Candidatura

Centro Criptológico Nacional

"Veinte años dedicados a la protección y defensa de la ciberseguridad de España"

Premios Socinfo Digital "Ciberseguridad AAPP"

18 de enero de 2024

ÍNDICE

1 Centro Criptológico Nacional

Desde su creación a través del Real Decreto 421/2004, 12 de marzo, hace ahora 20 años, el **Centro Criptológico Nacional** (CCN) del Centro Nacional de Inteligencia (CNI), se ha convertido en un referente nacional e internacional en materia de ciberseguridad en los ámbitos de prevención, detección y respuesta a amenazas. Este RD establecía las funciones y responsabilidades que el CCN ha llevado a cabo durante las dos últimas décadas con un firme compromiso: proteger, defender y fortalecer la ciberseguridad de España ante ciberamenazas que puedan atentar contra la seguridad nacional, el Estado de derecho, la prosperidad económica y el normal funcionamiento de la sociedad y de las administraciones públicas.

Fue el **primer organismo en adquirir competencias en esta materia** y, desde entonces, no ha cesado en su empeño de hacer del ciberespacio español un lugar más seguro y confiable, desplegando un sinfín de acciones dirigidas a la **prevención, protección y respuesta a amenazas**.

Así, presta su apoyo a todo el sector público y colabora con el privado a través de diferentes iniciativas y servicios como la **Capacidad de Respuesta a Incidentes** (CCN-CERT), la **Red Nacional de SOC**, el **Sistema de Alerta Temprana** de intrusiones, la **Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes**, la formación de profesionales TIC, la difusión de más de 500 **guías de ciberseguridad**, el **Catálogo de Productos y Servicios STIC**, la certificación de productos, el desarrollo de **23 herramientas propias** o la organización de las **Jornadas de Seguridad TIC** más importantes de España y Latinoamérica.

2 Servicios, proyectos e iniciativas lideradas por el CCN

2.1. CCN-CERT y Red Nacional de SOC

En cumplimiento de las misiones encomendadas en el Real Decreto 421/2004, a lo largo de las dos últimas décadas, el CCN ha potenciado las acciones de **prevención, detección y respuesta** a los ciberataques, que en estos 20 años han experimentado un notable incremento tanto en volumen y frecuencia como en sofisticación, con agentes de la amenaza cada vez más capacitados a nivel técnico y operativo.

Así, en 2006 el Centro Criptológico Nacional creó el **CCN-CERT**, su Capacidad de Respuesta a Incidentes de Seguridad con responsabilidad en ciberataques sobre sistemas clasificados y sobre sistemas del sector público y de empresas y organizaciones de interés estratégico para el país. Desde su creación ha gestionado más de **500.000 incidentes** (107.777 en el año 2023). De ellos, el 34% fueron clasificados con un nivel de peligrosidad alto, muy alto o crítico.

Precisamente, esta experiencia adquirida en la respuesta a ciberamenazas, ha llevado al CCN a liderar la Red Nacional de SOC, proyecto pionero en Europa para coordinar la colaboración y el intercambio de información entre este tipo de centros en España. Un paso más en esta línea será la futura integración con otros foros nacionales como CSIRT.es (también promovido por el CCN desde 2008) o internacionales como la Red Europea de SOC (ENSOC).

Además, cabe destacar su impulso al desarrollo de nuevas herramientas tecnológicas, entre las que destacan sus **23 soluciones de seguridad** (LUCIA, REYES, IRIS, microCLAUDIA, OLVIDO, INES, ÁNGELES, entre otras); el **Sistema de Alerta Temprana** para la detección en tiempo real de amenazas, que a día de hoy cuenta con más de 500 sondas desplegadas en la Administración; o el desarrollo de la **Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.**

3 Propulsor de la normativa de seguridad

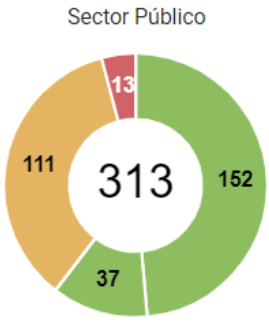
El CCN ha participado en la redacción de toda la legislación española aplicable en la materia. Ha sido esencial su contribución al desarrollo a las dos **Estrategias Nacionales de Ciberseguridad** existentes hasta la fecha (la primera publicada en el año 2013; y la segunda, en 2019).

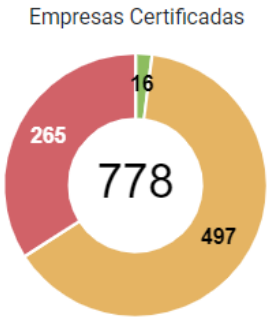
Además, el CCN trabajó en el **Real Decreto 43/2021**, de 26 de enero, a lo largo de todo el año 2020 con el fin de desarrollar la **trasposición de la Directiva NIS al ordenamiento jurídico español** en lo relativo al marco estratégico e institucional de seguridad de las redes y sistemas de información, la supervisión del cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales, y la gestión de incidentes de seguridad.

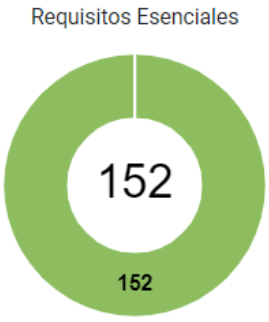
- **Esquema Nacional de Seguridad**

La participación del Centro Criptológico Nacional en el desarrollo e implantación del Esquema Nacional de Seguridad (ENS) —una legislación única en Europa, convertida en un marco normativo de referencia— ha sido clave para proporcionar al sector público en España un planteamiento común de seguridad para la protección de la información que maneja y los servicios que presta.

A finales de 2023, un total de 1.091 organizaciones estaban certificadas en el ENS: 313 del sector público y 778 del sector privado.







4 Certificación de productos y CPSTIC

El CCN constituye el Organismo de Certificación del **Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información**, de aplicación a productos y sistemas en su ámbito. Con el objetivo de impulsar el empleo de tecnologías de seguridad confiables, lidera la promoción y desarrollo de productos TIC confiables, verifica y acredita la seguridad de dichos productos, valora y acredita la capacidad de los productos de cifra para procesar, almacenar o transmitir información de forma segura, y desde 2017 elabora el Catálogo de Productos y Servicios STIC (CPSTIC) en el que se recoge un listado en constante actualización de productos y servicios de seguridad TIC con unas garantías contrastadas por el propio CCN. En estos momentos el Catálogo recoge 325 productos cualificados; 96 aprobados y 8 de Conformidad y Gobernanza.

5 Formación y concienciación

Una de las principales misiones del CCN es llevar a cabo **iniciativas de concienciación y formación en ciberseguridad** y, para ello, colabora con los organismos públicos en la **formación y capacitación de personal** especialista en el campo de la seguridad de los sistemas de las tecnologías de la información y la comunicación, y en la acreditación y auditoría de sistemas. Así, durante el año **2023, más de 32.955 personas** disfrutaron de alguna de las modalidades de formación ofrecidas: Cursos STIC (en colaboración con el INAP), Cursos Ad-Hoc o webinars.

Además, ha publicado y compartido centenares de normas, instrucciones, informes, y recomendaciones, con más de **550** Guías CCN-STIC publicadas y descargadas de su portal un total de **688.070** veces.

- **Portal Ángeles**

Con el deseo de promover la cultura de ciberseguridad, el Centro Criptológico Nacional puso en marcha, en octubre de 2020, el portal web de **ÁNGELES**, su solución dedicada íntegramente a la formación, concienciación, capacitación y talento de profesionales en esta materia.

En él se incluyen los diferentes cursos ofrecidos por el CCN, tanto de forma presencial como online y con todos los niveles; desde la formación básica, hasta los cursos de gestión o de especialización en diferentes materias. Esta sección engloba los diferentes Cursos STIC desarrollados en colaboración con el Instituto Nacional de Administración Pública (INAP), así como los webinars (sesiones formativas en directo).

En total, en 2023 había 32.955 personas registradas en este portal en el que también se encuentran las **plataformas de desafíos** del CCN, **ATENEA y ATENEA Escuela** (a través de las cuales los profesionales se enfrentan a diferentes retos, en función de su destreza) y una sección de **Concienciación y sensibilización**: en el que se recopilan diferentes recursos para un uso seguro de las TIC, como **ciberconsejos**, **recomendaciones y guías de buenas prácticas**.

6 Cultura de ciberseguridad

El Centro Criptológico Nacional acomete numerosas **acciones encaminadas a promover una cultura de ciberseguridad en España**, conscientes de su importancia para prevenir gran parte de las ciberamenazas que afectan a la sociedad en su conjunto.

- **Foro Nacional de Ciberseguridad**

El Foro Nacional de Ciberseguridad, cuya Vicepresidencia Segunda está asignada al CCN, se constituyó en 2020 con el objetivo de fomentar la cultura de ciberseguridad, ofrecer apoyo a la Industria e I+D+i y promover la formación y el talento, todo ello a través de un entorno de colaboración público-privada y bajo el paraguas del Consejo de Seguridad Nacional.

- **Eventos**

Desde el año 2007, el CCN-CERT organiza las **Jornadas STIC CCN-CERT** que se han convertido en el principal encuentro de expertos en ciberseguridad del país y que aglutina a los principales responsables de seguridad de las Administraciones Públicas y de empresas de interés estratégico. Dado el carácter abierto y transfronterizo del ciberespacio, en marzo de 2021, se **decidió internacionalizar el evento** y se celebraron las primeras Jornadas STIC. Capítulo Colombia, consciente de la necesidad de forjar **alianzas entre los países Iberoamericanos** y configurar así un escudo protector común. Los resultados obtenidos en cada nueva edición lo avalan hoy como el Congreso más importante en la región.

Además, el CCN organiza los **Encuentros CCN**, otro gran evento de carácter anual capaz de reunir a la Comunidad de la Ciberseguridad en torno a 4 módulos temáticos:

- Encuentro del ENS

  Ofrecer un marco común de seguridad al sector público y promover, al mismo tiempo, el intercambio de conocimiento entre las administraciones públicas españolas

- Jornada del SAT

  Un espacio privado, reservado para las organizaciones del sector público, en el que se da a conocer el estado de la amenaza, se ofrecen las últimas novedades desarrolladas por el CCN para mejorar su servicio y se intercambian impresiones para poder avanzar en la protección y defensa del ciberespacio.

- Encuentro de la RNS

  Reunir a los organismos y organizaciones adheridos a la Red Nacional de SOC y mostrar las novedades de esta iniciativa, impulsada por el Centro Criptológico Nacional, como instrumento para coordinar la colaboración y el intercambio de información entre todos los Centros de Operaciones de Ciberseguridad del sector público español.

- Encuentro QTEC

  Crear una comunidad nacional de tecnologías cuánticas, el CCN organiza el Encuentro QTEC, en el que se establece un foro multidisciplinar y colaborativo entre los distintos actores en tecnologías cuánticas

7 Otras actuaciones

7.1 Crisis “Wannacry”

En el año 2017, la acción del CERT fue fundamental en el desarrollo de **#NoMoreCry**, la **primera vacuna frente al ransomware Wannacry**, a la cual se aferraron numerosas organizaciones nacionales e internacionales. Precisamente, este descubrimiento fue el origen del centro de vacunación del CCN-CERT, **MicroCLAUDIA**, que actualmente protege a centenares de equipos de la Administración española.

7.2 Pandemia de la COVID-19

Desde los primeros días de la pandemia y ante el preocupante incremento del número de ciberataques registrados, el Centro Criptológico Nacional reforzó todas sus

capacidades para la defensa del ciberespacio español y, en especial, de su sector público y de los sectores estratégicos, con prioridad absoluta en el de la salud.

- El CCN-CERT fue **alertando a su Comunidad** de la detección de nuevas campañas de malware que empleaban temáticas relacionadas con la pandemia del coronavirus y se recopilaron en tres listas negras los **indicadores de compromiso** que permitían la detección y bloqueo de muchas de las campañas que se aprovechaban de la situación provocada por la crisis de la COVID-19.
- El CCN **llevó a cabo auditorías de seguridad** en 23 organismos y 185 hospitales y agencias, con el objetivo de reducir su superficie de exposición. Del mismo modo, dado el incremento de exámenes online, el CCN **protegió a las instituciones de enseñanza**, asegurando las plataformas de 25 universidades para que estas fueran resilientes a ataques de denegación de servicio.
- Además de adaptar las **acciones formativas** previstas a la modalidad online, el CCN organizó 30 webinars especialmente enfocados a la protección del teletrabajo. Además, publicó varios **documentos sobre los principales aspectos originados por esta crisis** y vinculados a la ciberseguridad, entre los que destacan: el Informe de Buenas Prácticas CCN-CERT BP/18 "Recomendaciones de Seguridad para situaciones de teletrabajo y refuerzo en vigilancia" y el documento sobre Acceso remoto seguro.
- En el portal del CCN-CERT se creó un **espacio de colaboración**, donde se compartió la labor llevada a cabo desde las Administraciones Públicas (AGE, CCAA y Entidades Locales) frente a la crisis generada por la COVID-19 y se desarrollaron diversas **campañas de concienciación**, en las que se compartieron diferentes recomendaciones de ciberseguridad para evitar los riesgos asociados al incremento de las campañas de malware. Asimismo, se creó un hilo en redes sociales bajo los hashtags #NoTeinfectesConElMail y #CiberCOVID19, con información actualizada sobre la detección de nuevas amenazas.

8 Nuevos retos

El imparable proceso de transformación digital en el que España y el mundo entero se encuentran inmersos exige **incrementar de forma notable los esfuerzos y recursos** necesarios para que la ciberseguridad guíe la implementación, aplicación y funcionamiento de este nuevo modelo porque **no hay transformación digital posible sin ciberseguridad**. Las **amenazas y vulnerabilidades se multiplican** en un mundo cada vez más digital y conectado.

En este escenario, los 20 años de experiencia que acumula el Centro Criptológico Nacional son y serán cruciales en la evolución, adaptación y respuesta de la ciberseguridad nacional a los retos que plantea un ciberespacio trasversal y global. El Centro Criptológico Nacional seguirá trabajando para hacer de él un lugar cada vez más seguro y confiable.