulty of attributing authorship. The greatest capabilities are mainly held by State players (intelligence or military organisations), that fundamentally operate via what are known as Advanced Persistent Threats (APT). This type of threat means that the opponent has sophisticated knowledge levels plus resources and infrastructures so that, by deploying multiple types of attacks, they can interact on their targets over a long period of time, adapt to defence strategies, and maintain the interaction level to meet its end.

In addition, a growing trend is now seen in what are known as hybrid threats, coordinated and synchronised actions aiming to deliberately attack systemic vulnerabilities in democratic states and institutions, through a wide range of media, such as traditional military actions, cyberattacks, information manipulation operations or elements of economic pressure. State and non-state players, either directly or through intermediaries, exploit the Internet's propensity for disinformation and propaganda and a generalised interest in obtaining and developing military capabilities to operate in cyberspace, including offensive capacities in many cases.

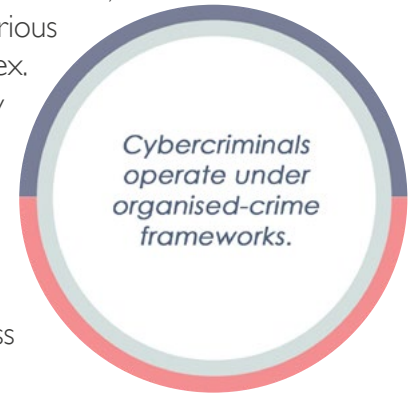


State and non-state players, either directly or through intermediaries, exploit the Internet's propensity for disinformation and propaganda.

Cybercrime, in turn, is a top-level citizen security issue, representing one of the widest-spread and generalised threats, continuously arising and increasingly victimising thousands of institutions, companies and citizens. The term Cybercrime refers to illicit activities in cyberspace, targeting elements, computer systems or any other legal property, whenever its planning, development and performance is determined by use of technological tools; depending on the nature of the actual punishable act, authorship,

motivation, or damage inflicted, this might refer to cyberterrorism, cybercrimes or, when appropriate, hacktivism.

Use of new financial and economic transaction methods, such as cryptocurrency, for illicit trafficking and trading of goods and providing services or extortion, fraud and forgery of non-monetary means of payment, poses a serious security challenge because they are both sophisticated and complex. They can be used for money laundering and tax evasion and they represent a source of income for organised crime; therefore, they facilitate other activities such as financing terrorism, making the most of how difficult it is to monitor these new techniques.

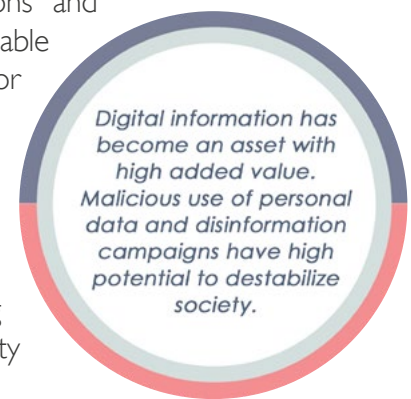


Cybercriminals operate under organised-crime frameworks and incessantly explore techniques for building low-risk lucrative business models, sheltered by the fact their actions are difficult to trace.

Terrorist groups attempt to make the most of cyberspace vulnerabilities to launch cyberattacks or activities to radicalise individuals and collectives, for financing, disseminating techniques and tools to commit a terrorist attack, and for recruitment, training or propaganda. Intimately linked to this, there is the threat against critical infrastructures, with the clear chance of using networks to bring about a collapse as essential services fall like dominoes.

Hacktivist groups carry out cyberattacks for ideological reasons and sometimes, making the most of products, services and tools available in cyberspace, they seek to develop attacks with a major media or social impact.

Nor can we ignore threats from the continuous surge of organisations contracting cybercriminal services to damage their competitors and their in-house technological and human resources that might be detrimental for the organisation, without forgetting all emerging threats and actions resulting from lack of cybersecurity culture.



On the other hand, digital information has become an asset with high added value. Analysis of personal data on the Net is used for a wide range of purposes from sociological studies to advertising campaigns. Malicious use of personal data and disinformation campaigns have high potential to destabilise society. Furthermore, exploiting personal data breaches represents infringement of this data's security, affecting people's privacy and their data's integrity and confidentiality.

As far as disinformation campaigns are concerned, they use elements such as fake news to influence public opinion. Internet and social media amplify the effect and scope of the information being sent out, with potential application against targets such as international organisations, States, political initiatives or public personalities or even democratic electoral processes.

CYBERTHREATS AND ACTIONS THAT USE CYBERSPACE FOR MALICIOUS PURPOSES

Disruptions or malicious manipulations that affect technological elements.
Actions that use cyberspace as a means to perform malicious or illicit activities.



CYBERESPIONAGE

Advanced
Persistent
Threats



HYBRID THREATS

Military Actions
Cyberattacks
Information manipulation
operations



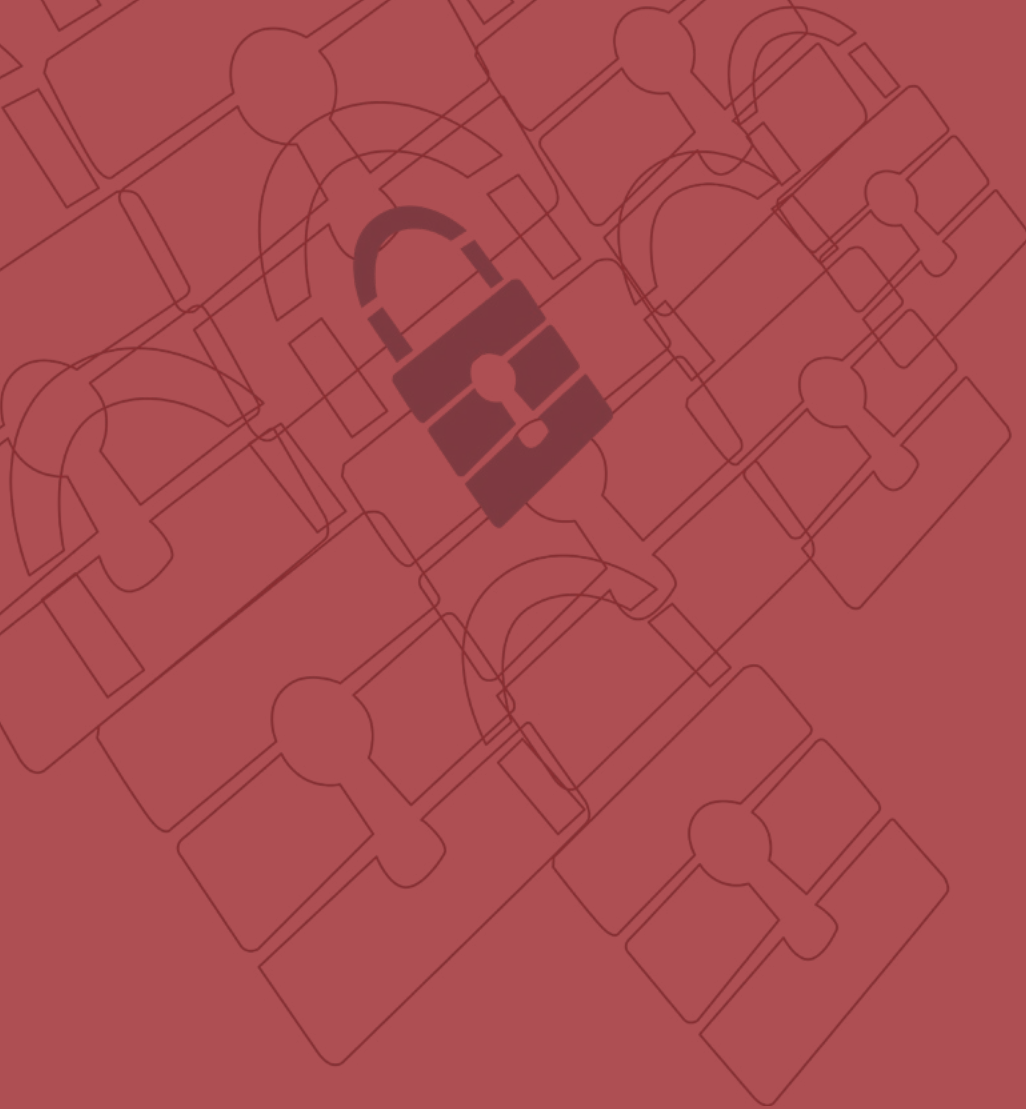
CYBERCRIME

Cyberterrorism
Cybercrimes



HACKTIVISM

Cyberattacks



Chapter 3

Proposal, principles and
goals for cybersecurity

Proposal, principles and goals for cybersecurity

This chapter outlines the proposal and principles governing the Strategy, plus one general and five specific goals.

Proposal

As the 2017 National Security Strategy established, Spain must guarantee secure, responsible use of information and communications networks and systems by strengthening capabilities for prevention, detection and response to cyber-attacks, developing and adopting specific measures to promote secure and reliable cyberspace

Therefore, the 2019 National Cybersecurity Strategy proposes to outline general directives for the cybersecurity field so as to meet 2017 National Security Strategy goals.

To do this, Spain must continue **strengthening skills** to tackle cyberthreats and malicious use of cyberspace. Consequently, measures will be sought that help guarantee our nation's

security, paying particular attention to the public sector and essential services, in a more coordinated framework featuring improved cooperation structures.

On the other hand, promoting **cybersecurity culture** should be one of the central themes being developed to make society aware of these threats and challenges. The right to secure, reliable use of cyberspace and contributing to this situation are shared responsibilities.

In addition, cybersecurity means progress, so singular **support and encouragement are required for the Spanish cybersecurity industry**, promoting an environment that nurtures research, development and innovation, plus participation from the academic world. On the other hand, our society prioritises attaining and maintaining **knowledge, skills**, experience and technological and professional capabilities because they are essential to tackle major cybersecurity challenges.

Cyberspace's transverse and global nature also demands cooperation and compliance from International Law, as well as utmost respect for the principles of the Constitution and the United Nations Charter; in coherence with the National Security Strategy and initiatives developed within European, regional and international frameworks, where national interests prevail at all times.



Governing Principles

The National Cybersecurity Strategy is upheld and inspired by the governing principles of National Security: action unit, anticipation, efficiency and resilience.

1. **Action Unit:** Any response to an incident in the cybersecurity field that might implicate different State agents will be strengthened if it is coherent, coordinated and resolved quickly and effectively. These qualities can be attained through careful preparation and appropriate organisation of the State's action unit.

Centralised management of cyberspace-related crises helps maintain full understanding of the threat situation and frees up available resources more quickly, efficiently, coherently and completely.


- 2. Anticipation:** The specific nature of cyberspace and the players involved requires anticipation mechanisms in specialised organisations to guide State Action in crisis situations, where the private sector should also get involved.

Anticipation prioritises preventive actions over reactions. Effective systems, with shared information as close as possible to real time, grant appropriate knowledge of the situation. This factor is essential to minimise response times which can be critical to reduce the effects of threats

- 3. Efficiency:** Cybersecurity requires the use of high-value, multi-offer systems featuring a high level of technology, that are associated with very demanding needs and high costs derived from their development, purchase and operation, plus the need for advance planning and the high complexity of sustaining it.

Furthermore, current and future scenarios are affected by economic austerity that, along with social responsibility to squeeze maximum performance from available resources, means that Spain should focus on optimisation and efficiency of resources devoted to cybersecurity, increasing the importance of the action unit, sharing information and integrating these resources for maximum efficiency.

- 4. Resilience:** Resilience is a fundamental feature for systems and critical infrastructures. The State must ensure availability of elements considered to be essential for the nation, improving their protection against cyberthreats. A special mention should be given to the reinforcement required for information and communication networks against cyberthreat activities or illicit use of cyberspace.



Current scenario is affected by economic austerity that, along with social responsibility to squeeze maximum performance from available resources, means that Spain should focus on optimization and efficiency of resources.

GOVERNING PRINCIPLES



Action Unit

Any response to an incident in the cybersecurity field that might implicate different State agents will be strengthened if it is coherent, coordinated and resolved quickly and effectively. These qualities can be attained through careful preparation and appropriate organization of the State's action unit.



Resilience

Resilience is a fundamental feature for systems and critical infrastructures. The State must ensure availability of elements considered to be essential for the nation, improving their protection against cyberthreats.



Anticipation

The specific nature of cyberspace and the players involved requires anticipation mechanisms in specialised organisations to guide State Action in crisis situations.

01

02

03

04



Efficiency

Cybersecurity requires the use of high-value, multi-offer systems featuring a high level of technology, that are associated with very demanding needs and high costs derived from their development, purchase and operation.

General Goal

New cybersecurity challenges have meant adapting the general goal to become more integrating, inclusive and less technified.

In line with the 2017 National Security Strategy and broadening the cybersecurity goal mentioned in it, Spain will guarantee secure, reliable use of cyberspace, protecting citizens' rights and freedoms and promoting socio-economic progress.

Based on this general goal, a series of specific goals are explained below to guide the State's action in this field.

Goal I

Security and resilience of information and communication networks and systems for the public sector and essential services.

A coherent, integrated national framework should be consolidated to help guarantee protection of information handled by the public sector and essential services, their systems and services, as well as the networks that support them. This framework will make it possible to develop and implant increasingly secure and efficient services.

To do so, security measures should be implemented, focussing on improving capabilities for prevention, detection and response to incidents, developing new solutions, reinforcing coordination and adapting the legal system accordingly.

Actions against cyberespionage particularly deserve a special mention as this ensures protection of Spain's Technological Patrimony, understood as the material or immaterial

assets that uphold the current business sector's intellectual and industrial property and condition future development.

The public sector and essential service operators should get actively involved in a continuous improvement process to protect their Information and Communication Technology systems based on constantly monitoring their threat exposure. These agents should act as a model for **cybersecurity management best practices**.

Applying the principle of shared responsibility, the public sector should work closely with companies that manage the relevant Information and Communication Technology Systems for national interests, exchanging knowledge that encourages appropriate coordination between the two and effective cooperation within the cybersecurity environment.

Strengthening cybersecurity requires systematic knowledge of the impact of potential interruption or destruction of the networks and systems that provide essential services, as well as security level metrics for these systems that help make the right decisions according to exposure levels.



Goal II

Secure and reliable use of cyberspace to ward off illicit or malicious use.

Cyberspace plays an increasingly important role in committing illicit or malicious acts and investigating them to encourage citizen trust. It is necessary to guarantee suitable prosecution of criminal phenomena that are taking place in it.

Fighting cybercrime can be divided into three fields: (i) cyberspace as the direct target of criminal acts, or the threat; (ii) cyberspace as the key medium for committing the crime; and (iii) cyberspace as the medium or direct investigation target for any type of illicit behaviour.

Based on solid and effective regulation that reinforces and guarantees fighting cybercrime, it is necessary to strengthen legal and police cooperation, both nationally and internationally, and assign sufficient resources to competent bodies on this matter and skills training for professionals working in this area.

In the same way, citizen collaboration and participation must be encouraged, facilitating procedures to access and transmit information that might be of legal or police interest and identifying aspects that require improving capabilities among police institutions and competent legal organisations



It is necessary to strengthen legal and police cooperation, both nationally and internationally, assigning sufficient resources, and encouraging citizen collaboration and participation.

Protecting the business and social ecosystem and citizens.

All persons and organisations have the right to use cyberspace securely. It is therefore the State's responsibility to promote and encourage measures to attain and maintain sufficient cybersecurity, particularly protecting the most vulnerable sectors of society and allowing proper socio-economic development for Spain.

Cybersecurity is a responsibility shared with private players that can affect them by action or omission; cybersecurity is not possible without their participation. Therefore, measures to be promoted should encourage cooperation to ensure common security.

Defending citizens, self-employed people and companies should reach beyond self-protection measures, so it is advisable to implement measures for their active cyberdefence. At the same time, all cyberspace users should demonstrate responsible use of the technology available to them.

Society's accelerated enthusiasm for emerging technologies makes risks evolve. Consequently, constant knowledge exchange with all players and monitoring mechanisms to protect the business and social ecosystem will be instruments to keep the Government informed and help it make the right decisions to update and adapt the actions taken as a result of this strategy.



Goal IV


Culture and commitment to cybersecurity and strengthening human and technological skills.

To tackle cybersecurity challenges, Spain should have technical and human resources to give it the necessary technological autonomy and appropriate skills training for secure use of cyberspace, making cybersecurity the key enabler for an entrepreneurial nation.

To do this, it must improve collective cybersecurity, diffusing cybersecurity culture with the help of public and private organisations and the media, strengthening information mechanisms and help for citizens and promoting spaces for encounters between civil society, administrations and companies.

It should also contribute to secure and responsible use of Information and Communication Technologies by promoting appropriate skills training on cybersecurity for professionals according to job market demands, stimulating professionals' development with their own skills, boosting specialised training and qualification, plus skills to generate knowledge, **develop R+D+i activities in cybersecurity and encourage use of certified products and services.**

In addition, special attention should be paid to protecting technological patrimony and industrial and intellectual property. To promote technological sovereignty and make the most of digital transformation opportunities, the Spanish cybersecurity industry should be encouraged and boosted hand-in-hand with good practice on development and implementation of information and communication systems.



Cybersecurity culture must improve to get human and technical resources that allow technological sovereignty.

International cyberspace security.

Spain will promote open, plural, secure and trustworthy cyberspace both in its bilateral relations and in multilateral, regional and international organisations, and in forums and conferences, where cyberspace plays a leading role.

It will advocate setting up an international framework for conflict prevention, cooperation and stability in cyberspace, applying principles from the whole United Nations Charter, International Law, Human Rights and Humanitarian Rights in War, as well as non-binding standards on responsible behaviour for States.

Aware of the importance of multilateralism, the United Nations' role is considered relevant to move forward building consensus that, along with adopting and setting in motion measures to promote trust, collaboration and participation from all players involved (States, private sector, civil society, users and academia), constitutes the groundwork to achieve security and stability in cyberspace and work towards regulation.

In line with our European partners, this goal will strengthen trust in the internet, digital transformation and development of new technologies, helping to consolidate a secure European cybernetic ecosystem that boosts progress towards the single digital market. To do this, it will defend an interoperative, neutral, open and diverse internet, a reflection of international cultural and linguistic plurality, based on a system of democratic, representative and inclusive governance resulting from agreement and consensus. In addition, it will provide access to global and generalised internet, thereby helping meet Sustainable Development Goals.

In this way, belonging to the European Union (EU) means that we have to strengthen security and European strategic autonomy by seeking synergy, technical, operative, strategic and political cooperation; to strengthen our resilience, our capacity to respond

to a crisis and the complementary nature of civil and military fields as EU partners and allies of the North Atlantic Treaty Organisation (NATO).

Based on the above, Spain will continue to take an active role in the EU and NATO; in the United Nations and in its offshoot forums such as the Internet Governance Forum (IGF); the Organisation for Security and Cooperation in Europe (OSCE), development and implementation of Confidence-Building Measures; the Organisation of American States (OAS). As well as the Global Forum on Cyber Expertise (GFCE) and the Freedom Online Coalition FOC, without forgetting our presence in the European Centre of Excellence to counter-attack Hybrid Threats (Hybrid CoE) plus the NATO Cooperative Cyberdefence Centre of Excellence (CCD CoE).

In addition, it will reinforce international bilateral cooperation on cybersecurity, promote fluid and trustworthy relations in this field, work jointly on building skills in third-party countries, paying particular attention to women and young people and promoting setting up information channels and experience exchange, boosting bilateral and multilateral agreements in this field.



STRATEGY GOALS

GENERAL GOAL

In line with the 2017 National Security Strategy and broadening the cybersecurity goal mentioned in it, Spain will guarantee secure, reliable use of cyberspace, protecting citizens' rights and freedoms and promoting socio-economic progress.



Goal

01

Security and resilience of information and communication networks and systems for the public sector and essential services.



Goal

02

Secure and reliable use of cyberspace to ward off illicit or malicious use.



Goal

03

Protecting the business and social ecosystem and citizens.



Goal

04

Culture and commitment to cybersecurity and strengthening human and technological skills.

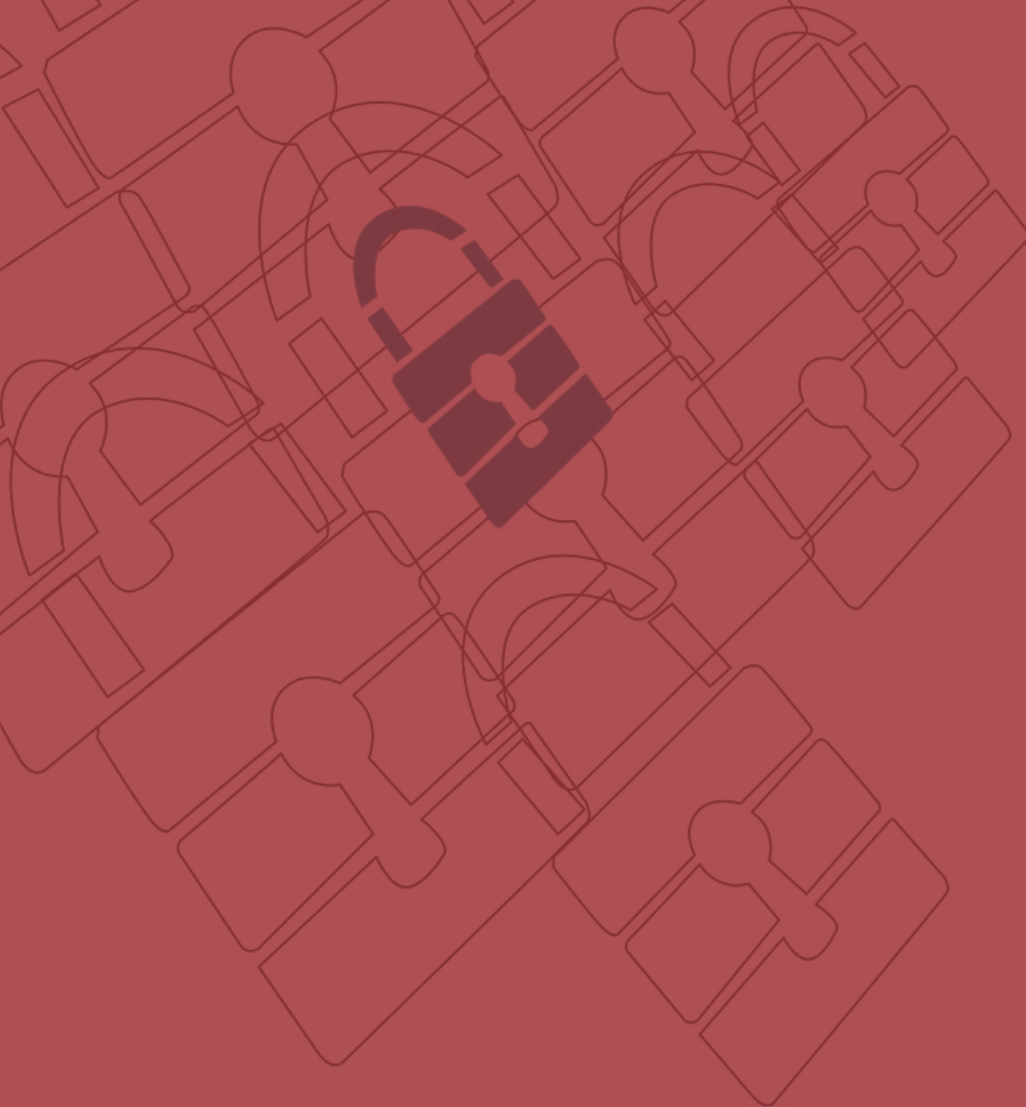


Goal

05

International cyberspace security.





Chapter 4

Lines of action and measures

Lines of action and measures

This chapter sets the lines of action to achieve the goals.

LINE OF ACTION I

Strengthen capabilities to deal with threats from cyberspace.

This line of action meets Goal I in the Strategy.

MEASURES

1. Extend and improve cyberthreat detection and analysis skills to be able to identify attack procedures and origins; also draw up the necessary intelligence for more effective protection, attribution and defence.
2. Encourage centres of excellence and research facilities to work together to tackle cyberthreats.
3. Strengthen creation, dissemination and application of best practices and standards for cybersecurity.
4. Ensure technical and operational coordination of organisations with cybersecurity responsibilities, companies and society.
5. Develop and update standards, procedures and instructions to respond to cybersecurity incidents, ensuring inclusion in the National Security System.
6. Strengthen cyberdefence and cyberintelligence capabilities.

7. Promote participation from companies on sector-based platforms for information exchange and analysis, and to measure sector-based risk, and suggest actions to mitigate this, alongside the legal requirements that regulate them.
8. Strengthen and support developments in the Spanish CSIRT network.
9. Boost development for notification platforms, exchange of information and coordination to improve sector-based cybersecurity.
10. Develop instruments for prevention, detection, response, return to normality and assessment focussed on crisis management for the cybersecurity field within the framework of National Security.
11. Guarantee coordination, cooperation and exchange of information on cyberincidents and intelligence on cyberthreats between the public sector, private sector and competent international organisations, encouraging prevention and early warnings.
12. Implanting active cyberdefence measures in the public sector to improve response capabilities.

LINE OF ACTION 2

Guarantee security and resilience for Spain's strategic assets.

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

MEASURES

1. Broaden and strengthen capabilities for prevention, detection, response, recovery and resilience against cyberattacks aimed at the public sector, essential services and strategic companies.
2. Strengthen development of the critical infrastructure protection standard, reinforcing security for information networks and systems that support them.
3. Ensure full implementation of the National Security Framework, the Critical Infrastructure Protection System and compliance and harmonisation of the critical infrastructure protection standard and essential services with a risk-based priority focus.
4. Within their competences, strengthen progressive implication and creation of cybersecurity infrastructures in Autonomous Regions, Autonomous Cities, Local Entities and in their affiliated or dependent organisations that will cooperate and be coordinated with national structures to improve national cybersecurity.
5. Develop the Spanish Central Administration Cybersecurity Operations Centre that improves prevention, detection and response skills and boosts regional and local development of cybersecurity operations centres.

6. Strengthen the implementation of telecommunications infrastructures and services and common horizontal information systems, also shared by Public Administrations, bolstering use and their security and resilience skills, whilst ensuring coordination with the former when common infrastructures and services are not used.
7. Boost development of a metrics system for major cybersecurity variables that allows competent authorities to determine security levels and how they might evolve.
8. Commit the public and private sector to supply chain risk management, particularly when affecting essential service provision.
9. Develop catalogues of qualified, certified products and services, for use in public sector contracting processes and essential services.
10. Reinforce security structures and surveillance capacity for information systems that handle classified information.
11. Promote cyberexercises and cybersecurity assessments, particularly in areas that affect National Security, Public Administration, essential services and sought-after companies.
12. Ensure protection of Singular Scientific-Technical Infrastructures and R+D+i reference centres.

LINE OF ACTION 3

Reinforce capabilities for investigation and prosecution of cybercrime, to guarantee citizen security and protect rights and freedoms in cyberspace.

This line of action meets Goal II in the Strategy.

MEASURES

1. Reinforce the legal framework for an effective response to cybercrime, relating to both defining types of crime and regulating the right investigation measures.
2. Promote citizen collaboration and participation, articulating instruments to exchange and transmit information that might interest the police and promoting cybercrime prevention campaigns aimed at citizens and businesses.
3. Reinforce actions to strengthen investigation, attribution and prosecution skills and, when appropriate, criminal action, against cybercrime.
4. Promote transfer of the criminal jurisdiction of information relating to criminal security incidents to competent organisations, particularly any that affect or might affect essential service provision and critical infrastructures.
5. Obtain access to information and material resources for legal operators that ensure better application of the legal and technical framework for fighting

cybercrime, giving them greater skills to investigate and judge the corresponding illicit acts.

6. Promote exchange of information, experience and knowledge among personnel with responsibilities cybercrime investigation and prosecution.
7. Ensure legal professionals and State Security Forces access to human and material resources, giving them the necessary knowledge to best apply the associated legal and technical framework.
8. Boost investigation coordination on cybercrime and other illicit uses of cyberspace among the different bodies and units with competence in this field.
9. Strengthen international legal and police cooperation.

LINE OF ACTION 4

Boost cybersecurity for citizens and companies.

This line of action meets Goal III in the Strategy.

MEASURES

1. Offer citizens and the private sector an integrated public cybersecurity service, which is good quality and easy to access, and that stimulates demand for cybersecurity business sector services.
2. Boost cybersecurity in SMEs, microSMEs and among self-employed workers by articulating public policies on cybersecurity, particularly developing resilience.
3. Promote cybersecurity to guarantee privacy and protection for personal data within the framework of citizen's digital rights in accordance with the legal system, promoting "digital identity" protection.
4. Create agile, secure complaint mechanisms for the private sector and citizens.
5. Stimulate cooperation between public and private players, particularly promoting commitment from Internet Service and Digital Service Providers to improve cybersecurity. National regulation will be boosted in this respect and measures will be implemented for active cyberdefence of citizens and SMEs.

6. Develop mechanisms to measure accumulated risk and how it changes, both for citizens and companies, to prioritise cybersecurity measures and keep society appropriately informed.
7. In the business sector, boost implementation of recognised cybersecurity standards. Working with national and international standardisation entities, stimulate creation, diffusion and application of sector-based cybersecurity best practices, including different certification frameworks.
8. Boost implementation of reliable electronic identification systems and trusted electronic services.
9. Promote setting up the National Cybersecurity Forum that incorporates representatives from civil society, independent experts, private sector, academia, associations, non-profit-making organisations, among others, to strengthen and set up public-private synergies, particularly generating knowledge on security opportunities and threats in cyberspace.

LINE OF ACTION 5

Strengthen the Spanish cybersecurity industry and its capacity to nurture and retain talent, to bolster digital autonomy.

This line of action meets Goal IV in the Strategy.

MEASURES

1. Boost R+D+i support programmes in digital security and cybersecurity in SMEs, businesses, universities and research centres, facilitating access to national and international incentive programmes and through innovative public purchasing programmes.
2. Revitalise the industrial and cybersecurity services sector, providing incentives for measures supporting innovation, investment, internationalisation and technology transfer, particularly in the case of microSMEs and SMEs.
3. Increase national activities to develop cybersecurity products, services and systems, and security right from design, specifically supporting any that uphold national interest needs to strengthen digital autonomy, and intellectual and industrial property.
4. Promote standardisation activities and cybersecurity requirements in the Information and Communication Technologies products and services, facilitate access to products and services that meet these requirements, promoting

compliance assessment and certification, and providing support for drawing up catalogues.

5. Update or, when appropriate, develop competence frameworks in cybersecurity that meet the job market's needs.
6. Identify needs for professional skills in cybersecurity, promoting collaboration between educational and training institutions by boosting continuous training, employment training and university education, promoting professional credential and certification systems.
7. Include professional cybersecurity profiles in public sector job descriptions.
8. Detect, encourage and retain talent in cybersecurity paying particular attention to the research field.
9. Boost specific R+D+i programmes in cybersecurity and cyberdefence.

LINE OF ACTION 6

Contribute to cyberspace security internationally, promoting open, plural, secure and trustworthy cyberspace, supporting national interests.

This line of action meets Goal V in the Strategy.

MEASURES

1. Strengthen and reinforce Spain's presence in the organisations, conferences and regional and international forums to which it belongs and where cybersecurity is a substantial part of its mandate, and support and participate actively in different initiatives, coordinating the position of the different national agents involved.
2. In the sphere of the United Nations, promote the search for consensus to fully abide by the United Nations Charter and application and implementation of International Law and States' rules for responsible behaviour. Likewise, move forward in adopting and implementing Confidence-Building Measures in cyberspace.
3. Take an active part in the European Union in terms of developing a secure European ecosystem that encourages progress and consolidation of the single market, and Europe's security and strategic autonomy, seeking complementary aspects and cooperation between the European Union and NATO.

4. Promote bilateral dialogue, cooperation and information and experience-exchange systems, and early warning devices to develop a coordinated focus on fighting cyberthreats with other countries, promoting negotiation and signing international agreements.
5. Promote development of technological skills and internet access in third-party countries to thereby aid compliance with Sustainable Development Goals.
6. Work with surrounding countries to develop greater awareness on Hybrid Threats, limiting impact on our countries' sovereignty and integrity.

LINE OF ACTION 7

Develop a cybersecurity culture.

The measures included in this Line of Action will contribute to the National Security Culture Plan and meet goal IV of the Strategy.

MEASURES

1. Increase awareness-raising campaigns for citizens and companies and provide them with useful information that is suitable for each profile, particularly in the field of self-employed workers and small and medium-sized companies.
2. Strengthen actions that bring about an surge in joint-responsibility and obligations from society regarding national cybersecurity.
3. Boost initiatives and plans for digital literacy in cybersecurity.
4. Promote the spread of cybersecurity culture as a best business practice and acknowledge companies' implication in improving collective cybersecurity as corporate social responsibility.
5. Promote a critical spirit in favour of truthful, high quality information that helps pinpoint fake news and disinformation.

6. Raise awareness among organisations' executives so that they can free up the necessary resources and promote cybersecurity projects as required by their entities.
7. Promote awareness-raising and training on cybersecurity in schools, adapted to all training levels and specialities.
8. Seek and recognise media collaboration and participation, to give citizen campaigns further reach, particularly among young people.

LINES OF ACTION

Goal I

Strengthen capabilities to deal with threats from cyberspace.

Guarantee security and resilience for Spain's strategic assets.

LINE OF ACTION I - II

Goal II

Reinforce capabilities for investigation and prosecution of cybercrime, to guarantee citizen security and protect rights and freedoms in cyberspace.

LINE OF ACTION III

Goal III

Boost cybersecurity for citizens and companies..

LINE OF ACTION IV

Goal IV

Strengthen the Spanish cybersecurity industry and its capacity to nurture and retain talent, to bolster digital autonomy.

LINE OF ACTION V

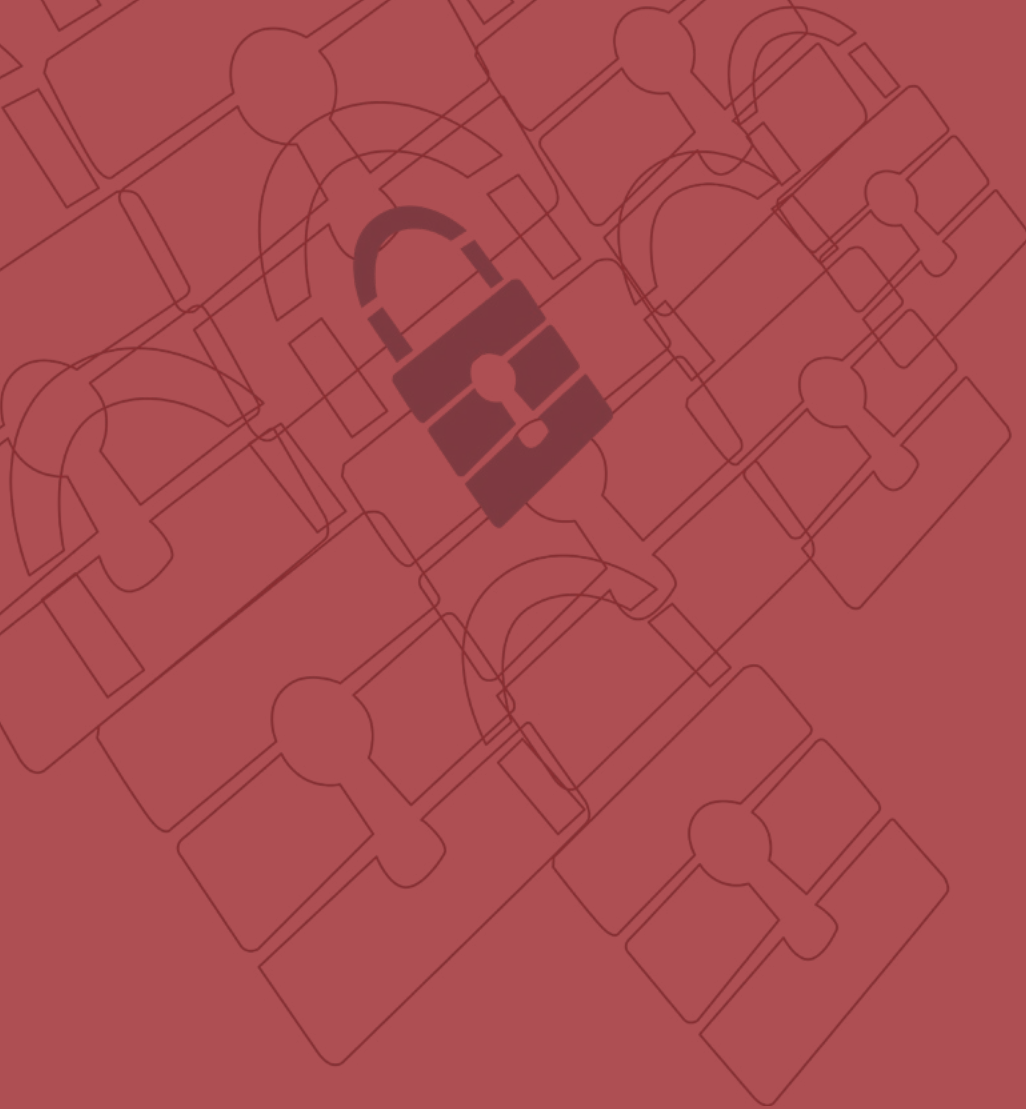
Develop a cybersecurity culture.

LINE OF ACTION VII

Goal V

Contribute to cyberspace security internationally, promoting open, plural, secure and trustworthy cyberspace, supporting national interests.

LINE OF ACTION VI



Chapter 5

Cybersecurity in the National Security System

Cybersecurity in the National Security System

This chapter considers how cybersecurity is incorporated into the current National Security System.

The 2013 National Cybersecurity Strategy and subsequent approval of the National Security Law in 2015, created a specific organic structure for cybersecurity. This 2019 Strategy boosts initiatives that complement further progress in the national governance model with European policies

Within the National Security System, the cybersecurity structure comprises the following components:

1. The National Security Council.
2. A single Specialised Situation Committee for the whole National Security System in crisis situations.
3. The National Cybersecurity Council
4. The Cybersecurity Standing Committee.
5. The National Cybersecurity Forum.
6. Competent public authorities and the national CSIRT.

The National Security Council

The National Security Council, as the Government's Delegate Commission for National Security, is the body which helps the Spanish Prime Minister to manage National Security Policy.

The National Security Council acts through the National Security Department as a single point of contact, as a link, and guarantees cross-border cooperation with other countries in the European Union

The Situation Committee

There is just one Situation Committee for the whole National Security Council and, supported by the National Security Department, it acts according to political-strategic guidelines dictated by the National Security Council on crisis management.

The National Cybersecurity Council

The National Cybersecurity Council helps the National Security Council meet its functions, particularly helping the Spanish Prime Minister manage and coordinate National Security Policy in the field of cybersecurity.

Its functions include reinforcing coordination, collaboration and cooperation between Public Administrations with competences in cybersecurity, and between public and private sectors, and easing decision-making for the actual Council by analysing, studying and suggesting initiatives and evaluating risks and threats, analysing possible crisis scenarios, studying how they might evolve, drafting and updating response plans and formulating directives for crisis management exercises in the field of cybersecurity and assessing their performance results, all in coordination with directly competent bodies and authorities.

The Cybersecurity Standing Committee

The Cybersecurity Standing Committee is set up to ease inter-ministerial coordination on an operational level in the field of cybersecurity. Presided over by the National Security Department, it comprises the bodies and organisations represented within the National Cybersecurity Council with operational responsibilities. This body helps the National Cybersecurity Council on aspects relating to technical and operative assessment of cybersecurity risks and threats.

The Commission's operation falls within the crisis management procedure in the field of cybersecurity. This procedure establishes its functions aimed at detecting and assessing risks and threats; eases the decision-making process and ensures an optimum, coordinated response from the State. Furthermore, it includes the National Security System's different activation levels plus instructions to manage public communication.

To provide a relevant response, in proportion to situations of special relevance in its functions, it will improve the definition of its skills and responsibilities.

National Cybersecurity Forum

It will act on strengthening and creating public-private synergies, particularly generating knowledge on opportunities, challenges and threats to security in cyberspace.

Setting up the **National Cybersecurity Forum**, and harmonising its operation with existing bodies, will require approval of the necessary standard-based provisions,

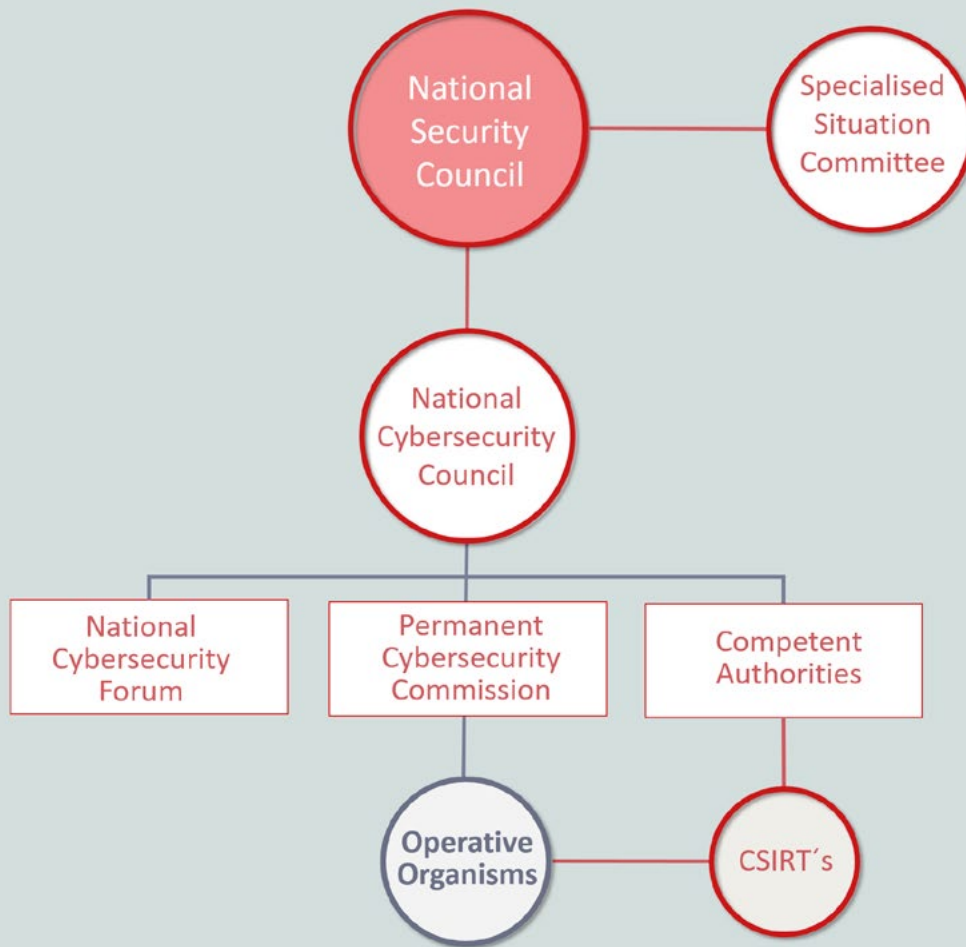
so that these components might be coordinated and run efficiently in the National Security System.

Competent public authorities and the national reference CSIRT

Cybersecurity's strategic, institutional framework is complemented by the competent public authorities on security in information networks and systems and the national CSIRTs that are compiled in the national legal framework.

In addition, CSIRTs from the Autonomous Regions and Autonomous Cities, from Local Entities and their affiliated or dependent bodies, from private entities, the CSIRT.es network and other relevant cybersecurity services should be coordinated with the above, depending on each one's competences. In the same way, working with regional and private CSIRTs, national CSIRTs will encourage initiatives that help meet national strategy goals

CYBERSECURITY IN THE NATIONAL SECURITY SYSTEM



Final considerations and evaluation

Thanks to experience from the 2013 National Cybersecurity Strategy, this document can express and update the ever-changing threats and challenges that we are facing. To adapt to this new, shifting scenario, Lines of Action are proposed plus more dynamic measures that, when necessary, allow the national cybersecurity ecosystem to adapt quickly, based on a considerably mature governance model, which should include active participation from the private sector and the rest of civil society.

In this respect, the Strategy is conceived as a living document that has to be adapted to gradual changes in cybersecurity, so it should be continuously revised, along with specific, sector-based plans derived from it. An annual assessment report will be drafted on the Strategy that will show how much it has been followed and if its goals have been met.

On the other hand, in the light of increasing cybersecurity threats and challenges as faced by countries around us, it is increasingly urgent to equip ourselves with economic, human and material resources to tackle them. One particularly relevant action here is to make sure that the Spanish Central Administration Cybersecurity Operations Centre is properly equipped.

