Aproximación española
a la Ciberseguridad

Decálogo
CCN-CERT
Junio 2019

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2019.05.31 12:14:10 +02'00'

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

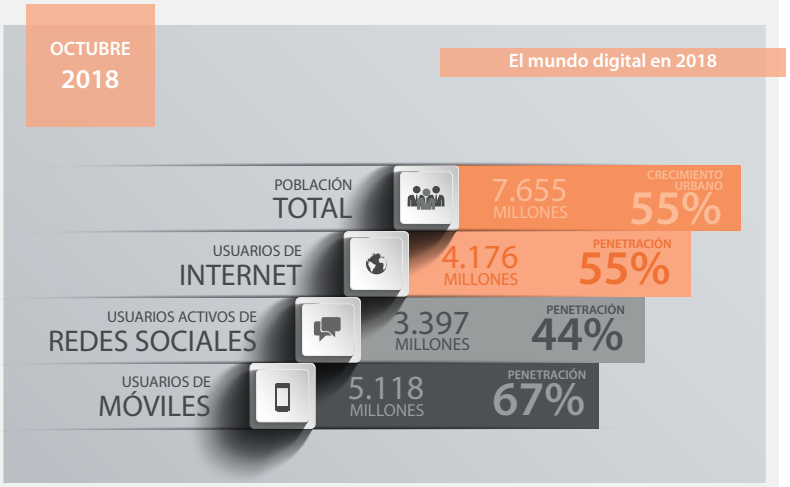
AVISO LEGAL

ÍNDICE

Introducción

Un nuevo espacio que proteger y nuevos derechos que defender

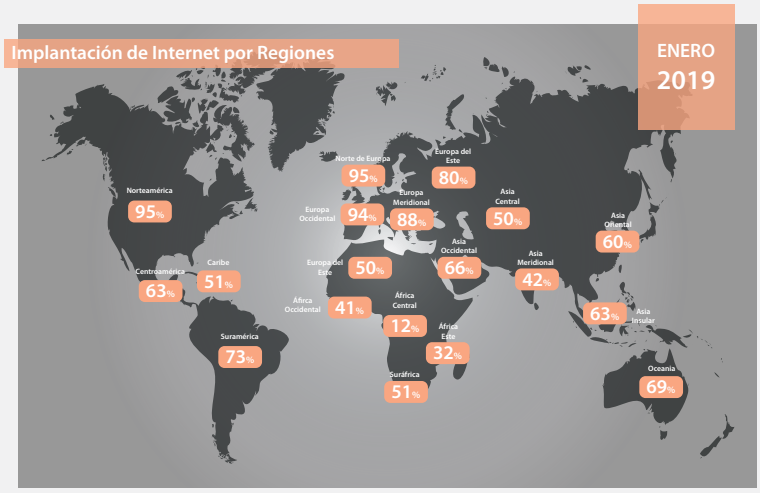
El avance de las Tecnologías de la Información y la Comunicación (TIC) presenta un nuevo paradigma. La expansión de internet, con más de 4.000 millones de usuarios en todo el mundo[1] −es decir, el 53% de la población mundial−, ha impulsado una profunda transformación de las estructuras mundiales. Los servicios públicos, la educación, la salud, los medios de comunicación, el ocio, el transporte, la cultura y, por supuesto, las relaciones personales han experimentado un proceso de cambio absoluto, debido a la influencia que la tecnología ejerce sobre la sociedad. Tanto es así que existe incluso una nueva realidad: el **ciberespacio**.



Este entorno global plantea un escenario de oportunidades económicas y sociales de gran alcance. Sin embargo, también conlleva una serie de riesgos, que se incrementan día a día. Las amenazas del ciberespacio, favorecidas por la rentabilidad económica o política, el bajo coste de las herramientas empleadas y la posibilidad de actuar desde cualquier lugar del mundo de manera anónima, se dirigen y afectan transversalmente a los sectores público y privado, así como a los ciudadanos. En este contexto, los ciberdelincuentes, los hacktivistas o los propios estados, son capaces de explotar las vulnerabilidades tecnológicas con el objeto de recabar información, sustraer activos de gran valor y amenazar servicios básicos para el normal funcionamiento de un país.

1-. Global Digital Report 2019
(https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates/)

Así pues, garantizar e implementar **seguridad en el ciberespacio**, al tiempo que se **respeta la privacidad y la libertad**, se ha convertido en una de las prioridades estratégicas de los países más desarrollados, debido a su impacto directo en la seguridad nacional, en la competitividad de las empresas, y en la prosperidad de la sociedad en su conjunto. El mundo ciber exige un **compromiso constante** ante la evolución tecnológica y la creciente sofisticación de los ataques.



La adaptación a este escenario implica mejorar las capacidades de prevención y vigilancia y diseñar respuestas cada vez más eficaces frente a los ataques. Asimismo, requiere de un mayor grado de coordinación y cooperación. Por un lado, a nivel nacional, entre todos los niveles de la Administración del Estado y las empresas y entidades privadas; por otro, a nivel internacional, con países y organizaciones multilaterales.

Precisamente, en el marco de la cooperación, tanto nacional como internacional, se enmarca este documento. Solo a través del diálogo y la colaboración en materia de ciberseguridad, haciendo frente de forma conjunta a los nuevos desafíos, se favorecerá el desarrollo y bienestar de los Estados, y por ende de sus ciudadanos.

CCN-CERT, un caso de éxito en ciberseguridad

La protección y la defensa de un ciberespacio seguro y confiable se ha introducido como objetivo en la agenda de la inmensa mayoría de los países e instituciones supranacionales. No obstante, en función de las características de cada uno, de los recursos disponibles o del grado de madurez de uno u otro servicio, la implementación de las medidas más adecuadas para conseguir este objetivo será diferente.

Con este documento se pretende realizar una aproximación al desarrollo, implantación y mejora de un esquema general de Ciberseguridad Nacional, que permita facilitar esta tarea, independientemente del grado de madurez de cada Estado y de los agentes que participen en ella. Partiendo del desarrollo realizado en España en los últimos 20 años, y con el caso concreto del **CCN-CERT**, se busca aportar un modelo de **desarrollo** para afrontar, a nivel nacional, los diferentes desafíos que emanan de la protección de los Sistemas de un país y, por extensión, de su Administración, empresas y ciudadanos. La capacidad de los Estados para hacer frente a los retos que plantea la ciberseguridad debe ser un elemento estratégico de primer orden, tanto para protegerse como para progresar en el complejo panorama geopolítico actual.

Esta aproximación, aquí expuesta, no pretende ser un modelo estático, pues cada país presenta ciertas singularidades y un estado de madurez diferente. Este documento aspira a ser una referencia que contribuya a la creación de un programa nacional sobre ciberseguridad en el que se ofrezca una **visión holística** de esta materia. Para ello, se recogen un conjunto de parámetros aceptados a la hora de implementar una política de ciberseguridad nacional, y que se pueden ajustar a las características y necesidades de cada Estado.

El reto común de diseñar políticas que preserven los intereses nacionales, en el ámbito político, económico y social y el desafío de hacer frente a los riesgos y amenazas que se ciernen sobre el ciberespacio, requiere una política que, englobada en una **Estrategia de Ciberseguridad Nacional**, posibilite una correcta plasmación de todos sus objetivos. Asimismo, demanda la regulación de los procedimientos de actuación ante los distintos desafíos, la coordinación de los distintos agentes encargados de su implementación y la creación de los organismos responsables de dicha coordinación.

Esta política ha de estar alineada con la realidad empresarial de cada país. Debe incrementar las capacidades de prevención, detección, respuesta y recuperación ante las amenazas; impulsar la seguridad y la resiliencia de las Tecnologías de la Información y la Comunicación en el sector privado; y concienciar de la importancia de la ciberseguridad y del uso responsable de las tecnologías. Todo ello, acompañado de controles de seguridad en las organizaciones; controles de índole técnica, organizativa y jurídica, tanto a nivel global −para preservar la seguridad nacional− como a nivel interno −para que las empresas puedan seguir operando sin ver afectados sus procesos de negocio, sus activos de información y los activos de sus clientes−.

En definitiva, se ha elaborado un decálogo que emplea como ejemplo los pasos dados por el Centro Criptológico Nacional y su Capacidad de Respuesta a Incidentes. Su objetivo es orientar la acción de cada Estado en su respuesta a los desafíos actuales a través del empleo flexible y eficaz de los recursos disponibles.

Con este documento se pretende realizar una aproximación al desarrollo, implantación y mejora de un esquema general de Ciberseguridad Nacional, que permita facilitar esta tarea, independientemente del grado de madurez de cada Estado y de los agentes que participen en ella.

La aproximación española a la ciberseguridad incluye los siguientes diez apartados:

1. Establecimiento de la visión, el alcance, los objetivos y las prioridades: **Estrategia de Ciberseguridad**.

2. Instauración de una estructura de gobierno clara, que identifique e involucre a las partes interesadas: **Gobernanza**

3. Hacer un balance de las políticas, regulaciones y capacidades existentes: **Desarrollo reglamentario posibilista**. Apoyo en un marco jurídico operativo y eficaz.

4. Incremento de la capacidad de prevención, detección y respuesta ante ciberamenazas, creando **CSIRT de referencia y por sectores**.

5. Desarrollo e implementación de Sistemas de Alerta Temprana. **Capacidad de Detección** y establecimiento de mecanismos de notificación de incidentes.

6. **Incremento de la vigilancia**, con un servicio de **evaluación continua** y **cibervigilancia** basado en Centros de Operaciones de Ciberseguridad (**SOC**), que permitan conocer en cada momento la superficie de exposición ante una posible amenaza y así asignar los recursos de manera óptima y priorizada.

7. **Fomento, desarrollo y mantenimiento de perfiles profesionales cualificados** en todos los niveles (dirección, gestión, implantación y usuarios) para protegerse de las ciberamenazas. La **búsqueda de talento** se ha convertido en un elemento crítico.

8. Se impulsarán y liderarán acciones destinadas a reforzar la **colaboración público-privada** y la seguridad y robustez de las redes, productos y servicios de las TIC empleados por el sector industrial. Institucionalizar la cooperación entre los organismos públicos y la empresa privada como clave para construir comunidad.

9. Implementación de mecanismos confiables **de intercambio de información** entre organismos, públicos y privados, tanto de análisis de ciberamenazas como de notificación de ciberincidentes, para **generar confianza.**

10. **Comunicación y promoción,** orientada a la consecución de objetivos estratégicos. Todo ello, conscientes de la necesidad de darse a conocer, difundir servicios hasta alcanzar el reconocimiento y confianza de toda su comunidad, convirtiéndose en punto de referencia en materia de ciberseguridad.

1 | Necesidad de una Estrategia de Ciberseguridad 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.

En Estados Unidos, en 2009, el Departamento de Defensa creó el US Cyber Command (CYBERCOM) para controlar las capacidades de ciberdefensa y ciberguerra del Ejército y, en 2011, publicó su Estrategia. En Europa, la Agencia Europea de Ciberseguridad (ENISA) elaboró una Guía de Buenas Prácticas en Estrategias Nacionales de Ciberseguridad2. Por su parte, en el Reino Unido se editó la primera Estrategia de Ciberseguridad Nacional.

Del mismo modo, la Organización de Estados Americanos (OEA) desarrolló varios programas para promover la Estrategia Interamericana para Combatir las Amenazas de la Seguridad Cibernética y, en 2011, Colombia presentó su Estrategia de Ciberseguridad y Ciberdefensa del Estado Colombiano.

Así pues, en España, ya en 2011, era evidente la necesidad de desarrollar un sistema nacional de ciberseguridad que fomentara la integración de todos los actores e instrumentos, públicos y privados, con el fin de preservar el ciberespacio de todo tipo de riesgos y ataques y, por tanto, defender los intereses nacionales y contribuir al desarrollo de la Sociedad Digital. Un **modelo de ciberseguridad integrado** que, dirigido por el Gobierno, garantizara al país su seguridad y su progreso, a través de la adecuada coordinación de todas las Administraciones Públicas entre sí, con el sector privado y con los ciudadanos; y que canalizase las iniciativas y esfuerzos internacionales en defensa del ciberespacio.

De este modo, y después de varios años de intenso trabajo a través de diferentes grupos y organismos, en **abril de 2019** se publicó la **Estrategia de Ciberseguridad Nacional**[3] , alineada con la Estrategia de Seguridad Nacional, que contemplaba la ciberseguridad dentro de sus doce ámbitos de actuación (actualizada en 2018).

Estrategia de Ciberseguridad Nacional

La Estrategia Nacional de Ciberseguridad, aprobada el 30 de abril de 2019, desarrolla las previsiones de la Estrategia de Seguridad Nacional de 2017 en el ámbito de la ciberseguridad. Considerando los objetivos generales, el objetivo del ámbito y las líneas de acción establecidas para conseguirlo, el documento se estructura en cinco capítulos:

- **El ciberespacio, más allá de un espacio común global**, que proporciona una visión de conjunto del ámbito de la ciberseguridad, los avances realizados en materia la materia desde la aprobación de la Estrategia de 2013, las razones que afianzan la elaboración de la Estrategia Nacional de Ciberseguridad 2019, así como las principales características que impulsan su desarrollo.
- **Las amenazas y desafíos en el ciberespacio**, determina las principales amenazas del ciberespacio que derivan de su condición de espacio global común, de la elevada tecnificación y de la gran conectividad que posibilita la amplificación del impacto ante cualquier ataque. Clasifica estas amenazas y desafíos en dos categorías: por un lado, las que amenazan a activos que forman parte del ciberespacio; y por otro, aquellos que usan el ciberespacio como medio para realizar actividades maliciosas e ilícitas de todo tipo.
- **Propósito, principios y objetivos para la ciberseguridad**, aplica los principios rectores de la Estrategia de Seguridad Nacional 2017 (Unidad de acción, Anticipación, Eficiencia y Resiliencia) a cinco objetivos específicos.
- **Líneas de acción y medidas**, donde se establecen siete líneas de acción y se identifican las medidas para el desarrollo de cada una de ellas.
- **La ciberseguridad en el Sistema de Seguridad Nacional**, define la arquitectura orgánica de la ciberseguridad. Bajo la dirección del Presidente del Gobierno, la estructura se compone de tres órganos: el Consejo de Seguridad Nacional, como Comisión Delegada del Gobierno para la Seguridad Nacional; el Consejo Nacional de Ciberseguridad, que apoya al Consejo de Seguridad Nacional y asiste al Presidente del Gobierno en la dirección y coordinación de la política de Seguridad Nacional en el ámbito de la ciberseguridad, y fomenta las relaciones de coordinación, colaboración y cooperación entre Administraciones Públicas y entre estas y el sector privado, y el Comité de Situación que, con el apoyo del Departamento de Seguridad Nacional, apoyará a la gestión de las situaciones de crisis en cualquier ámbito, que por su transversalidad o dimensión, desborden las capacidades de respuesta de los mecanismos habituales.

2.-NCSS Good Practice Guide (https://www.enisa.europa.eu/publications/ncss-good-practice-guide)
3.-BOE https://www.boe.es/boe/dias/2019/04/30/pdfs/BOE-A-2019-6347.pdf

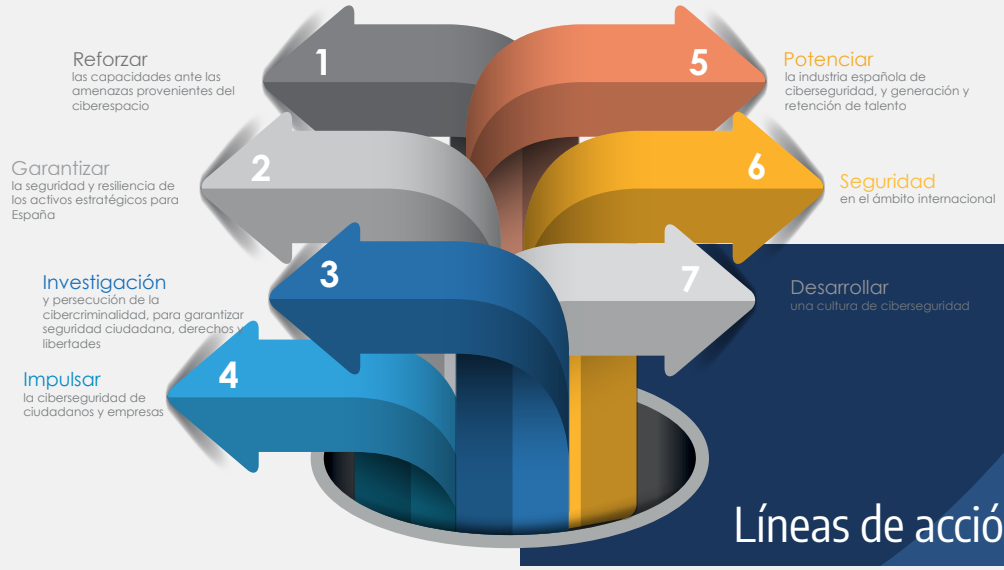
Objetivo General

España garantizará el uso seguro y fiable del ciberespacio, protegiendo los derechos y las libertades de los ciudadanos y promoviendo el progreso socio económico.

Objetivos Específicos

Estrategia de Ciberseguridad Nacional

1. Seguridad y resiliencia en sector público y servicios esenciales
2. Uso seguro y fiable del ciberespacio frente a su uso ilícito o malicioso
3. Protección del ecosistema empresarial y social y de los ciudadanos
4. Cultura y compromiso con la ciberseguridad y potenciación de las capacidades humanas y tecnológicas
5. Seguridad del ciberespacio en el ámbito internacional



Líneas de acción

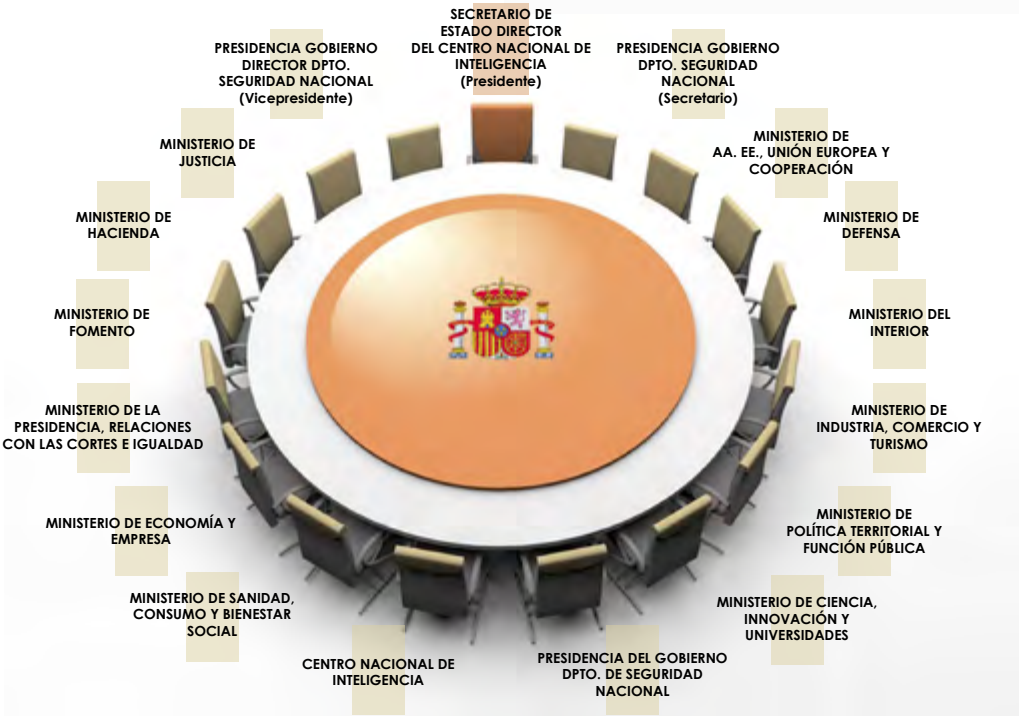
La experiencia del Centro Criptológico Nacional (CCN) al frente del Consejo Nacional de Ciberseguridad permite al CCN ofrecer su apoyo y contribución a distintos Estados en sus esfuerzos para el desarrollo de sus respectivas estrategias de ciberseguridad

2 | La Gobernanza de la Ciberseguridad

La visión estratégica proporciona un panorama amplio del entorno de la ciberseguridad y permite una mejor preparación ante los posibles riesgos y amenazas futuras. Sin embargo, no es suficiente. Se requiere priorizar los recursos disponibles y organizar la toma de decisiones a través de un sistema institucional centralizado, que asegure una acción integrada, eficaz y, sobre todo, coordinada.

Es preciso, de un lado, fortalecer las capacidades de los gobiernos, mejorando los instrumentos puestos a su disposición y, de otro, fijar los **actores de la ciberseguridad** que definan el sentido de la dirección a tomar, y que incluyan la función que cada uno debe desempeñar.

La Estrategia desarrolla el marco institucional de la ciberseguridad, compuesto por las **autoridades competentes** y los **CSIRT de referencia,** por una parte, y la **cooperación público-privada**, por otra. Así, pues, en la gobernanza de la ciberseguridad conviene establecer una **estructura nítida y centralizada**, en la que se definan los distintos **agentes** que la componen y su rol correspondiente.



La composición del **Consejo Nacional de Ciberseguridad (CNCS**), presidido por el Secretario de Estado Director del Centro Nacional de Inteligencia (CNI) y Director del Centro Criptológico Nacional (CCN), refleja el espectro de los ámbitos de los departamentos, organismos y agencias de las Administraciones Públicas con competencias en materia de ciberseguridad, aunque su estructura es flexible y prevé la incorporación de otros representantes, autonómicos y del sector privado, según la naturaleza de los temas que vayan a ser tratados.

De esta manera, el Consejo Nacional de Ciberseguridad contribuye a reforzar las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias en materia de ciberseguridad, así como entre los sectores públicos y privados, y facilita la toma de decisiones del propio Consejo mediante el análisis, estudio y propuesta de iniciativas tanto en el ámbito nacional como en el internacional. Este Consejo es, además, el **punto único de contacto** a la hora de tramitar incidentes con impacto transfronterizo.

Las **autoridades competentes** ejercen las funciones de vigilancia y aplican el régimen sancionador cuando procede, impulsando la subsanación de la infracción antes que su castigo. Asimismo, son responsables de promover el desarrollo de las obligaciones y medidas de seguridad a aplicar, evitando crear obligaciones duplicadas, innecesarias o excesivamente onerosas.

Por último, los **CSIRT** (Computer Security Incident Response Team) son la puerta de entrada de las notificaciones de incidentes, lo que permite organizar rápidamente una respuesta oportuna. Además, se ha de prever la utilización de una plataforma común para la notificación de incidentes a la autoridad competente, destinataria final de las notificaciones, a través de los CSIRT de referencia.

2.1. Actores en la Ciberseguridad Nacional

Dentro de la estructura desarrollada para la implantación de forma coherente de la ciberseguridad nacional, varios han sido los actores que se han formado a lo largo de los últimos quince años:

1 **Centro Criptológico Nacional (CCN)**, adscrito al **Centro Nacional de Inteligencia (CNI)**, cuya Ley reguladora (Ley 11/2002, de 6 de mayo) encomienda a dicho Centro el ejercicio de las funciones relativas a la seguridad de las Tecnologías de la Información y de protección de la información clasificada, a la vez que se confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional. Por ello, el CCN comparte con el CNI medios, procedimientos, normativa y recursos. En el **RD 421/2004** se regulan sus funciones.

Capacidad de Respuesta a Incidentes del Centro Criptológico Nacional (CCN-CERT), creado en el año 2006, como CERT Gubernamental Nacional español, y cuya misión es contribuir a la mejora de la ciberseguridad española, al ser el centro de alerta y respuesta nacional que coopera y ayuda a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Organismo de Certificación (OC) del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, de aplicación a productos y sistemas (Orden PRE/2740/2007). El OC del CCN realiza tres tipos de certificación en función de los aspectos de seguridad que se evalúen: Certificación Funcional, Criptológica y TEMPEST.

2 **INCIBE-CERT: Instituto Nacional de Ciberseguridad**, anteriormente Instituto Nacional de Tecnologías de la Comunicación (INTECO), es una sociedad dependiente del Ministerio de Economía y Empresa a través de la Secretaría de Estado para el Avance Digital. Es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores estratégicos.

INCIBE-CERT, es el centro de respuesta a incidentes de ciberseguridad operado por INCIBE, trabaja para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, aumentar la ciberresiliencia de las organizaciones y el diseño de medidas preventivas para atender a las necesidades de la sociedad en general y, en virtud del Convenio de Colaboración suscrito entre la Secretaría de Estado de Seguridad del Ministerio del Interior y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, a las necesidades de seguridad de las infraestructuras críticas, de apoyo en la investigación y lucha frente a ciberdelitos y ciberterrorismo.

3 **Centro Nacional de Protección de Infraestructuras y Ciberseguridad, CNPIC,** es el órgano responsable del impulso, coordinación y supervisión de todas las políticas y actividades relacionadas con la protección de las infraestructuras críticas españolas y con la ciberseguridad en el seno del Ministerio del Interior, al amparo de la Ley 8/2011, de 28 de abril (Ley PIC) y por el Real Decreto 704/2011, de 20 de mayo, por el que se regula la protección de infraestructuras críticas. El CNPIC depende del Secretario de Estado de Seguridad, máximo responsable del Sistema Nacional de Protección de las Infraestructuras Críticas y de las políticas de ciberseguridad del Ministerio.

La **Oficina de Coordinación Cibernética (OCC)** se creó en 2015, como canal específico de coordinación y comunicación entre los Centros de Respuesta a Incidentes Cibernéticos (CSIRT) nacionales de referencia y la Secretaría de Estado de Seguridad. Además, la OCC se establece como punto de contacto nacional de coordinación operativa para el intercambio de información con la Comisión Europea y los Estados miembros en el marco de lo establecido por la Directiva 2013/40/UE, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información.

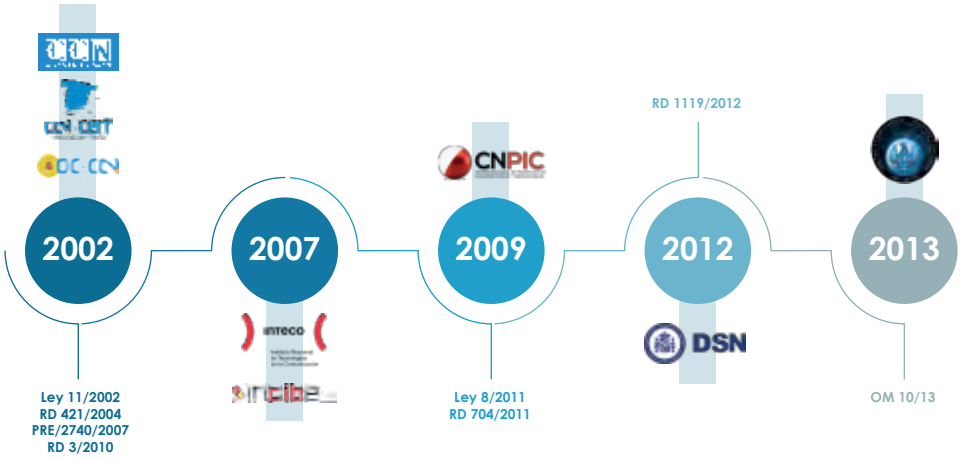
4 **Departamento de Seguridad Nacional, DSN**, del Gabinete de la Presidencia del Gobierno es el órgano de asesoramiento al presidente del Gobierno en materia de Seguridad Nacional. Mantiene y asegura el adecuado funcionamiento del Centro de Situación del Departamento de Seguridad Nacional para el ejercicio de las funciones de **seguimiento y gestión de crisis**, así como las comunicaciones especiales de la Presidencia del Gobierno. Fue creado por el **Real Decreto 1119/2012 de 20 de julio**, de modificación del Real Decreto 83/2012, de 13 de enero, por el que se reestructura la Presidencia del Gobierno.

5 **Mando Conjunto de Ciberdefensa**, es el órgano de la estructura operativa, subordinado al Jefe de Estado Mayor de la Defensa (**JEMAD**), responsable del planeamiento y la ejecución de las acciones relativas a la Ciberdefensa en las redes y sistemas de información y telecomunicaciones del Ministerio de Defensa u otras que pudiera tener encomendadas, así como contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional. Fue creado el 19 de febrero de 2013, a través de la "**Orden Ministerial 10/2013**, por la que se crea el Mando Conjunto de Ciberdefensa".

6 **Unidad de Investigación Tecnológica (UIT)**, que actúa como Centro de Prevención y Respuesta E-Crime del Cuerpo Nacional de Policía. Esta unidad es la encargada de la investigación y persecución de las actividades delictivas que impliquen la utilización de la información y las comunicaciones (TIC) y el ciberdelito de ámbito nacional y transnacional.

7 **Grupo de Delito Telemáticos (GDT)**, creado para investigar, dentro de la Unidad Central Operativa de la Guardia Civil, todos aquellos delitos que se valen de las redes y sistemas de información para su comisión.

Actores en la Ciberseguridad Nacional

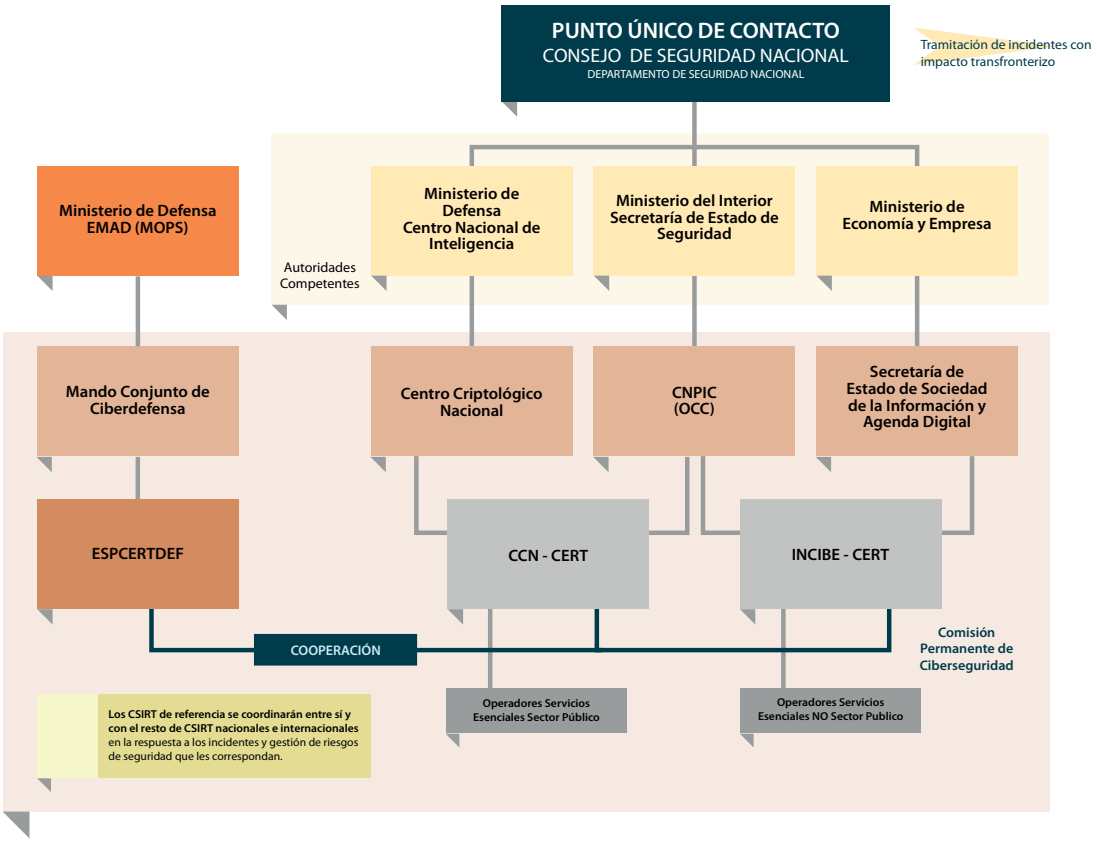


Los organismos aquí citados, adscritos cada uno de ellos a una Autoridad Competente, operan con un CERT/CSIRT de referencia y actúan como componente fundamental de la capacidad nacional de preparación, intercambio de información, coordinación y respuesta.

El desarrollo de capacidades de ciberseguridad, y la experiencia acumulada durante la última década, ha permitido al estado español llegar a un nivel de madurez en el que se han identificado los ámbitos competenciales de los diferentes actores en el panorama de la ciberseguridad nacional, sin que se produzcan solapamientos.

A todo ello ha contribuido, en gran medida, la transposición de la **Directiva UE 2016/1148 del Parlamento Europeo** y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión (conocida como directiva NIS), y su trasposición al reglamento jurídico español (**Real Decreto-ley 12/2018, de 7 de septiembre**, de seguridad de las redes y sistemas de información) que ha permitido identificar a los operadores de servicios esenciales, establecer medidas de seguridad y determinar las autoridades competentes y CERT/CSIRT de referencia asociados.

Actores en la Ciberseguridad Nacional



3 | Marco Regulatorio y desarrollo reglamentario posibilista

En toda actividad en la que se desarrollan interacciones, se requiere de normas que regulen el comportamiento de los sujetos que en ella intervienen. Unas normas que no solo regulen los derechos y deberes, sino que, además, actúen como catalizadoras del sector y favorezcan la creación, el crecimiento y el fortalecimiento de la actividad.

En el caso del sector TIC y su seguridad ha sido necesario que las diferentes leyes existentes se adapten para regular y proteger a los ciudadanos y a las empresas de los ataques cibernéticos, en la medida de lo posible, estableciendo también nuevas normas y protocolos que regulen las situaciones nuevas, no previstas hasta ahora en el mundo físico.

La aproximación a este nuevo marco regulatorio debe contemplar la actualización permanente y posibilista. El cuerpo de leyes, decretos, reales decretos, órdenes ministeriales y reglamentos por las cuales se gobierna en materia de ciberseguridad debe ser ágil y aprovechar las situaciones existentes para conseguir un ciberespacio seguro y confiable, en función de los organismos y entidades que lo conforman.

Así pues, ha sido y es necesario adecuar las legislaciones a la nueva realidad, tanto en el ámbito penal (delitos informáticos, con tipos delictivos específicos), como en el de la seguridad y la protección de los datos personales.

En España, existe el **Código de Derecho de la Ciberseguridad**[4], publicado en el Boletín Oficial del Estado, que cita las principales normas a tener en cuenta con relación a la protección del ciberespacio y para velar por la mencionada ciberseguridad (algunas de las cuales, como la Estrategia de Ciberseguridad, ya ha sido mencionada). Los principales capítulos de este Código son los siguientes:

1. CONSTITUCIÓN ESPAÑOLA
2. NORMATIVA DE SEGURIDAD NACIONAL
3. INFRAESTRUCTURAS CRÍTICAS
4. NORMATIVA DE SEGURIDAD
5. EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD
6. TELECOMUNICACIONES Y USUARIOS
7. CIBERDELINCUENCIA
8. PROTECCIÓN DE DATOS
9. RELACIONES CON LA ADMINISTRACIÓN

4.- https://www.boe.es/legislacion/codigos/codigo.php?id=173_Codigo_de_Derecho__de_la_Ciberseguridad, cuya última modificación es de 25 de mayo de 2018.

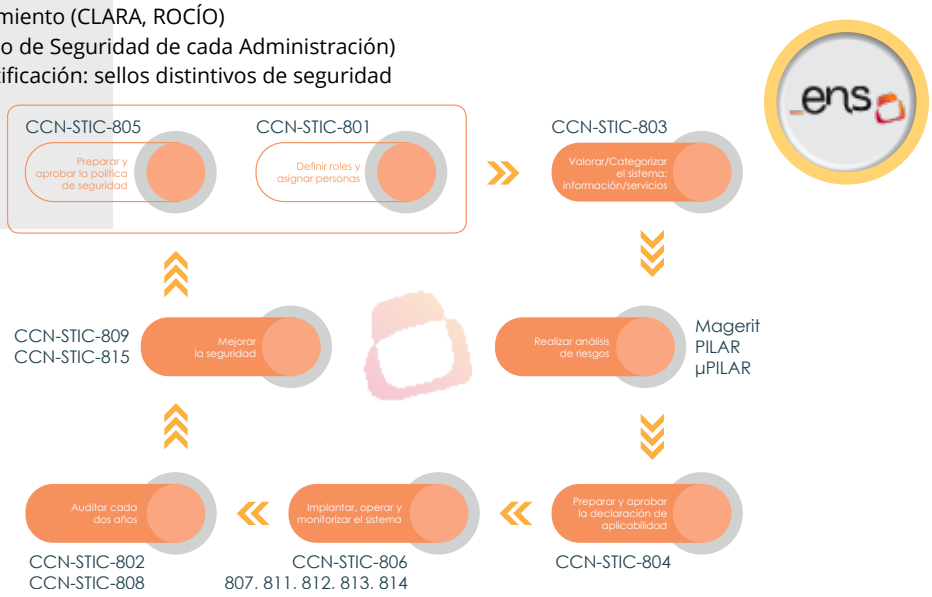
3.1. Esquema Nacional de Seguridad

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos estableció el **Esquema Nacional de Seguridad** que, aprobado mediante **Real Decreto 3/2010, de 8 de enero**, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en el sector público. Su mandato esencial es que todo el sector disponga de una política de seguridad que garantice el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios ofrecidos. En definitiva, sienta las bases necesarias para promover la confianza de los ciudadanos en la utilización de los medios electrónicos, al tiempo que se promueve su uso.

Este Real Decreto, actualizado en el año 2015 y en cuyo desarrollo participó activamente el Centro Criptológico Nacional (CCN), recoge **seis principios básicos** que sirven de guía; **quince requisitos mínimos**, de obligado cumplimiento y que permiten una protección adecuada; y **75 medidas de seguridad** de la información, que abarcan tanto el marco organizativo, como operacional y medidas de protección. Todo ello, **atendiendo a distintos niveles de exigencia**, basados en la categorización de sistemas determinados en función de la información que se maneja y los servicios que se prestan.

El compromiso del CCN con el desarrollo e implantación del ENS se ha concretado en el desarrollo de soluciones y en el apoyo necesario para que se lleve a cabo. No se trata simplemente de fijar requisitos a cumplir, sino que se debe permitir su materialización con la adopción de distintas medidas, imprescindibles para su correcto establecimiento:

- Serie 800 Guías CCN-STIC (53 documentos)
- Auditorías de cumplimiento
- PILAR (análisis de riesgo y continuidad de negocio)
- Soluciones de análisis de cumplimiento (CLARA, ROCÍO)
- INES (Informe Nacional del Estado de Seguridad de cada Administración)
- Conformidad y entidades de certificación: sellos distintivos de seguridad



El ENS ha aportado numerosas ventajas, tanto para el sector público como para el sector privado:

- Sector público
  - Crea un marco de gestión, que incluye los principios básicos y requisitos mínimos necesarios, para una protección adecuada de la información de los ciudadanos. (riesgo residual)
  - Ayuda a cumplir con los requisitos legales para las Administraciones Públicas nacionales, regionales o locales y de sus proveedores.
  - Permite establecer un lenguaje/taxonomía común de peligrosidad y clasificación de incidentes.
  - Establece un cuadro de mandos y métricas, mediante un sistema de trazabilidad y seguimiento de incidentes.
  - Posibilita la integración entre plataformas digitales de la Administración.
- Sector privado
  - Ayuda a desarrollar y demostrar la conformidad con la legislación (Directiva NIS, protección de datos, infraestructuras críticas, etc.).
  - Facilita la contratación de servicios y soluciones tecnológicas con organismos de la Administración.
  - Ofrece un marco de gestión aplicable en su organización.

3.2. Directiva NIS

El ordenamiento jurídico español está sujeto a los actos jurídicos emanados de la Unión Europea (UE): principalmente Reglamentos y Directivas. Estas últimas tienen como finalidad fijar los objetivos concretos, lo que supone que los Estados miembros deben adaptar su legislación interna para la consecución de dichos objetivos, adaptación o trasposición que debe realizar cada Estado con libertad.

En el ámbito de la ciberseguridad, la UE ha trabajado para garantizar una mayor seguridad en las redes y sistemas de información. En este sentido, en febrero de 2013 se publicó la Estrategia de Ciberseguridad de la Unión Europea (Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace). Este documento se complementa con la **Directiva UE 2016/1148 del Parlamento Europeo** y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión (conocida como **Directiva NIS**) y que entró en vigor el 9 de agosto de 2016 (su trasposición al ordenamiento jurídico español se ha producido a través del **Real Decreto-ley 12/2018, de 7 de septiembre**, de seguridad de las redes y sistemas de información).

La Directiva establece requisitos mínimos comunes en materia de desarrollo de capacidades y planificación, intercambio de información, cooperación y requisitos comunes de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales, a quienes insta a adoptar las medidas oportunas para gestionar los riesgos en seguridad y notificar los incidentes que tendrían un efecto perturbador significativo a las Autoridades Nacionales Competentes, proponiendo la creación de una red de cooperación entre todos los diferentes Estados Miembros.

La Directiva, en uno de sus puntos más importantes, hace referencia a la notificación, sin dilación indebida, a la **autoridad competente a través del CSIRT de referencia** de los incidentes que tengan efectos significativos en los servicios esenciales que se presten para que se puedan tomar medidas con carácter institucional o nacional al respecto, en su caso.

En España, el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información transpone al ordenamiento jurídico español esta Directiva, con el objetivo de "regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales, al tiempo que establece un marco institucional para la coordinación entre autoridades competentes y con los órganos de cooperación relevantes en el ámbito comunitario". El CCN-CERT, según lo dispuesto en este Real Decreto-ley, ejercerá la coordinación nacional de la respuesta técnica de los tres CSIRT de referencia establecidos en los supuestos de especial gravedad que reglamentariamente se determinen y que requieran un nivel de coordinación superior al necesario en situaciones ordinarias.

3.3. Cibercrimen

Los delitos e infracciones informáticas/digitales son una forma más de comisión de infracciones ya registradas en el mundo físico (ampliados, eso sí, por su difusión y anonimato). Sin embargo, también es cierto que las nuevas tecnologías e internet han fomentado la aparición de nuevas modalidades de delincuencia, que contemplan ataques a los bienes jurídicos preestablecidos, como la libertad sexual, propiedad, intimidad, honor, etc.

La particularidad de este tipo de delincuencia dificulta la investigación y su posterior esclarecimiento de los hechos. A ello hay que sumarle que la legislación pronto queda obsoleta, debido a la rápida evolución de las nuevas tecnologías y plataformas que se van creando, así como la ausencia de fronteras y, por lo tanto, la inexistencia de una legislación común.

En España, se han realizado inclusiones parciales en el **Código Penal**, en la Ley Orgánica 5/2000, del 12 de enero, reguladora de la responsabilidad penal de los menores; o en el Real Decreto de aprobación de la Ley de Enjuiciamiento Criminal. En estos preceptos se han tenido en cuenta ciberdelitos como la tenencia de pornografía infantil y su difusión, los fraudes por Internet, delitos contra la intimidad, la suplantación de identidad, el espionaje industrial o los derechos de propiedad intelectual.

Asimismo, España ratificó, el 23 de noviembre de 2010, el **Convenio sobre ciberdelincuencia**, también conocido como Convenio de Budapest. El citado acuerdo constituye el primer tratado internacional, que busca hacer frente a los delitos informáticos y a los delitos en internet, mediante la armonización de leyes nacionales de derecho penal de fondo de infracciones y las disposiciones conectadas al área de los delitos informáticos, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones.

El Convenio sobre ciberdelincuencia fue elaborado por el Consejo de Europa en Estrasburgo, con la participación activa de los estados observadores de Canadá, Estados Unidos, Japón, Chile, Costa Rica y Filipinas, y se han previsto nuevas adhesiones de otros Estados no europeos como México, El Salvador, Argentina, Uruguay y Chile.

3.4. Protección de Datos

En España, en el año 1999, se redactó una Ley Orgánica de Protección de Datos de Carácter Personal (L.O. 15/1999, de 13 de diciembre), cuyo Reglamento de desarrollo se plasmó en un Real Decreto en 2007 (RD 1720/2007, de 21 de diciembre).

Sin embargo, desde el 25 de mayo de 2018, todos los países de la Unión Europea deben estar adaptados al **Reglamento General de Protección de Datos** (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE -Reglamento general de protección de datos-).

Aunque tiene similitudes con la norma anterior (LOPD), el nuevo RGPD contiene una serie de importantes cambios que exigen la actualización de los procedimientos en todas las organizaciones. Algunos de los aspectos novedosos de este Reglamento son la figura del Delegado de Protección de Datos; los nuevos derechos que el RGPD otorga a los ciudadanos; el análisis de riesgos y las evaluaciones de impacto o el establecimiento de códigos de conducta.

4 | CERT/CSIRT de referencia y sectoriales

En **1988**, y ante lo que se consideró el primer gran ataque de la historia (gusano Morris), el Departamento de Defensa de Estados Unidos encargó a la Universidad Carnegie Mellon, en Pittsburgh, la creación de un equipo capaz de hacer frente a este nuevo tipo de amenazas. El resultado fue la constitución del denominado *Computer Emergency Response Team* (CERT®); es decir, Equipo de Respuesta a Incidentes de Seguridad Informática.

Bajo estas mismas siglas comenzaron a formarse otros grupos en distintas universidades norteamericanas, encargados de estudiar la seguridad de las redes y ordenadores para proporcionar servicios de respuesta ante incidentes a víctimas de ataques, publicar alertas relativas a amenazas y vulnerabilidades y ofrecer información que ayudara a mejorar la seguridad de estos sistemas.

A su vez, empezó a consolidarse el término CSIRT (*Computer Security and Incident Response Team*), para completar el concepto de CERT® y ofrecer, como valor añadido, los servicios preventivos y de gestión de seguridad. Hoy en día se emplean de forma similar ambos términos.

En España, en el **año 2005**, se aprobó el denominado **Plan Avanza**, para el desarrollo de la Sociedad de la Información y de Convergencia con Europa y entre Comunidades Autónomas y Ciudades Autónomas. En este plan se mencionaba la creación de una infraestructura básica de centros de alerta y respuesta ante incidentes de seguridad, que atendiera a las demandas específicas de los diferentes segmentos de la sociedad. Sectores críticos, agencias gubernamentales, Administraciones Públicas, Pequeñas y Medianas Empresas (PYME), grandes corporaciones y ciudadanos recibirían el adecuado asesoramiento por parte de estos centros.

En este sentido, se hablaba de la creación de centros de seguridad y del establecimiento de los procedimientos y protocolos que permitiesen coordinar sus funciones y actuaciones. Asimismo, se adelantaba la creación de un CERT para la Administración/ Gubernamental, un CERT para PYMEs y una unidad de lucha contra la violación de la privacidad (lucha contra el spam, el phishing y otros fraudes).

En este contexto, y teniendo en cuenta, además, el continuo incremento de las amenazas y vulnerabilidades sobre los Sistemas de Información de todo el mundo, en el año 2004, se afianzó lo que sería el CERT Gubernamental Nacional español, a raíz del citado Real Decreto 421/2004, que regula la actividad del Centro Criptológico Nacional (CCN). Así, y tras dos años de intenso trabajo, en el **año 2006**, se presentó la **Capacidad de Respuesta a Incidentes de Seguridad de la Información**, del CCN (**CCN-CERT**), dependiente del Centro Nacional de Inteligencia.

4.1. CCN-CERT. CERT Gubernamental Nacional

Desde su creación, el CCN-CERT estableció como misión contribuir a la mejora del nivel de seguridad de los sistemas de información de las **Administraciones Públicas** españolas (tanto la administración central, como las autonómicas y locales) y, como principal objetivo, convertirse en el **centro de alerta nacional**, que coopera y ayuda al sector público a responder de forma rápida y eficiente a los incidentes de seguridad que pudieran surgir y afrontar de forma activa las nuevas amenazas a las que hoy en día están expuestos.

Del mismo modo, se le asignaba la capacidad de propulsar la creación de otros CERT/CSIRT, facilitando la información, formación, recomendaciones y herramientas necesarias para que el resto de administraciones públicas pudieran desarrollar sus propias capacidades de respuesta a incidentes, así se reconocía al **CCN-CERT como coordinador público estatal.**

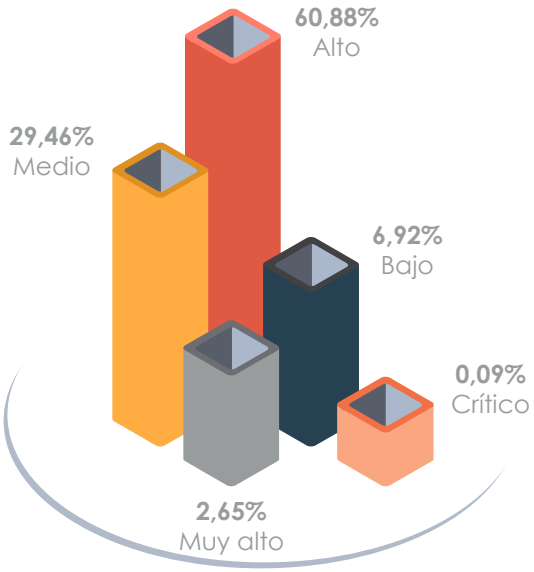
Con su creación, se constituía además el **CERT Gubernamental Nacional español**, a imagen y semejanza de los existentes en otros países de su entorno, que actúa como componente fundamental de las capacidades nacionales de preparación, intercambio de información, coordinación y respuesta. Debe, además, participar de manera efectiva en la cooperación transfronteriza y en el intercambio de información en foros internacionales, impulsando a organizaciones existentes, como el EGC Group (Grupo de CERT gubernamentales europeos).

Las distintas normativas posteriores fueron perfilando sus funciones −RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS) o Ley 40/2015 de Régimen Jurídico del Sector Público− y, en la actualidad, su misión incluye la **coordinación a nivel público estatal** de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, que preserve la información clasificada y la información sensible; defendiendo el patrimonio tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a la normativa, es competencia del CCN-CERT la **gestión de ciberincidentes que afecten a cualquier organismo o empresa pública**. En el caso de **operadores críticos del sector público**, la gestión de ciberincidentes la realizará el CCN-CERT en coordinación con el CNPIC.

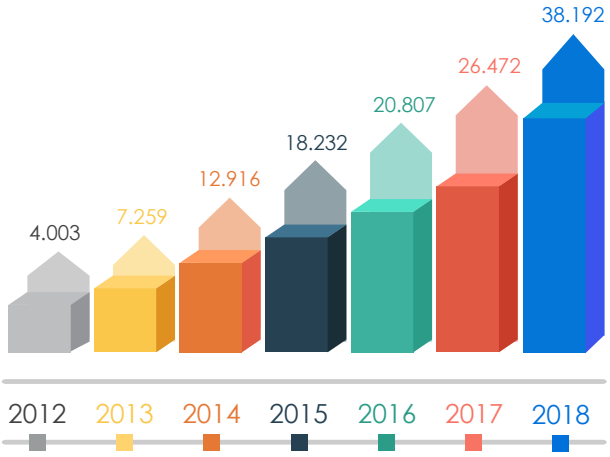
Desde un primer momento, el CERT Gubernamental Nacional brindó todos sus servicios, de forma gratuita, al sector público español. **Unos servicios, fácilmente replicables a otras instituciones u organismos** y que, siguiendo el patrón internacionalmente aceptado, podrían resumirse en los siguientes apartados:



Peligrosidad de los incidentes gestionados por el CCN-CERT en 2018

SERVICIOS REACTIVOS

- Gestión de Incidentes (cerca de 38.200 en 2018)
- Información sobre vulnerabilidades, alertas y avisos de nuevas amenazas: 80 alertas y avisos, emitidos en 2018, y 2.928 vulnerabilidades.
- Análisis de código dañino
- Capacidad forense e ingeniería inversa



Incidentes gestionados por el CCN-CERT

SERVICIOS DE GESTIÓN

- Análisis y gestión de riesgos: Pilar
- Guías CCN-STIC: normas, instrucciones y recomendaciones de seguridad: 335 en 2018
- Cursos presenciales en colaboración con INAP: 14 (620 alumnos en 2018)
- Cursos online (www.ccn-cert.cni.es): 5 cursos. 1.295 horas lectivas
- Plataforma Vanesa: 13 cursos y 1.200 personas
- Informes de Ciberseguridad (Amenazas, Código Dañino, Buenas Prácticas y Técnicos): 76 en 2018
- Artículos divulgativos y notas de prensa para medios: 125 en 2018
- Evaluación y Certificación de Productos

SERVICIOS PROACTIVOS

- Detección de intrusiones
- Sistemas de Alerta Temprana en IT y OT
- Auditorías y evaluaciones de seguridad continuas
- Desarrollo de soluciones de seguridad
- Cibervigilancia

4.2. CERT/CSIRT Nacionales, sectoriales y SOC

En su papel de catalizador de la ciberseguridad nacional, el CCN-CERT ha promovido y facilitado a otras organizaciones, públicas y privadas, la creación y constitución de otros Equipos de Respuesta a Incidentes sectoriales −particularmente en las distintas Administraciones Públicas y Centros de Operaciones de Seguridad (SOC)−, con el objetivo común de mantener e incrementar una vigilancia continua de la Red.

A todos ellos, el CCN-CERT les ha brindado ayuda y colaboración, tanto en su constitución inicial, como en su desarrollo posterior. Así, se han consolidado a lo largo de los años, más de 20 CSIRT (miembros del FIRST) y diferentes SOC.

- Otros CERT/CSIRT de referencia:
  - INCIBE-CERT: Seguridad e Industria gestionado por INCIBE y CNPIC
  - ESP DEF CERT: CERT del Mando Conjunto de Ciberdefensa
- CERT/CSIRT sectoriales que se pueden citar:
  - RedIRIS: primero en constituirse en España
  - AndaluciaCERT: organismos y entidades de la Administración de la Junta de Andalucía
  - CESICAT-CERT: Centro de Seguridad Informática de Cataluña
  - CSIRT-CV (Comunidad Valenciana)
  - CSIRT.GAL (Junta de Galicia)
  - Basque Cibersecuirty Centre CSRIT (País Vasco)

5 | Capacidad de detección y análisis. Sistema de Alerta Temprana (SAT)

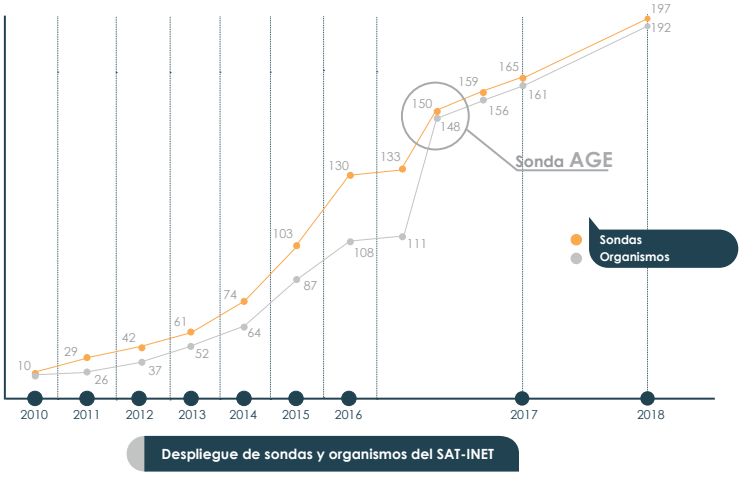
Para garantizar un nivel de seguridad adecuado en los sistemas, es necesario actuar antes de que se produzca un incidente o, por lo menos, ser capaz de detectarlo en un primer momento para reducir su impacto y alcance.

Por este motivo, desde el año **2008** el CCN-CERT ha desarrollado un Sistema de Alerta Temprana (SAT) para la detección rápida de incidentes y anomalías, que permite realizar acciones preventivas, correctivas y de contención. Su principal función, por lo tanto, es la detección temprana de un incidente para que puedan aplicarse las medidas necesarias de contención y de eliminación de la amenaza y poder evitar que el intento de ataque sea fructífero o, en su caso, minimizar el posible impacto.

Este sistema cuenta con tres vertientes: **SAT-SARA** (monitorización de la Intranet de la Administración, SARA); **SAT-INET** (monitorización de las salidas de Internet de los organismos adscritos al servicio) y **SAT-ICS** (Sistemas de Control Industrial).

El SAT, en cualquiera de sus tres modalidades, permite detectar en tiempo real las amenazas e incidentes existentes en el tráfico que fluye entre la red interna del Organismo adscrito. Sus sistemas de detección, a través de sondas, abarcan todas las actividades de:

- Despliegue de detectores y sistemas de alerta
- Recolección de logs, monitorización de tráfico y vigilancia de la red
- Análisis de malware, ingeniería inversa y análisis forense
- Caracterización técnica de la amenaza y elaboración de inteligencia técnica sobre la misma

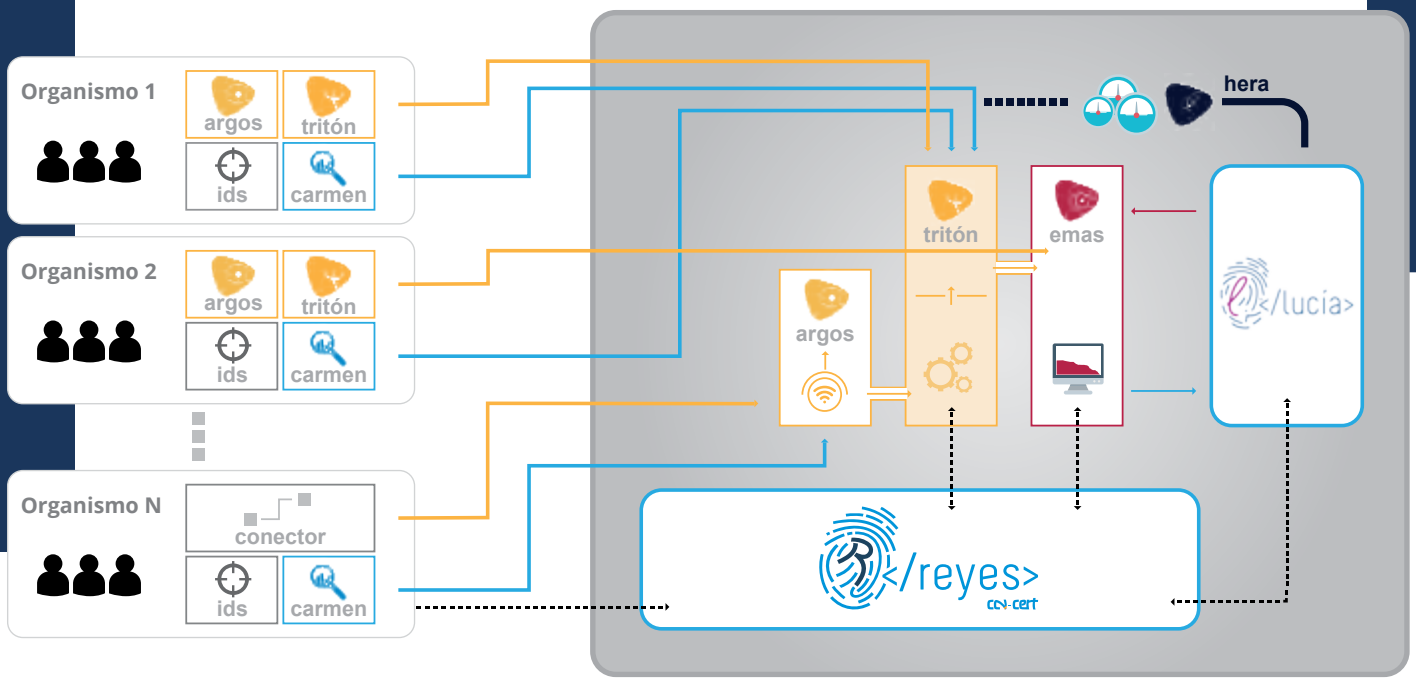


Despliegue de sondas y organismos del SAT-INET

A través de este servicio, el CCN-CERT, en colaboración con el organismo adscrito, tiene capacidad para detectar multitud de tipos de ataques, evitar su expansión, responder de forma rápida ante el incidente detectado y generar normas de actuación que eviten futuros incidentes. Al tiempo, y gracias al almacenamiento de un número progresivo de eventos, es posible contar con una panorámica completa y veraz de la situación de los sistemas de las administraciones públicas españolas, que posibilita una acción preventiva frente a las amenazas que sobre ellas se ciernen.
En general, las ventajas para cualquier organización podrían resumirse en las siguientes:

- Acceso al mayor conjunto de **reglas de detección**, tanto propias como externas, integradas por el equipo de expertos del CCN-CERT, que permite la detección de un mayor número de amenazas.
- **Detección** de todo tipo de ataques e incidentes, incluyendo **detección avanzada interdominio** (detección temprana de un incidente que se haya replicado en otro de los dominios monitorizados).
- **Correlación**. El sistema central no solo detecta incidentes importantes de forma individual, sino que es capaz de detectar eventos mucho más complejos que pueden involucrar a distintos dominios.
- **Información** de gran valor para los responsables TIC de las administraciones públicas, que pueden ver en tiempo real el estado de su red con respecto a la seguridad, así como acceder a informes estadísticos.
- **Soporte a la resolución de incidentes**. Como CERT Gubernamental Nacional español, el CCN-CERT ofrece a todos los organismos su colaboración para una detección, contención y eliminación de cualquier ataque que puedan sufrir sus sistemas.
- **Automatización y reducción de tiempos de respuesta**. Reducción del trabajo manual y repetitivo de los operadores/analistas de seguridad en los procesos de detección y respuesta a incidentes.

En este sentido, la integración de las capacidades de «*Security Information and Event Management*» (SIEM), notificación de incidentes y ciberinteligencia se hace especialmente necesaria para las mejoras de las técnicas de correlación compleja de eventos y gestión de incidentes.



6 | Incremento de la vigilancia. Centros Operacionales de Ciberseguridad (SOC)

Un CSIRT puede proporcionar alertas a las entidades o gestionar un incidente; sin embargo, en distintas circunstancias, las propias organizaciones no saben cómo llevar a cabo la asignación de recursos. En ocasiones, desconocen la superficie de exposición de sus sistemas a esas alertas o amenazas lanzadas por el Equipo de Respuesta a Incidentes.

Por este motivo, en el trabajo diario, y como un escalón más de la ciberseguridad, es preciso disponer de un servicio de evaluación continua que permita conocer en cada momento la superficie de exposición ante una posible amenaza y así asignar los recursos de manera óptima y priorizada.

A través de un Centro de Operaciones de Ciberseguridad (SOC) se realizan tareas de prevención, detección y vigilancia, supervisando a las personas, los procesos y la tecnología que intervienen en todos los aspectos operativos de la ciberseguridad.

El CCN-CERT ha ofrecido servicios de vigilancia, sin coste asociado, a diversos organismos de la Administración Pública española, promocionando la creación de este tipo de Centros.

El SOC dispone de tres niveles:

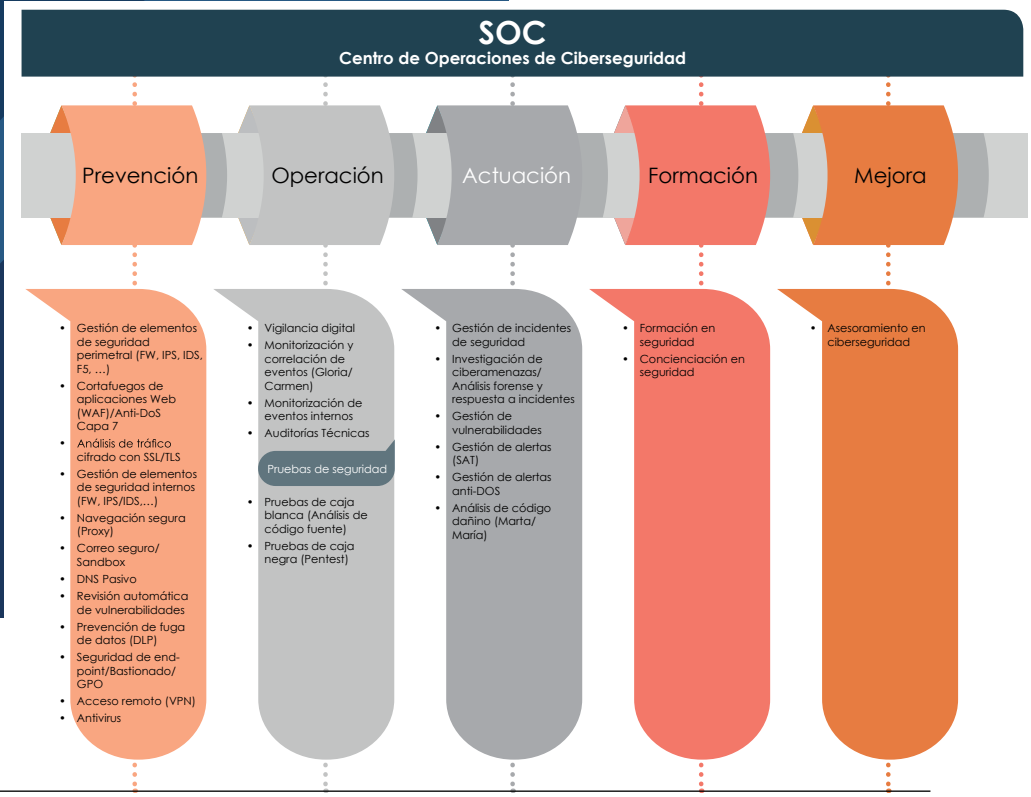
1 OPERACIÓN

2 VIGILANCIA

3 INTELIGENCIA DE CIBERSEGURIDAD

Su objetivo final es aumentar las capacidades existentes de vigilancia y detección de amenazas en la operación diaria, así como su capacidad de respuesta ante cualquier ataque, siendo prioritarios los siguientes aspectos:

- Monitorizar y evaluar de manera continua las medidas de seguridad en uso, verificando su implementación.
- Actuar de manera proactiva, incrementando y ampliando las capacidades de detección, vigilancia, protección y reacción ante incidentes.
- Parametrizar la amenaza mediante inteligencia de ciberseguridad, que permita integrar la información. En este sentido, es fundamental mejorar la notificación de incidentes e incrementar el intercambio de información sobre la amenaza.



Virtual SOC

El constante aumento de los ciberataques, unido a las posibles consecuencias que para un país tendría que un incidente de seguridad afectase a sus sistemas, conlleva la necesidad de incrementar y mejorar de las capacidades de prevención, monitorización, vigilancia y respuesta, a través de los **Centros de Operaciones de Ciberseguridad (SOC)**.

Por este motivo, el Centro Criptológico Nacional está trabajando en la implementación de Centros de Operaciones de Seguridad virtuales (vSOC) en las **entidades locales**, para mejorar así sus capacidades de vigilancia, detección y respuesta ante cualquier posible ataque, así como para optimizar sus recursos en función de la información que manejan y los servicios que prestan.

De este modo, a través del vSOC, ayuntamientos y diputaciones tendrán más visibilidad e información sobre vulnerabilidades, fallos de configuración e incidentes, mayor capacidad de despliegue, protección y actuación, al disponer de una gestión centralizada que permitirá aumentar el número de entidades adscritas a cada vSOC.

7 | Formación. Capacitación y Talento

7.1. Capacitación y certificación de personas

Dado que las amenazas son cada vez más complejas y, a veces, difíciles de detectar, se hace necesaria la formación del personal en todas las organizaciones para luchar contra la ingenuidad, la ignorancia de las buenas prácticas y la falta de concienciación existente sobre la necesidad de preservar la seguridad de la información y los servicios que se prestan a los ciudadanos.

Se precisa, por tanto, de la capacidad de **fomentar, desarrollar y mantener perfiles profesionales cualificados** en todos los niveles (dirección, gestión, implantación y usuarios) para protegerse de las ciberamenazas. Del mismo modo, es necesario hacer frente a la creciente brecha de conocimiento y a un cambio de paradigma educativo, basado en el **aprendizaje permanente** como potencial fuerza laboral.

Históricamente el Centro Criptológico Nacional ha tenido entre sus funciones principales la de formar al personal de la Administración española a través de un amplio programa de cursos. Una función que desempeña con gran éxito y que ha ido ampliando, tanto en la oferta formativa que ofrece −incorporando cursos online y a través de vídeo en *streaming*−, como en el público receptor de la misma −algunos de sus cursos están abiertos a la participación de cualquier usuario−.

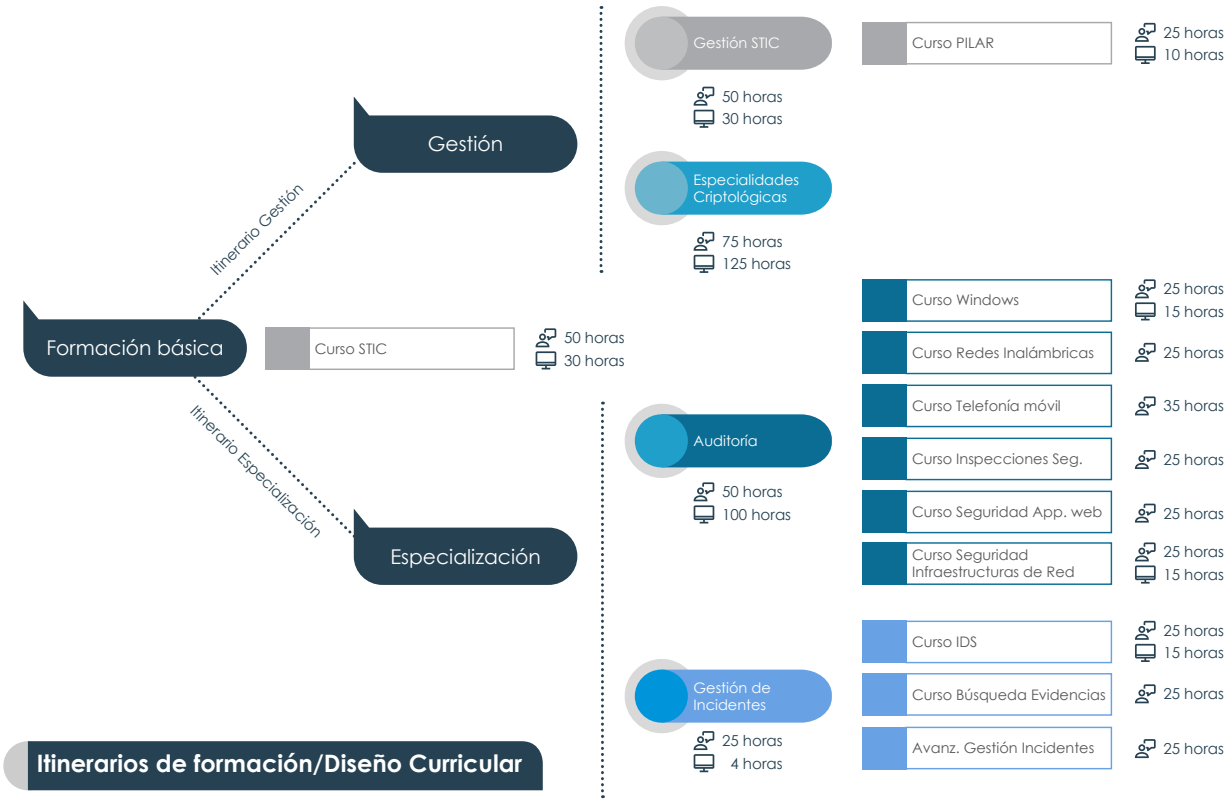
Así, el CCN mantiene un Plan de Formación con tres modalidades de cursos:

- **Presencial**: 20 cursos publicados en el BOE y aquellos desarrollados *ad hoc* para algún organismo nacional o internacional.

- **Online**: El portal del Centro Critpológico Nacional permite a los usuarios la realización de distintos cursos a través de esta plataforma. Se emplea una metodología docente 100% online, tanto en los contenidos de los temarios, como en los exámenes que se realizan una vez finalizado el curso. En la actualidad, hay disponibles ocho en el portal web.

    - Curso básico de fundamentos Linux.
    - Introducción al Esquema Nacional de Seguridad.
    - Curso INES (Informe Nacional del Estado de la Seguridad).
    - Curso básico STIC - Seguridad en entornos Windows.
    - Curso básico STIC - Seguridad en entornos Linux.
    - Curso de Análisis y Gestión de Riesgos de los Sistemas de Información.
    - Curso del Esquema Nacional de Seguridad.
    - Curso de Seguridad de las Tecnologías de la Información y las Comunicaciones.

- **Plataforma Vanesa**, con formación en *streaming* y cuyas grabaciones y material formativo queda alojado en la propia plataforma. Los cursos que se imparten, de una duración aproximada de cuatro (4) horas, abordan el estado del arte de la tecnología, así como la descripción de las soluciones desarrolladas por el CCN-CERT.



Itinerarios de formación/Diseño Curricular

El Plan de Formación del Centro Criptológico Nacional se ha diseñado atendiendo a la necesidad de capacitar, tanto presencialmente como a distancia, a profesionales cualificados, que disponen de distinto perfil y nivel de formación. Por este motivo, se ha establecido una formación BÁSICA que, a través del Curso STIC, introduce al alumno en el ámbito de la Seguridad de las Tecnologías de la Información y la Comunicación.

Completada la formación básica, el profesional que desee perfeccionar sus conocimientos podrá elegir entre dos (2) itinerarios diseñados para lograr tal fin, el itinerario de gestión y el de especialización (dirigido a personal más técnico). El CCN otorga, a los concurrentes que lo hayan superado con aprovechamiento, un **Certificado**, que especifica las materias y créditos asociados.

7.2. Búsqueda de talento. Necesidad de personal experto

El talento especializado en ciberseguridad constituye un conjunto de habilidades de **escasa oferta y alta demanda**. Podría decirse que la carencia de personal cualificado en esta materia es uno de los mayores problemas a los que se enfrenta el sector. Por este motivo, aquellas empresas u organizaciones que sean capaces de atraer y retener personas especializadas en la rama de ciberseguridad tendrán más éxito en la administración del riesgo y en el aprovechamiento de la transformación digital.

Algunas de las recomendaciones que se ofrecen para adquirir y retener este talento[5] son:

- Aplicar técnicas innovadoras para encontrar talento de ciberseguridad.
- Buscar los espacios en los que el talento de ciberseguridad pasa su tiempo.
- Incentivar a los empleados para actualizar sus habilidades de seguridad digital.
- Promover la inclusión de género, cambiando la percepción actual.

Conscientes de esta problemática, el CCN-CERT lanzó en 2017 **ATENEA**, una nueva plataforma de desafíos de ciberseguridad, en la que cualquier persona puede demostrar su conocimiento y destreza ante diferentes desafíos en la materia. En ella se encuentran retos de distinta dificultad y de muy diversas temáticas: criptografía y esteganografía; exploiting, forense, análisis de tráfico, reversing y hacking web.

Entre sus principales objetivos se encuentran:

- Concienciar al personal TIC sobre los riesgos existentes en este campo.
- Involucrar a los profesionales con experiencia en ciberseguridad con el fin de que puedan demostrar su ingenio y capacidad.
- Demostrar a todas las personas con menos experiencia en la seguridad TIC que los retos son divertidos y que la ciberseguridad es más sencilla de lo que parece. No es una ciencia oculta que nunca entenderían.

5.-Capgemini. Informe 2018 Talento especializado en ciberseguridad: la gran brecha en la ciberprotección. https://www.capgemini.com/es-es/resources/talento-especializado-en-ciberseguridad-la-gran-brecha-contra-los-ciber-ataques/

8 | Cooperación Público-Privada. Construir comunidad

Si bien la elaboración de las políticas relacionadas con la ciberseguridad compete en primera instancia a los Estados, todos los agentes públicos y privados con responsabilidad en esta materia, incluyendo también a los propios ciudadanos, han de implicarse en ella. El fortalecimiento de la ciberseguridad proporcionará al Sector Público, al tejido industrial y empresarial, a la comunidad científica y a los ciudadanos en general, una mayor confianza en el uso de las TIC.

En aplicación del **principio de responsabilidad compartida**, las Administraciones Públicas deben mantener estrechas relaciones con las empresas que gestionan sistemas de información relevantes para los intereses nacionales, intercambiando el conocimiento que permita una adecuada coordinación entre ambos y la mutua comprensión del entorno de la ciberseguridad.

En este sentido, merece especial mención las acciones para asegurar la **protección del patrimonio tecnológico** en el ciberespacio, entendido como aquellos activos materiales o inmateriales que sustentan la propiedad intelectual e industrial del sector empresarial, y que conforman el presente de un país y condicionan su futuro.

Es de interés también determinar el impacto que para un país puede tener una potencial interrupción o destrucción de los sistemas y redes que proporcionan servicios esenciales a la sociedad (infraestructuras críticas), dado que, en gran medida, el sector privado posee la titularidad de buena parte de estos sistemas.

Por tanto, uno de los objetivos es la **mejora de la seguridad** y la **resiliencia de las redes**, productos y servicios que emplea el sector industrial en el desarrollo de su actividad, reforzando la colaboración público-privada con el sector industrial y, en particular, con el de la seguridad TIC. Se valorará, entre otros, la participación de los Colegios y Asociaciones profesionales.

Las Guías CCN-STIC están a libre disposición de cualquier usuario. Son más de 300 documentos que recogen normas, instrucciones, guías y recomendaciones con el fin de mejorar el grado de ciberseguridad de las organizaciones

Entre sus principales medidas destacan:

- Impulsar la cooperación entre los sectores público y privado, promoviendo el intercambio de información sobre vulnerabilidades, ciberamenazas y sus posibles consecuencias, especialmente en lo relativo a la protección de los sistemas de interés nacional.
- Promover la cooperación con los sectores de la industria y los servicios de la ciberseguridad, con el fin de mejorar conjuntamente las capacidades de detección, prevención, respuesta y recuperación frente a los riesgos de seguridad del ciberespacio, impulsando la participación activa de los proveedores de servicios, así como el desarrollo y adopción de códigos de conducta y buenas prácticas.
- Impulsar el desarrollo de estándares en ciberseguridad, a través de los organismos y entidades de normalización y certificación nacionales e internacionales, y promover su adopción.

En línea con estas medidas, el CCN-CERT ha brindado buena parte de sus servicios al sector privado y, muy especialmente, a las empresas de interés estratégico para el país (a su Sistema de Alerta Temprana están adheridas diversas empresas que por su actividad requieren una especial protección). En este sentido, el grueso de la actividad del CCN (apoyo frente a ciberincidentes, servicios de alerta temprana, formación, Informes, avisos, alertas, vulnerabilidades, Guías, soluciones, etc.) está publicado en su **portal web (www.ccn-cert.cni.es)** y es de libre disposición para cualquier usuario.

Soluciones del CCN-CERT

El Centro Criptológico Nacional está realizando una importante labor para la mejora de las capacidades tecnológicas, de inteligencia y de comunicación que permitan una respuesta eficaz. Así, está inmerso en un plan de desarrollo de soluciones, en colaboración con la industria española que, a su vez, permite utilizarlas en todo tipo de organizaciones (públicas y privadas). Son soluciones en materia de detección, análisis, auditoría, intercambio de información y formación.

La plataforma **CSIRT.es** es otra de las iniciativas promovidas por el CCN-CERT para ofrecer una respuesta coordinada ante ataques globales. Este grupo de **CSIRT con presencia en España** tiene como objetivos la protección del ciberespacio español, el intercambio de información sobre ciberseguridad y la actuación de forma rápida y coordinada ante cualquier incidente que pueda afectar simultáneamente a distintas entidades españolas.

CSIRT.es está compuesto por los principales equipos de respuesta a incidentes de seguridad CERT/CSIRT, sean públicos o privados, cuyo ámbito de actuación o comunidad de usuarios en la que opera se encuentra dentro del territorio español.

Asimismo, el CCN también mantiene una estrecha relación con las empresas, al velar por la utilización de productos de seguridad confiables. Así constituye el **Organismo de Certificación** (OC), responsable de la certificación de la seguridad de productos o sist emas de acuerdo a unos determinados criterios o normativa (Common Criteria o ISO15408/ISO18045, ITSEC, ISO19790/ISO24759 y la recientemente creada metodología LINCE - Certificación Nacional Esencial de Seguridad).

Además, mantiene permanentemente actualizado un **Catálogo de Productos STIC (CPSTIC)** en el que se incluye un listado de productos con unas garantías de seguridad contrastadas al tener certificadas sus funciones de seguridad fundamentales, de acuerdo a los criterios establecidos por el CCN. El catálogo se compone de:

Listado de Productos Cualificados: aptos para ser utilizados en sistemas afectados por el ENS por requerir un nivel alto de seguridad en cualquiera de sus dimensiones (Confidencialidad, Integridad, Disponibilidad, Trazabilidad y Autenticidad).

Listado de Productos Aprobados: cuyo uso está aprobado en sistemas que manejen información clasificada.

9 | Intercambio de Información. Generación de confianza

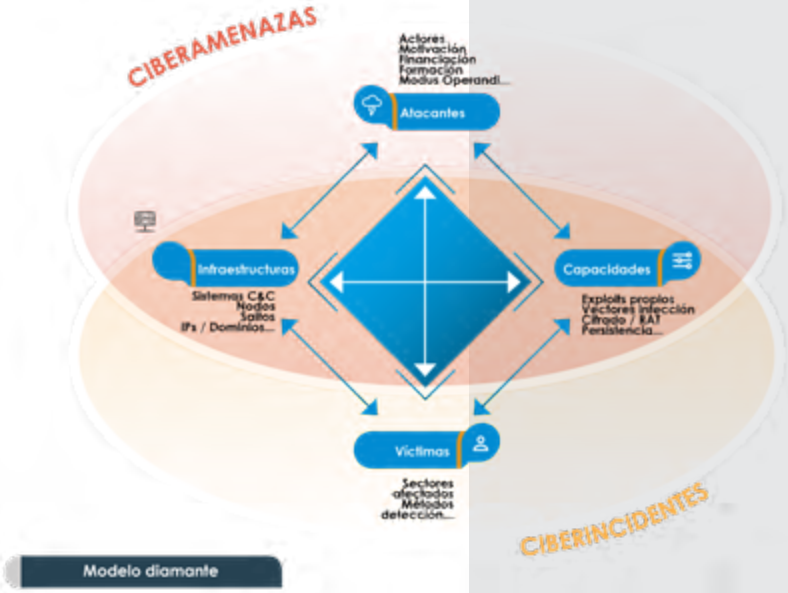
Los riesgos y amenazas del ciberespacio han demostrado ser globales y su resolución solo puede llevarse a cabo mediante una respuesta conjunta. Una respuesta que debe implicar un mayor grado de coordinación y cooperación. Por un lado, a nivel nacional, entre todos los niveles de la Administración del Estado y las empresas y entidades privadas; por otro, a nivel internacional, con otros países y organizaciones multilaterales.

Cualquier mecanismo utilizado para la gobernanza será verdaderamente eficaz si todos los participantes disponen de **información fidedigna** que les permita actuar. Ello es especialmente importante en el caso de los gobiernos, a los que compete garantizar la seguridad y el bienestar de los ciudadanos.

En el **ámbito nacional**, se necesita un modelo basado en el intercambio de información entre organismos, públicos y privados, proveniente tanto del análisis de ciberamenazas como de ciberincidentes, con el objetivo de mejorar y agilizar la detección y actuación frente a los ataques.

Este intercambio siempre es más efectivo a través de la confianza entre las partes que por imposición normativa (aunque existe alguna normativa que obliga al intercambio de información de ciberincidentes).

Dicha confianza permitirá que todos los agentes implicados vean beneficio en invertir tiempo y dinero en foros y sistemas de intercambio y, asimismo, que se produzca una actuación recíproca, en la que la información aportada sea paralela a la obtenida para optimizar sus defensas.



Modelo diamante

Para que este modelo funcione, las aportaciones respecto a ciberamenazas y ciberincidentes deben estar compensadas, pues es necesaria tanto la información del atacante (sus capacidades e infraestructuras) como de la víctima (procedimiento de ataque, impacto sufrido y técnicas de detección / resolución de éxito). De este modo, se podrán cubrir todos los vértices del modelo de diamante y conocer las técnicas, tácticas y procedimientos (TTP) del atacante.

La industria de ciberseguridad nacional, sobre todo la de servicios, debe actuar como catalizador de esta compartición de información de valor, dando especial énfasis al factor humano, y a la formación de un buen equipo de analistas e investigadores, que aporten conocimiento y sean capaces de interpretar la ingente cantidad de información.

En esta tarea, el CCN-CERT ofrece dos de sus soluciones más destacadas: Lucía y Reyes. La primera de ellas, para la notificación de incidentes y contextualización de la amenaza; la segunda, para el conocimiento y parametrización de la amenaza, permitiendo la elaboración de ciberinteligencia.

9.1. Cooperación internacional

Junto a la cooperación nacional, resulta fundamental que cualquier equipo de respuesta a incidentes mantenga contacto, en caso de ataque, con otros equipos del resto del mundo y asegure así las fuentes de información fiables. De ahí, la importancia de los distintos foros internacionales existentes, tanto en el ámbito europeo como mundial. El CCN-CERT participa en las siguientes reuniones y grupos de trabajo internacionales:

- **Fórum de respuesta Incidentes y Equipos de Seguridad Informática, FIRST** (*Forum of Incident Response and Security Teams*), la primera y más importante de las organizaciones internacionales existentes, con miembros de Europa, América, Asia y Oceanía, procedentes del entorno gubernamental, económico, educativo, empresarial y financiero. De hecho, desde su creación en noviembre de 1990, ha pasado de contar con nueve equipos de seguridad de EE.UU. y uno europeo, a los 440 miembros que lo componen en la actualidad.
- **NCIRC de la OTAN** (*Nato Computer Incident-Response Capability*), en el que los distintos CERT de los países miembros de esta Organización analizan y comparten información sobre seguridad.
- **Agencia Europea de la Seguridad de las Redes y la Información** (ENISA – *European Network & Information Security Agency*) de la Unión Europea.
- **APWG** (Anti-Phishing Working Group), programa del Consejo de Europa enfocado a eliminar todo tipo de fraude y robo de identidad a través del phishing, el pharming o los correos fantasma.
- **Trusted Introducer**, principal foro europeo en el que colaboran, innovan y comparten información los CERT más destacados del continente, y que forma parte de TERENA, la Asociación Transeuropea de Investigación y Educación de Redes.
- **EGC** (*European Goverment CERTs*), organización que reúne a los principales CERT gubernamentales en Europa.

10 | Comunicación y promoción

Cuando se inició en el año 2004 el trabajo para la constitución, en el seno del **Centro Criptológico Nacional**, de la Capacidad de Respuesta a Incidentes, CCN-CERT, este tipo de equipos eran prácticamente desconocidos en España. La palabra ciberseguridad ni siquiera se empleaba y, aunque ya se vislumbraban los riesgos y amenazas que representaban las nuevas tecnologías e internet, apenas existía concienciación de la verdadera naturaleza del problema.

Por este motivo, y desde un primer momento, el CERT Gubernamental Nacional decidió realizar un **Plan de Comunicación anual**, concebido como una herramienta de gestión orientada a la consecución de los objetivos estratégicos del Centro. Todo ello, conscientes de la necesidad de darse a conocer, difundir sus servicios hasta alcanzar el reconocimiento y la confianza de toda su comunidad, con el objetivo de convertirse en el punto de referencia en materia de ciberseguridad. De igual forma, uno de sus propósitos ha sido, y es a día de hoy, lograr el mayor número de contactos con los que mantener una comunicación directa y fluida.

En sus primeros pasos, los objetivos fueron claros:

Obtener el reconocimiento e integración del CCN-CERT en los principales foros internacionales con el fin de optimizar la gestión de incidentes.

Lograr el reconocimiento y la confianza de su comunidad (Responsables de Seguridad de las distintas administraciones públicas españolas: Central, Autonómica y Local) hasta convertirse en un punto de referencia.

Generar una cultura de la ciberseguridad, apoyando cualquier labor de sensibilización, formación y divulgación de información y buenas prácticas de seguridad de la información, tanto entre su comunidad como en la sociedad en general.


El CNI crea un nuevo servicio para **combatir la ciberdelincuencia** contra Administraciones Públicas

Expansión
economíadigital
Así se protege España del ciberespionaje


LA VANGUARDIA
JORNADAS INTELIGENCIA
Centro Criptológico del CNI gestiona 18.653 ciberataques, un 44% más que 2014

10/12/2015 13:17
Madrid, 10 dic (EFE).- El Centro Criptológico Nacional (CCN), organismo adscrito al Centro Nacional de Inteligencia (CNI), ha gestionado este año un total de 18.653 ciberincidentes, que supone una media de 51 al día, lo que representa un incremento del 44 por ciento respecto a 2014.

Del total de incidentes registrados, 412 han sido considerados por el ...

El Gobierno se une a la red CERT con dos nuevos centros contra ataques informáticos

Para ello, el CCN-CERT realizó una serie de acciones de relevancia:

- Integración en los principales foros de CERT de todo el mundo: FIRST, EGC (CERT Gubernamentales Europeos), TI, NCIRC (OTAN).
- Plan de visitas (roadshows) por las distintas Comunidades Autónomas presentando sus servicios.
- Desarrollo de eventos periódicos de comunicación con la prensa.
- Participación y/o patrocinio de encuentros de Seguridad (ferias, congresos, jornadas, etc.).
- Relaciones con los medios de comunicación. Publicación y envío de artículos y notas de prensa con material de sensibilización e información.
- Difusión de informes y boletines de seguridad, mensuales y temáticos, entre los que destacan algunos informes de Buenas Prácticas (recomendaciones básicas de seguridad, implementación de HTTPS, dispositivos móviles, uso seguro del correo electrónico, etc.), de amenazas o código dañino; así como su Informe Anual de Ciberamenazas y Tendencias, en el que se analiza en profundidad el panorama nacional e internacional de la ciberseguridad.
- Firma de acuerdos con diversas instituciones españolas: Federación Española de Municipios y Provincias (FEMP), INCIBE, Universidades, Gobiernos Autonómicos y locales (Andalucía, Cataluña, Comunidad Valenciana, Murcia, etc.)
- Elaboración de material informativo y de promoción: trípticos, catálogo de servicios, Memoria de Actividades, etc.

10.1. Portal CCN-CERT y redes sociales

El portal del CCN-CERT[6] es la principal herramienta de coordinación y soporte a su comunidad. A través de este sitio web, los usuarios pueden acceder a todos los servicios ofrecidos por este organismo. No obstante, dada la sensibilidad de algunos contenidos, el portal dispone de una sección de acceso restringido, a la que únicamente se puede acceder cumplimentando el formulario de inscripción publicado en esta página.

Asimismo, en el año 2015, el CCN-CERT creó sus perfiles en las principales redes sociales (LinkedIn, Twitter y YouTube), a través de las cuales informa sobre toda su actividad, ofrece avisos y alertas o publica información de interés para un público más generalista.

En apenas dos años, ha conseguido más de 12.000 seguidores en Twitter y más de 11.000 en LinkedIn.

10.2. Jornadas CCN-CERT

Las Jornadas CCN-CERT, celebradas desde el año 2007, constituyen una de las actividades insignia del Centro Criptológico Nacional. El evento se ha convertido en el encuentro principal de expertos en ciberseguridad en España, no solo por el gran éxito de convocatoria, sino también por la calidad de los temas abordados y la experiencia y conocimiento de los ponentes.

La última edición, inaugurada por Su Majestad el Rey, congregó a 2.464 asistentes, los días 12 y 13 de diciembre, y contó con el respaldo de las principales empresas y asociaciones del sector.

Aproximación española a la Ciberseguridad