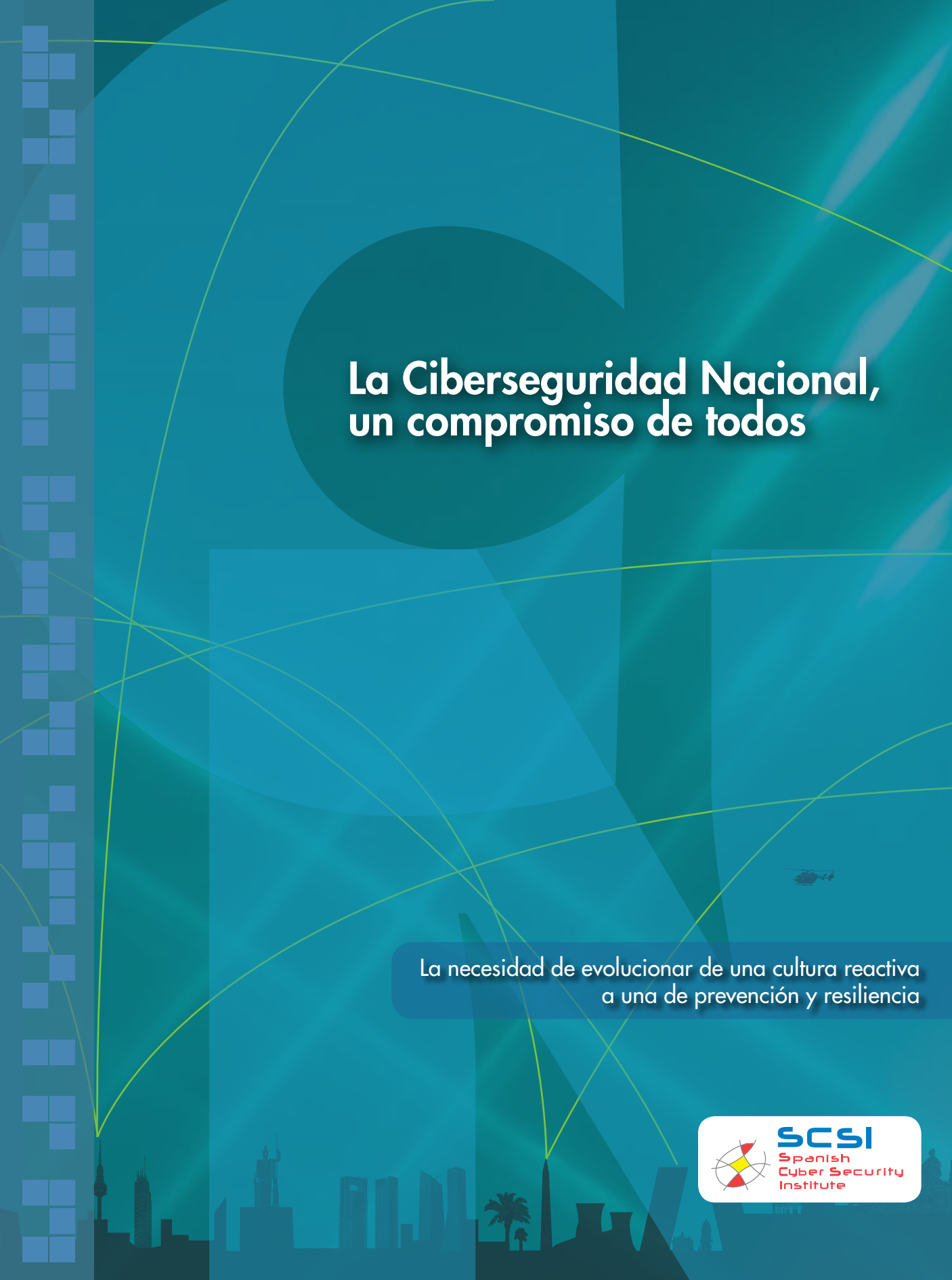
La Ciberseguridad Nacional, un compromiso de todos

La necesidad de evolucionar de una cultura reactiva a una de prevención y resiliencia



SCSI
Spanish Cyber Security Institute

La Ciberseguridad Nacional, un compromiso de todos

La necesidad de evolucionar de una cultura reactiva a una de prevención y resiliencia

Autores
Enrique Fojón Chamorro
José Ramón Coz Fernández
Ramón Miralles López
Samuel Linares Fernández

Coordinador
Miguel Rego Fernández

Editores
Gianluca D'Antonio
Nathaly Rey Arenas

Índice

1. Introducción 4

2. Sobre el SCSI 7

2.1. Misión del SCSI 8

2.2. Visión del SCSI 8

2.3. Principales actividades del SCSI 8

3. Evolucionando a un modelo de seguridad integral 9

4. El Ciberespacio y su seguridad 11

4.1. Una aproximación al concepto de ciberespacio 12

4.2. Ciberseguridad 13

5. El Ciberespacio: La nueva dimensión del entorno operativo 14

6. Estado de riesgo del Ciberespacio 16

6.1. Objetivos 17

6.2. Amenazas 17

6.3. Autoría 18

7. Ciberseguridad en España: Su estado actual 21

8. Diagnóstico sobre el estado actual de la Ciberseguridad Nacional 25

9. ¿Por qué necesita España una Estrategia Nacional de Ciberseguridad? 28

9.1. ¿Qué preocupa? (Riesgos-Amenazas) 29

9.2. ¿Quién se preocupa? (Responsables) 29

9.3. ¿Cómo se responde a esa preocupación? (Políticas) 30

10. Funciones de la Ciberseguridad Nacional 31

10.1. Funciones generales 32

10.2. Funciones operativas 33

11. Habilitadores de la Ciberseguridad Nacional 34

11.1. Habilitadores principales 35

11.2. Habilitadores secundarios 37

12. Estructura organizativa de la Ciberseguridad Nacional 40

13. Objetivos de la Ciberseguridad Nacional 2012-2015 44

14. Acciones para alcanzar los objetivos de la Ciberseguridad Nacional 46

15. Conclusiones 53

16. Bibliografía principal, auxiliar y sitios web consultados 56

1. Introducción

1. Introducción

Las Tecnologías de la Información y la Comunicación (TIC) han coadyuvado al bienestar y progreso de las sociedades de forma que gran parte de las relaciones públicas y privadas dependen de estas tecnologías. Con el tiempo y la evolución de las TIC, han aparecido riesgos que hacen necesario gestionar su seguridad.

Inicialmente, la ciberseguridad se ocupó de proteger la información de una manera reactiva, pero posteriormente ha evolucionado hacia una posición proactiva que identifica y gestiona los riesgos que amenazan el ciberespacio.

Dentro del marco del Instituto Español de Ciberseguridad (SCSI, Spanish Cyber Security Institute) e ISMS Forum, se ha realizado un estudio en el cual se desarrolla una aproximación a los conceptos de ciberespacio y ciberseguridad, a los riesgos y amenazas conocidos, a la gestión existente en España y a la necesidad de desarrollar un sistema nacional de ciberseguridad que fomente la integración de todos los actores e instrumentos, públicos o privados, para aprovechar las oportunidades de las nuevas tecnologías y hacer frente a los retos que presentan, obteniéndose unas conclusiones principales que se resumen en el presente documento.

Organización del documento

El presente documento se divide en 15 capítulos, incluido el presente capítulo de introducción.

En el capítulo 2 se presenta el Instituto Español de Ciberseguridad (SCSI, Spanish Cyber Security Institute), destacando su misión, valores y principales actividades.

En el capítulo 3 se introduce el estudio, explicando la necesidad de evolucionar desde una cultura reactiva a una de prevención y resiliencia así como la necesidad de transitar hacia un modelo de seguridad integral.

En el capítulo 4 se realiza una aproximación a los conceptos de ciberespacio y ciberseguridad.

En el capítulo 5 se identifica la importancia estratégica del ciberespacio como nueva dimensión del entorno operativo.

En el capítulo 6 se analiza el Estado del Riesgo del ciberespacio, describiéndose los principales objetivos de los ciberataques, las principales amenazas cibernéticas así como la tipología de autores de los ciberataques.

En el capítulo 7 se resume el estado actual de la ciberseguridad a nivel nacional.

En el capítulo 8 se lleva a cabo un diagnóstico de la Ciberseguridad Nacional en el cual se enumeran las principales causas que han impedido alcanzar un grado de ciberseguridad acorde a un estado de riesgo conocido y controlado.

En el capítulo 9 se analiza el porqué de la necesidad de una Estrategia Nacional de Ciberseguridad.

En el capítulo 10 se enumeran y definen las principales funciones que debe tener asignada la Ciberseguridad Nacional.

En el capítulo 11 se enumeran y desarrollan los habilitadores de la ciberseguridad, los cuales posibilitarán el funcionamiento de la Ciberseguridad Nacional.

En el capítulo 12 se propone una estructura organizativa que posibilitará dirigir, controlar y gestionar la Ciberseguridad Nacional.

En el capítulo 13 se marcan los objetivos principales de la Ciberseguridad Nacional para el periodo 2012-2015

En el capítulo 14 se enumeran un conjunto de acciones que permitirán alcanzar los objetivos descritos en el capítulo 13.

Por último, en el capítulo 15 se enumeran las principales conclusiones del estudio.

2. Sobre el SCSI

2. Sobre el SCSI

En noviembre de 2011 nace, en el seno del **ISMS Forum Spain,** el **Instituto Español de Ciberseguridad** – *Spanish Cyber Security Institute, en adelante SCSI.*

2.1. Misión del SCSI

La **Misión** del SCSI es realizar y difundir estudios, así como fomentar los debates y el intercambio de ideas y conocimientos, sobre la dependencia que el desarrollo socio-económico de España tiene respecto de las Tecnologías de la Información y la Comunicación (TIC), y así crear un estado de conciencia de la necesidad de la ciberseguridad para controlar y gestionar el estado de riesgo que dicha dependencia genera.

2.2. Visión del SCSI

El SCSI aspira a convertirse en el punto de encuentro de los organismos, privados y públicos, y profesionales relacionados con las prácticas y tecnologías de la ciberseguridad, así como en la referencia nacional para la difusión de aquéllas para toda la sociedad española.

2.3. Principales actividades del SCSI

Las principales actividades del SCSI son:

1. Estudios y publicaciones en materia de ciberseguridad.
2. Interlocución con autoridades y reguladores nacionales e internacionales.
3. Programas de ciber - educación/ ciber - concienciación.
4. Celebración de eventos relacionados con la ciberseguridad.

3. Evolucionando hacia un modelo de seguridad integral

3. Evolucionando hacia un Modelo de Seguridad Integral

La seguridad, en cualquiera de sus dimensiones o ámbitos, es la primera responsabilidad de cualquier Gobierno. Históricamente, la seguridad ha sido principalmente gestionada desde el sector de la defensa ya que los principales riesgos para la supervivencia e integridad de las naciones tenían naturaleza militar. Sin embargo, la aparición de nuevos actores y riesgos de naturaleza heterogénea ha provocado que muchos Estados de nuestro entorno geopolítico estén llevando a cabo una profunda revisión y transformación de sus políticas de seguridad y defensa.

Esta revisión y transformación obedece a un cambio en el **marco rector de la seguridad**. Fundamentalmente, este cambio ha sido propiciado por:

1. **La seguridad de los Estados ya no está restringida a la defensa de sus fronteras y su soberanía,** sino que también debe garantizar el bienestar de sus sociedades frente a los nuevos riesgos.

2. **La globalización fomenta riesgos y amenazas transfronterizos** como el terrorismo, la proliferación de armas de destrucción masiva o la ciberdelincuencia, entre otros.

3. **La aparición de actores de orígenes y motivaciones heterogéneas** con voluntad de desafiar el Estado de Derecho y el orden internacional con capacidad de actuar en cualquiera de las dimensiones de la seguridad, dificulta la atribución de las agresiones y, por tanto, disminuye la capacidad de respuesta de los Estados agredidos.

Además, este nuevo modelo de seguridad exige la necesidad de identificar anticipadamente los riesgos. En otras palabras, es necesario evolucionar de la actual **cultura reactiva** a una de **prevención y resiliencia.**

El fenómeno de la **globalización,** arriba mencionado, se manifiesta con la libertad de movimientos de personas, mercancías, servicios y capitales propiciando una evolución hacia la **"seguridad lineal"** donde ya no aplica la separación entre la seguridad interior y exterior, entre la política de defensa y la de interior y entre lo público y privado.

Por tanto, la **seguridad nacional** ya no se identifica con un tipo de seguridad o defensa, no es responsabilidad de un ministerio particular, ni se separa en un escenario interior o exterior o con un enfoque reactivo o preventivo, sino con todos ellos de forma **omnicomprensiva**.

La aparición del ciberespacio y la necesidad de asegurarlo han propiciado que esta evolución en el modelo de seguridad se haya acelerado.

4. El ciberespacio y su seguridad

4. El Ciberespacio y su Seguridad

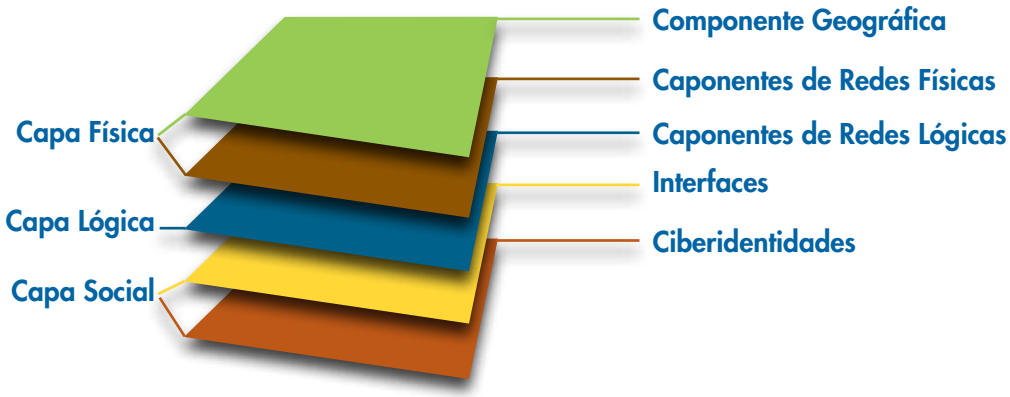
El ciberespacio es ya parte esencial de nuestras sociedades, economías e, incluso, puede llegar a ser factor determinante de la evolución de las culturas, o quizás de su convergencia.

4.1. Una aproximación al concepto de Ciberespacio

El **ciberespacio** es el conjunto de medios y procedimientos basados en las Tecnologías de la Información y la Comunicación (TIC) configurados para la prestación de servicios. El ciberespacio está constituido por hardware, software, Internet, servicios de información y sistemas de control que garantizan la provisión de aquellos servicios esenciales para la actividad socio-económica de cualquier nación, y en especial aquellos ligados a sus infraestructuras críticas.

El ciberespacio se vertebra sobre tres capas superpuestas: **capa física, capa lógica** y **capa social,** que a su vez están compuesta por 5 componentes (ver figura): componente geográfica, componente de las redes físicas, componente de las redes lógicas, persona y ciber-identidades.

El Ciberespacio: Capas y componentes



La **capa física** engloba la componente geográfica y la componente de las redes físicas. La componente geográfica se refiere a la localización física de los elementos de la componente de las redes físicas. La componente de las redes físicas está formada por el hardware e infraestructura que soportan las redes y sus conectores físicos (cableado, cifradores, routers, servidores, ordenadores, etc...).

La **capa lógica** está formada por la componente de redes lógicas que son las conexiones lógicas que existen entre los nodos de las redes, entendiendo por nodo cualquier dispositivo que está conectado a las redes de comunicaciones y sistemas de información.

La **capa social** está formada por los componentes persona y ciber-identidad. El componente persona está formado por los individuos que interactúan con el ciberespacio. La relación entre personas y ciber-identidades puede ser de 1 a n y de n a 1, es decir, una persona puede disponer de una o más ciber-identidades y una ciber-identidad puede ser utilizada por una o más personas. Estas ciber-identidades pueden ser reales o suplantadas, lo que permite gozar de cierto anonimato o impunidad en las acciones que se ejecuten en el ciberespacio siendo, por tanto, difícil relacionar de manera unívoca una ciber-identidad con una persona. Las ciber-identidades están constituidas, entre otros, por cuentas de correo electrónico, cuentas de usuarios en redes o perfiles en redes sociales.

4.2. Ciberseguridad

Anteriormente, la ciberseguridad obedecía a un enfoque de protección de la información (***Information Security***) donde solamente se trataba de proteger la información a accesos, usos, revelaciones, interrupciones, modificaciones o destrucciones no permitidas.

En la actualidad, este enfoque está evolucionando hacia la gestión de riesgos del ciberespacio (***Information Assurance***) donde la ciberseguridad consiste en la aplicación de un proceso de análisis y gestión de los riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información o datos y los sistemas y procesos usados basándose en los estándares internacionalmente aceptados.

Una de las razones para este nuevo enfoque es la caracterización del ciberespacio de una determinada entidad como un sistema TIC que proporciona servicios, de manera que la seguridad del sistema se consigue cuando éste se encuentra en un estado de riesgo conocido y controlado. Realmente, ambos enfoques, information security e information assurance, son diferentes pero complementarios, y con mucha frecuencia son utilizados indistintamente de manera errónea.

Además, la ciberseguridad de una nación requiere plantear, al menos, dos dimensiones:

1. La protección de bienes, activos, servicios, derechos y libertades dependientes de la jurisdicción estatal;

2. Y la responsabilidad compartida con otros Estados, bilateralmente o a través de organismos supranacionales, sobre la ciberseguridad.

La dificultad estriba en lograr que la agregación de soluciones parciales aplicadas por los Estados, aunque se haga de forma coordinada, resuelva los problemas globales creados por unas tecnologías que derriban fronteras. El ciberespacio está en continuo crecimiento y acelerada evolución, alcanzando una capilaridad tal que permite sostener las relaciones y dependencias sociales, económicas y culturales, que son fundamentales para el desarrollo y crecimiento de nuestro país.

En definitiva, la ciberseguridad debe formularse proactivamente como un proceso continuo de análisis y gestión de los riesgos asociados al ciberespacio.

5. El Ciberespacio: La nueva dimensión del entorno operativo

5. El Ciberespacio: La nueva dimensión del entorno operativo

Algunos de nuestros principales aliados ya han identificado, de manera formal, al ciberespacio como una nueva dimensión del entorno operativo. Por ello, están dotando a sus Fuerzas Armadas de las capacidades cibernéticas necesarias para el ejercicio de sus funciones.

Las Fuerzas Armadas no sólo dependen de las TIC y de los sistemas de información para comunicarse, mandar y controlar las operaciones, coordinar acciones de fuego, obtener y distribuir información de inteligencia, realizar acciones de vigilancia y reconocimiento, entre otras actividades militares, sino que, además, están transformando el modo en el que éstas se planifican y ejecutan. Al mismo tiempo, los adversarios, en cualquiera de sus formas (naciones, grupos criminales o terroristas, etc.) tienen acceso y pueden utilizar las mismas tecnologías de un modo completamente innovador y singular.

Dado que las Fuerzas Armadas son, cada vez más, dependientes de los recursos electromagnéticos y las redes informáticas, los cuales están en un continuo proceso de convergencia, está emergiendo un "campo de batalla cibernético". Como la tecnología que permite la comunicación y procesado de la información cambia tan rápidamente, las Fuerzas Armadas deben evaluar continuamente qué aptitudes y capacidades son las necesarias para conseguir, conservar y explotar las ventajas en este emergente campo de batalla.

El modo en el que las tecnologías del ciberespacio se integran y emplean, según las circunstancias operativas de cada momento, afectará significativamente al desarrollo y resultado de las operaciones militares. Si bien es importante estar a la vanguardia en el conocimiento y aplicación de las TIC, no lo es menos el establecer una aproximación integral a todos los aspectos de las ciber-operaciones y ser capaces de obtener ventaja al combinarlos y adaptarlos a las condiciones operativas de cada momento. Como en el resto de las dimensiones del entorno operativo (tierra, mar, aire, espacio exterior), conseguir el dominio en el ciberespacio implica progresar simultáneamente en dos aspectos de las operaciones: obtener superioridad y mantenerla.

Aunque el empleo de las tecnologías emergentes antes de que lo hagan los adversarios proporciona una gran ventaja, deben tenerse en cuenta, y mitigarse, las vulnerabilidades y dependencias que genera su implementación en las redes, sistemas y sensores propios. Probablemente, será incluso más importante conseguir la desactivación, interrupción y anulación de las mismas capacidades en poder de los adversarios. Para ello, las Fuerzas Armadas deben integrar capacidades desde un principio, convirtiéndolas en los elementos de una misma dimensión de las operaciones modernas. Sin embargo, si no se consigue dicha integración el progreso de las operaciones será desigual, en el mejor de los casos, o se producirán fracasos operativos.

La concurrencia y participación en este espacio operativo por parte de los cuerpos y fuerzas de seguridad, junto con iniciativas civiles de organizaciones claves en el contexto de la seguridad nacional, van a tener también un peso específico en el modo operacional, y por tanto deberán articularse mecanismos que permitan, no solo un intercambio fluido de informaciones con la fuerzas armadas, sino incluso en determinadas situaciones una estrecha colaboración.

6. Estado de riesgo del Ciberespacio

6. Estado de riesgo del Ciberespacio

La rápida evolución de las Tecnologías de la Información y la Comunicación (TIC) está aumentando la velocidad, capacidad, agilidad, eficiencia y utilidad de las redes y sistemas actuales, tanto en el ámbito civil como militar. Estas tecnologías están cambiando el modo en el que las personas interactúan entre sí y también con su entorno.

Esta continua y acelerada evolución de las TIC ha propiciado que los ataques sean cada vez más sofisticados y numerosos, dando lugar a un ciberespacio cada vez más hostil, obligando a los responsables nacionales de la ciberseguridad a disponer de medios técnicos y humanos vanguardistas para poder hacer frente a las amenazas y sus posibles impactos.

A continuación se describen cuáles son los principales objetivos de los ciberataques, las principales amenazas cibernéticas así como los autores de los ciberataques.

6.1. Objetivos

Los objetivos de los ciberataques se clasifican en tres grandes grupos:

- **Gobiernos**
- **Sector Privado.** Dentro del sector privado se incluyen a los operadores de Infraestructuras Críticas.
- **Ciudadanos**

6.2. Amenazas

Las principales amenazas relacionadas con el ciberespacio se pueden clasificar en dos grandes grupos:

- **Amenazas contra la información**
- **Amenazas contra la infraestructura TIC**

Las amenazas contra la información, son aquellas cuya materialización provocan una pérdida, manipulación, publicación o uso inadecuado de información. Entre estas amenazas se encuentran:

- Espionaje. Dentro de esta categoría se incluyen toda la variedad de espionaje, desde el espionaje de Estado al espionaje industrial.
- Robo y publicación de información clasificada o sensible.
- Robo y publicación de datos personales.
- Robo de identidad digital.
- Fraude.
- Amenazas persistentes avanzadas (APT).

Las amenazas contra la infraestructura TIC son aquellas cuya materialización pueden provocar la interrupción temporal, parcial o total de determinados servicios o sistemas.

Entre estas amenazas se encuentran:

- Ataques contra infraestructuras críticas.
- Ataques contra las redes y sistemas.
- Ataques contra servicios de Internet.
- Ataques contra sistemas de control y redes industriales.
- Infección con malware.
- Ataques contra redes, sistemas o servicios a través de terceros.

6.3. Autoría

Los ciberataques pueden ser clasificados, en función de su autoría e impacto, según las siguientes categorías:

- **Ataques patrocinados por Estados.** Los conflictos del mundo físico o real tienen su continuación en el mundo virtual del ciberespacio. En los últimos años se han detectado ciberataques contra las infraestructuras críticas de países o contra objetivos muy concretos, pero igualmente estratégicos. Algunos ejemplos, ya conocidos para gran parte de la opinión pública, son el ataque a parte del ciberespacio de Estonia en 2007, que supuso la inutilización temporal de muchas de las infraestructuras críticas del país báltico, el ciberataque de Rusia a Georgia en 2008 como paso previo a la invasión terrestre, los casos Stuxnet con ciberataques a sistemas SCADA, Duqu con ciberataques a organizaciones industriales, los ciberataques sufridos por las redes clasificadas del gobierno estadounidense a manos de atacantes con base en territorio chino o el reciente descubrimiento de Flame. Del mismo modo, en los últimos años se ha detectado que algunos Estados han invertido grandes recursos económicos, técnicos y humanos en el desarrollo de *amenazas persistentes avanzadas* (APT) que atacan de forma agresiva y escogen objetivos muy concretos para mantener una presencia constante dentro de las redes de las víctimas. Los ataques de las APTs son muy difíciles de detectar debido a que utilizan componentes y técnicas especialmente diseñadas para infiltrarse dentro de sus objetivos y quedarse allí sin ser detectados.

- **Ataques patrocinados por organizaciones privadas.** Muchas organizaciones privadas tienen como objetivo los secretos industriales de otras organizaciones o gobiernos. Este tipo de ataque, en muchas ocasiones, se ejecutan con el apoyo gubernamental haciendo uso igualmente de APTs.

- **Terrorismo, extremismo político e ideológico.** Los terroristas y grupos extremistas utilizan el ciberespacio para planificar sus acciones, publicitarlas y reclutar adeptos para ejecutarlas. Estos grupos ya han reconocido la importancia estratégica y táctica del ciberespacio para sus intereses. Las redes sociales y los foros se han convertido en el principal instrumento utilizado por los terroristas.

- **Ataques del crimen organizado.** Las bandas del crimen organizado (ciber-gangs) han comenzado a trasladar sus acciones al ciberespacio, explotando las posibilidades de anonimato que éste ofrece. Este tipo de bandas tienen como objetivo la obtención de información sensible para su posterior uso fraudulento y consecución de grandes beneficios económicos.

- **Hacktivismo.** Durante 2011, el hacktivismo se ha convertido en una de las mayores amenazas para los gobiernos y organismos. Este movimiento tiene como principios el anonimato y la libre distribución de información a través del ciberespacio, esencialmente a través de Internet. Los hacktivistas se agrupan de manera descentralizada utilizando el under-ground de Internet para comunicarse y planificar sus acciones. Entre estos grupos se encuentran Anonymous o Luzsec, pero no son los únicos. Su misión es 'atacar' el ciberespacio que represente a personas, empresas u organizaciones que atente contra alguno de sus principios o intereses. Tanto es así que el ciberespacio de los gobiernos de la mayoría de los países del mundo, bancos, empresas de telecomunicaciones, proveedores de infraestructuras críticas, proveedores de servicios de Internet y en definitiva todo el ciberespacio es susceptible de recibir ataques de denegación de servicios (DDoS) o ser hackeados con el objetivo principal de robar información sensible que posteriormente será distribuida en Internet para libre acceso.

- **Ataques de perfil bajo.** Este tipo de ataques son ejecutados, normalmente, por personas con ciertos conocimientos TIC que les permiten llevar a cabo ciberataques de naturaleza muy heterogénea y por motivación, fundamentalmente, personal.

- **Ataques de personal con accesos privilegiados (insiders).** Este grupo suponen una de las mayores amenazas para la seguridad del ciberespacio de las naciones y empresas ya que suelen ser parte integrante de todos los ataques arriba expuestos. Desde un espía infiltrado por un Estado, a un empleado captado por bandas de terroristas o cibercriminales pasando por un empleado descontento, todos ellos pueden ser considerados *intruders*.

A continuación, en la tabla siguiente, se relacionan a los actores objetivos, la autoría y la tipología de los ciberataques.

Resumen de estado de riesgo del Ciberespacio

AUTORÍA	OBJETIVOS		
	Gobierno	Sector Privado	Ciudadanos
Ataques patrocinados por Estados	Espionaje, ataques contra infraestructuras críticas, APT	Espionaje, ataques contra infraestructuras críticas, APT	
Ataques patrocinados por Sector Privado	Espionaje	Espionaje	
Terroristas, extremismo político e ideológico	Ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros	Ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicio de terceros	
Hacktivistas	Robo y publicación de información clasificada o sensible, ataque contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicio de terceros	Robo y publicación de información clasificada o sensible, ataque contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicio de terceros	Robo y publicación de datos personales
Crimen Organizado	Espionaje	Robo de identidad digital y fraude	Robo de identidad digital y fraude
Ataques de perfil bajo	Ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicio de terceros	Ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicio de terceros	
Ataques de personal con accesos privilegiados (Insiders)	Espionaje, ataques contra infraestructuras críticas, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicio de terceros, robo y publicación de información sensible y clasificada, infección con malware, APT	Espionaje, ataques contra infraestructuras críticas, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicio de terceros, robo y publicación de información sensible y clasificada, APT	

	Alto
Impacto	Medio
	Bajo

7. Ciberseguridad en España: Su estado actual

7. Ciberseguridad en España: Su estado actual

España cuenta con 31 millones de internautas, lo que supone una tasa de penetración de Internet del 65.5% respecto de la población nacional. Este dato sitúa a nuestro país en el puesto número 49 a nivel mundial en cuanto a tasa de penetración de los servicios de la sociedad de la información (correo electrónico, redes sociales, comercio electrónico.

Es preciso identificar cuáles son los activos dependientes del ciberespacio en España, qué regulación existe, cuáles son los organismos con funciones y responsabilidades en la materia y quiénes son los participantes. La defensa de nuestro ciberespacio abarca a todos los activos y actores imaginables, pero debe centrarse, fundamentalmente, en la defensa de las infraestructuras críticas, el tejido empresarial y las libertades y derechos individuales. Las infraestructuras críticas de nuestro país se encuentran agrupadas en los siguientes 12 sectores:

Sectores de Infraestructuras Críticas

En cualquiera de estos sectores, el grado de penetración del ciberespacio, tanto para la gestión interna como para la provisión de servicios, alcanzó su grado crítico ya hace tiempo. Cualquier contingencia que pudiese afectar a alguno de los activos clave pertenecientes a cualquiera de los 12 sectores estratégicos podría comprometer la seguridad nacional. En cuanto al tejido empresarial español, la gran mayoría de las **grandes empresas** disponen de una organización interna lo suficientemente madura que les permite implementar las actividades y medidas que se enmarcan dentro de las prácticas de seguridad de la información.

En el caso de las **pequeñas y medianas empresas y autónomos** (más del 99% del total del tejido empresarial español), la falta de ciberconcienciación y cibereducación así como la escasez de recursos económicos y humanos impiden la adecuada implementación de las medidas de ciberseguridad, limitándose a actividades centradas en las TIC.

Actores Gubernamentales con competencias en materia de Ciberseguridad

Organismo	Administración	Ministerio / Ámbito	Competencias en Ciberseguridad
INTECO	Central	Ministerio de Industria	Operacional, Análisis, Respuesta Incidentes, relaciones internacionales
CCN	Central	Ministerio de la Presidencia	Operacional, Análisis, Respuesta Incidentes, Normativa, relaciones internacionales
CNPIC	Central	Ministerio de Interior	Operacional, Análisis, Respuesta Incidentes, Normativa, relaciones internacionales
REDIRIS	Central	Ministerio de Industria	Operacional, Análisis, Respuesta Incidentes
Unidad de Delitos Telemáticos de la Policía	Central	Ministerio de Interior	Operacional, Análisis, Respuesta Incidentes
Brigada de Delitos telemáticos de la Guardia Civil	Central	Ministerio de Interior	Operacional, Análisis, Respuesta Incidentes
Agencia Española de Protección de Datos	Central	Ministerio de Justicia	Regulador y autoridad de control (implica análisis de incidentes y sanción)
Ministerio Defensa (Diversos órganos y organismos)	Central	Ministerio de Defensa	Operacional, Análisis, Respuesta Incidentes, Normativa
Unidad de Delitos Informáticos de los Mozos de Escuadra (Policía de Cataluña)	Autonómica	Departamento de Interior (Generalitat de Cataluña)	Operacional, Análisis, Respuesta Incidentes
Unidad de Delitos Informáticos de la Ertzaintza (Policía de Euskadi)	Autonómica	Consejería de Interior (Gobierno Vasco)	Operacional, Análisis, Respuesta Incidentes
CSIRT-CV (Comunidad Valenciana)	Autonómica	Autonómico	Operacional, Análisis, Respuesta Incidentes
CESICAT (CERT - Cataluña)	Autonómica	Autonómico	Operacional, Análisis, Respuesta Incidentes, asesoramiento y formación
CERT – Andalucía	Autonómica	Autonómico	Operacional, Análisis, Respuesta Incidentes
Agencia de Protección de Datos de la Comunidad de Madrid	Autonómica	Autonómico	Regulador y autoridad de control (implica análisis de incidentes y sanción)
Autoridad Catalana de Protección de Datos	Autonómica	Autonómico	Regulador y autoridad de control (implica análisis de incidentes y sanción)
Agencia Vasca de Protección de Datos	Autonómica	Autonómico	Regulador y autoridad de control (implica análisis de incidentes y sanción)

Las competencias relacionadas con la gestión de la ciberseguridad están repartidas entre un conjunto de organismos e instituciones, que dependen de diferentes ministerios del gobierno central y gobiernos autonómicos. Entre los más relevantes se encuentran:

- El **Instituto Nacional de Tecnologías de la Comunicación (INTECO),** dependiente del Ministerio de Industria, Turismo y Comercio, es responsable de gestionar a través de su CERT la defensa del ciberespacio relacionado con las PYMES españolas y los ciudadanos en su ámbito doméstico.

- El **Centro Criptológico Nacional (CCN),** dependiente del Centro Nacional de Inteligencia (CNI) que tiene, entre sus misiones, la gestión de la seguridad del ciberespacio dependiente de cualquiera de los tres niveles de las administraciones públicas: estatal, autonómico y local. El CCN-CERT (Capacidad de Respuesta ante Incidentes de Seguridad) es el centro de alerta nacional que coopera con todas las administraciones públicas para responder rápidamente a los incidentes de seguridad en su parte del ciberespacio y, además, es el responsable último de la seguridad de la información nacional clasificada.

- El **Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC),** dependiente del Ministerio del Interior se encarga de impulsar, coordinar y supervisar todas las actividades relacionadas con la protección de las infraestructuras críticas españolas. Su objetivo principal es impulsar y coordinar los mecanismos necesarios para garantizar la seguridad de las infraestructuras que proporcionan los servicios esenciales a la sociedad, fomentando para ello la participación de todos y cada uno de los agentes del sistema en sus correspondientes ámbitos competenciales.

- El **Grupo de Delitos Telemáticos de la Guardia Civil y la Unidad de Investigación de la Delincuencia en Tecnologías de la Información de la Policía Nacional,** dependientes ambos del Ministerio del Interior son responsables de combatir la delincuencia que se produce en el ciberespacio.

- La **Agencia Española de Protección de Datos (AEPD),** autoridad de control independiente, responsable de velar por el cumplimiento de la normativa en materia de protección de datos personales. En algunas comunidades autónomas (Madrid, Cataluña y País Vasco) también existen autoridades de protección de datos con funciones equivalentes a las de la AEPD, cada una en sus respectivos territorios.

Del mismo modo, en la administración autonómica existen centros homólogos a los referidos a nivel estatal como los CERT´s de la Comunidad Valenciana, Cataluña y Andalucía.

Además, las Fuerzas Armadas españolas, tanto en el ámbito específico de los Ejércitos y la Armada, como en el conjunto, liderado por el Estado Mayor de la Defensa, desarrollan distintos programas TIC con el objetivo de proporcionar redes y sistemas seguros que incorporen las tecnologías precisas para proporcionar los servicios y aplicaciones que apoyen a los Mandos militares en el cumplimiento de sus misiones.

8. Diagnóstico sobre el estado actual de la Ciberseguridad Nacional

8. Diagnóstico sobre el estado actual de la Ciberseguridad Nacional

Hasta la aprobación, en mayo de 2011, de la vigente Estrategia Nacional de Seguridad no se había identificado, de manera formal, al ciberespacio como una amenaza real para la seguridad nacional.

El tardío reconocimiento de la importancia estratégica de disponer de un ciberespacio seguro ha provocado, entre otras cosas, que el Gobierno de España no haya creado aun un sistema de Ciberseguridad Nacional completo, es decir, el conjunto de órganos, organismos y procedimientos que permitan la dirección, control y gestión de la seguridad de nuestro ciberespacio.

A continuación se enumeran las principales causas por las cuales aún no se ha alcanzado un grado de ciberseguridad nacional acorde al estado de riesgo del ciberespacio. Estas causas se dividen en 4 grupos: Organizacionales, Operacionales, Jurídicas y Políticas.

Organizacionales

a) **Ausencia de un órgano de dirección en materia de ciberseguridad.** La ausencia de un órgano de Dirección de la Ciberseguridad Nacional impide la implantación de una metodología común de trabajo, que facilite la toma de decisiones, así como la coordinación e integración de todos los actores bajo unos procedimientos comunes.

b) **Gestión disjunta de la Ciberseguridad Nacional debido a un enfoque departamental.** La gestión de la Ciberseguridad Nacional está repartida, de manera disjunta, entre un conjunto de organismos en el ámbito de múltiples ministerios. (Ver gráfico pág. 22 del presente documento).

c) **Insuficientes recursos humanos, técnicos y económicos.** Los organismos de gestión existentes no disponen de los recursos humanos, técnicos y económicos necesarios para implantar y gestionar las capacidades que permitan alcanzar un nivel de ciberseguridad acorde a un estado de riesgo conocido y controlado.

Operacionales

d) **Conocimiento parcial e insuficiente de la ciber-situación nacional.** Disponer de un estado de ciber-situación fiable y actualizado es esencial para la toma de decisiones y la gestión de crisis en el ciberespacio. En la actualidad, el Gobierno de España dispone de un conocimiento parcial e insuficiente del ciberespacio de las administraciones del Estado y, en menor medida, las del sector privado.

e) **Ausencia de un marco de trabajo que posibilite la compartición de información en materia de ciberseguridad.** El insuficiente nivel de comunicación entre los organismos públicos relacionados con la Ciberseguridad Nacional y entre estos organismos públicos y el sector privado se debe, fundamentalmente, a la ausencia de un marco de trabajo procedimentado, estable y abierto que posibilite una compartición fluida y segura de información.

f) **Insuficientes métricas respecto al grado de resiliencia de las infraestructuras TIC de las redes gubernamentales y de las principales infraestructuras críticas del país.** La falta de métricas conlleva que la incertidumbre sobre el grado de resiliencia de las infraestructuras TIC en la que residen las redes gubernamentales y las infraestructuras críticas de nuestro país sea grande.

g) **Escaso protagonismo de los actores privados en materia de ciberseguridad.** La Ciberseguridad Nacional, hoy en día, es un sistema cerrado y exclusivo de los actores gubernamentales. En la actualidad, más del 80% de las infraestructuras críticas de nuestro país son propiedad, están dirigidas y gestionadas por el sector privado (empresas nacionales e internacionales). Por tanto, la aportación del sector privado al proceso de construcción de la Ciberseguridad Nacional resulta esencial.

Jurídicas

h) **Ausencia de legislación específica y completa en materia de ciberseguridad.** Existe legislación distribuida en distintos ámbitos normativos o materias, pero ésta no ha sido desarrollada a partir de una política común que abarque el ámbito nacional y establezca el carácter estratégico de la ciberseguridad.

Políticas

i) **Ausencia de políticas que fomentan la colaboración público-privada en materia de ciberseguridad.** La colaboración público-privada es uno de los pilares para alcanzar un nivel de seguridad acorde a un estado de riesgo conocido y controlado. En la actualidad, España no dispone de un marco de colaboración público–privado en el ámbito de la ciberseguridad.

j) **Ausencia de una política estatal en materia de ciber-concienciación y ciber-educación.** Muchos países de nuestro entorno están desarrollando ambiciosas políticas en materia de ciber-concienciación y ciberseguridad como eje fundamental para la creación de una cultura de ciberseguridad. Estas políticas han sido desarrolladas e impulsadas, en primera instancia, por el sector privado y, posteriormente, han recibido un fuerte apoyo gubernamental.

En este caso, cabe destacar una doble función, por un lado, concienciar y educar al conjunto de la ciudadanía de los riesgos del ciberespacio y, por otro, identificar futuros talentos en el campo de la ciberseguridad dentro de la comunidad escolar y universitaria.

En España, INTECO y el CCN disponen de programas de ciber-concienciación y ciberseguridad. Desde el sector privado, organismos como el ISMS Forum Spain, han lanzado su propia campaña de ciber-concienciación bajo la denominación protegetuinformacion.com. De momento, estas iniciativas tienen una repercusión insuficiente en la sociedad civil.

k) **Ausencia de políticas específicas para el I+D+i nacional en materia de ciberseguridad.** No existen políticas, programas o iniciativas para el I+D+i de ámbito nacional que promuevan y faciliten actividades en materia de ciberseguridad, lo que contrasta con el gran protagonismo que a nivel europeo el nuevo marco de trabajo del Horizonte 2020 (continuación del 7º Programa Marco) otorga a la Ciberseguridad.

9. ¿Por qué necesita España una estrategia nacional de Ciberseguridad?

9. ¿Por qué necesita España una estrategia nacional de ciberseguridad?

La estrategia nacional de ciberseguridad debe ser un instrumento que guíe a los responsables de la dirección y gestión de la Ciberseguridad Nacional así como de sus beneficiarios pero, además, deberá servir como instrumento de disuasión para sus potenciales transgresores.

El Gobierno de España, a través de la Estrategia Española de Ciberseguridad, deberá explicar el modelo de ciberseguridad que proporcionara a la sociedad española en el actual contexto de riesgo global. La estrategia nacional de ciberseguridad deberá definir el concepto de ciberseguridad en base a las tres siguientes cuestiones:

Concepto de Ciberseguridad

9.1. ¿Qué preocupa? (Riesgos-Amenazas)

La novedad, diversidad y heterogeneidad de los riesgos y amenazas relacionados con el ciberespacio, hacen necesario un conocimiento de ciber-situación fiable y actualizada que proporcione a los responsables de la Ciberseguridad Nacional el conocimiento necesario para su dirección, control y gestión. En el capítulo 6 del presente documento se analiza el estado de riesgo actual del ciberespacio.

9.2. ¿Quién se preocupa? (Responsables)

La seguridad del ciberespacio nacional es responsabilidad del gobierno. **Presidencia del Gobierno** debe asumir el liderazgo de la seguridad nacional. Para ello, deberá crear un **Sistema Nacional de Ciberseguridad,** que debería estar integrado el sistema nacional de ciberseguridad.

A pesar de que la responsabilidad es del Gobierno de España deberá propiciar la participación no solo con los actores gubernamentales tradicionales, sino también con los actores privados, comunidad universitaria, expertos nacionales y representantes de la ciudadanía.

9.3. ¿Cómo se responde a esa preocupación? (Políticas)

El Gobierno de España deberá mostrar una **determinación política** para hacer frente a los riesgos y amenazas cibernéticos y, por ello, deberá **fijar unos objetivos y prioridades.**

Del mismo modo, la creación del sistema de Ciberseguridad Nacional permitirá reducir el riesgo de que cada ministerio y agencia decida sus líneas de actuación sin tener en cuenta la de los demás y, como resultado, que los gobiernos luego se vean obligados a hacer un esfuerzo desproporcionado de coordinación.

Las principales políticas deben ir dirigidas a fomentar:

- La resiliencia de nuestro ciberespacio;
- la colaboración público – privada;
- la educación y concienciación;
- el I+D+i y
- la colaboración internacional.

10. Funciones de la Ciberseguridad Nacional

10. Funciones de la Ciberseguridad Nacional

La Ciberseguridad Nacional deberá tener asignadas el siguiente conjunto de funciones:

Funciones de la Ciberseguridad Nacional

• Establecer los objetivos y prioridades de la Ciberseguridad Nacional.
• Integrar políticas y actores.
• Asesorar a los responsables de la seguridad nacional en materia de ciberseguridad.
• Fomentar una cultura de ciberseguridad.
• Valorar el estado de riesgo del ciberespacio.
• Planificar las políticas y gestionar las crisis cibernéticas.
• Potenciar las capacidades nacionales de prevención, reacción y recuperación ante riesgos y ataques cibernéticos.
• Disuadir a los potenciales agresores.

10.1. Funciones generales

- **Establecer los objetivos y prioridades de la Ciberseguridad Nacional.** La Ciberseguridad Nacional debe establecer un conjunto de objetivos. Estos objetivos deben ser alcanzables, medibles, verificables y mantenidos en el tiempo, adaptándose a las necesidades que el ciberespacio y su estado de riesgo vayan marcando en cada momento.

- **Integrar políticas y actores.** Es necesario evitar el actual modelo compartimentado y de escasa coordinación para evolucionar hacia una gestión integral y unificada, con una capacidad de planeamiento y análisis que permita formular propuestas comunes para la adopción de decisiones estratégicas, supervisar su ejecución y evaluar y controlar sus resultados. Para ello será necesaria la participación de todos los actores: públicos, privados, estatales, autonómicos, municipales e, incluso, internacionales.

- **Asesorar a los responsables de la seguridad nacional en materia de ciberseguridad.** El sistema nacional de ciberseguridad deberá asesorar al Presidente del Gobierno y a todos los implicados en cuestiones de seguridad nacional, manteniendo el enlace entre ellos y otros actores nacionales o internacionales, públicos o privados.

- **Fomentar una cultura de ciberseguridad.** La función de comunicación resulta esencial en la creación y fomento de la cultura de ciberseguridad. Esta función consiste en dirigir la estrategia de comunicación sobre los asuntos de Ciberseguridad Nacional y las situaciones de crisis, impulsar la participación parlamentaria y social en la revisión y aprobación de las estrategias, promover la comunicación público-privada y entre las administraciones, difundir alertas y recomendaciones a la población. La cultura de la ciberseguridad se alcanzara mediante la correcta combinación e implantación de los habilitadores de ciberseguridad descritos en el capítulo 11 del presente documento.

10.2. Funciones Operativas

- **Valorar el estado de riesgo del ciberespacio.** EL gobierno de España tiene la responsabilidad de disponer de capacidades que permitan la gestión de la Ciberseguridad Nacional. Como primer paso para cumplir con esta responsabilidad se deberá conocer cuál es el estado de riesgo de nuestra ciberseguridad, cuantificando la probabilidad de que se materialicen las amenazas y estimando su posible impacto.

- **Planificar las políticas y gestionar las crisis cibernéticas.** La planificación de las políticas y la gestión de las crisis requieren un cambio en el modelo de gestión de la ciberseguridad, pasando de la coordinación a la integración y unificación con el objeto de optimizar la aportación de todos los actores involucrados. La gestión integral no consiste en duplicar las mismas tareas y capacidades de otros ni en coordinar iniciativas autónomas, sino en orientar la contribución de todos los actores y políticas implicadas desde el primer momento.

- **Potenciar las capacidades nacionales de prevención, reacción y recuperación ante riesgos y ataques cibernéticos.** El Gobierno de España debe tener a su disposición capacidades de prevención, reacción y recuperación ante riesgos y ataques cibernéticos. Estas capacidades deben permitir el conocimiento del estado de ciber - situación de modo fiable. Además, su aplicación introduce mecanismos de racionalización de los recursos y capacidades, potencia economías de escala y multiplica la sinergia y rendimiento mediante iniciativas de formación, adiestramiento, investigación, y evaluación en común.

- **Disuadir a los potenciales agresores.** Disponer de un ciberespacio resiliente y seguro es el mejor mecanismo de disuasión contra posible agresores, estatales y no estatales.

11. Habilitadores de la Ciberseguridad Nacional

11. Habilitadores de la Ciberseguridad Nacional

El carácter novedoso del ciberespacio, así como su continua evolución y transformación, suponen un reto para la Ciberseguridad Nacional. Por ello, es necesario construir la seguridad del ciberespacio nacional de una manera progresiva, con capacidad de evolucionar y adaptación a un escenario en continuo cambio.

Los **habilitadores de la Ciberseguridad Nacional** son aquellos elementos que posibilitan las funciones de la Ciberseguridad Nacional y se dividen en dos grandes grupos: principales y secundarios:

- Los **habilitadores principales** son aquellos que posibilitan la construcción del sistema nacional de ciberseguridad.
- Los **habilitadores secundarios** son aquellos que posibilitan el funcionamiento del sistema nacional de ciberseguridad. Los habilitadores secundarios, de manera aislada, podrían realizar su función específica aunque no alcanzaría su eficiencia y eficacia crítica.

Habilitadores de la Ciberseguridad

11.1. Habilitadores Principales

Los habilitadores principales de la Ciberseguridad Nacional son:

- **Liderazgo del Estado**
  El Estado tiene la obligación de legislar y actuar para proteger, o hacer que se protejan, los servicios que se prestan en el ciberespacio y que permiten a los ciudadanos, sus organizaciones y empresas desarrollarse en los ámbitos social, cultural y económico, entre otros. Cumplir con tal obligación implica el ejercicio del liderazgo para la definición de políticas, estrategias y normativa jurídica en materia de ciberseguridad, además de crear los instrumentos organizativos que permitan su aplicación.

La Presidencia del Gobierno debe ejercer este liderazgo junto al Gobierno de España. Entre sus funciones se encuentran aprobar, revisar y comunicar las estrategias y políticas en materia de Ciberseguridad Nacional pero, además, supervisar su elaboración y ejecución, así como crear los organismos necesarios y elegir a los responsables de los mismos.

- **Estructura organizativa**

  El Estado debe crear una estructura organizativa que permita la dirección y gestión de la Ciberseguridad Nacional y ejecute las *funciones de la* Ciberseguridad Nacional descritas en el capítulo 10 "*Funciones de la Ciberseguridad Nacional*"del presente documento. Del mismo modo, en el capítulo 12 "*Estructura Organizativa de la Ciberseguridad Nacional"* se propone una estructura organizativa de alto nivel para la Ciberseguridad Nacional.

- **Marco legislativo**

  A pesar de que la esencia de la legislación necesaria para regular la gestión y explotación del ciberespacio nacional ya existe, se encuentra dispersa entre distintos ámbitos normativos, y no ha sido desarrollada a partir de una política común que refleje el ámbito nacional y el carácter estratégico de la ciberseguridad. Por ello, será necesario desarrollar un marco legislativo que de soporte a la Ciberseguridad Nacional, que resulte eficaz y a la vez tenga en cuenta los derechos fundamentales y libertades públicas del Estado de Derecho. Cuanto menos dispersas sean las normas que formen parte de ese marco legislativo, el nivel de seguridad jurídica será mayor.

- **Metodología de trabajo en materia de Ciberseguridad**

  El carácter novedoso del ciberespacio y la complejidad de su seguridad hacen necesario desarrollar una metodología de trabajo que proporcione un mejor entendimiento sobre la importancia estratégica del ciberespacio así como de su estado de riesgo. Esta metodología deberá proporcionar.

  - Un lenguaje común. Este lenguaje común deberá abarcar desde términos tecnológicos a legales.
  - Unos fundamentos teóricos homogeneizados.
  - Procedimientos en los que se describa el modo de proceder en materia de ciberseguridad.

- **Tecnología**

  La tecnología es el fundamento del ciberespacio. El conocimiento y adaptación a la continua evolución tecnológica y técnica resultan fundamentales para mejorar la resiliencia y seguridad de nuestro ciberespacio.

11.2. Habilitadores secundarios

Los habilitadores secundarios de la Ciberseguridad Nacional son:

- **Conocimiento de ciber-situación**

  El conocimiento de la ciber-situación debe proporcionar el conocimiento inmediato del ciberespacio propio, el del resto de naciones, el del enemigo y el de cualquier otro de interés, así como el conocimiento del estado y disponibilidad de las capacidades operativas que son necesarias para el planeamiento, dirección y gestión de las operaciones necesarias para la seguridad del ciberespacio.

  El conocimiento de la ciber-situación no solo se obtiene como resultado de la combinación de actividades de inteligencia y operativas en el ciberespacio, sino también en el espacio electromagnético y en cualquier otra de las dimensiones del entorno operativo (tierra, mar, aire y espacio).

  Los procesos, procedimientos y capacidades del conocimiento de ciber-situación, deben ser desarrollados para contribuir al conocimiento de situación global de los responsables de la dirección de la seguridad nacional así como a la consecución de sus objetivos.

  Por tanto, el conocimiento de ciber-situación deberá:

  - Proporcionar a los responsables de la Ciberseguridad Nacional la visibilidad, en tiempo real, de las redes, sistemas, servicios propios y sus dependencias.
  - Proporcionar a los responsables de la Ciberseguridad Nacional la visibilidad, en tiempo real, de las acciones del enemigo sobre las redes, sistemas y servicios propios, así como el posible impacto en la consecución de los objetivos operativos.
  - Proporcionar a los responsables de la Ciberseguridad Nacional el conocimiento del impacto operativo de sus decisiones sobre las ciber-operaciones, en su ámbito de actuación, contribuyendo al proceso de toma de decisiones.
  - Suministrar a los responsables de la seguridad nacional información lo más detallada posible, incluyendo información de inteligencia fundamental para apoyar el proceso de toma de decisiones acerca del ciberespacio y las ciber-operaciones.
  - Coordinar y compartir esfuerzos entre los diferentes actores (organismos auxiliares de la administración general del Estado, Fuerzas y Cuerpos de Seguridad del Estado, Fuerzas Armadas, el sector privado, la industria, aliados y cualquier otro socio privado o público nacional o internacional) para obtener un conocimiento de la ciber-situación lo más completo posible.
  - Identificar amenazas en el ciberespacio, incluyendo los adversarios potenciales, para contribuir al Conocimiento de la Situación de los responsables de dirigir la seguridad nacional y los objetivos operativos y de inteligencia.

- Estudiar las motivaciones, los objetivos y el análisis de los adversarios potenciales en sus posibles decisiones para dirigir ciber-ataques a los intereses nacionales, de modo que se pueda planificar una defensa ante los mismos.

- **Compartición de información**

Se deben articular un conjunto de mecanismos que permitan a los diferentes actores de la Ciberseguridad Nacional compartir información de manera eficiente y eficaz. Además, la compartición de información:

- Ayudará a conseguir un conocimiento de ciber-situación fiable y actualizado;
- Mejorará la disponibilidad y resiliencia de los activos de la Ciberseguridad Nacional;
- Permitirá gestionar de modo eficaz y eficiente las crisis cibernéticas;
- En otro contexto, permitirá optimizar la inversión económica en materia de ciberseguridad racionalizando el uso de recursos humanos y técnicos.

- **Concienciación y educación en materia de Ciberseguridad**

La sociedad española debe conocer el alcance y la complejidad de la Ciberseguridad Nacional así como tomar conciencia de los riesgos individuales (privacidad e intimidad) y colectivos (seguridad nacional, prosperidad económica, social y cultural) a los que está expuesta si se hace un uso irresponsable del ciberespacio. El Gobierno de España deberá liderar e impulsar un modelo educativo en materia de ciberseguridad. Los objetivos de este modelo son:

1. Concienciar a la sociedad española sobre los riesgos cibernéticos. Es necesario crear un estado de opinión homogéneo sobre la necesidad de disponer de un ciberespacio seguro para garantizar la prosperidad de nuestra sociedad y economía.

2. Formar a la sociedad española en el uso responsable del ciberespacio. Es necesario abordar un ambicioso plan educativo que permita la formación continua en materia de ciberseguridad desde temprana edad (primaria) hasta la universidad. Del mismo modo, se deberán fomentar programas de formación para el resto de sectores de la sociedad española.

3. Identificar y formar a los "ciber-talentos nacionales". La educación temprana en materia de ciberseguridad permitirá identificar a los "cibertalentos nacionales". Estos ciber-talentos deberán recibir una formación especializada guiada a su futura incorporación en los organismos de gestión y control de la Ciberseguridad Nacional.

- **Comunicación estratégica**

Es necesario elaborar una política de comunicación estratégica sobre los asuntos de la Ciberseguridad Nacional y las situaciones de crisis cibernéticas, así como impulsar el debate parlamentario y social en la revisión y aprobación de las estrategias, promover la comunicación público-privada y entre las administraciones, difundir alertas y recomendaciones a la población.

- **I+D+i**

  La fuerte componente tecnológica del ciberespacio y la ciberseguridad obliga a fomentar la competitividad y el I+D+i en el sector público y privado nacional. Para ello el Gobierno de España deberá desarrollar un conjunto de políticas que tengan como objetivo que las empresas nacionales puedan comercializar sus productos y servicios, que el Estado mantenga un estado tecnológico avanzado y, lo que resulta más importante, que disponga de unos "socios" ágiles para responder a la dinámica evolución de las TIC.

- **Colaboración público-privada**

  La heterogeneidad y el cambiante escenario del estado de riesgo del ciberespacio suponen un desafío continuo para la Ciberseguridad Nacional. El Gobierno de España no dispone, por sí mismo, de las capacidades necesarias para garantizar la seguridad del ciberespacio nacional y, por tanto, deberá contar con el sector privado, entre otros, para alcanzar un nivel de seguridad acorde a un estado de riesgo conocido y controlado.

  Es responsabilidad del Gobierno de España crear y fomentar un marco de colaboración público–privado.

  Esta colaboración público-privada en materia de ciberseguridad deberá coadyuvar a:

  - Mejorar el conocimiento del ciber-estado. Los organismos privados son víctimas de continuos e innumerables ciberataques de diferente naturaleza. Por este motivo han implantado sus propias capacidades para garantizar la seguridad de su ciberespacio específico. Estas capacidades generan información y conocimiento que debe ser compartido con los órganos y organismos públicos responsables de la dirección y gestión de la ciberseguridad. Es necesario que la compartición sea bi-direccional.

  - Optimizar las capacidades cibernéticas nacionales evitando duplicidad de recursos y esfuerzos.

  - Mejorar la resiliencia del ciberespacio nacional.

  - Mejorar la competitividad de las empresas nacionales en el campo de la ciberseguridad.

  - Mejorar el I+D+i en materia de ciberseguridad.

  - Fomentar la concienciación y educación en materia de ciberseguridad .

12. Estrucutura Organizativa de la Ciberseguridad Nacional

12. Estrucutura Organizativa de la Ciberseguridad Nacional

A continuación se propone una estructura organizativa de alto nivel para dirigir, controlar y gestionar la Ciberseguridad Nacional.

Estructura Organizativa de la Ciberseguridad Nacional

- **El Órgano Nacional de Ciberseguridad** tendrá la responsabilidad de dirigir la Ciberseguridad Nacional. Este órgano deberá posibilitar la ejecución de las funciones encomendadas a la Ciberseguridad Nacional. Estas funciones han sido descritas anteriormente en el presente documento.

- **Operaciones.** El Órgano Nacional de Ciberseguridad deberá procurar las capacidades de detección, prevención, contención y respuesta ante cualquier ataque o contingencia cibernética. Todas estas capacidades operacionales deberán ser gestionadas desde un CERT Nacional de Referencia y un CERT de Defensa.

- **Evaluación y seguimiento.** El área de evaluación y seguimiento tendrá asignadas las siguientes funciones:

    - **Conocimiento de ciber-situación.** El conocimiento de ciber-situación nacional y global es un aspecto fundamental para una eficiente dirección y gestión de la Ciberseguridad Nacional. Un estado de ciber-situación fiable y actualizado se alcanza mediante la integración y transformación de la información proveniente de múltiples fuentes: CERT Nacionales, servicios de inteligencia, Fuerzas y Cuerpos de Seguridad del Estado, resto de organismos de las Administraciones del Estado, operadores de infraestructuras críticas, proveedores de servicios de Internet, empresas de hardware y software, ciudadanía, empresas privadas, organizaciones privadas y la comunidad internacional.

Conocimiento de Ciber-situación

- **Análisis de riesgos.** El conocimiento de ciber-situación permitirá identificar las causas de las amenazas y probables eventos cibernéticos no deseados así como de los daños y consecuencias que éstos pueden provocar en la seguridad nacional. El carácter innovador y de rápida transformación que caracteriza al ciberespacio hace necesario un análisis de riesgos continuo que permita adoptar las medidas de seguridad que el estado de riesgo del ciberespacio imponga.

- **Planificación.** La planificación permitirá disponer de una visión a largo plazo de los procedimientos, las actividades y los recursos involucrados para dar un soporte a la gestión de la ciberseguridad.

- **Gestión de contingencias cibernéticas.** La continua transformación del ciberespacio provoca que los órganos y organismos que dirigen y gestionan la Ciberseguridad Nacional deban enfrentarse a eventos no conocidos que comprometen la resiliencia y/o seguridad de nuestro ciberespacio. Estos eventos no conocidos son conocidos como contingencias.

- **Alertas.** Será necesario disponer de un mecanismo que permita informar a todos los actores involucrados en la Ciberseguridad Nacional sobre cuestiones relevantes. Del mismo modo deberá habilitarse un canal de comunicación que permita.

- **Lecciones aprendidas.** La recopilación de los éxitos y fracasos en la dirección y gestión de la Ciberseguridad Nacional resulta esencial para mejorar las debilidades y afianzar las fortalezas de nuestro ciberespacio con el objetivo de hacerlo mas resiliente y seguro.

- **Doctrina.** En base al conocimiento de ciber-situación y al conjunto de lecciones aprendidas será necesario crear un conjunto de enseñanzas coherentes o instrucciones en materia de ciberseguridad.

- **Elaboración de políticas y procedimientos.** Como resultado de todo lo anteriormente expuesto será necesario desarrollar políticas y procedimientos que posibiliten el control y la gestión de la Ciberseguridad Nacional. Estas políticas y procedimientos deberán tener en cuenta no solo aspectos tecnológicos sino también legales, operativos y cualquier otra dimensión que pudiese afectar a la Ciberseguridad Nacional.

• **Programas estratégicos**. La auto-adaptación del ciberespacio nacional a un estado de riesgo conocido y controlado es un aspecto clave para la Ciberseguridad Nacional.

Para ello, será necesario trabajar de manera continua y evolutiva en un conjunto de programas estratégicos que faciliten una adaptación progresiva a un estado de riesgo conocido y controlado del ciberespacio. A continuación enumeramos algunos de esos programas estratégicos:

- I+D+i. Será necesario disponer y fomentar políticas que posibiliten que las empresas nacionales puedan comercializar sus productos y servicios en materia de ciberseguridad y así conseguir que el Estado pueda mantener un estado tecnológico avanzado y, lo que resulta más importante, que disponga de unos "socios" ágiles para responder a la dinámica evolución de las TIC y su seguridad.

- Concienciación y Formación. La formación y concienciación continua de todos los sectores de la sociedad española resulta esencial para la seguridad del ciberespacio nacional. La evolución imparable del ciberespacio hace necesario disponer de instrumentos y canales ágiles que permitan adaptar los programas de concienciación y formación en materia de ciberseguridad.

- Ciber –ejercicios. Con el objeto de conocer el verdadero estado de madurez de la Ciberseguridad Nacional será necesario realizar, de manera periódica, ciber-ejercicios. Estos ciber-ejercicios deberán realizarse no solo en el ámbito del ciberespacio nacional sino también en el seno de las principales organizaciones internacionales (OTAN, UE, etc.)

- Estándares y Buenas Prácticas. Será necesario desarrollar estándares y buenas prácticas que mejoren la resiliencia y seguridad de nuestro ciberespacio. Muchos de estos estándares y buenas prácticas ya existen y tienen un consenso y aceptación internacional.

13. Objetivos de la Ciberseguridad Nacional 2012-2015

13. Objetivos de la Ciberseguridad Nacional 2012-2015

El fin último de la estrategia nacional de ciberseguridad debe ser la consecución de un conjunto de objetivos. A continuación se incluyen los objetivos que en materia de ciberseguridad deberían alcanzarse durante el periodo 2012-2015.

Objetivo Principal		
Proporcionar un ciberespacio seguro que garantice la prosperidad social, cultural y económica de nuestro país así como las libertades fundamentales de los ciudadanos a través de una cultura basada en la prevención y resilencia en la que participen, de manera activa e integrada, todos los sectores de la sociedad española.		
Objetivo 1	**Objetivo 2**	**Objetivo 3**
Disponer de un conocimiento de ciber-situación fiable y actualizado.	Mejorar la resilencia nacional respecto de la amenaza cibernética.	Crear y fomentar una cultura de ciberseguridad.

El objetivo principal de la Ciberseguridad Nacional es proporcionar un ciberespacio seguro que garantice la prosperidad social, cultural y económica de nuestro país así como las libertades fundamentales de los ciudadanos a través de una cultura basada en la prevención y resiliencia en la que participen, de manera activa e integrada, todos los sectores de la sociedad española.

Para alcanzar este objetivo principal es necesario, previamente, alcanzar los siguientes objetivos parciales:

- **Objetivo 1. Disponer de un conocimiento de ciber-situación fiable y actualizado.** Es necesario disponer de un conocimiento inmediato del ciberespacio propio, del resto de naciones, del enemigo y de cualquier otro de interés, así como el conocimiento del estado y disponibilidad de las capacidades operativas que son necesarias para el planeamiento, dirección y gestión de las operaciones necesarias para la seguridad del ciberespacio.

- **Objetivo 2. Mejorar la resiliencia nacional respecto de la amenaza cibernética.** Es necesario disponer de las capacidades que posibiliten resistir y recuperarse de los impactos negativos derivados de las actividades conocidas, desconocidas, predecibles, impredecibles, inciertas e inesperadas, en el ciberespacio. Este esfuerzo debe ir dirigido, especialmente, a mejorar la resiliencia de las infraestructuras críticas de nuestro país.

- **Objetivo 3. Crear y fomentar una cultura de ciberseguridad.** Los habilitadores de la Ciberseguridad Nacional, descritos en el punto 6 del presente documento, deben propiciar la creación de una cultura de Ciberseguridad Nacional. De modo recíproco, la 'esencia' de la cultura de Ciberseguridad Nacional creada deberá optimizar el manejo de estos habilitadores y, por tanto, propiciar la consolidación de la cultura de ciberseguridad.

14. Acciones para alcanzar los Objetivos de la Ciberseguridad Nacional

14. Acciones para alcanzar los Objetivos de la Ciberseguridad Nacional

Para alcanzar los objetivos descritos el capítulo 13 del presente documento será necesario llevar a cabo un conjunto de acciones que permitan:

- Mejorar el conocimiento de ciber-situación.
- Mejorar las capacidades de detección y análisis de ciber-amenazas.
- Mejorar los canales de comunicación entre los diferentes actores involucrados en la Ciberseguridad Nacional.
- Mejorar la resiliencia y seguridad del ciberespacio nacional.
- Fortalecer el marco jurídico nacional e internacional en materia de ciber-crimen.
- Mejorar la concienciación, educación, formación y desarrollo profesional en materia de ciberseguridad.
- Fomentar programas de I+D+i en materia de ciberseguridad.
- Apoyar la competitividad del sector privado en materia de ciberseguridad.
- Fomentar la cooperación internacional.

A continuación se enumeran las acciones que deberían ejecutarse en el periodo 2012-2015 con el objeto de mejorar la resiliencia y seguridad del ciberespacio nacional

Acción 1. Aprobación de la Estrategia Nacional de Ciberseguridad. Para construir el sistema de Ciberseguridad Nacional que permita la dirección, control y gestión de la Ciberseguridad Nacional es necesario aprobar la estrategia nacional de ciberseguridad.

Estructura Organizativa

Acción 2. Designar o crear el CERT Nacional de Referencia. Se deberá crear o designar, entre los ya existentes, el CERT Nacional de Referencia. El CERT Nacional de Referencia tendrá como misión recopilar la información operacional relativa al estado del ciberespacio nacional proveniente de medios propios y del resto de CERTs nacionales existentes y de los CERTS internacionales con los cuales se hayan suscritos convenios de colaboración.

Acción 3. Crear el CERT del Ministerio de Defensa. Se deberá dotar al actual Centro Operativo de Seguridad de las Fuerzas Armadas de los recursos humanos, económicos y técnicos necesarios para propiciar su evolución a CERT.

Acción 4: Crear el Centro Nacional de Seguimiento y Evolución de Ciberseguridad. Este centro deberá desarrollar las actividades descritas en las acciones del área de Seguimiento y Evaluación descritos en el capítulo 12 del presente documento.

Acción 5: Crear el Centro Nacional de Programas Estratégicos en materia de ciberseguridad. La imparable evolución y transformación del ciberespacio hace necesario desarrollar programas estratégicos en este ámbito que permitan la adaptación de la seguridad nacional a un estado de riesgo conocido y controlado. En el capítulo 12 del presente documento se definen los principales programas estratégicos en materia de ciberseguridad identificados a fecha de hoy. Estos programas deberán ser dirigidos y controlados por el Centro Nacional de Programas Estratégicos en materia de ciberseguridad y la gestión de los mismos deberá estar repartida entre organismos competentes en el ámbito de la Administración General del Estado.

Operacionales

Acción 6. Asignación de los recursos humanos necesarios para la dirección, control y gestión de la Ciberseguridad Nacional. Sera necesario dotar a todos los organismos de nueva creación y a los ya existentes del conjunto de profesionales necesarios. Estos perfiles deberán cubrir todas las áreas de conocimiento en el campo de la ciberseguridad.

Acción 7. Mejorar y ampliar las capacidades tecnológicas que permitan la detección, prevención, contención y respuesta ante ciberataques. Para mejorar las capacidades de detección, prevención, contención y respuesta ante ciberataques será necesario:

- Mejorar y ampliar la red de sensores de alerta temprana;
- Mejorar las capacidades de monitorización;
- Mejorar las capacidades de análisis de vulnerabilidades;
- Mejorar las capacidades de resolución de incidencias cibernéticas.

Acción 8. Crear un marco de trabajo para la compartición de información entre los diferentes actores de la Ciberseguridad Nacional. El Órgano Nacional de Ciberseguridad deberá articular los mecanismos que permitan coordinar e integrar a los actores involucrados en la Ciberseguridad Nacional para posibilitar una compartición de información fluida y eficaz. Este marco de trabajo deberá incluir medidas legislativas que propicien un entorno de seguridad jurídica respetuoso con los derechos fundamentales y libertades públicas sin pérdida de eficacia.

Acción 9. Mejorar los canales de alerta. Sera necesario mejorar los canales de comunicación que permitan comunicar, en forma y tiempo, a los diferentes sectores de la sociedad española y actores de la ciberseguridad las contingencias cibernéticas que supongan una amenaza para la seguridad nacional.

Acción 10. Desarrollar una metodología para la mejora de la resiliencia y seguridad del ciberespacio nacional.

Acción 11. Fomentar y propiciar la resiliencia y seguridad de la infraestructura TIC del sector privado. Sera necesario llevar a cabo políticas que propicien una mejora en que puedan mejorar la resiliencia y seguridad de su infraestructura TIC.

Cooperación internacional

Acción 12. Acuerdos bilaterales o multilaterales con otras naciones en materia de ciberseguridad. El carácter global del ciberespacio hace necesario acuerdos bilaterales y multilaterales con otras naciones en el ámbito de la ciberseguridad con el objetivo de mejorar la seguridad de nuestro ciberespacio. España forma parte de muchos organismos internacionales pero, dependiendo de la naturaleza de la amenaza cibernética, será necesario suscribir acuerdos bilaterales o multilaterales con determinados países de nuestro entorno geopolítico o fuera de él. Estos acuerdos deberán mejorar los canales de información, detección y/o respuesta coordinada antes ciberincidentes. Especial relevancia deben tener aquellos acuerdos destinados a la lucha contra el cibercrimen en cualquiera de sus formas.

Acción 13. Participación en los foros multilaterales e internacionales relacionados con la ciberseguridad. España deberá participar de manera activa en todos los foros multilaterales e internacionales donde se aborde la ciberseguridad. (OTAN, UE, ONU, Interpol, Europol, OCDE,…)

Acción 14. Trabajar de manera coordinada con los aliados para implantar la Política de Ciberseguridad de la OTAN. La cumbre de la OTAN de Lisboa de 2010 identificó al ciberespacio como una nueva amenaza para los intereses de la Organización. España deberá trabajar junto al resto de sus aliados en la proteccion del ciberespacio de la Alianza.

Colaboración público-privada

Acción 15: Creación de la Plataforma Nacional para la Coordinación y Cooperación Público-Privada en materia de ciberseguridad. Se deberá crear una plataforma nacional para la coordinación y cooperación público-privada en materia de ciberseguridad, donde estén representados los principales actores en la sociedad española: sector público, sector privado (con representación de las distintas tipologías de organizaciones, grandes empresas y PYMES), la comunidad académica, centros tecnológicos y de investigación, asociaciones y organizaciones.

Acción 16: Creación de Grupos de Trabajo Sectoriales dentro de la Plataforma Nacional para la Coordinación y Cooperación Público-Privada en Ciberseguridad. Como continuación a la creación de la plataforma nacional, deberán crearse grupos de trabajo sectoriales que fomenten una comunicación eficiente y eficaz.

Educación y concienciación

Acción 17: Desarrollar un programa nacional de educación en materia de ciberseguridad. Este programa deberá fomentar la concienciación, educación, formación y desarrollo profesional en materia de ciberseguridad. Para ello será necesario llevar a cabo las acciones que se plantean a continuación.

Acción 18: Desarrollar una campaña nacional de ciber-concienciación. Se debe desarrollar una campaña de ciberconcienciación con el objeto de que la sociedad española tome conciencia sobre los riesgos individuales (privacidad e intimidad) y colectivos (seguridad nacional, prosperidad económica, social y cultural) que se deriven de un uso inadecuado del ciberespacio. En este terreno la especial sensibilidad con los menores por parte de las autoridades de protección de datos y de la legislación en la materia, pueden ser un elemento de especial dinamismo en el desarrollo y diseminación de este tipo de campañas. Igualmente, se deberán llevar a cabo campañas específicas dirigidas a padres y profesorado. Se propone la campaña www.protegetuinformacion.com de ISMS Forum Spain como el embrión de esta campaña nacional de ciberconcienciación. En esta campaña el papel de las principales empresas privadas del país así como de los principales medios de comunicación (TV, Radio, periódicos, Internet…) resulta crítico.

Acción 19: Incorporación de materias relacionadas con el uso responsable de las nuevas tecnologías y ciberseguridad en los planes de estudio de educación primaria, secundaria, universitaria y post-universitaria. Sera necesario incorporar materias relacionadas con la ciberseguridad. Esta formación debe iniciarse a temprana edad (educación primaria) y ser ampliada a lo largo de la educación secundaria, universitaria y post-universitaria. El objeto de iniciar la educación a temprana edad pretende, por un lado, homogeneizar los conocimientos en el uso de las nuevas tecnologías así como su uso responsable y, por otro lado, identificar a los 'ciber-talentos' nacionales.

Acción 20: Modificación de los programas educativos de las materias relacionados con Ciencia, Tecnología e Ingeniería, haciendo hincapié en el importante papel de las matemáticas y el pensamiento computacional, sin olvidar los aspectos legislativos y normativos.

Todas las iniciativas en materia de Educación Superior, incluyendo la implantación de Programas Educativos específicos sobre Ciberseguridad deberán de ser coordinadas con la Agencia Nacional de Evaluación de la Calidad y Acreditación (ANECA), como fundación estatal que tiene como objetivo contribuir a la mejora de la calidad del sistema de educación superior mediante la evaluación, certificación y acreditación de enseñanzas, profesorado e instituciones.

Acción 21: Incorporación de materias relacionadas con las nuevas tecnologías y ciberseguridad en los planes de estudio en las academias militares. Los oficiales y suboficiales de la Fuerzas Armadas Españolas deberán recibir una sólida formación en teoría de la información, electrónica, propagación de ondas radioeléctricas, entre otros, así como en la aplicación de éstos a las tácticas, operaciones y estrategias militares.

Acción 22: Incorporación de materias relacionadas con las nuevas tecnologías y ciberseguridad en los planes de estudio de las escuelas de negocio. Los futuros directivos de las empresas nacionales deberán recibir formación en nuevas tecnologías y ciberseguridad. El apoyo de la alta dirección de las organizaciones es crucial para implantar en ellas una cultura de ciberseguridad.

Acción 23: Creación de un programa de centros académicos de excelencia en materia de ciberseguridad. La colaboración público – privada entre las Administraciones del Estado, el sector privado y la comunidad universitaria deberá permitir designar a un conjunto de universidades nacionales como centros académicos de excelencia donde se impartirá enseñanza en materia de ciberseguridad como parte de los programas estratégicos del Gobierno en esta materia. Estos centros deberán impartir formación especializada y promover el I+D+i en materia de ciberseguridad.

Acción 24: Planes de formación y concienciación, de carácter obligatorio, destinados a los empleados de empresa pública, privada y autónoma.

Acción 25: Planes de formación continua del personal responsable de la dirección y gestión del ciberespacio y de las Administraciones del Estado así como de los organismos, públicos y privados, que gestionan y administran las infraestructuras críticas de nuestro país. Será necesario elaborar un plan de formación donde se incluyan cursos, grados, másteres y certificaciones en materia de ciberseguridad dirigidos al personal responsable de la dirección y gestión del ciberespacio de la Administraciones del Estado así como de los organismos, públicos y privados, que gestionan y administran las infraestructuras críticas de nuestro país.

I+D+i y competividad

Acción 26: Crear un Plan Estratégico Nacional de I+D+i en Ciberseguridad y su correspondiente Desarrollo en Programas de Trabajo Anuales. Acompañando a la Estrategia Nacional de Ciberseguridad y con un marco temporal similar al plan de acción definido, deberá desarrollarse un plan estratégico de desarrollo de I+D+i en Ciberseguridad alineado tanto con las necesidades nacionales transmitidas por parte de los sectores público y privado, como con el alineamiento estratégico marcado por el nuevo marco de trabajo europeo Horizonte 2020. Este plan estratégico deberá ser desarrollado en Programas de Trabajo Anuales que incluyan temáticas y objetivos concretos en el camino del posicionamiento, mejora y desarrollo de las capacidades de ciber-protección de los distintos sectores, público y privado, y de la propia ciudadanía, además de la promoción del mercado, los productos y servicios nacionales de ciberseguridad.

Acción 27: Crear un Observatorio de Vigilancia Tecnológica de I+D+i en Ciberseguridad Internacional. Con el fin de mantener un estado avanzado de conocimiento de la vanguardia tecnológica y de ciber-situación de la ciberseguridad, deberá establecerse un proceso de vigilancia tecnológica de I+D+i en ciberseguridad que garantice el conocimiento, la valoración de colaboraciones y la promoción de proyectos en cooperación, que aseguren la total integración y el máximo aprovechamiento de las oportunidades, los recursos y los avances internacionales en las organizaciones nacionales en este ámbito.

Acción 28: Crear un Centro Nacional de Certificación de productos TIC. La implantación de determinados productos TIC requerirá la certificación previa por parte de un centro nacional de certificación. Este centro deberá mantener actualizado el catálogo de productos certificados. Este catálogo contendrá aquellos productos (hardware y software) que cumplen con los requisitos de seguridad para formar parte de las infraestructuras TIC del sector público y de las principales infraestructuras críticas del país, para los cuales será de obligado cumplimiento. Del mismo modo, este catálogo servirá como guía para el resto del sector privado, aconsejándose el uso de los mismos.

Otras acciones

Acción 29: Designar la primera semana del mes de noviembre como 'Semana para la concienciación en materia de ciberseguridad'. Con el objeto de fomentar la concienciación en materia de ciberseguridad, y aprovechando el comienzo del curso escolar, se recomienda llevar cabo una semana de concienciación en materia de ciberconcienciación en todos los centros educativos del Estado (educación primaria, secundaria, universitaria y post-universitaria).

Acción 30: Albergar la Conferencia sobre el ciberespacio de 2014 ó 2015. Durante 2011 tuvo lugar en Londres la primera conferencia internacional sobre el ciberespacio con la presencia de los principales líderes mundiales. Esta conferencia se celebrara en Hungría en 2012 y Corea del Sur en 2013.

Acción 31: Promover y liderar el primer ciberejecicio iberoamericano en 2013. España deberá promover y liderar el primer ciber-ejercicio iberoamericano. Este ejercicio permitirá medir el grado de madurez de nuestra ciberseguridad. Además permitirá afianzar el liderazgo de España en el ámbito del ciberespacio iberoamericano alcanzando acuerdos en materia de ciberseguridad con una gran cantidad de países.

15. Conclusiones

15. Conclusiones

España, a pesar de los grandes esfuerzos realizados, no dispone aún de una capacidad sólida que permita realizar una dirección, control y gestión eficaces y eficientes de nuestra ciberseguridad.

El gobierno de España deberá asumir el liderazgo en materia de ciberseguridad para concienciar a los ciudadanos de la necesidad de proteger el ciberespacio del que dependen nuestros servicios básicos, infraestructuras críticas, economía y progreso como sociedad.

Las TIC no son el problema, son parte de la solución y su resiliencia, protección y empleo seguro no son sólo responsabilidad del gobierno, sino de las demás administraciones autonómicas y locales junto con el sector privado, empresarial y doméstico. Todos son corresponsables, pero le corresponde al gobierno el liderazgo y la dirección de la gestión nacional de la ciberseguridad. Responsabilidades que no pueden delegarse y que deben traducirse en proporcionar el impulso, las ideas y la dirección que España necesita.

La seguridad, en cualquiera de sus dimensiones o ámbitos, es una responsabilidad esencial de cualquier Gobierno.

Los cambios experimentados en su marco rector en los últimos años, incluyendo la aparición de nuevos riesgos y amenazas (amenazas transfronterizas, la globalización o la aparición de actores no estatales, entre otros) hace que sea necesario evolucionar hacia un concepto de seguridad integral y una cultura de prevención y resiliencia.

Esta evolución pasa por considerar el ciberespacio como un elemento clave en la gestión global de riesgos de la seguridad nacional y, por tanto, otorgar la importancia necesaria a la ciberseguridad como proceso continuo de análisis y gestión de los riesgos asociados al ciberespacio.

El escenario de riesgos ha evolucionado y está evolucionando día a día. El incremento en cantidad y variedad de las amenazas contra la información y las infraestructuras TIC, la mayor cantidad y sofisticación de los ciberataques o la variedad en sus objetivos, incluyendo la ciudadanía, el sector privado y los gobiernos, suponen cambios determinantes que, junto con la diversidad de autores y partes interesadas, como estados, organizaciones privadas, organizaciones terroristas, crimen organizado o *hacktivistas,* deben ser tenidos en cuenta a la hora de desarrollar una estrategia de ciberseguridad adecuada.

Otro de los aspectos clave a tener en cuenta en la futura Estrategia Nacional de Seguridad, es la identificación del ciberespacio como nueva dimensión del entorno operativo junto a las ya tradicionales (tierra, mar, aire y espacio). Por tanto será necesario dotar a nuestras Fuerzas Armadas de aquellas ciber-capacidades y recursos humanos, técnicos y económicos necesarios para el ejercicio de sus funciones.

En este sentido, cualquier contingencia que pudiese afectar a alguno de los activos clave de los doce sectores en los que se agrupan en nuestras infraestructuras críticas, podría comprometer la seguridad nacional.

De estos aspectos y otros relacionados con la gestión de la Ciberseguridad Nacional se encargan diferentes actores gubernamentales repartidos en el ámbito de múltiples ministerios. Aún así, hasta la aprobación en mayo de 2011 de la vigente Estrategia Nacional de Seguridad, no se había identificado, de manera formal, al ciberespacio como una amenaza real para la seguridad nacional, lo que ha provocado, entre

otras cosas, que el Gobierno de España no haya creado aún un sistema de Ciberseguridad Nacional completo.

Se hace, por tanto, necesario desarrollar y aprobar la Estrategia Nacional de Ciberseguridad. Esta estrategia deberá ser un instrumento que guíe a los responsables de la dirección, control y gestión de la Ciberseguridad Nacional así como de sus beneficiarios pero, además, deberá servir como instrumento de disuasión para sus potenciales transgresores. Esta estrategia deberá tener asignada un conjunto de funciones que se podrán alcanzar a partir del siguiente conjunto de habilitadores principales:

- El liderazgo indiscutible del Estado a través de Presidencia del Gobierno;
- La creación de un sistema nacional de ciberseguridad integrado en el sistema de seguridad nacional;
- Una metodología de trabajo adecuada que proporcione un lenguaje común, unos fundamentos teóricos homogeneizados y unos procedimientos que describan el modo de proceder en materia de ciberseguridad;
- Y todo ello acompañado de la evolución tecnológica necesaria que los soporte.

Además, estos habilitadores principales deberán ser 'nutridos' por:

- Un conocimiento de ciber-situación;
- Una compartición de información adecuada entre los distintos actores;
- Una concienciación y educación que venga dada por el impulso de un modelo educativo en materia de ciberseguridad;
- Una política de comunicación estratégica sobre los asuntos de la Ciberseguridad Nacional y las situaciones de crisis cibernéticas;
- El fomento y promoción de la I+D+i en el sector público y privado nacional;
- Y un marco de colaboración público-privada en materia de ciberseguridad.

El objetivo principal de la Ciberseguridad Nacional, es por tanto, proporcionar un ciberespacio seguro que garantice la prosperidad social, cultural y económica de nuestro país, así como las libertades fundamentales de los ciudadanos, a través de una cultura basada en la prevención y resiliencia en la que participen, de manera activa e integrada, todos los sectores de la sociedad española.

16. Bibliografía principal, auxiliar y sitios web consultados

16. Bibliografía y sitios web consultados

Bibliografia principal

- **ARTEAGA, FÉLIX** "Propuesta para la implantación de una Estrategia de Seguridad Nacional en España" DT 19/2011. Diciembre 2011. Real Instituto Elcano.
- **BETZ, DAVID J. & STEVENS, TIM** "Cyberspace and the State. Toward a strategy for cyber-power". IISS.
- **CLARKE, RICHARD & KNAKE, ROBERT "CYBERWAR".** 2010. Ed Harper Collins.
- **COZ FERNÁNDEZ, JOSÉ RAMÓN & FOJÓN CHAMORRO,** ENRIQUE "La Geoestrategia del Conocimiento en Ciberseguridad". Enero 2012. Revista RED SEGURIDAD.
- **COZ FERNÁNDEZ, JOSÉ RAMÓN & FOJÓN CHAMORRO, ENRIQUE** "Un modelo educativo para una Estrategia Nacional de Ciberseguridad". Octubre 2011. Congreso ENISE (Encuentro Internacional de la Seguridad de la Información).
- **FOJÓN CHAMORRO, ENRIQUE & SANZ VILLALBA, ÁNGEL FRANCISCO** "Ciberseguridad en España: Una propuesta para su gestión" ARI 102/2010. Junio 2010 Real Instituto Elcano.
- **FOJÓN CHAMORRO, ENRIQUE & COZ FERNÁNDEZ, JOSÉ RAMÓN** "Panorama Internacional en el establecimiento de Estrategias Nacionales de Ciberseguridad. Junio 2011. Revista SIC". Seguridad, Informática y Comunicaciones.
- **FOJÓN CHAMORRO, ENRIQUE & SANZ VILLALBA, ÁNGEL FRANCISCO** "El ciberespacio: La nueva dimensión del entorno operativo" perteneciente al documento de seguridad y defensa n° 44 "Adaptación de la fuerza conjunta a la guerra asimétrica". Noviembre de 2011. Centro Superior de la Defensa Nacional (CESEDEN). http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/docSegyDef/ficheros/DSEGD_44.pdf
- **KNAPP, ERIC D.** "Industrial Network Security". 2011. Ed. SYNGRESS.
- **LIBICKI, MARTIN** "Cyberdeterrence and Cyberwar". RAND project Air Force.
- **MULLIGAN, DEIRDRE K. & SCHNEIDER, FRED B.** "Doctrine for Cybersecurity" Septiembre 2011. Universidad Berkley.
- **SHOSTACK, ADAM & STEWART,ANDREW** "The new school of information security". 2008. Ed Addison-Wesley.
- **STIENNON, RICHARD** "Surviving Cyberwar". 2010.

Bibliografia auxiliar

- **ESTRATEGIA ESPAÑOLA DE SEGURIDAD.** Junio 2011. http://www.lamoncloa.gob.es/NR/rdonlyres/D0D9A8EB-17D0-45A5-ADFF-46-A8AF4C2931/0/EstrategiaEspanolaDeSeguridad.pdf

- **CYBER SECURITY STRATEGY OF THE UNITED KINGDOM** http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf

- **THE US NATIONAL COMPREHENSIVE NATIONAL CYBERSECURITY STRATEGY,** http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

- **Canada's Cyber Security Strategy. For a stronger and more prosperous Canada**: http://www.capb.ca/uploads/files/documents/Cyber_Security_Strategy.pdf

- **CYBER SECURITY STRATEGY FOR GERMANY.** http://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1

- **CYBER SECURITY STRATEGY OF THE CZECH REPUBLIC FOR THE 2011 – 2015 PERIOD.** http://www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_20112015.PDF

- **CYBER SECURITY STRATEGY OF THE UNITED KINGDOM** http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf

- **DÉFENSE ET SÉCURITÉ DES SYSTÈMES D'INFORMATION STRATÉGIE DE LA FRANCE.** http://www.enisa.europa.eu/media/news-items/french-cyber-security-strategy-2011

- **ENHANCING THE USABILITY AND AVAILABILITY OF INFORMATION INFRASTRUCTURE ESSENTIAL FOR SECURING THE VITAL FUNCTIONS OF SOCIETY".** http://www.lvm.fi/c/document_library/get_file?folderId=1551284&name=DLFE-11788.pdf&title=Julkaisuja%203-2011

- **ESTONIA CYBER SECURITY STRATEGY,** http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf

- **INDIA CYBERSECURITY STRATEGY.** http://www.mit.gov.in/content/cyber-security-strategy

- **JAPAN: THE FIRST NATIONAL STRATEGY ON INFORMATION SECURITY.** http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf

- **JOHN H. DEXTER. THE CYBER SECURITY MANAGEMENT SYSTEM: A CONCEPTUAL MAPPING.** The SANS Institute, February 2002.

- **KOWTKO, M. SECURING OUR NATION AND PROTECTING PRIVACY. SYSTEMS, APPLICATIONS AND TECHNOLOGY CONFERENCE (LISAT),** 2011 IEEE Long Island Issue Date: 6-6 May 2011. On page(s): 1 – 6. ISBN: 978-1-4244-9878-9.

- **LARGE OIL COMPANIES FALL VICTIM TO CYBER-ESPIONAGE POSSIBLE CONNECTION WITH OPERATION AURORA.** http://news.softpedia.com/news/Large-Oil-Companies-Fall-Victim-to-Cyber-Espionage-133317.shtml

- **NEW ZEALAND: THE DIGITAL 2.0 STRATEGY".** ISBN 978-0-478-31645-2. http://www.med.govt.nz/upload/11162/Digital%20Strategy%202.0%20FINAL.pdf

- **RAIN OTTIS. ANALYSIS OF THE 2007 CYBER-ATTACKS AGAINST ESTONIA FROM THE INFORMATION WARFARE PERSPECTIVE. PROCEEDINGS OF THE 7TH EUROPEAN CONFERENCE ON INFORMATION WARFARE AND SECURITY.** University of Plymouth UK. June 2008

- **SINGAPORE'S STRATEGY IN SECURING CYBERSPACE.** http://www.ida.gov.sg/News%20and%20Events/20050717164621.aspx?getPagetype=21

- **STEW MAGNUSON. CYBER EXPERTS HAVE PROOF THAT CHINA HAS HIJACKED U.S.-BASED Internet TRAFFIC: UPDATED.** NDA's Business and Technology Magazine. December 2010.

- **STOP. THINK. CONNECT. THE ANTI-PHISHING WORKING GROUP (APWG) AND NATIONAL CYBER SECURITY ALLIANCE (NCSA).** U.S. Department of Homeland Security. http://stopthinkconnect.org/

- **T.M. CHEN. "STUXNET, THE REAL START OF CYBER WARFARE?"** Network, IEEE Issue Date: November-December 2010. Volume: 24 Issue: 6 on page(s): 2 – 3. ISSN: 0890-8044. Digital Object Identifier: 10.1109/MNET.2010.5634434. November 2010.

- **THE NATIONAL CYBER SECURITY STRATEGY (NCSS).** Publication Ministry of Security and Justice. P.O.Box 20301 | 2500 EH | The Hague. The Netherlands. June 2011 | J-9228

Sitios web consultados

- **www.inteco.es**
- **www.ccn-cert.cni.es/**
- **www.dhs.gov**
- **www.whitehouse.gov**
- **thehackernews.com/**
- **www.ciberseguridad.es**

Una iniciativa de:

C/ Castello, 24, 5° Derecha, Escalera 1
28001 Madrid T.: 34 91 186 13 50

Más información: www.ismsforum.es