Estrategia de Ciberseguridad Nacional

Ante la constatación de la existencia de múltiples riesgos y amenazas para un ciberespacio seguro, en diciembre de 2013, y a iniciativa del Consejo de Seguridad Nacional, España se dota de un documento estratégico en el que se recogen los elementos necesarios para proteger nuestro ciberespacio: la Estrategia de Ciberseguridad Nacional. Con su aprobación, también se crea una nueva estructura dirigida a mejorar la coordinación de la ciberseguridad a nivel nacional y apoyar a la toma de decisiones del más alto nivel en esta materia: el Consejo Nacional de Ciberseguridad y el Comité especializado en la gestión de crisis, el Comité de Situación.

MAR LÓPEZ GIL
Jefa de la Oficina de Seguridad y TI. Responsable del Área de Ciberseguridad. Departamento de Seguridad Nacional. Gabinete de la Presidencia del Gobierno

El comienzo de este proceso debe iniciarse reseñando la creación en julio de 2012, en el seno del Gabinete de la Presidencia del Gobierno, del Departamento de Seguridad Nacional. El Departamento nace con la idea de impulsar una nueva concepción de la Seguridad Nacional, acometiendo inicialmente la tarea de revisar la Estrategia Española de Seguridad de 2011. Fruto de casi un año de trabajo, a finales de mayo, el Consejo de Ministros aprobaba la Estrategia de Seguridad Nacional de 2013. Por primera vez España se dota de forma simultánea de la combinación de un documento estratégico del más alto nivel y su desarrollo orgánico inmediato, el Consejo de Seguridad Nacional.

Este documento, desde una visión integral, presenta doce riesgos y amenazas a la Seguridad Nacional con un enfoque innovador y transversal. Ámbitos tales como la ciberseguridad conviven con otros más tradicionales como la defensa nacional o la lucha contra el terrorismo.

Además, la Estrategia de Seguridad Nacional configura el nuevo Sistema de Seguridad Nacional, compuesto por el Consejo de Seguridad Nacional y los Comités Especializados, todo ello bajo la dirección del Presidente del Gobierno.

La ciberseguridad un ámbito prioritario en la Seguridad Nacional

Fruto del trabajo del Consejo, en diciembre de 2013, se aprobó la Estrategia de Ciberseguridad Nacional. Tan importante ha sido el proceso de elaboración, como el documento finalmente aprobado dado que, bajo la coordinación del Departamento de Seguridad Nacional del Gabinete de la Presidencia del Go-

FIGURA 1. Riesgos y amenazas a la Ciberseguridad Nacional

bierno, en éste han participado todos los actores clave de la ciberseguridad nacional.

Con este impulso decidido, la ciberseguridad en España se ha convertido en uno de los ámbitos de actuación prioritaria para la Seguridad Nacional, materializándose definitivamente con la publicación de la Estrategia de Ciberseguridad Nacional en la que se establece la dirección política-estratégica del uso seguro del ciberespacio en España.

Un objetivo que requiere el esfuerzo y compromiso de todos

La Estrategia de Ciberseguridad Nacional desarrolla las previsiones de la Estrategia de Seguridad Nacional de 2013 en ámbito de la Ciberseguridad, fijando como objetivo lograr un uso seguro de los Sistemas de Información a través del fortalecimiento de nuestras capacidades de prevención, defensa, detección y respuesta a los ciberataques.

Éste es el objetivo de referencia y desarrollo de la Estrategia de Ciberseguridad Nacional (ECSN), que nace como la respuesta a la responsabilidad del Estado, del conjunto de los españoles y de la multiplicidad de actores que actúan sobre la ciberseguridad y por tanto, un objetivo común a cumplir.

Para ello la ECSN se articula en torno a cinco capítulos en los que se pone de manifiesto la relevancia del ciberespacio para nuestra sociedad, se establece el propósito y los principios rectores de la ciberseguridad en España, se fijan seis objetivos específicos, se recogen las líneas de acción estratégicas y finalmente, se establece la estructura orgánica al servicio de la ciberseguridad.

La importancia del ciberespacio

En España cada día millones de ciudadanos utilizan las Tecnologías de la Información y las Comunicaciones en su actividad diaria: búsqueda y envío de información, compra y venta de bienes y servicios, formación, participación en redes sociales, banca electrónica, transacciones económicas...actualmente más del 70 % de los hogares españoles dispone de acceso a Internet, manteniendo la tendencia ascendente. De igual forma, las Administraciones Públicas dependen de estas tecnologías, tanto como base de su funcionamiento interno, como de los servicios que prestan a los ciudadanos ya que actualmente el 95% de los servicios públicos se encuentran operativos a través de Internet. Por su parte, las empresas mantienen un uso intensivo de las TIC como soporte de su negocio y como motor de crecimiento y creación de

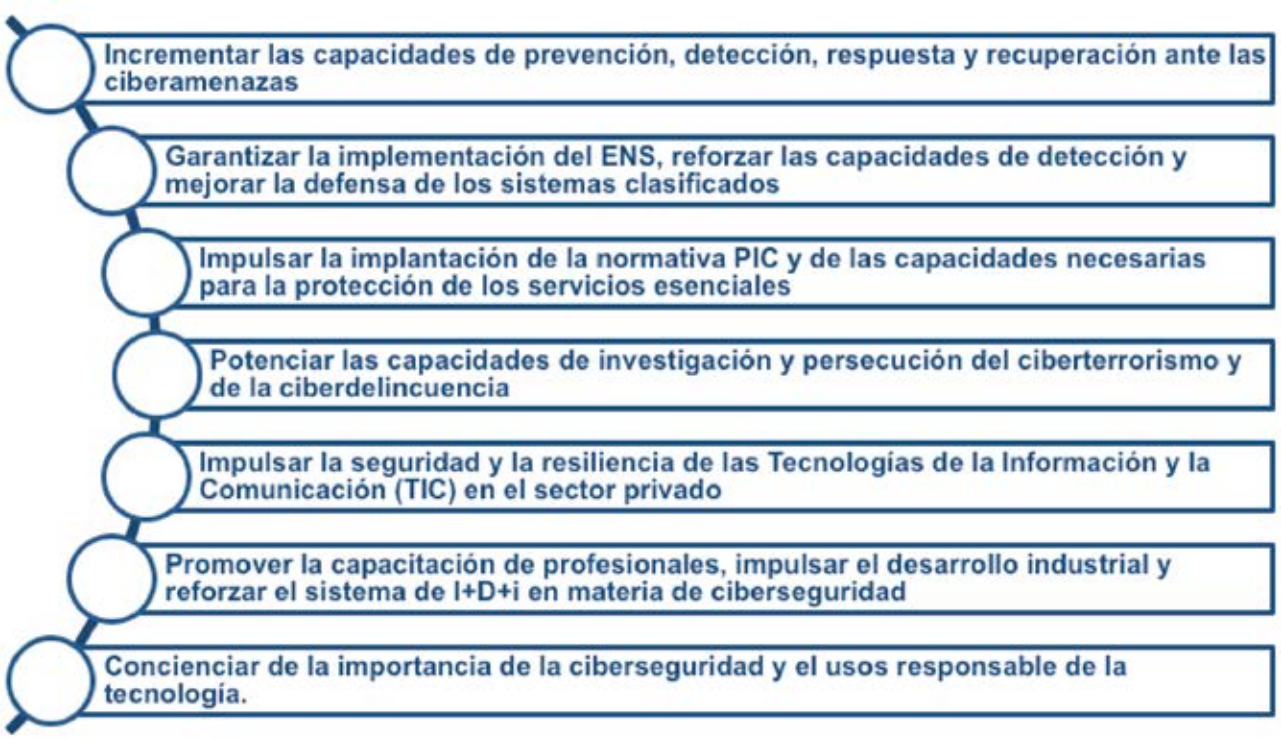

FIGURA 2. Retos que nos presenta la sociedad de la información

nuevas oportunidades. El 98,9% de las pymes y las grandes empresas y el 71,7% entre las microempresas utilizan las TIC en este sentido.

Hoy existen más de 2,8 mil millones de usuarios de Internet en todo el mundo, 566 millones en Europa, 35 millones en España. En 1 minuto en Internet se mandan más de 200 millones de mails y se hacen más de 4 millones de búsquedas en Google.

Estos datos demuestran que el Ciberespacio está redefiniendo profundamente las relaciones entre las empresas, los ciudadanos y los gobiernos, a la vez que éste crece, se amplifica nuestra total dependencia de él.

Acorde con este rápido cambio tecnológico, se hace cada vez más necesario prever las consecuencias que la implantación de una tecnología puede tener ahora y en el futuro. El desarrollo tecnológico se puede orientar en múltiples direcciones, ya sean nuevas oportunidades, pero también nuevos retos y amenazas.

Las cifras que presentan los distintos CERTS **(1)** nacionales respecto al número de ciberataques y los incidentes que día a día se publican en los medios de comunicación, dan muestra de la magnitud real de este gran reto, que se acrecienta día a día debido al aumento de la dependencia de nuestra sociedad respecto de las Tecnologías de la Información y de las Comunicaciones (TIC) y del ciberespacio.

Propósito y principios rectores de la ciberseguridad. Objetivos

La Estrategia de Ciberseguridad Nacional, bajo el propósito de fijar las directrices del uso seguro del espacio, extiende al ámbito ciber el espíritu de la Estrategia de Seguridad Nacional **(2)**, incorporando los siguientes cuatro principios rectores: liderazgo nacional y coordinación de esfuerzos, responsabilidad compartida, proporcionalidad, racionalidad y eficacia, y cooperación internacional.

Estos principios guían la necesaria evolución hacia una política de apoyo decidido al desarrollo del mercado tecnológico y de generación de conocimiento en la materia, desde una visión integral que defienda nuestros intereses nacionales y fomente el posicionamiento y la cooperación internacional.

Bajo el objetivo global de lograr un uso seguro de los Sistemas de Información a través del fortalecimiento de nuestras capacidades de prevención, defensa, detección y respuesta a los ciberataques, la Estrategia de Ciberseguridad Nacional fija seis objetivos específicos.

Estos objetivos, orientados al fortalecimiento de la ciberseguridad y de la confianza en el uso de las TICs, son la implantación de un marco nacional de referencia en el impulso de

la protección del "patrimonio tecnológico"; el fortalecimiento y la potenciación de la cooperación del ámbito judicial y policial frente a las actividades del terrorismo y la delincuencia en el ciberespacio; la promoción de una sólida cultura de ciberseguridad; el aumento de la capacitación de los profesionales; el fomento del I+D+i y la mejora de la ciberseguridad en el ámbito internacional.

Líneas de acción

Es esencial detenerse en el contenido de un plano en el que se está procediendo de manera muy activa. Me refiero al cuarto capítulo, donde se recogen las diversas líneas de acción de la ciberseguridad nacional. Indicar que todas ellas, ocho en concreto, orientan la actuación en un ámbito lleno oportunidades e imprescindible para el desarrollo de todo nuestro potencial económico y social, pero que a su vez y simultáneamente, conlleva grandes desafíos para la seguridad y bienestar de los ciudadanos.

Las Líneas de Acción Estratégicas se han definido para alcanzar los objetivos señalados anteriormente y recogen el necesario incremento de las capacidades de prevención, reacción, respuesta y recuperación simultáneamente para la seguridad de los Sistema de Información y Telecomunicaciones que soportan las Administraciones Públicas y el impulso de la seguridad de los Sistema de Información y Telecomunicaciones que soportan las Infraestructuras críticas; el desarrollo de la capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia, así como en el incremento de la seguridad y resiliencia de las Tecnologías de la Información y de la Comunicación y la promoción del conocimiento, las competencias y el I+D+i, en el ámbito de la ciberseguridad, dentro del sector privado.

Muy relacionado con este aspecto, la Estrategia confiere una importancia particular a la promoción de la cultura de ciberseguridad, una de las prioridades a desarrollar en el marco del Sistema de Seguridad Nacional.

Este empeño en proporcionar una respuesta adecuada a los nuevos retos que nos presenta la sociedad de la información no puede lograrse sin la integración del esfuerzo nacional en el marco de las iniciativas de nuestros socios y aliados para promover un ciberespacio internacional seguro y confiable.

La ciberseguridad en el Sistema de Seguridad Nacional

Por último, en su quinto capítulo, la visión de la ciberseguridad nacional queda plasmada en una estructura orgánica que, bajo la dirección del Presidente del Gobierno, se integra en el marco del Sistema de Seguridad Nacional bajo tres órganos: el Consejo de Seguridad Nacional, el Consejo Nacional de Ciberseguridad y el Comité de Situación.

En concreto:

- El *Consejo de Seguridad Nacional*, como Comisión Delegada del Gobierno para la Seguridad Nacional.
- *El Consejo Nacional de Ciberseguridad*, como órgano colegiado de apoyo al Consejo de Seguridad Nacional, cuya función principal es el fomento de la coordinación, cooperación y colaboración entre Administraciones Públicas y entre éstas y el sector privado. Se encuentran representados todos los ministerios con competencias en materia de ciberseguridad.
- Y por último el *Comité de Situación*, que apoyándose en el Centro de Situación del Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno, presta apoyo al Consejo de Seguridad Nacional en la dirección político-estratégica de situaciones de interés para la Seguridad Nacional, es decir, aquellas que por su transversalidad o su dimensión desborden las capacidades de respuesta de los mecanismos habituales.

Ha llegado el momento de emprender una acción coordinada y eficaz conforme a estos nuevos parámetros, a través de la articulación de un sistema que realmente se adapte a los nuevos retos identificados día a día

El apoyo al Consejo Nacional de Ciberseguridad es prestado por el Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno en su condición de Secretaría Técnica y órgano de trabajo permanente el Consejo de Seguridad Nacional.

Este Sistema quedará plenamente establecido con la aprobación de la Ley Orgánica de Seguridad Nacional —actualmente en fase de trámite reglamentario—, que dará el soporte legal necesario a toda esta estructura.

Logros y retos

Sin duda, la ciberseguridad ha entrado de lleno en el debate político y

La Estrategia de Seguridad Nacional marca como objetivo principal "lograr un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección y respuesta a los ciberataques".

social de nuestra vida cotidiana. No ha sido de forma repentina, ni imprevisible. Las señales de que algo estaba cambiando en la forma de considerar las nuevas tecnologías y su peso en las relaciones sociales, económicas y políticas han sido cada vez más manifiestas.

En este último año se ha avanzado en todo lo relativo a la ciberseguridad en España y en buena medida estos avances parten y se explican por la Estrategia de Ciberseguridad y la puesta en marcha del Consejo de Ciberseguridad Nacional.

Por lo tanto, los elementos estructurales de la Ciberseguridad Nacional ya están delineados y habrá que configurarlos para cumplir con implicaciones como las derivadas de la futura aprobación de la Directiva Europea para la Seguridad de las Redes y la Información (conocida como Directiva NIS, actualmente en proceso de elaboración en las Instituciones Europeas), que establecerá, entre otros temas, mecanismos para garantizar a nivel nacional un elevado grado de seguridad de las redes y la información de los principales operadores que presten servicios en sectores esenciales para el desarrollo las actividades económicas y sociales de cada país (como Internet, energía, transporte, banca, salud, etc.)

Es el momento de emprender una acción coordinada y eficaz conforme a este nuevo enfoque de la ciberseguridad, a través de la articulación de un sistema que realmente se adapte a los nuevos retos identificados día a día.

Por poner un ejemplo, parte de esa acción ha sido la aprobación, el 31 de octubre de 2014 por el Consejo de Seguridad Nacional, del Plan Nacional de Ciberseguridad. En él destaca la asignación de responsabilidades para el cumplimiento de la Estrategia de Ciberseguridad Nacional, asignando cometidos específicos a los órganos y organismos representados en el Consejo de Ciberseguridad Nacional, pero, esto es solo un punto de partida y el trabajo comienza ahora. Aún existen retos que nos quedan por abordar.

Debemos adaptarnos a las nuevas situaciones y adelantarnos a las que puedan sucederse, esto no se conseguirá sin el esfuerzo de todos los implicados en la ciberseguridad nacional, ya sean el Estado, las empresas o los ciudadanos.

Las oportunidades para seguir avanzando en el camino emprendido son numerosas. Hoy en día ya contamos con instrumentos para cumplir mejor con las responsabilidades que plantea el gran reto de la ciberseguridad y, sin duda, estamos en el buen camino. ✱

NOTAS

(1) Equipo de Respuesta a incidentes de Seguridad de la Información.

(2) Los principios informadores de la Estrategia de Seguridad Nacional 2013 son: unidad de acción, anticipación y prevención, eficiencia y sostenibilidad en el uso de los recursos y resiliencia o capacidad de resistencia y recuperación.