El Centro Criptológico Nacional como pilar del fortalecimiento de la ciberseguridad en España

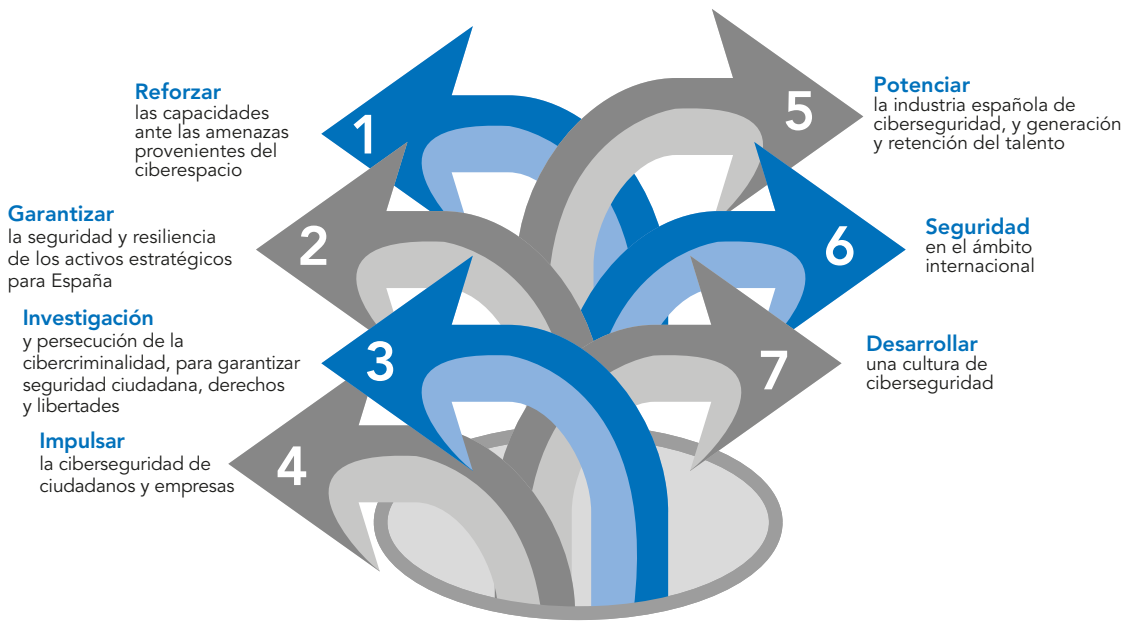
La Estrategia Nacional de Ciberseguridad es un documento en el que se plasma la necesidad de mejorar la seguridad de las TIC en España y se detallan los objetivos y medidas para cumplir con este propósito. El Centro Criptológico Nacional, Organismo adscrito al Centro Nacional de Inteligencia, es responsable de garantizar la ciberseguridad y contribuye a través de numerosas acciones e iniciativas para evitar, mitigar y restaurar los daños derivados de los riesgos del ciberespacio.

Javier Candau // Jefe del Departamento de ciberseguridad del Centro Criptológico Nacional

La ciberseguridad, con el paso de los años, se ha introducido entre las prioridades de un gran número de Gobiernos, considerada ahora un asunto de seguridad nacional y eje fundamental de la sociedad y de sus sistemas económicos. Todo ello ha justificado la necesidad de disponer de estrategias de ciberseguridad nacionales que, al amparo de las estrategias de seguridad, permiten enmarcar los objetivos y las medidas para alcanzar y mantener un elevado nivel de seguridad de las redes y sistemas de información de los estados.

Así pues, en España se elaboró con la ayuda de diversos Organismos la **Estrategia Nacional de Ciberseguridad**, un documento publicado por el Boletín Oficial del Estado el 30 de abril de 2019, por medio de la Orden PCI/487/2019, de 26 de abril. Estructurada en

Figura 1: Líneas de Acción de la Estrategia Nacional de Ciberseguridad 2019



cinco capítulos, se presentan los principios y objetivos a cumplir en esta materia, así como un total de **siete líneas de acción y las medidas** para el desarrollo de cada una de estas.

Uno de los Organismos que contribuyó a su elaboración fue el **Centro Nacional de Inteligencia (CNI)**, a través de su Centro Criptológico Nacional (CCN), el cual a su vez ha venido actuando con el propósito fijado en el documento a través de sus tres principales integrantes: su **Capacidad de Respuesta a incidentes de Seguridad de la Información (CCN-CERT)**, como gestor de los ciberataques al sector público y empresas y organizaciones de interés estratégico; el **Organismo de Certificación de productos y sistemas (OC)**, para valorar y acreditar la capacidad de un producto para manejar información de forma segura; así como su **Departamento de Productos y Tecnologías (CCN-PYTEC)**, para la aplicación de políticas y procedimientos seguros y el empleo y promoción de productos y tecnologías de seguridad.

Su contribución a la consecución de los objetivos planteados y la adopción de las medidas acordadas ha sido de vital importancia. De las siete líneas de acción recogidas, el papel del CCN ha sido y continúa siendo especialmente relevante en lo que respecta a las líneas 1, 2 y 7 (ver Figura 1).

Línea de acción 1: Reforzar las capacidades ante las amenazas provenientes del ciberespacio

Una de las medidas recogidas dentro de esta línea consiste en "impulsar el desarrollo de plataformas de notificación, intercambios de información y coordinación para la mejora de la ciberseguridad sectorial". El CCN-CERT, como CERT Gubernamental Nacional, colabora con todos los organismos públicos y empresas de interés estratégico en la detección, notificación, evaluación, respuesta, tratamiento y aprendizaje de ciberincidentes que puedan sufrir sus sistemas. Una de sus iniciativas principales para este fin fue el desarrollo, en 2008, de su **Sistema de Alerta Temprana (SAT)**, cuyo propósito es poder prevenir un incidente o, por lo menos, detectarlo en un primer momento para reducir su impacto y alcance.

Figura 2: Sistema de Intercambio de Información de Ciberincidentes en los Sistemas de Información de las AAPP

El CCN-CERT actúa como Nodo de Intercambio de Información de Ciberincidentes en los Sistemas de Información de las AAPP

En línea también con la medida ya mencionada, el CCN-CERT actúa como Nodo de Intercambio de Información de Ciberincidentes en los Sistemas de Información de las Administraciones Públicas, así como principal coordinador con los organismos adecuados en dicho intercambio, una misión para la cual ha desarrollado hasta el momento numerosas soluciones, siendo de especial interés para este respecto dos: **LUCIA** (Listado Unificado de Coordinación de Incidentes y Amenazas), una herramienta para la Gestión de Ciberincidentes y mejorar la coordinación entre el CERT Gubernamental Nacional y los distintos organismos y organizaciones con las que colabora; y **REYES**, cuya finalidad es agilizar la labor de análisis de ciberincidentes y compartir información de ciberamenazas (ver Figura 2).

Línea de acción 2: Garantizar la seguridad y resiliencia de los activos estratégicos para España

Una de las principales misiones encomendadas al CCN-CERT es la de ofrecer servicios de vigilancia, sin coste asociado, a organismos de la Administración Pública, promoviendo la creación de **Centros de Operaciones de Seguridad (SOC)** en los que realizar tareas de prevención, detección y vigilancia. En este sentido, su papel ha sido esencial en el desarrollo del **SOC-Justicia** y el **SOC de la Administración General del Estado (AGE)** y sus organismos públicos. La creación de este último era, precisamente, mencionada como una de las medidas a adoptar para cumplir con lo expuesto en esta línea.

Asimismo, este apartado exponía la necesidad de potenciar la progresiva implicación y creación de infraestructuras de ciberseguridad en las Comunidades Autónomas, las Ciudades Autónomas, las Entidades Locales y en sus organismos vinculados o dependientes. Y para dar respuesta a ello, desde el CCN se ha estado trabajando a lo largo de los últimos años en la implementación de **SOC virtuales (vSOC)** en las entidades locales, gracias a los cuales incrementan su visibilidad e información sobre vulnerabilidades, fallos e incidentes, así como aumentan su capacidad de despliegue, protección y actuación.

Además, unas vez adscritos a los diferentes vSOC implantados, estos ayuntamientos y diputaciones pasan a formar parte de la comunidad de referencia del CCN-CERT, basada en la cooperación con terceras entidades y organismos, a los que ofrece su colaboración para contrarrestar y mitigar las ciberamenazas. Esta cooperación tiene un valor fundamental, pues promueve el intercambio de información sobre incidentes, lo cual permite mejorar y agilizar la detección y actuación frente a posibles ataques.

Otra de las medidas en la mencionada línea consiste en "desarrollar catálogos de productos y servicios cualificados y certificados, para su empleo en los procesos de contratación del sector público y de los servicios esenciales". En este sentido, cabe mencionar que la evaluación y certificación de un producto o servicio de seguridad TIC es una responsabilidad asignada al CCN. Por ello, el Organismo dispone de la guía CCN-STIC 105 Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC), un documento que lleva elaborando y actualizando de forma periódica desde hace años, con la finalidad de ofrecer a los organismos de la Administración un conjunto de productos o servicios STIC de referencia y que han sido certificadas.

La creación del Organismo de Certificación y del CCN-CERT ha supuesto la respuesta más importante en los últimos años para hacer frente a las ciberamenazas

Por otro lado, en 2006 nacía, con el objetivo de cumplir con una de las principales responsabilidades asignadas al CCN en el mencionado RD, un organismo que ha sido clave en la valoración y acreditación de la capacidad de un producto para manejar información de forma segura: el **Organismo de Certificación (OC)** de la seguridad de los productos y sistemas. Su creación, así como la del CCN-CERT ha supuesto la respuesta más importante en los últimos años para afrontar las ciberamenazas.

Línea de acción 7 – Desarrollar una cultura de ciberseguridad

El objetivo marcado en esta línea se debe a que muchas de las medidas de protección frente a la rápida evolución de las amenazas dependen de los propios usuarios, quienes a pesar de haber sabido integrar las tecnologías en su día a día, desconocen los riesgos asociados a estas. Para que esta realidad cambie, el CCN-CERT ha llevado a cabo desde sus orígenes numerosas acciones de sensibilización y divulgación de buenas prácticas, para lo cual ha sido clave tener una importante presencia en Internet, medio cada vez más utilizado para informarse.

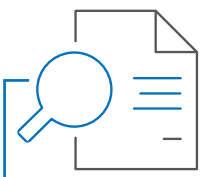
Por este motivo, el CCN, a través del CCN-CERT, decidió hace años crear un perfil de usuario en las redes sociales **LinkedIn**, **Twitter**, **YouTube** y **Telegram**, canales que, a día de hoy, suponen uno de los principales medios a través de los cuales el CCN-CERT comunica sus actividades, con un público de más de 22.500 seguidores en LinkedIn y más de 21.500 en Twitter.

Siguiendo esta misma línea, el departamento puso en marcha en 2017 la **Plataforma de desafíos Atenea**, donde los usuarios pueden demostrar sus conocimientos y destrezas resolviendo retos de distinta dificultad y diversas temáticas. Ante el éxito de acogida que tuvo, en 2018 se lanzó una nueva plataforma con un nivel más básico para fomentar el conocimiento entre usuarios menos entendidos: **Atenea Escuela**.

Por último, una de las más recientes iniciativas puestas en marcha por parte del CCN para educar y formar en ciberseguridad ha sido la creación de **ÁNGELES**, un portal con numerosos recursos destinados a incrementar los conocimientos en esta materia. Cabe destacar su sección de **Ciberconsejos**, donde se recopilan recomendaciones para evitar las ciberamenazas, luchar contra la desinformación, así como hacer un uso seguro de las redes sociales y las tecnologías.

> El Centro Criptológico Nacional dispone de numerosos recursos para que la sociedad en su conjunto aprenda a hacer un uso seguro de las TIC

Todas estas iniciativas contribuyen a que nuestra sociedad alcance y mantenga los conocimientos, habilidades y capacidades profesionales, pues solo así, como señala la Estrategia, "se podrá responder a los grandes retos de la ciberseguridad". ●



PARA SABER MÁS

- Centro Criptológico Nacional: https://www.ccn.cni.es/index.php/es/
- CCN-CERT: https://www.ccn-cert.cni.es/
- CCN-PYTEC: https://www.ccn.cni.es/index.php/es/menu-pytec-es
- Organismo de Certificación (OC): https://www.ccn.cni.es/index.php/es/menu-organismo-de-certificacion-es
- Sistema de Alerta Temprana (SAT): https://www.ccn-cert.cni.es/gestion-de-incidentes/sistema-de-alerta-temprana-sat.html2
- LUCIA: https://www.ccn-cert.cni.es/soluciones-seguridad/lucia.html
- REYES: https://www.ccn-cert.cni.es/soluciones-seguridad/reyes.html
- SOC Virtuales (vSOC): https://www.ccn.cni.es/index.php/es/ccn-cert-menu-es/virtual-soc
- Real Decreto 421/2004, de 12 de marzo: https://www.boe.es/buscar/doc.php?id=-BOE-A-2004-5051
- CCN-STIC 105 Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC): https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion/file.html
- ATENEA: https://atenea.ccn-cert.cni.es/
- ÁNGELES: https://angeles.ccn-cert.cni.es/index.php/es/ciberconsejos/amenazas