CCN
centro criptológico nacional

Informe de Actividades

Activity report

2017/2018

Paz Esteban López
Secretaria General Directora Interina del CNI
Secretary General Interim Director of the CNI

Querido/a lector/a

Cuando escribo estas líneas, el **Centro Criptológico Nacional (CCN)**, adscrito al **Centro Nacional de Inteligencia (CNI)**, está de celebración. Se cumplen 15 años desde que el 19 de marzo de 2004, se publicara en el Boletín Oficial del Estado, el Real Decreto 421/2004, de 12 de marzo, que regulaba y daba cuerpo a las funciones del CCN. Este RD venía a definir el ámbito y funciones de este Organismo, cuya actividad había sido recogida previamente en la Ley 11/2002, de 6 de mayo, reguladora del CNI. Se daba cuerpo a un departamento surgido a principios de los años 80, en el seno del propio Centro, que ya había alcanzado un profundo conocimiento en amenazas, vulnerabilidades y riesgos de los sistemas de información y comunicaciones.

Hoy, 15 años después, lo que intuíamos desde el CNI y empezábamos a advertir a todas las Instituciones, aunque pareciera en ocasiones ciencia ficción, se ha cumplido. De un lado, las posibilidades de comunicación y progreso de la sociedad, las corporaciones y los organismos públicos se han desarrollado hasta alcanzar unas cotas impensables un tiempo atrás. De otro, los peligros y las amenazas provenientes del ciberespacio, también. El aumento de la superficie de exposición (especialmente dispositivos móviles, Internet de las Cosas y los entornos cloud), el big data, la conectividad universal, así como la acelerada adopción por toda la sociedad de las tecnologías emergentes nos ha hecho más vulnerables y ha provocado nuevos desafíos. Un reto que será aún mayor con la generalización del 5G; la nueva generación de comunicaciones que multiplicará exponencialmente el tráfico de datos, la velocidad de conexión y los dispositivos interconectados.

Y precisamente, para proteger el ciberespacio español y coordinar la acción de los diferentes organismos de la Administración en la materia, surgió y se ha ido desarrollando el Centro Criptológico Nacional. Durante estos 15 años (los dos últimos desglosados en este **Informe de Actividades 2017-2018** que ahora presentamos), el CCN ha trabajado para mantener la infraestructura y los sistemas de información con unos niveles óptimos de seguridad, proteger la información y el patrimonio tecnológico del país, formar al capital humano necesario y desarrollar las estrategias y marcos legales posibilistas que permitieran a España beneficiarse de todas las bondades de la tecnología, pero de una forma segura. Se trata, no de poner límites al gran avance que nos brinda Internet, sino, todo lo contrario; garantizar la seguridad, la intimidad y la libertad de todos los ciudadanos para promocionar todavía más esta Red.

Así pues, a lo largo de estos 15 años, la actividad del CCN (recogida de forma pormenorizada en sus seis Informes de Actividad publicados hasta la fecha) ha ido adecuándose a una realidad cambiante como pocas. Su contribución ha sido fundamental para el desarrollo de la **Estrategia de Ciberseguridad Nacional**, la implantación del **Esquema Nacional de Seguridad (ENS)** o la creación del **CERT Gubernamental español (CCN-CERT)** como gestor de los ciberataques al sector público y empresas y organizaciones de interés estratégico para el país. De igual manera, ha tenido un papel central en la formación del personal experto en la materia, la constitución del Organismo de Certificación de productos y sistemas, la aplicación de políticas y procedimientos seguros y el empleo y promoción de productos y tecnologías de seguridad, a través de **CCN-PYTEC**.

Este compromiso constante del CCN por fortalecer la ciberseguridad nacional seguirá guiando nuestros pasos en el futuro. Y lo hará de forma coordinada y conjunta con otras instituciones públicas, universidades, empresas y ciudadanos, sabedores de que la ciberseguridad requiere del compromiso de todos. Un reto colectivo que nos ayude a sortear los riesgos y las amenazas y permita aprovecharnos de las infinitas posibilidades que se nos brindan. Nuestra seguridad nacional, el desarrollo de nuestro tejido empresarial y el bienestar y prosperidad de la ciudadanía, así lo requieren. Hagámoslo posible.

Dear reader

As I write these lines, the **National Cryptologic Centre (CCN)**, attached to the **National Intelligence Centre (CNI)**, is celebrating. It has been 15 years since the Royal Decree 421/2004, dated 12th March, which regulates and embodies the functions of the CCN, was published in the Spanish Official State Gazette on 19th March 2004. This RD defined the scope and functions of this Body, whose activity had previously been included in Law 11/2002, dated 6th May, regulating the CNI. A department emerged in the early 1980s, within the Centre itself, which had already acquired a deep knowledge of threats, vulnerabilities and risks in information and communication systems.

Today, 15 years later, what we sensed from the CNI and began to warn all the Institutions against, although it sometimes seemed science fiction, is now a reality. On the one hand, the possibilities of communication and progress of society, corporations and public bodies have developed to levels unthinkable not so long ago. On the other hand, dangers and threats from cyberspace have too. The increase in exhibition space (especially mobile devices, the Internet of Things and cloud environments), big data, universal connectivity and the accelerated adoption by society of emerging technologies has made us more vulnerable and has given rise to new challenges. A challenge which will be even greater with the generalization of 5G; the new generation of communications which will exponentially multiply data traffic, connection speed and interconnected devices.

In order to protect Spanish cyberspace and coordinate the actions of the different government agencies in this area, the National Cryptologic Centre was created and has been evolving ever since. During these 15 years (the last two developed in this **Activity Report 2017-2018** which we now present), the CCN has worked to maintain the infrastructure and information systems with optimum levels of security, protect the country's information and technological heritage, train the necessary human capital and develop the enabling strategies and legal frameworks which would allow Spain to make the most of all the benefits of technology, but in a safe manner. It is not a question of placing limits on the great advance that the Internet offers us, but quite the opposite; to guarantee the security, privacy and freedom of all citizens in order to promote this Network even more.

Thus, over these last 15 years, the activity of the CCN (collected in detail in its six Activity Reports published to date) has been adapting to a changing reality like few others. Its contribution has been fundamental for the development of the **National Cybersecurity Strategy**, the implementation of the **National Security Framework (ENS)** or the creation of the **Spanish Governmental CERT (CCN-CERT)** as a manager of cyberattacks to the public sector and companies and organizations of strategic interest to the country. Likewise, it has played a central role in the training of experts, the constitution of the Certification Body for products and systems, the application of safe policies and procedures and the use and promotion of security products and technologies, through **CCN-PYTEC**.

CCN's ongoing commitment to strengthening national cybersecurity will continue to guide our steps into the future. And it will do so in a coordinated manner and jointly with other public institutions, universities, companies and citizens, knowing that cybersecurity requires the commitment of everyone. A collective challenge which helps us avoid risks and threats and allows us to take advantage of the infinite possibilities offered to us. Our national security, the development of our business fabric and the well-being and prosperity of our citizens require it. Let's make it possible.

Índice
Table of contents

Centro CRIPTOLÓGICO Nacional (CCN)

National Cryptologic Centre

El **Centro Criptológico Nacional (CCN)** es el Organismo adscrito al **Centro Nacional de Inteligencia (CNI)** responsable de garantizar la seguridad de las Tecnologías de la Información y la Comunicación (TIC) en las diferentes entidades del Sector Público, así como la seguridad de los sistemas que procesan, almacenan o transmiten información clasificada.

The National Cryptologic Centre (CCN) is the body attached to the **National Intelligence Centre (CNI)** responsible for guaranteeing the security of Information and Communication Technologies (ICT) in the different entities of the public sector, as well as of the systems that process, store or transmit classified information.

Las **funciones** concretas del CCN, planteadas en el Real Decreto 421/2004, de 12 de marzo, son las siguientes:
The specific functions of the CCN, set out in Royal Decree 421/2004, 12th March, are as follows:

Normativa Regulation

Elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas TIC (Guías CCN-STIC).
To elaborate and disseminate norms, instructions, guides and recommendations to ensure the security of the ICT systems (CCN-STIC Guides)

Formación Training

Formar al personal del Sector Público especialista en el campo de la seguridad.
To train those employees of the Public Sector specialized in the security field.

Vigilancia y auditoría Vigilance and Audit

Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en su ámbito de competencia.
To ensure the fulfilment of the regulations regarding the protection of the classified information in the area of its competences.

Desarrollo Development

Coordinar la promoción, desarrollo, obtención, adquisición y puesta en explotación y uso de tecnologías de seguridad.
To coordinate the promotion, development, obtaining, acquisition, exploitation and use of security technologies.

Evaluación Evaluation

Valorar y acreditar la capacidad de los productos de cifra y de los sistemas para manejar información de forma segura.
To evaluate and confirm the capacity of the encryption products and the systems to manage information safely.

Certificación Certification

Constituir 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.
To be the certification body of the National Framework for the Evaluation and Certification of Information Technology Security applicable to products and systems in the its field.

Detección y Respuesta Detection and Response

Contribuir a la mejora de la ciberseguridad española, a través del CCN-CERT, afrontando de forma activa las amenazas que afecten a sistemas del Sector Público, a empresas y organizaciones de interés estratégico para el país, en coordinación con el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) y a cualquier sistema TIC que procese información clasificada.
To contribute to the improvement of Spanish cybersecurity, through the CCN-CERT, actively facing the threats which are affecting the systems of the Public Sector, companies and organizations of strategic interest to the country, in coordination with the National Center for Infrastructure Protection and Cybersecurity (CNPIC) and any ICT system which processes classified information.

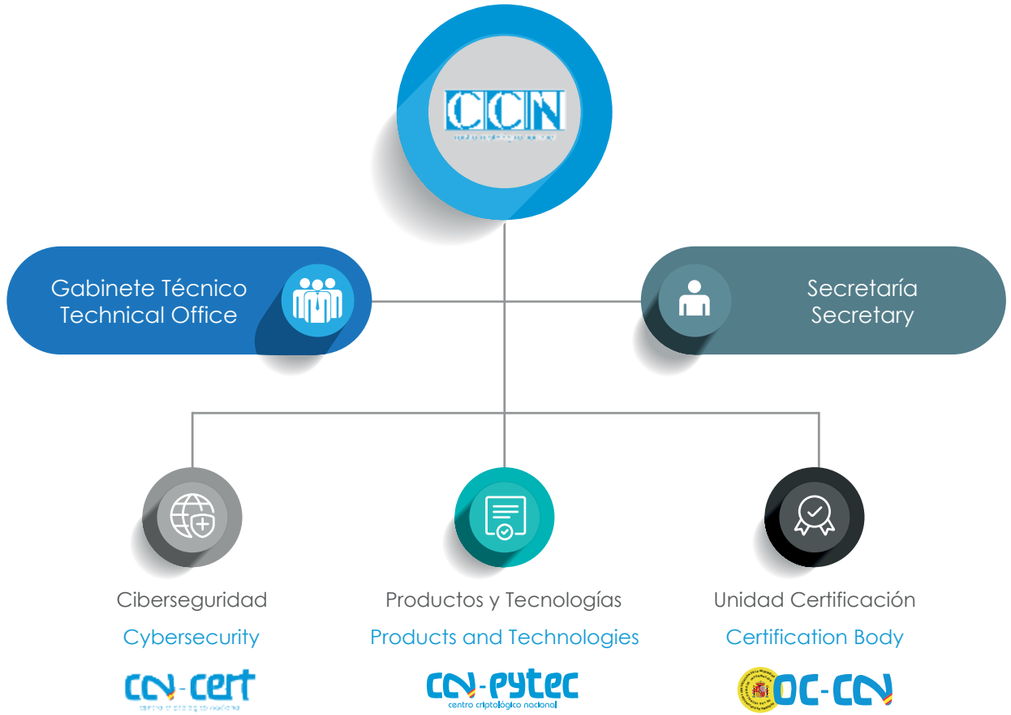
Relaciones Relations

Establecer las necesarias relaciones y firmar los acuerdos pertinentes con organizaciones similares de otros países, para el desarrollo de las funciones mencionadas.
To stablish the necessary relations and sign the corresponding agreements with similar organizations in other countries, for the development of the aforementioned functions.

3.1 ORGANIGRAMA
ORGANIZATIONAL Chart

La organización de los recursos del Centro Criptológico Nacional ha sido diseñada con el objetivo de cumplir con las misiones que tiene encomendadas por el RD 421/2004, de 12 de marzo. Así, y con el objetivo de garantizar la seguridad de los sistemas de las Tecnologías de la Información y la Comunicación que procesan, almacenan o transmiten información clasificada, así como la de aquellos sistemas que transmiten información en formato electrónico, que normalmente requieren protección y que incluyen medios de cifra, el CCN se articula en dos departamentos: Ciberseguridad y Productos y Tecnologías, junto con la Unidad de Certificación.

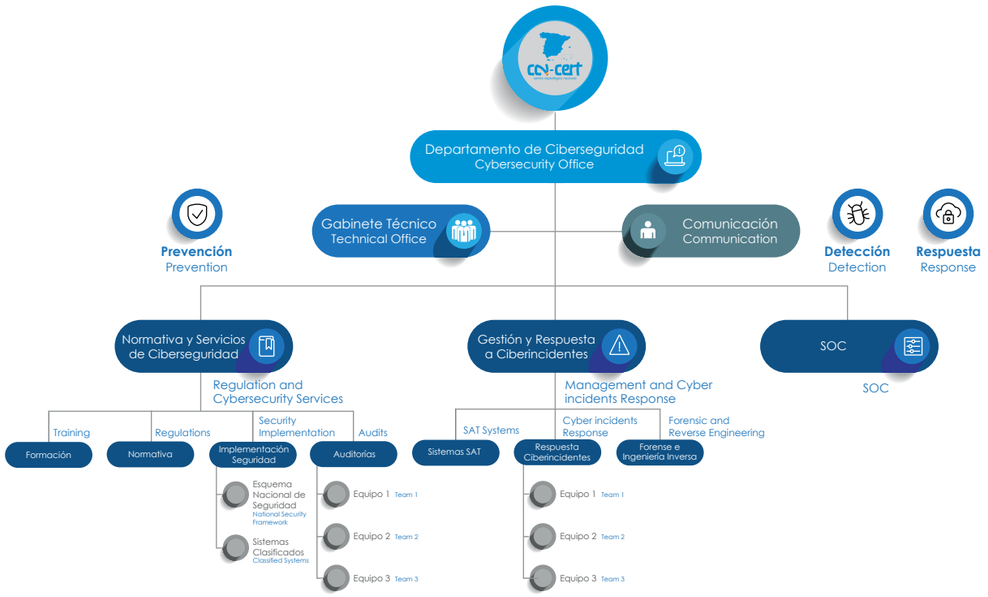
The organization of the resources of the National Cryptologic Centre has been designed with the objective of fulfilling the missions entrusted to it by RD 421/2004, 12th March. Thus, and with the aim of guaranteeing the security of the ICT systems that process, store or transmit classified information, as well as that of those systems that transmit information in electronic format, which normally require protection and include means of encryption, the CCN is divided into two departments: Cybersecurity and Products and Technologies, as well as the Certification Body.



Departamento de Ciberseguridad (CCN-CERT)
Cybersecurity Department (CCN-CERT)

- **Formación, normativa y cultura de ciberseguridad:** actividades formativas, acciones de concienciación y sensibilización, y publicación de normas, instrucciones y recomendaciones. Todo ello, con el fin último de mejorar la ciberseguridad de las organizaciones.
- **Implementación de seguridad:** acreditación de sistemas que manejan información clasificada, así como desarrollo de soluciones y apoyo necesario para la implantación del Esquema Nacional de Seguridad.
- **Auditoría:** evaluación del estado de la seguridad de los sistemas TIC e inspecciones de seguridad que permiten verificar la seguridad implementada en un sistema y que los servicios y recursos utilizados cumplen con los mínimos especificados y requeridos en la política de seguridad.
- **Sistema de Alerta Temprana (SAT):** detección rápida de incidentes y anomalías, que permite realizar acciones preventivas, correctivas y de contención.
- **Gestión y respuesta a incidentes:** constituye el centro de alerta y respuesta nacional que coopera y ayuda a responder de forma rápida y eficiente a los ciberataques y afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes (CERT/CSIRT) o Centros de Operaciones de Ciberseguridad (SOC) existentes.
- **Centros de Operaciones de Ciberseguridad:** prestación de servicios horizontales de ciberseguridad que permiten aumentar la capacidad de vigilancia y detección de amenazas en la operación diaria de los sistemas de información y comunicaciones de la Administración, así como la mejora de su capacidad de respuesta ante cualquier ataque.

- **Training, regulation and cybersecurity culture:** training activities, awareness-raising actions, and publication of standards, instructions and recommendations. All this, with the ultimate aim of improving organizations' cybersecurity.
- **Security implementation:** accreditation of systems that handle classified information, as well as development of solutions and necessary support for the implementation of the National Security Framework.
- **Audit:** evaluation of the security status of ICT systems and inspections to verify the security implemented in a system and the compliance of the services and resources used with the minimum requirements specified in the security policy.
- **Early Warning System (SAT):** rapid detection of incidents and anomalies, which allows preventive, corrective and containment actions.
- **Cyber Incident Response and Management:** it is the national alert and response centre that cooperates and helps to respond quickly and efficiently to cyberattacks and actively address cyber threats, including the coordination at the state public level of the Computer Emergency Response Teams (CERT), Computer Security Incident Response Teams (CSIRT) or Security Operations Centres (SOC).
- **Security Operations Centres:** provision of horizontal cybersecurity services that increase the capacity for surveillance and detection of threats in the daily operation of the Administration's ICT systems, as well as the improvement of its capacity to respond to any attack.



Departamento de Productos y Tecnologías (CCN-PYTEC)

Products and Technologies Department (CCN-PYTEC)

- **Promoción y desarrollo de productos de cifra y seguridad TIC:** su objetivo es garantizar que los productos utilizados por la Administración cumplan con los niveles de seguridad exigidos.
- **Evaluación y certificación:** la evaluación y certificación de productos de seguridad TIC son el único medio objetivo que permite valorar y acreditar la capacidad de un producto para manejar información segura.
- **Seguridad Productos TIC:** elabora un Catálogo de Productos STIC, CPSTIC, en el que ofrece un listado de productos de seguridad con unas garantías por el propio CCN.

- **Promotion and development of ICT encryption and security products:** its objective is to guarantee that the products used by the Administration comply with the required security levels.
- **Evaluation and certification:** the evaluation and certification of ICT security products are the only objective means of assessing and accrediting a product's ability to handle secure information.
- **ICT Security Products:** it elaborates a STIC Products Catalogue, CPSTIC, in which it offers a list of security products with guarantees corroborated by the CCN.

3.2 Marco NORMATIVO del CCN

CCN REGULATORY Framework

El ámbito de competencia del CCN está definido por el siguiente marco normativo:

- **Ley 11/2002**, de 6 de mayo, reguladora del CNI.
- **Real Decreto 421/2004**, de 12 de marzo, regulador del CCN.
- **Orden Ministerio Presidencia PRE/2740/2007**, de 19 de septiembre, que regula el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, y que confiere al CCN la capacidad de actuar como Organismo de Certificación (OC) de dicho Esquema.
- **Real Decreto 03/2010**, de 8 de enero, de desarrollo del ENS, (actualizado en el RD 951/2015, de 23 de octubre) en el que se establecen los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración.
- **Comisión Delegada del Gobierno para Asuntos de Inteligencia**, que define anualmente los objetivos del CNI mediante la Directiva de Inteligencia, que marca la actividad del Centro.

The CCN's scope of competence is defined by the following regulatory framework:

- **Law 11/2002, dated 6th May**, regulating the CNI
- **Royal Decree 421/2004, dated 12th March**, regulating the CCN
- **Order of the Ministry of the Presidency PRE/2740/2007, dated 19th September**, which regulates the National Framework for the Evaluation and Certification of Information Technology Security, and which confers on the CCN the capacity to act as the Certification Body (OC) of suck Framework.
- **Royal Decree 03/2010, dated 8th January**, on the development of the ENS (updated in RD 951/2015, 23rd October), which establishes the basic principles and minimum requirements, as well as the protection measures to be implemented in the Administration's systems.
- **The Government's Delegated Committee for Intelligence Affairs**, which annually defines the objectives of the CNI through the Intelligence Directive, which marks the activity of the Centre.

Otra normativa

Other regulations

Además de la legislación anteriormente expuesta, varias han sido las normativas publicadas en los dos últimos años que afectan muy directamente al sector de la ciberseguridad y, por ende, a la actividad del CCN. Entre otras, podemos citar:

- **Ley 39/2015,** de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- **Ley 40/2015,** de 1 de octubre, de Régimen Jurídico del Sector Público, que amplía el ámbito de aplicación del Esquema Nacional de Seguridad al Sector Público institucional y con ello la responsabilidad del CCN.
- **Instrucción Técnica de Seguridad (ITS) de conformidad con el ENS**. Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas.
- **Instrucción Técnica de Seguridad (ITS) de Informe del Estado de la Seguridad**. Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas.
- **Ley Orgánica 1/2015**, de 30 de marzo, por la que se modifica la **Ley Orgánica 10/1995,** de 23 de noviembre, del Código Penal en materia de delitos de terrorismo incluyendo tipos penales de ciberterrorismo.
- **Instrucción Técnica de Seguridad (ITS) de Notificación de Incidentes de Seguridad**. Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública.
- **Instrucción Técnica de Seguridad (ITS) de Auditoría de la Seguridad de los Sistemas de Información**. Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública.
- **Real Decreto-ley 12/2018**, de 7 de septiembre, de seguridad de las redes y sistemas de información.

In addition to the aforementioned legislation, there have been several standards published over the last two years that directly affect the cybersecurity sector and consequently the CCN's work as well. Among others, we might mention:

- **Law 39/2015, dated 1st October**, on the Common Administrative Procedure for Public Administrations.
- **Law 40/2015, dated 1st October**, on the Legal Regime of the Public Sector, which extends the scope of application of the National Security Framework (ENS) to the institutional public sector and thus the responsibility of the CCN.
- **Technical Security Instruction (ITS)** in compliance with the National Security Framework. Resolution dated 13th October 2016 from the Secretary of State for Public Administrations.
- **Technical Security Instruction (ITS)** from the State Security Report. Resolution dated 7th October 2016, from the Secretary of State for Public Administrations to approve the Technical Security Instruction in the Security Status Report.
- **Organic Law 1/2015, 30th March**, modifying **Organic Law 10/1995**, dated 23rd November, on Criminal Law regarding terrorism crimes including criminal cyberterrorism.
- **Organic Law 10/1995, dated 23rd November**, on the Criminal Code in the area of terrorist offences, including criminal types of cyberterrorism.
- **Technical Security Instruction (ITS)** of Notification of Security Incidents. Resolution of 13th April 2018 of the Secretariat of State of Public Function.
- **Technical Security Instruction (ITS)** of Information Technology Security Audit. Resolution of 27th March 2018 of the Secretary of State for Public Function.
- **Royal Decree-law 12/2018**, dated 7th September, on networks and information systems security.

Marco JURÍDICO general

General LEGAL framework

En los dos últimos años, España ha ido ganando peso en el contexto internacional de la ciberseguridad, particularmente a nivel europeo. Al mismo tiempo, el marco jurídico también ha experimentado una notable adaptación. Entre 2017 y 2018 se han desarrollado o actualizado alguna de las principales normativas que afectan al sector: Estrategia Nacional de Ciberseguridad, Esquema Nacional de Seguridad, la denominada Directiva NIS y el Reglamento General de Protección de Datos (RGPD).

In the last two years, Spain has been becoming more relevant in the international context of cybersecurity, particularly at the European level. At the same time, the legal framework has also undergone considerable adaptation. Between 2017 and 2018 some of the main regulations affecting the sector have been developed or updated: National Cybersecurity Strategy, National Security Framework, the so-called NIS Directive and the General Data Protection Regulation (GPDR).

4.1 Estrategia Nacional de CIBERSEGURIDAD

National CYBERSECURITY Strategy

Entre 2017 y 2018 se ha trabajado en la actualización de la nueva Estrategia Nacional de Ciberseguridad, con el fin de desarrollar las previsiones de la Estrategia de Seguridad Nacional de 2017 en el ámbito de la ciberseguridad y garantizar el uso seguro y fiable del ciberespacio, protegiendo los derechos y las libertades de los ciudadanos y promoviendo el progreso económico. Una ciberseguridad que se extiende más allá del campo meramente de la protección del patrimonio tecnológico para adentrarse en las esferas política, económica y social.

En esta Estrategia se fijan cinco objetivos específicos para orientar la acción del Estado:

- Seguridad y Resiliencia de las redes y los sistemas de información y comunicaciones del Sector Público y de los servicios esenciales.
- Uso seguro y fiable del ciberespacio frente a un uso ilícito o malicioso.
- Protección del ecosistema empresarial y social de los ciudadanos.
- Cultura y compromiso con la ciberseguridad y protección de las capacidades humanas y tecnológicas.
- Seguridad del ciberespacio en el ámbito internacional.

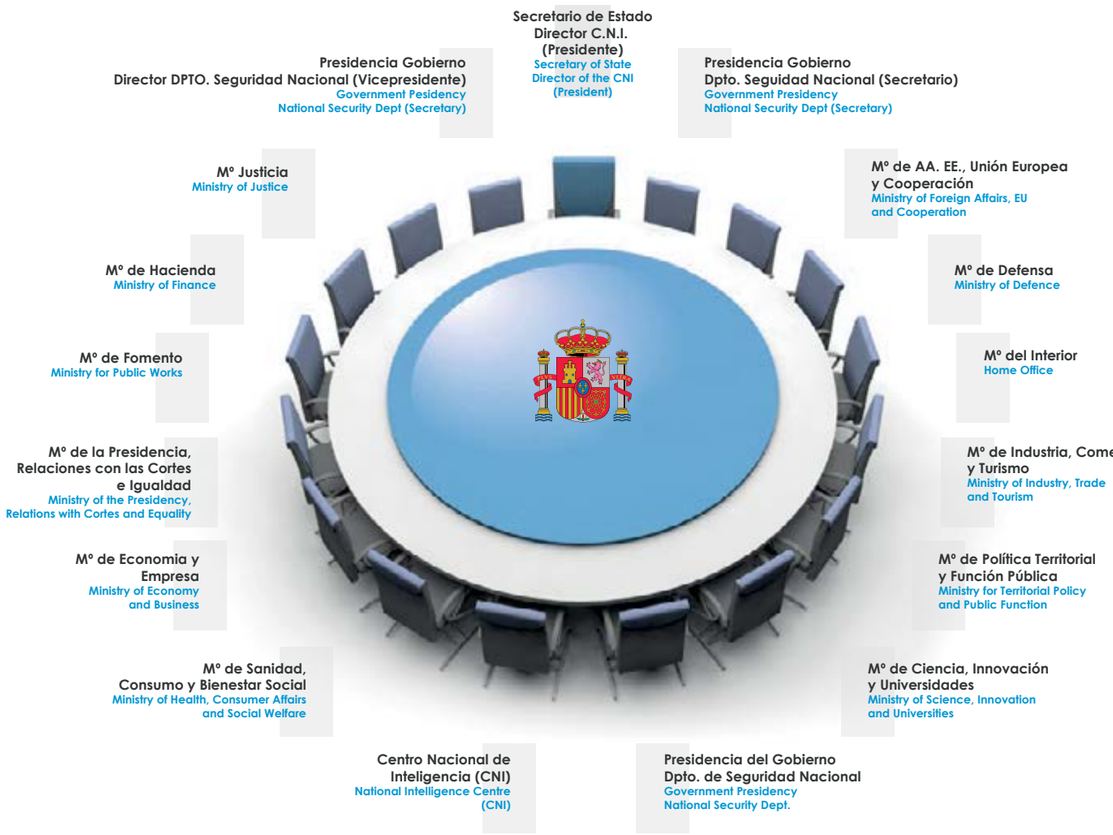
Between 2017 and 2018 the CCN has been working on the update of the new National Cybersecurity Strategy, with the aim of developing the forecasts of the 2017 National Security Strategy in the area of cybersecurity and ensuring the safe and reliable use of cyberspace, protecting the rights and liberties of citizens and promoting economic progress. A cybersecurity that extends beyond the mere protection of technological heritage to the political, economic and social spheres.

In this Strategy five specific objectives to guide the State action in this area are set:

- Security and resilience of public sector networks, ICT systems and essential services.
- Safe and reliable use of cyberspace against unlawful or malicious use.
- Protection of the business and social ecosystem of citizens.
- Culture and commitment to cybersecurity and protection of human and technological capacities.
- International cyberspace security.

El **Centro Nacional de Inteligencia** ha participado activamente en la elaboración de esta Estrategia. No en vano, ha presidido el **Consejo Nacional de Ciberseguridad** desde su creación en 2014 como órgano de apoyo al Consejo de Seguridad Nacional, coordinador de los organismos con competencia en la materia a nivel nacional.

Gobernanza de la Ciberseguridad
Governance of Cybersecurity



The **National Intelligence Centre** has actively participated in the elaboration of this Strategy. Not in vain, it has held the presidency of the **National Cybersecurity Council** since its beginning in 2014 as a body which supports the National Security Council, coordinator of agencies with competence in the field nationwide.

4.2 Esquema Nacional de SEGURIDAD

National SECURITY Framework

El 8 de enero de 2020 hará diez años desde que se aprobara el **Real Decreto 3/2010**, que recogía el **Esquema Nacional de Seguridad** y su finalidad: "la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios".

Esquema Nacional de Seguridad

Cinco años después, en 2015, se publicó su modificación a través del **RD 951/2015, de 23 de octubre**, en respuesta a la evolución del entorno regulatorio (en especial de la Unión Europea) de las tecnologías de la información y de la experiencia de la implantación del propio Esquema.

Además, la **Línea de Acción 2** de la citada Estrategia Nacional de Ciberseguridad de 2019, aborda la necesidad de garantizar la seguridad y resiliencia de los activos estratégicos para España y, entre las medidas a adoptar, se encuentra asegurar la plena implantación del ENS.

On 8th January 2020 it will be ten years since **Royal Decree 3/2010** was approved, which included the **National Security Framework (ENS)** and its purpose: "*the creation of the necessary conditions of confidence in the use of electronic media, through measures that ensure the security of systems, data, communications and electronic services, allowing citizens and public administrations the exercise of rights and compliance with duties through these means.*"

Five years later, in 2015, its modification was published through **Royal Decree 951/2015, dated 23rd October**, in response to the evolution of the regulatory environment (especially that of the European Union) of information technologies and of the experience from the implementation of this Framework.

Furthermore, **Line of Action 2** of the aforementioned 2019 National Cybersecurity Strategy addresses the need to guarantee the security and resilience of strategic assets for Spain and, among the measures to be adopted, is to ensure the full implementation of the ENS.

En todo este proceso, el CCN, en colaboración con el Ministerio de Política Territorial y Función Pública (anteriormente de Hacienda y Administraciones Públicas) ha participado activamente en su desarrollo e implementación. De hecho, buena parte de los instrumentos para la adecuación al ENS han sido promovidos por el CCN:

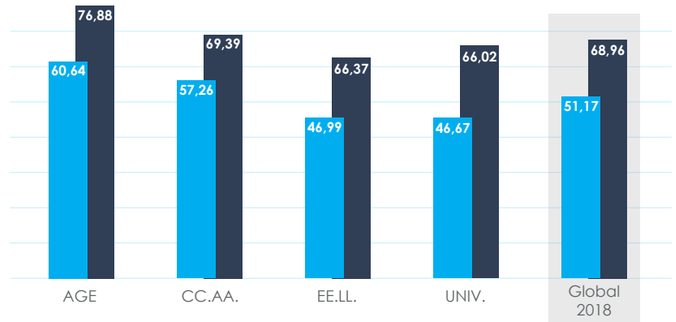
- **Guías CCN-STIC:** Serie 800 de las Guías CCN-STIC *(véase apartado correspondiente)*
- **Instrucciones Técnicas** (mencionadas anteriormente)
- **Auditorías Servicios Web**
- **Análisis de riesgos**, a través de la herramienta PILAR.
- **Cumplimiento del ENS**, gracias a la herramienta CLARA, desarrollada por el propio CCN para analizar las características de seguridad técnicas definidas en el RD.
- **Productos cualificados:** Catálogo de Productos STIC, CPSTIC, elaborado por el Departamento de Productos y Tecnologías del CCN (CCN-PYTEC), con unas garantías de seguridad contrastadas, para organismos del Sector Público o entidades privadas que den servicio a éstos y que se encuentren afectados por el ENS *(véase apartado correspondiente)*

Throughout this process, the CCN, in collaboration with the Ministry for Territorial Policy and Public Function (formerly the Ministry of Finance and Public Administrations) has actively participated in its development and implementation. In fact, many of the instruments for the adaption to the ENS have been promoted by the CCN:

- **CCN-STIC Guides:** 800 series (see corresponding section)
- **Technical Instructions** (mentioned above)
- **Web Services Audits**
- **Risk analysis,** through the PILAR tool.
- **Compliance with the ENS,** thanks to the CLARA tool, developed by the CCN to analyse the technical security characteristics defined in the RD.
- **Qualified products:** STIC Products Catalogue, CPSTIC, drawn up by the CCN's Products and Technologies Department (CCN-PYTEC), with contrasted security guarantees, for Public Sector bodies or private entities providing services to these and which are affected by the ENS (see corresponding section).

Del mismo modo, el CCN desarrolló en el año 2015 los criterios para alcanzar el cumplimiento con el ENS y su correspondiente **Declaración y Certificación de Conformidad**, de aplicación a sistemas de categoría Básica y Media o Alta, respectivamente. En principio, todos los sistemas del ámbito de aplicación del ENS deberían haber estado adecuados antes del 4 de noviembre de 2017. Sin embargo, a finales de 2018, poco más del 68% lo estaban.

Likewise, in 2015, the CCN developed the criteria to achieve compliance with the ENS and its corresponding **Declaration and Certification of Conformity**, applicable to Basic and Medium or High category systems, respectively. In principle, all systems within the scope of the ENS should have been adapted by 4th November 2017. However, by the end of 2018, just over 68 % were.



Índice de adecuación de los sistemas de la Administración al ENS
Index of adequacy of the Administrationıs systems to the ENS

2007
Ley/Law 11/2007
Ley/Law 37/2007 RISP
RD 1720/20017
Orden/Order PRE/2470/2007
Reglamento de evaluación y certificación de TI/Regulations of IT evaluation and certification

2009
RD 1671/2009
Declaración Ministerial Malmö /Malmö Ministerial Declaration

2010
ENI
ENS
EIF v1

2011
NTIs
Doc-e, Exp-e
Digitalización /Digitalization
RD 1708/2011
Ley/Law 18/2011 EJIS
Ley/Law 8/2011 PIC
RD 721/2011 PIC
AVANZA2

2012
NTI
Política de gestión de documentos-e /e-documents management policy
Esquema de Metadatos
Guías de aplicación /Metadata Scheme Application Guides
Plan MEJORA/MEJORA Plan

2013
Estrategia Ciberseguridad /Cybersecurity Strategy
Informe CORA/CORA Report
Ley/Law 19/2013
Transparencia /Transparency
Agenda Digital España/Digital Schedule Spain

2014
RD 806/14
Gobernanza/Governance
RD 802/14 DTIC
CI@ve
Reglamento UE eIDAS/EU eIDAS Regulations
R.E.(UE) 2015/1501
Marco Int. eIDAS /International Framework eIDAS

2015
Estrategia para un Mercado Único Digital/Strategy for a Digital Single Market
Ley/Law 39/2015, Ley/Law 40/2015
Estrategia TIC AGE/Strategy ICT AGE
Declaración servicios compartidos/Shared services declaration
RD 951/2015 modif ENS

2016
ENS-ITS
Conformidad
Informe ENS/ENS Report Conformity
RGPD/GDPR
Dir.NIS
Dir. Accesibilidad /Dir. Accessibility
eGov Action Plan

2017
Plan TRANSFORMA /TRANSFORMA Plan
Marco Europeo de Interop. EIF v2/European Interoperability Framework EIF v2
Declaración Ministerial Tallín/Tallin Ministerial Declaration
Estrategia de Seguridad Nacional/National Security Strategy

2018
ENS-ITS
Auditoría/Audit
Notificación de incidentes /Incidents notification
RDL 12/2018 NIS
RD Accesibilidad/RD Accessibility
LO 3/2018 PDP y GDD/LO 3/2018 PDP and GDD
LINCE Certificación productos /LINCE Products Certification

2019
Guía nacional de notificación y Gestión de ciberincidentes/National Guide of notification and management of cyber incidents
ACM centro de operaciones de Ciberseguridad/ACM Cybersecurity Operations Centre
Estrategia Nacional de Ciberseguridad 2019/National Cybersecurity Strategy
Reglamento de la ciberseguridad /Cybersecurity Regulations

Tras dos años de funcionamiento del esquema de certificación del ENS, al término del 2018, existían tan solo 26 organismos públicos certificados ante el mismo, frente a 101 empresas privadas.

After two years of operation of the ENS certification framework, at the end of 2018, there were only 26 public bodies certified, compared to 101 private companies.

Acreditación ENS			Acreditación STIC (DL)		
Acreditadas		En proceso	Acreditadas		
AENOR	Cámara Certifica	OCA GLOBAL	AENOR	Isdefe	Sidertia
AUDERTIS	LEET	EC	AUDERTIS	Entelgy Innotec	
BDO	Applus+				

Entidades de certificación acreditadas

Accredited certification entities

Informe Nacional del Estado de Seguridad (INES)
National Security Status Report (INES)

EL CCN desarrolló la solución INES (Informe Nacional del Estado de Seguridad) buscando cumplir con la obligación, por parte de las Administraciones Públicas, de evaluar regularmente el estado de la seguridad de los sistemas. Para cumplir con este mandato, INES proporciona un conocimiento más rápido e intuitivo de su nivel de adecuación al ENS y del estado de seguridad de sus sistemas.

Para ello, permite la recogida de información organizada, delegada y supervisada. Desde el año 2014 se viene recopilando la información anualmente de forma que pueda verse la evolución del país y que cada organismo pueda cotejar su posición particular respecto a la media nacional.

The CCN developed the INES solution (National Security Status Report) seeking to comply with the obligation of the Public Administrations to regularly evaluate the security status of the systems. In order to comply with this mandate, INES provides a quicker and more intuitive knowledge of their level of adaptation to the ENS and the security status of their systems.

To this end, it allows for the collection of organised, delegated and supervised information. Since 2014, information has been compiled annually so that the evolution of the country can be seen and each organization can compare its particular position with respect to the national average.

En el año 2018, se creó el **Consejo de Certificación del Esquema Nacional de Seguridad (CoCENS)** cuyo objetivo es ayudar a la adecuada implantación del ENS y, en consecuencia, a la mejor y más garante prestación de los servicios públicos, objetivo último del ENS. Como queda recogido en la guía CCN-STIC 809 Declaración y Certificación de Conformidad con el ENS y distintivos de cumplimiento, corresponde al CoCENS las siguientes funciones:

a. Velar por la adecuada implantación de la Certificación del ENS, adoptando las medidas que, en Derecho, correspondan.

b. Alentar los procesos de Certificación de la Conformidad con el ENS en las entidades de su ámbito subjetivo de aplicación, de los sectores público y privado.

c. Proponer para su análisis y, en su caso, redactar y publicar Normas, Criterios o Buenas Prácticas en materia de Certificación de la Conformidad con el ENS.

d. Asesorar a las partes implicadas respecto de los métodos, procedimientos, herramientas y criterios en materia de Certificación de la Conformidad con el ENS y, en general, con su implantación, orientando su gestión al mejor servicio del sector público y la mayor y mejor colaboración con el sector privado, fabricantes y suministradores de productos o servicios.

e. Asesorar a las partes implicadas en la identificación de otros esquemas, arreglos o acuerdos, donde la defensa de la validez y reconocimiento mutuo de los certificados emitidos sea de interés para los sectores público y privado.

f. Informar a sus Departamentos constituyentes y al Consejo Nacional de Ciberseguridad sobre el grado de implantación de la certificación de Conformidad con el Esquema Nacional de Seguridad.

In 2018, the **Certification Council of the National Security Framework (CoCENS)** was created with the aim of helping the proper implementation of the ENS and, consequently, the best and most reliable provision of public services, the ultimate objective of the ENS. As stated in the guide CCN-STIC 809 Declaration and Certification of Conformity with the ENS and compliance marks, the CoCENS has the following functions:

a. Ensuring the adequate implementation of the ENS Certification, adopting the measures that, in Law, correspond.

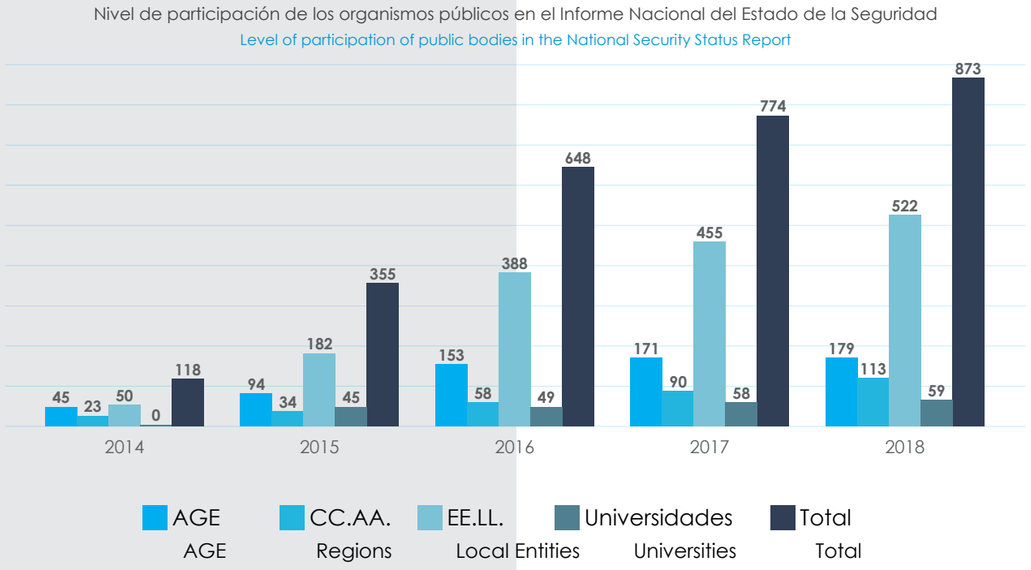
b. To encourage the processes of Certification of Conformity with the ENS in the entities of its subjective scope of application, in the public and private sectors.

c. To propose for analysis and, where appropriate, `to draft and publish Standards, Criteria or Good Practices in the field of Certification of Conformity with the ENS.

d. To advise the parties involved regarding the methods, procedures, tools and criteria for the Certification of Conformity with the ENS and, in general, its implementation, orienting its management to the best service of the public sector and the greatest and best collaboration with the private sector, manufacturers and suppliers of products or services.

e. To advise the parties involved in the identification of other frameworks, arrangements or agreements, where the defence of the validity and mutual recognition of the certificates issued is of interest to the public and private sectors.

f. To inform its constituent Departments and the National Cybersecurity Council about the degree of implementation of the Certification of Conformity with the National Security Framework.



Próximos objetivos del ENS
Next objectives of the ENS

En los próximos meses se espera adoptar las siguientes medidas:

- Plena implantación del ENS, flexibilizando su aplicación a las necesidades específicas de cada Organismo.
- Actualización del ENS, para facilitar la respuesta a tendencias y necesidades de seguridad.
- Alineamiento y claridad para proporcionar seguridad en la Administración Digital, eliminando aspectos no necesarios o excesivos.

Todo ello, unido al desarrollo del **Centro de Operaciones de Ciberseguridad de la AGE** y continuando con las Instrucciones Técnicas de Seguridad.

The following measures are expected to be taken in the coming months:

- Full implementation of the ENS, adapting its application to the specific needs of each organization.
- ENS update, to facilitate the response to security trends and needs.
- Alignment and clarity to provide security in the Digital Administration, removing unnecessary or excessive aspects.

All this together with the developing of the **AGE's Security Operations Centre** and the continuation of the Technical Security Instructions.

4.3 Directiva NIS
NIS Directive

El 6 de julio de 2016 la Unión Europea publicó en su Boletín Oficial la **Directiva (UE) 2016/1148** relativa a las médidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (más conocida como Directiva NIS). Sin embargo, la trasposición al ordenamiento jurídico español se realizó dos años después; en concreto en el **Real Decreto-ley 12/2018,** de 7 de septiembre, de seguridad de las redes y sistemas de información.

La Directiva NIS busca mejorar la fragmentación existente en los Estados y homogeneizar los distintos planteamientos, estableciendo **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 todos ellos les 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 los diferentes Estados Miembros.

On 6th July 2016 the European Union published in its Official Journal the **Directive (EU) 2016/1148** on measures to ensure a high common level of security of networks and information systems in the Union (better known as the NIS Directive). However, the transposition into Spanish law took place two years later, specifically in **Royal Decree-Law 12/2018**, dated 7th September, on the security of networks and information systems.

The NIS Directive seeks to improve the fragmentation of the States and homogenise the different approaches by establishing **common minimum requirements** for capacity building and planning, exchange of information, cooperation and common security requirements for essential service operators and digital service providers. It urges all of them to take appropriate measures to manage security risks and to report incidents that would have a significant disruptive effect to the Competent National Authorities, proposing the creation of a cooperation network between the different Member States.

4.4 Reglamento General de Protección de Datos (RGPD)
General Data Protection Regulation (GDPR)

También en el año 2016, la UE aprobó el Reglamento General de Protección de Datos (RGPD) que, si bien entró en vigor en mayo de ese año, fue de aplicación a partir del **25 de mayo de 2018**. Al tratarse de un Reglamento no necesita trasposición al ordenamiento jurídico español, por lo que su contenido es directamente aplicable.

Esta norma europea desplazó a la Ley Orgánica 15/1999,

In 2016, the European Union approved the General Data Protection Regulation (GPDR) which, although it entered into force in May of that year, was applicable from **25th May 2018**. Since this is a Regulation, it does not need to be transposed into Spanish law, and its content is therefore directly applicable.

de 13 de diciembre, de Protección de Datos de Carácter Personal y su Reglamento de Desarrollo, e introdujo una serie de cambios en los tratamientos de datos personales que realicen los responsables, así como las notificaciones de quiebras de seguridad que puedan afectar a estos y las evaluaciones de impacto en la protección de datos.

Con el fin de adaptar este marco normativo, el Consejo de Ministros en su sesión de 10 de noviembre de 2017 aprobó un proyecto de ley orgánica, remitido a las Cortes Generales, que actualmente se encuentra en tramitación parlamentaria. Además, en 2018, se aprobó el **Real Decreto-ley 5/2018, de 27 de julio**, de medidas urgentes para la adaptación del Derecho español a la normativa de la UE en materia de protección de datos.

Ante la nueva situación, el CCN, junto a la **Agencia Española de Protección de Datos (AEPD)**, estableció un mecanismo de colaboración, con el objetivo de ofrecer al Sector Público una referencia de cumplimiento normativo en materia de protección de datos y seguridad ante la entrada en vigor del RGPD.

Fruto de esta colaboración, el CCN-CERT y la AEPD trabajaron de forma conjunta para ofrecer una solución que facilitase esta labor. Así, la herramienta **PILAR** incluye un módulo de cumplimiento que **permite a las AAPP verificar los requisitos establecidos en el RGPD**, facilitando la gestión normativa tanto del Reglamento como del ENS.

This European regulation displaced Organic Law 15/1999, dated 13th December, on the Protection of Personal Data and its Implementing Regulations, and introduced a series of changes in the processing of personal data carried out by those responsible, as well as notifications of security breaches that may affect these and the impact assessments on data protection.

With the aim of adopting this regulatory framework, the Council of Ministers at its session of 10th November 2017 approved a draft organic law, submitted to the Cortes Generales (Spanish Parliament), which is currently in parliamentary procedure. In addition, in 2018, **Royal Decree-Law 5/2018 of 27th July** on urgent measures for the adaptation of Spanish law to EU legislation on data protection was approved.

In view of the new situation, the CCN, together with the **Spanish Data Protection Agency (AEPD)**, established a collaboration mechanism, with the aim of offering the public sector a reference of regulatory compliance in the area of data protection and security before the entry into force of the RGPD.

As a result of this collaboration, the CCN-CERT and the AEPD worked together to offer a solution to facilitate this work. Thus, the **PILAR** tool includes a compliance module that **allows the Public Administration to verify the requirements established in the GDPR**, facilitating the regulatory management of both the Regulation and the ENS.

FORMACIÓN

TRAINING

Para lograr un ciberespacio seguro, en el que los riesgos puedan mitigarse hasta un margen asumible, es fundamental concienciar y sensibilizar a la sociedad, pues solo a través de una capacitación continua se pueden prevenir y tratar de manera oportuna los incidentes de ciberseguridad.

Ante la necesidad de fomentar y desarrollar perfiles profesionales cualificados para el Sector Público, el CCN ofrece un amplio programa de **cursos formativos**, adaptado a las necesidades planteadas por su comunidad de referencia. Este **Plan de Formación**, con un diseño curricular y flexible, se ha ido transformando a medida que lo han hecho las tecnologías, adaptándose así al nuevo escenario que presenta el ciberespacio.

La oferta formativa del CCN se ha elaborado para dar una respuesta eficaz a los retos del siglo XXI. Ante la necesidad de que esta respuesta sea global, el CCN pone a disposición del Sector Público, del sector privado e, incluso, de otros Estados, su conocimiento y experiencia en la formación de personal en el ámbito de la ciberseguridad.

Además, como garantía de superación de la formación realizada, el CCN otorga, a los concurrentes que la hayan superado con aprovechamiento, un certificado que especifica las materias y créditos asociados.

In order to achieve a safe cyberspace, where risks can be mitigated to an acceptable margin, it is essential to raise awareness among citizens, since only through continuous training can cybersecurity incidents be prevented and dealt with in a timely manner.

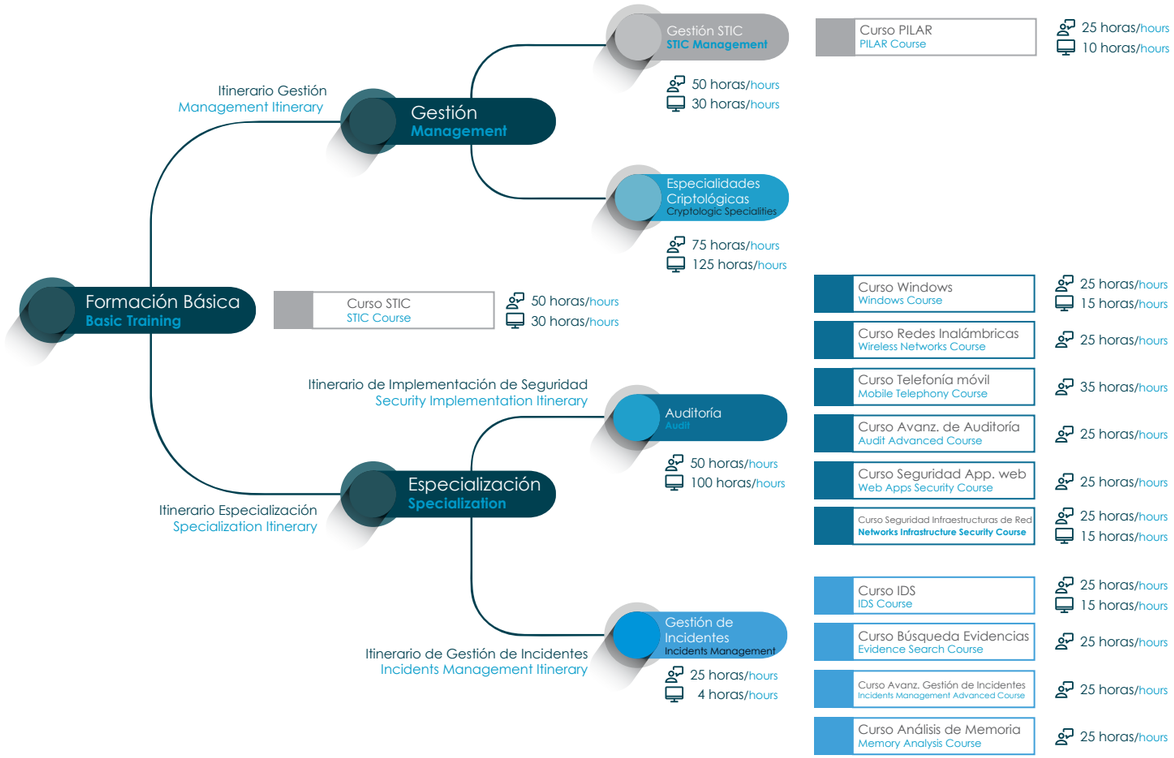
Faced with the need to promote and develop qualified professional profiles for the public sector, the CCN offers a wide range of **training courses**, adapted to the needs raised by its community of reference. This **Training Plan**, with a flexible curricular design, has been transformed as technologies have, adapting to the new cyberspace scenario.

The CCN's training offer has been designed to provide an effective response to the challenges of the 21st century. In view of the need for this response to be global, the CCN offers its knowledge and experience in training cybersecurity professionals to the public and private sector, and even other States.

In addition, as a guarantee of passing the training period, the CCN grants the attendees who have passed it successfully a certificate specifying the subjects and associated credits.

5.1 Itinerarios de FORMACIÓN
TRAINING itineraries

El Plan de Formación del CCN 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 esta, el profesional puede elegir entre dos (2) itinerarios: **gestión** o **especialización** (dirigido a personal más técnico).



The CCN Training Plan has been designed taking into account the need to train, both in the classroom and at a distance, qualified professionals with different profiles and levels of training. For this reason, a BASIC training has been established which, through the STIC Course, introduces the student to the field of ICT Security. Once completed, the professional may choose between two (2) itineraries: **management** or **specialization** (aimed at more technical staff).

5.2 FORMACIÓN online
Online TRAINING

Durante 2017 y 2018, el CCN ha seguido ampliando su oferta formativa a través de métodos de enseñanza a distancia y e-learning. Un total de 7.317 usuarios hicieron los cursos online durante el año 2017 y hasta 10.256 fueron los inscritos en 2018, lo que hace un total de 17.573 en los últimos dos años.

Los cursos disponibles en el portal del CCN-CERT son:

During 2017 and 2018, the CCN has continued extending its training offer, through online and e-learning teaching methods. A total of 7,317 users took the courses online during 2017 and up to 10,256 were enrolled in 2018, which makes a total of 17,573 in the last two years.

The courses available on the CCN-CERT website are:

Un total de 17.573 usuarios hicieron alguno de los cursos online del CCN (2017-2018)

A total of 17,573 users took one of the CCN's online courses (2017-2018)

CURSOS GENERALES
GENERAL COURSES

Cursos online de acceso público (sin certificado) o de acceso restringido a los usuarios registrados del portal.

Online courses of public access (without certificate) or of access limited to users who are registered on the 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 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

- Basic Linux Fundamentals Course
- National Security Framework Introduction
- INES Course (National Security Status Report)
- Basic STIC Course – Windows Environments Security
- Analysis and Risk Management on Information Systems Course
- National Security Framework Course
- Information and Communication Technologies Security Course

CURSOS «AD HOC»
«AD HOC» COURSES

Cursos específicos desarrollados por el CCN a petición de una organización.

Specific courses created by the CCN at the request of an organization.

5.3 VANESA

VANESA

La solución VANESA, del CCN-CERT, es una plataforma de **retransmisión** de sesiones formativas en directo, que permite la asistencia de cientos de personas desde cualquier lugar del mundo.

Además, conserva las grabaciones y el material empleado, de manera que permite su posterior visionado.

Durante 2017 y 2018 se realizaron 24 sesiones formativas con 4.559 alumnos inscritos en cursos de diversas temáticas, entre las que destacaron las siguientes: soluciones CCN-CERT, Productos y Tecnologías de Ciberseguridad, Auditoría, Malware y código dañino, Gestión de Incidentes y Nuevas Tecnologías y Big Data.

The CCN-CERT VANESA solution is a platform for **broadcasting** live training sessions, which allows the assistance of hundreds of people from anywhere in the world.

In addition, it preserves the recordings and the material used, allowing its later viewing.

During 2017 and 2018, 24 training sessions were held with 4,559 students enrolled in courses on various subjects, some of them stand out: CCN-CERT solutions, Cybersecurity Products and Technologies, Auditing, Malware, Incident Management and New Technologies, 5G and Big Data.

5.4 ATENEA

ATENEA

En diciembre de 2017 se lanzó Atenea, la **plataforma de desafíos** del CCN-CERT que, mediante una serie de retos de distinta dificultad y muy diversas temáticas (criptografía y esteganografía, exploiting, forense, análisis de tráfico, reversing, etc.) permite al usuario demostrar sus conocimientos y destrezas.

Fue desarrollada con el fin de que cualquier persona con inquietudes en el campo de la ciberseguridad pueda poner a prueba su conocimiento. 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 para demostrar su ingenio y capacidad.
- Mostrar a las personas con menos experiencia que los retos son divertidos y que la seguridad no es una ciencia secreta que nunca entenderán.

Desde su puesta en marcha, han sido 77 los retos publicados y 7.694 las personas inscritas.

Se han publicado 77 retos en Atenea y hay 7.694 personas inscritas

77 challenges have been published in Athena and there are 7,694 people registered.

In December 2017, ATENEA was launched, the CCN-CERT **challenges platform** that, through a series of challenges of different difficulty and very diverse topics (cryptography and steganography, exploiting, forensics, traffic analysis, reversing, etc.) allows users to demonstrate their knowledge and skills.

It was developed with the aim of allowing anyone with concerns in the field of cybersecurity test their knowledge. Among its main objectives are:

- To make ICT staff aware of the existing risks in this field.
- To involve professionals with experience in cybersecurity so that they can demonstrate their ingenuity and abilities.
- To show people with little experience that challenges are fun and that security is not a secret science that they will never understand.

Since its inception, 77 challenges have been published and 7,694 people registered.

5.5 ATENEA ESCUELA

ATENEA SCHOOL

Ante el éxito de acogida de Atenea, en 2018, el CCN-CERT decidió lanzar una nueva plataforma de desafíos, pero esta vez con un nivel más básico, conscientes de la necesidad de fomentar el conocimiento y el uso seguro de las TIC, tanto en el Sector Público como en la ciudadanía en general. Atenea Escuela está compuesta por diferentes retos para fomentar el aprendizaje de los usuarios menos entendidos en el campo de la seguridad.

91

Número de retos que hay publicados hasta la fecha en Atenea Escuela

Number of challenges published to date in ATENEA School

Given the success of Atenea, the CCN-CERT decided in 2018 to launch a new platform of challenges, but this time with a more basic level, aware of the need to promote knowledge and safe use of ICT systems, both in the Public Sector and in the general public. Atenea School comprises different challenges to encourage the learning of users with little knowledge in security. 91 challenges have been published so far.

Guías CCN-STIC

CCN-STIC Security Guides

Las **Series CCN-STIC** son normas, instrucciones, guías y recomendaciones desarrolladas por el CCN, con el fin de mejorar el grado de ciberseguridad de las organizaciones. Periódicamente son actualizadas y completadas con otras nuevas, en función de las amenazas y vulnerabilidades detectadas por el CCN-CERT.

Concretamente, en 2017 se publicaron 29 nuevas guías y en 2018 otras 28. En cuanto a aquellas que ya estaban publicadas, pero fue necesario actualizar, en 2017 ascendieron a 22 y en 2018 sumaron 25. Gracias a estos 129 nuevos documentos, al término de 2018 había 356 Guías CCN-STIC, 85 de las cuales están fuera de soporte.

Además, el CCN colabora en la elaboración de otras guías destacadas de organismos nacionales e internacionales, como fue el caso de la editada por la Agencia Europea de Cibersguridad (**ENISA**), con quién se elaboró una Guía de Buenas Prácticas para el uso de taxonomías en la detección y prevención de incidentes de seguridad, en 2017.

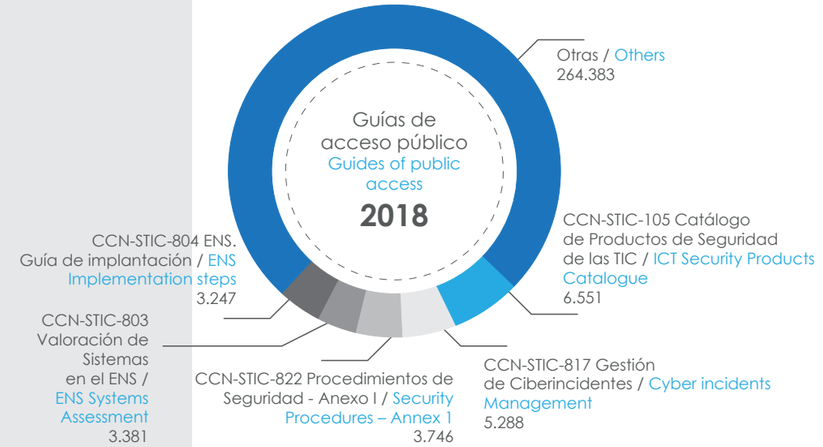
The **CCN-STIC series** is made up of regulations, guidelines, guides and recommendations developed by the CCN in order to enhance cybersecurity within organizations. These guides are regularly updated and supplemented with new information, according to the threats and vulnerabilities detected by the CCN-CERT.

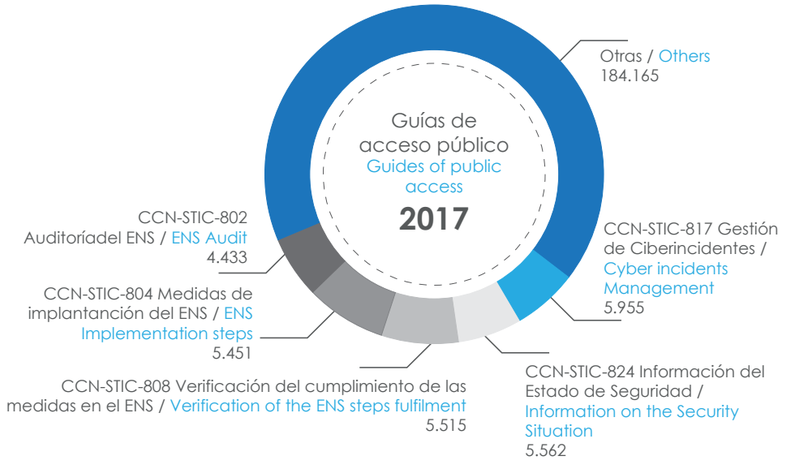
Specifically, 29 new guides were published in 2017 and 28 in 2018. As for those that were already published, but it was necessary to update, in 2017 there were 22 and in 2018 there were 25. Thanks to these 129 new documents, by the end of 2018 there were 356 CCN-STIC Guides, 85 of which are no longer being updated.

In addition, the CCN collaborates in the elaboration of other outstanding guides of national and international organizations, as was the case of the one published by the European Union Agency for Cybersecurity (**ENISA**) in 2017 on Best Practices for the use of taxonomies in the detection and prevention of security incidents.

Número de descargas del portal del CCN-CERT
Number of CCN-CERT's website downloads

Al término de 2018 había 356 Guías CCN-STIC
At the end of 2018 there were 356 CCN-STIC Guides





Listado de Guías CCN-STIC 2018
List of CCN-STIC 2018 Guides

Fuera de soporte / Out of support — * **Difusión limitada** / Limited difussion — ** **Confidencial** / Confidential

Serie 000: Políticas
SERIE 000: POLICIES

001	Seguridad de las TIC en la Administración ICT Security in the Public Administration	JUN 16
002	Coordinación Criptológica en la Administración Cryptologic Coordination	MAR 11
003*	Uso cifradores certificados protección inf. clasificada Use of Certified Cipher Equipment	MAY 13

Serie 100: Procedimientos
SERIE 100: PROCEDURE

101	Acreditación sistemas que manejan Información Nacional Clasificada en la Administración National Accreditation Procedure in Public Administration	DIC 16
102*	Procedimiento de evaluación de productos criptológicos Cryptologic products evaluation procedure	OCT 17
103*	Catálogo de productos con certificación criptológica Catalogue of products with cryptologic certification	JUL 16
104	Catálogo de Productos con clasificación Zoning Zoning products clasification catalogue	ENE 19
105	Catálogo de productos STIC (CPSTIC) Catalogue of products SICT	MAY 19
106	Inclusión productos STIC cualificados en el Catálogo de Productos Inclusion of products SICT in the catalogue of products	ABR 19
120	Procedimiento de certificación de empresas para la realización de auditorías Procedure for the certification of companies to carry out audits	OCT 18
130*	Requisitos de los productos de cifra para superar la evaluación criptológica Requirements of the code products to pass the cryptological evaluation	OCT 17
140	Taxonomías de referencia para productos de seguridad TIC Reference taxonomies for ICT security products	JUL 19
151*	Evaluación y Clasificación TEMPEST de Equipos TEMPEST Evaluation and Classification of Equipment	MAR 17
152*	Evaluación y Clasificación ZONING de Locales Facility ZONING, Evaluation and Classification	MAR 17
153	Evaluación y Clasificación de Armarios Apantallados Evaluation and Classification of Shielded Cabinets	MAR 17
154*	Medidas de protección TEMPEST para instalaciones Protection TEMPEST Measures for Facilities	MAR 17

Serie 200: Normas
SERIE 200: STANDARDS

201	Organización y gestión para la seguridad Organization and management for security	ENE 09
202	Estructura y Contenido Declaración Requisitos Seg. DRS SSRS. Structure and Content	MAR 05
203	Estructura y Contenido Procedimientos Operativos POS SecOps. Structure and Content	MAR 05
204	Estructura y Contenido CO-DRES-PO estaciones aisladas y pequeñas redes. Formulario CO-DRES-POC Structure and Content Isolated station and smal networks. Form	ENE 09
205	Actividades Seguridad Ciclo Vida CIS Security Life Cycle Activities (CIS)	DIC 07
207	Estructura y Contenido del Concepto de Operación Concept of Operation. Structure and Content	NOV 05
210*	Norma de Seguridad en las Emanaciones TEMPEST Security Standard TEMPEST Emanations	JUL 12
211*	Gestión del material de cifra en las cuentas de cifra Encryption material managment	Pendiente

Serie 300: Instrucciones Técnicas
SERIE 300: TECHNICAL INSTRUCTIONS

301	Requisitos STIC SICT Security Requirements	ABR 18
302	Interconexión sistemas que manejan inform. nacional clasificada en la Administración Interconnection of systems managment classified national information	JUL 12
303	Inspección STIC SICT Security Inspection	ENE 09
304	Baja y destrucción de Material Criptológico Destructing and Taking Cryptologic material out of Circulation	MAR 11
305	Destrucción y sanitización de Soportes Media Sanitization and Destruction	MAY 17
307*	Seguridad en Sistemas Multifunción Security in Multifunction Systems	ENE 09

Serie 400: Guías Generales
SERIE 400: GENERAL GUIDES

400	Manual STIC SICT Security Manual	MAY 13
401	Glosario / Abreviaturas Glossary / Abbreviations	MAR 18
402	Organización y Gestión STIC SICT Security Organization and Management	DIC 06
403	Gestión de Incidentes de Seguridad Security Incidents Management	DIC 07
404	Control de soportes informáticos Computing Devices Control	DIC 06
405	Algoritmos y parámetros de firma electrónica Electronic Signature: Algorithms and Parameters	FEB 12
406	Seguridad en redes inalámbricas estándar 802.11 Wireless Security	JUL 17
407	Seguridad en telefonía móvil Mobile Phone Security	DIC 06
408	Seguridad perimetral – Cortafuegos Perimeter Security – Firewalls	MAR 10
409A*	Colocación de Etiquetas de Seguridad Security Labels	MAY 13
409B**	Colocación de Etiquetas de Seguridad en Equipos de Cifra Security Labels in Encryption Equipments	MAY 13
410	Análisis riesgos en sistemas de la Administración Risk Analysis in the Administration	DIC 06
411	Modelo de Plan de Verificación STIC Plan Model of ICT Security verification	ENE 09
412	Requisitos seguridad entornos y aplicaciones Web Security Requirements for Environments and Web Applications	ENE 09
414	Seguridad en Voz sobre IP VoIP Security	ENE 09
415	Identificación y Autenticación Electrónica Electronic Identification and Authentication	DIC 07
416	Seguridad en Redes Privadas Virtuales VPN Security	DIC 07
417	Seguridad en PABX PABX Security	MAY 10
418	Seguridad en Bluetooth Bluetooth Security	ENE 09
419	Configuración Segura con IPtables Secure Configuration with IPtables	DIC 07
421	Copias de seguridad y recuperación ante desastres Backup and disaster recovery	Pendiente
422	Desarrollo seguro de aplicaciones web Secure Development of web applications	JUL 13
423	Indicadores de Compromiso (IOC) Indicators of Commitment (IOC)	OCT 15
424	Intercambio de información de ciberamenazas. STIX-TAXII. Empleo en REYES Exchange of information on cyberthreats. STIX-TAXII. Employment in REYES	OCT 15
425	Seguridad en IP versión 6 IPv6 Security	OCT 15
426	REYES. Manual de usuario REYES. Handbook	NOV 17
430	Herramientas de Seguridad Security Tools	ENE 09
431	Herramientas de Análisis de Vulnerabilidades Tools for Vulnerabilities Evaluation	DIC 06
432	Seguridad Perimetral – IDS Perimeter Security – Intrusion Detection Systems	ENE 09
434	Herramientas para el análisis de ficheros de logs Tools for Log Files Analysis	JUN 09
435	Herramientas de monitorización de tráfico Tools for Data Flow Monitoring	DIC 12
436	Herramientas de análisis de contraseñas Password Analysis Tools	DIC 07
437	Herramientas de cifrado software Encryption Software Tools	DIC 07
438	Esteganografía Steganographia	SEP 11
440	Mensajería Instantánea Instant Messaging	DIC 07
441	Configuración Segura de entornos virtuales VMWare Secure Configuration of VMWare	ENE 10
443	Tecnología de identificación por radiofrecuencia RFID RFID	ENE 09
444	Seguridad en redes inalámbricas IEEE 802.16 WiMAX WiMax Security	MAR 11
445A	Curso Especialidades Criptológicas. Probabilidad (correspondencia) Cryptologic Specialised Course (CEC) – Probability	JUL 10
445B	Curso de Especialidades Criptológicas. Principios digitales (correspondencia) Cryptology Specialist Course. Digital Principles	JUL 10
445C	Curso de Especialidades Criptológicas. Teoría de números (correspondencia) CEC – Numbers Theory	JUL 10
450	Seguridad en dispositivos móviles Security on Mobile Devices	MAY 13
451	Seguridad en Windows Mobile 6.1 Security on Windows Mobile 6.1	MAY 13
452	Seguridad en Windows Mobile 6.5 Security on Windows Mobile 6.5	MAY 13
453	Seguridad en Android 2.1 Security in Android 2.1	MAY 13
453B	Seguridad en dispositivos móviles: Android 4.x Security in Android 4.x	ABR 15
453C	Seguridad en dispositivos móviles: Android 5.x Security in Android 5.x	MAR 18
453D	Seguridad en dispositivos móviles: Android 6.x Security in Android 6.x	JUN 18
453E	Seguridad en dispositivos móviles: Android 7.x Security in Android 7.x	SEP 18
453F	Seguridad en dispositivos móviles: Android 8.x Security in Android 8.x	MAR 19
453G	Seguridad en dispositivos móviles: Android 9.x Security in Android 9.x	MAR 19
454	Seguridad en dispositivos móviles iPad (iOS 7.x) Security in iPad (iOS 7.x)	JUL 14
455	Seguridad en dispositivos móviles iPhone (iOS 7.x) Security in iPhone (iOS 7.x)	JUL 14
455B	Seguridad en dispositivos móviles iPhone (iOS 10.x) Security in iPhone (iOS 10.x)	Pendiente
455C	Seguridad en dispositivos móviles iPhone (iOS 11.x) Security in iPhone (iOS 11.x)	OCT 18
455D	Seguridad en dispositivos móviles iPhone (iOS 12.x) Security in iPhone (iOS 12.x)	OCT 18
456	Servicios Google para Android Google Services for Android	SEP 18
457	Herramientas de gestión de dispositivos móviles: MDM Mobile Device Management Tool	NOV 13
460	Seguridad en WordPress WordPress Security	JUL 15
461	Seguridad en Drupal Drupal Security	JUN 16
462	Seguridad en Joomla Joomla Security	AGO 16
470A	Manual de usuario PILAR 4.1 PILAR 4.1 Handbook	DIC 07
470B	Manual de usuario PILAR 4.3 PILAR 4.3 Handbook	DIC 08
470C	Manual de usuario PILAR 4.4 PILAR 4.4 Handbook	FEB 10
470D	Manual de usuario PILAR 5.1 PILAR 5.1 Handbook	MAY 11
470E1	Manual de usuario PILAR 5.2 PILAR 5.2 Handbook	JUL 12
470E2	Manual de usuario PILAR 5.2. Análisis del Impacto y Continuidad del Negocio PILAR 5.2 Impact Analysis and Business Continuity Handbook	JUL 12
470F1	Manual de usuario PILAR 5.3 PILAR 5.3 Handbook	NOV 13
470F2	Manual de usuario PILAR 5.3. Análisis del Impacto y Continuidad del Negocio PILAR 5.3 Impact Analysis and Business Continuity Handbook	NOV 13
470G1	Manual de usuario PILAR 5.4 PILAR 5.4 Handbook	AGO 14
470G2	Manual de usuario PILAR 5.4. Análisis del Impacto y Continuidad del Negocio PILAR 5.4 Impact Analysis and Business Continuity Handbook	AGO 14
470H1	Manual de usuario PILAR 6.2 PILAR 6.2 Handbook	ABR 17
470H2	Manual de usuario PILAR 6.2. Análisis del Impacto y Continuidad del Negocio PILAR 6.2 Impact Analysis and Business Continuity Handbook	ABR 17
470I1	Manual de usuario PILAR 7 PILAR 7 Handbook	MAY 18
470I2	Manual de usuario PILAR 7. Análisis del Impacto y Continuidad del Negocio PILAR 7 Impact Analysis and Business Continuity Handbook	MAY 18
471B	Manual de Usuario de RMAT 4.3 RMAT 4.3 Handbook	DIC 08
471C	Manual de Usuario de RMAT 5.1 RMAT 5.1 Handbook	AGO 11
471D	Manual de Usuario de RMAT 5.4 RMAT 5.4 Handbook	AGO 14
471E	Manual de Usuario de RMAT 5.5 RMAT 5.5 Handbook	ABR 17
472A	Manual de usuario PILAR BASIC 4.3 PILAR BASIC 4.3 Handbook	DIC 08
472B	Manual de usuario PILAR BASIC 4.4 PILAR BASIC 4.4 Handbook	FEB 10
472C	Manual de usuario PILAR BASIC 5.2 PILAR BASIC 5.2 Handbook	JUL 12
472D	Manual de usuario PILAR BASIC 5.3 PILAR BASIC 5.3 Handbook	NOV 13
472E	Manual de usuario PILAR BASIC 5.4 PILAR BASIC 5.4 Handbook	AGO 14
472F	Manual de usuario PILAR BASIC 6.2 PILAR BASIC 6.2 Handbook	ABR 17
472G	Manual de usuario PILAR BASIC 7 PILAR BASIC 7 Handbook	MAY 18
473A	Manual de usuario µPILAR µPILAR Handbook	MAR 11
473B	Manual de usuario µPILAR 5.2 µPILAR 5.2 Handbook	JUL 12
473C	Manual de usuario µPILAR 5.3 µPILAR 5.3 Handbook	NOV 13
473D	Manual de usuario µPILAR 5.4 µPILAR 5.4 Handbook	AGO 14
473E	Manual de usuario µPILAR 6.2 µPILAR 6.2 Handbook	ABR 17
473F	Manual de usuario µPILAR 7 µPILAR 7 Handbook	MAY 18
480	Seguridad en Sistemas SCADA Security on SCADA systems	MAR 10
480A	Seguridad en el control de procesos y SCADA. Guía de Buenas Prácticas SCADA- Best Practices	FEB 10
480B	Seguridad en el control procesos SCADA. Guía 1. Comprender el Riesgo del Negocio SCADA- Understanding Business Risks	MAR 10

Fuera de soporte / Out of support
***** **Difusión limitada** / Limited difussion
****** **Confidencial** / Confidential

480C	Seguridad en el control de procesos y SCADA. Guía 2. Implementar una Arquitectura Segura SCADA- Implementing Secure Architecture	MAR 10
480D	Seguridad en el control de procesos y SCADA. Guía 3. Establecer Capacidades de Respuesta SCADA- Establishing Response Capabilities	MAR 10
480E	Seguridad en el control de procesos SCADA. Guía 4. Mejorar la concienciación y las habilidades Improving Awareness and Capabilities	ENE 10
480F	Seguridad en el control de procesos y SCADA. Guía 5. Gestionar el riesgo de terceros SCADA- Dealing with Risks Derived from Third Parties	MAR 09
480G	Seguridad en el control de procesos y SCADA. Guía 6. Afrontar Proyectos SCADA- Confront Projects	MAR 09
480H	Seguridad en el control de procesos y SCADA . Guía 7. Establecer una dirección permanente SCADA – Establishing a Permanent Address	MAR 10
490	Dispositivos biométricos de huella dactilar Biometric Fingerprints Devices	DIC 07
491	Dispositivos biométricos de iris Iris Biometric Devices	DIC 08
492	Evaluación de parámetros de rendimiento en dispositivos biométricos Evaluation of Performance Parameters in Biometric Devices	MAR 11
495	Seguridad en IPv6 Security in IPv6	JUL 16
496	Comunicaciones móviles seguras Secure mobile communications	JUN 18
497*	Uso tecnologías inalámbricas wifi (802.11) en redes clasificadas Use of wireless wifi technologies (802.11) in classified networks	MAR 19

Serie 500: Guías de entornos Windows
SERIE 500: WINDOWS ENVIRONMENTS GUIDES

501A	Seguridad en Windows XP SP2 (cliente en dominio) Windows XP SP2 Security (client within a domain)	DIC 07
501B	Seguridad en Windows XP SP2 (cliente independiente) Windows XP SP2 Security (independent client)	DIC 07
502	Seguridad en Aplicaciones Cliente. Navegador y Correo Electrónico Client Windows Security: Browser and E-mail	DIC 08
502B	Seguridad en Aplicaciones Cliente Windows Vista. Navegador y Correo Electrónico Client Windows Vista Security. Browser and E-mail	ENE 10
503A	Seguridad en Windows 2003 Server (controlador de dominio) Windows 2003 Server Security (domain controller)	NOV 05
503B	Seguridad en Windows 2003 Server (servidor independiente Windows 2003 Server Security (independent server)	DIC 07
504	Seguridad en Internet Information Server Internet Information Server Security	OCT 05
505	Seguridad en Bases de Datos SQL 2000 BD SQL Security	DIC 06
506	Seguridad en Microsoft Exchange Server 2003 MS EXCHANGE Server 2003 Security	JUN 07
507	Seguridad en ISA Server ISA Server Security	DIC 06
508	Seguridad en Clientes Windows 2000 Windows 2000 Clients Security	DIC 07
509	Seguridad en Windows 2003 Server. Servidor de Ficheros Security on Windows 2003 Server. File Server	DIC 07
510	Seguridad en Windows 2003 Server. Servidor de Impresión Security on Windows 2003 Server. Printing Server	ENE 09
512	Gestión de Actualizaciones de Seguridad en Sistemas Windows Security Updates Management	DIC 05
515	Seguridad Servidor de Impresión en Windows 2008 Server R2 Print Server in Windows 2008 Server R2 Security	FEB 16
517A	Seguridad en Windows Vista (cliente en dominio) Windows Vista Security (client within a domain)	ENE 10
517B	Seguridad Windows Vista enterprise con SP1 (cliente independiente) Windows Vista enterprise Security with SP1 (independent client)	ENE 09
519A	Configuración Segura Internet Explorer 7 y Outlook en Windows XP Secure Configuration Internet Explorer 7 and Outlook in Windows XP	ENE 10
520	Configuración Segura de Internet Explorer 11 Secure Configuration of Internet Explorer 11	MAR 18
521A	Seguridad en Windows Server 2008 R2 (controlador de dominio o miembro) Windows 2008 Server Security (domain controller)	ABR 18
521B	Seguridad en Windows Server 2008 R2 Instalación completa e independiente Windows 2008 Server Security (independent server)	ABR 18
521C	Seguridad en Windows Server 2008 Core (controlador de dominio o miembro) Windows 2008 Server Core Security (domain controller)	MAY 18
521D	Seguridad en Windows Server 2008 R2 Core (servidor independiente) Windows 2008 Server Core Security (independent server)	JUN 13
522A	Seguridad en Windows 7 Enterprise (cliente en dominio) Windows 7 Security (domain client)	ABR 18
522B	Seguridad Windows 7 Enterprise (cliente independiente) Windows 7 Security (independent client)	ABR 18
523	Seguridad en Windows Server 2008 R2. Servidor de Ficheros Windows 2008 Server Security. File Server	FEB 12
524	Seguridad en Internet Information Server (IIS) 7.5 sobre Windows Server 2008 R2 Internet Information Server 7.5 Security	FEB 14
525	Microsoft Exchange Server 2007 sobre Windows Server 2003 Microsoft Exchange Server 2007 on Windows 2003 security	JUN 13
526	Seguridad en Microsoft Exchange Server 2007 sobre Windows Server 2008 Microsoft Exchange Server 2007 on Windows 2008 security	AGO 13
527	Microsoft Windows 2008 R2 clúster de conmutación Failover Clustering para Windows 2008 Server R2	AGO 13
528	Implementación Hyper-V sobre Windows 2008 R2 Core Hyper-V Windows 2008 Sever R2 Core Security	DIC 13
529	Seguridad en Microsoft Office 2013 Microsoft Office 2013 Security	ENE 15
530	Seguridad en Microsoft Office 2010 Microsoft Office 2010 Security	JUL 13
531	Seguridad en Sharepoint Server 2007 Sharepoint Server Security 2007	DIC 12
532	Seguridad en Microsoft Sharepoint Server 2007 sobre Windows Server 2008 R2 Microsoft Sharepoint Server 2007 on Windows Server 2008 R2 Security	SEP 14
533	Seguridad en Microsoft Sharepoint Server 2010 sobre Windows Server 2008 R2 Microsoft Sharepoint Server 2010 on Windows Server 2008 R2 Security	NOV 14
534	Seguridad en Microsoft SharePoint Server 2013 SP1 en Microsoft Windows Server 2012 R2 Microsoft SharePoint Server 2013 SP1 on Microsoft Windows Server 2012 R2 Security	ABR 17
540	Seguridad en Bases de Datos SQL Server 200 Database SQL Server 2000 Security	ABR 14
541	Microsoft SQL Server 2014 en Microsoft Windows Server 2012 R2 Microsoft SQL Server 2014 on Microsoft Windows Server 2012 R2 Security	ABR 17
550	Seguridad en Microsoft Exchange Server 2010 sobre Windows Server 2008 R2 Microsoft Exchange Server 2010 on Windows Server 2008 R2 Security	AGO 15
552	Microsoft Exchange Server 2013 en Windows Server 2012 R2 Microsoft Exchange Server 2013 on Windows Server 2012 R2	NOV 16
560A	Seguridad en Windows 2012 Server R2 (controlador de dominio) Windows 2012 Server R2 Security (domain controller)	ABR 18
560B	Seguridad en Windows 2012 Server R2 (servidor independiente) Windows 2012 Server R2 Security (independent server)	ABR 18
560C	Windows Server 2012 R2 instalación core, controlador de dominio o servidor miembro Windows Server 2012 R2 (domain controller)	MAY 18
561	Servidor de Impresión Windows Server 2012 R2 Print Server Windows Server 2012 R2	OCT 16
562	Servidor de Ficheros Windows Server 2012 R2 Data Server Windows Server 2012 R2	SEP 16
563	Internet Information Service 8.5 sobre Windows Server 2012 R2 en servidor miembro de dominio Internet Information Service 8.5 Windows Server 2012 R2 in domain controller	NOV 16
564	Cluster de conmutación por error Windows Server 2012 R2 Failover Cluster Windows Server 2012 R2	AGO 17
566	Servicios de escritorio remoto sobre Windows Server 2012 R2 Remote APP Windows Server 2012 R2	FEB 17
567	Implementación de Hiper V en MS Windows Server 2012 R2 core Hiper V MS Windows Server 2012 R2 core	DIC 16
568	Windows Server Update Service (WSUS) Windows Server Update Service (WSUS)	JUL 17
569	Terminal Server sobre Windows Server 2008 R2 Terminal Server on Windows Server 2008 R2	FEB 17
570A	Microsoft Windows Server 2016, instalación completa, controlador de dominio o servidor miembro Windows Srv. 2016, full install., domain controller or member server	DIC 18
570B	Microsoft Windows Server 2016, instalación completa, serv. indep. Microsoft Windows Server 2016, full installation, standalone server	DIC 18
572	Servidor de impresión Microsoft Windows Server 2016 Microsoft Windows Server 2016 Print Server	DIC 18
573	Servidor de Ficheros Windows Server 2016 Windows Server 2016 File Server	DIC 18
574	Implementación de Internet Information Service 10 sobre Windows Server 2016 en servidor miembro de dominio Implementation of Internet Information Service 10 on Windows Server 2016 on domain member server	DIC 18
575	Microsoft SQL Server 2016 en Microsoft Windows Server 2016 Microsoft SQL Server 2016 on Microsoft Windows Server 2016	MAY 19
576	Microsoft Exchange Server 2016 en Windows Server 2016 Microsoft Exchange Server 2016 on Windows Server 2016	JUN 19
577	Microsoft SharePoint Server 2016 en Microsoft Windows Server 2016 Microsoft SharePoint Server 2016 on Microsoft Windows Server 2016	Pendiente
578	Microsoft Hyper-V en Windows Server 2016 Microsoft Hyper-V on Windows Server 2016	FEB 19
585	Configuración segura en MS Office 2016 en Windows 10 Secure configuration in MS Office 2016 in Windows 10	FEB 19
590	Recolección y consolidación de eventos - Windows Server 2008 R2 Collecting and consolidating events Windows Server 2008 R2	ABR 14
593	Configuración segura SCCM 2012 sobre Windows Server R2 2012 SCCM 2012 Secure Configuration on Windows Server R2 2012	Pendiente
594	Configuración segura SCCM 2016 sobre Windows Server 2016 SCCM 2016 Secure Configuration on Windows Server 2016	Pendiente
595	Entidad de Certificación en Windows Server 2008 R2 Certification Entity in Windows Server 2008 R2	NOV 18
596	Protección de sistema con AppLocker AppLocker	FEB 16
597	Entidad de Certificación en Windows Server 2012 R2 Certification Entity in Windows Server 2012 R2	NOV 18
598	Entidad de Certificación en Windows Server 2016 Certification Entity in Windows Server 2016	Pendiente
599A	Configuración segura de Windows 10 (Cliente miembro de dominio) Secure Windows 10 Configuration (Client Domain Member)	DIC 17
599B	Configuración segura de Windows 10 (Cliente independiente) Secure Windows 10 Setup (Standalone Client)	DIC 17
599A18	Configuración segura de Windows 10 (Cliente miembro de dominio) Secure Windows 10 Configuration (Client Domain Member)	OCT 18
599B18	Configuración segura de Windows 10 (Cliente independiente) Secure Windows 10 Setup (Standalone Client)	OCT 18

Serie 600: Guías de otros entornos
SERIE 600: GUIDELINES FOR OTHER OS AND EQUIPMENT SECURITY

601	Seguridad en HP-UX v 10.20 HP-UX v 10.20 Security	DIC 06
602	Seguridad en HP-UX 11i HP-UX 11i Security	OCT 04
603	Seguridad en AIX-5L AIX-5L Security	MAR 11
606	Configuración segura en Mac OS X 10.10.X Yosemite Secure configuration Mac OS X 10.10 X Yosemite	SEP 15
610	Seguridad en Red Hat Linux 7 Red Hat Linux 7 Security	DIC 06
611	Seguridad en Suse Linux SUSE Linux Security	DIC 06
612	Seguridad en sistemas basados en Debian Debian Security	AGO 14
614	Seguridad en Red Hat Linux (Fedora) Red Hat Linux (Fedora) Security	DIC 06
617	Configuración segura de SUSE Linux Enterprise 12 (Servidor independiente) SUSE Linux Enterprise 12 Secure Configuration (Standalone Server)	MAR 19
619	Configuración segura de CentOS 7 (Cliente independiente) CentOS 7 Secure Configuration (Independent Client)	ABR 19
621	Seguridad en Sun Solaris 8.0 Sun-Solaris 8.0 Security	JUL 04
622	Seguridad en Sun Solaris 9.0 para Oracle 8.1.7 Sun-Solaris 9.0 Security for Oracle 8.1.7	DIC 06
623	Seguridad en Sun Solaris 9.0 para Oracle 9.1 Sun-Solaris 9.0 Security for Oracle 9.i	DIC 06
624	Seguridad en Sun Solaris 9.0 para Oracle 9.2 Sun-Solaris 10 Security for Oracle 9.2	DIC 06
625	Seguridad en Sun Solaris 10g Oracle 10g | Sun-Solaris 10 Security for Oracle 10g	MAR 10
626	Guía de Securización de Sun Solaris 10 con NFS Security Guide for Sun Solaris 10 with NFS	DIC 07
627	Guía de Securización de Sun Solaris 9 con Workstation Security Guide for Sun Solaris 9 with Workstation	DIC 07
628	Guía de Securización de Sun Solaris 9 con NFS Security Guide for Sun Solaris 9 with NFS	DIC 07
629	Guía de Securización de Sun Solaris 10 con Workstation Security Guide for Sun Solaris 10 with Workstation	DIC 07
631	Seguridad en Base de Datos Oracle 8.1.7 sobre Solaris Security for DB Oracle 8.1.7 on Solaris	SEP 05
633	Seguridad en Base de Datos Oracle 9i sobre Red Hat 3 y 4 Security for DB Oracle 9i on Red Hat 3 y 4	DIC 07
634	Seguridad en Base de Datos Oracle 9i sobre Solaris 9 y 10 Security for DB Oracle 9i on Solaris 9 y 10	DIC 07
635	Seguridad en Base de Datos Oracle 9i sobre HP-UX 11i Security for DB Oracle 9i on HP-UX 11i	DIC 07
636	Seguridad en Base de Datos Oracle 10gR2 sobre Red Hat 3 y 4 Security for DB Oracle 10gR2 on Red Hat 3 y 4	DIC 07
637	Seguridad en Base de Datos Oracle 10gR2 sobre Solaris 9 y 10 Security for DB Oracle 10gR2 on Solaris 9 y 10	DIC 07
638	Seguridad en Base de Datos Oracle 10gR2 sobre HP-UX 11i Security for DB Oracle 10gR2 on HP-UX 11i	DIC 07
639	Seguridad en Base de Datos Oracle 10g sobre Windows 2003 Server Security for DB Oracle 10g on Windows 2003 Server	AGO 10
641	Seguridad en Equipos de Comunicaciones. Router Cisco Security for Communication Equipment. Routers Cisco	NOV 13
642	Seguridad en Equipos de Comunicaciones. Switches Enterasys Security for Communication Equipment. Switches Enterasys	DIC 06
642B	Seguridad en Extreme Networks 440G2 Extreme Networks 440G2 Security	ENE 19
643A	Seguridad en Equipos de Comunicaciones.Allied Telesis. Security for Communication Equipment. allied telesis	SEP 13
643B	Seguridad en Equipos de Comunicaciones. Allied Telesis AT-8100S/AT-8100L y FS970M Security in Communications Equipment. Allied Telesis AT-8100S/AT-8100L and FS970M	MAY 15
644	Seguridad en Equipos de Comunicaciones. Switches Cisco Security for Communication Equipment. Switches Cisco	DIC 07
645	Sistemas de Gestión de Red (Cisco Works LMS) Network Management systems (Cisco Works LMS)	MAR 11
646	Seguridad router HUAWEI AR150&200 Security router HUAWEI AR150&200	SEP 14
646B	Seguridad en conmutadores HUAWEI S7700 Security in switches HUAWEI S7700	FEB 18
647	Seguridad en switches HP COMWARE HP COMWARE Switch Security	ENE 16
647B	Configuración segura de equipos de red Aruba para entornos WiFi Secure configuration of Aruba network equipment for WiFi environments	FEB 18
647C	Seguridad en conmutadores HPE Aruba Aruba HPE Switch Security	MAY 18
648	Seguridad en conmutadores Netgear Prosafe Netgear Prosafe Switch Security	NOV 17
650	Seguridad en cortafuegos Fortigate Firewall security Fortigate	ABR 15
651	Seguridad en cortafuegos Cisco ASA Firewall security Cisco ASA	JUL 15
651B	Seguridad en cortafuegos Cisco FIREPOWER Firewall security Cisco FIREPOWER	ABR 19
652	Seguridad en cortafuegos Palo Alto Firewall security Palo Alto	OCT 17
653	Seguridad en Check Point Security at Check Point	MAY 18
655	Guía de Securización para Sun Solaris 9 con Oracle 10 Security Guide for Sun Solaris 9 with Oracle 10	DIC 07
656	Guía de Securización para Sun Solaris 9 con Oracle 10 y VCS 4.1 Guide for Sun Solaris 9 with Oracle 10 and VCS 4.1	DIC 07

660	Seguridad en Proxies Proxies Security	MAY 14
661	Seguridad en Firewalls de Aplicación Application Firewalls Security	MAR 11
662	Seguridad en Apache Traffic Server Security of Apache Traffic Server	NOV 12
663	Seguridad en DNS (BIND) SECURITY OF DNS (BIND)	ABR 14
664	Passive DNS Passive DNS	MAR 14
665	Configuración segura de SSH SSH secure configuration	OCT 14
671	Seguridad en Servidores Web Apache Security of Web Apache Server	DIC 06
672	Seguridad en Servidores Web Tomcat Tomcat Web Server Security	ENE 09
673	Seguridad en Servidores Web Tomcat 7 Tomcat 7 Web Server Security	Pendiente
674	Seguridad en GlassFish 3.1 Security in GlassFish 3.1	ENE 13
681	Seguridad en Servidores de Correo Postfix Security of Postfix Email Server	DIC 06
682	Configuración Segura de Sendmail Secure Configuration for Sendmail	ENE 10
683	Configuración Segura de Citrix Virtual Apps and Desktops Secure Configuration of Citrix Virtual Apps and Desktops	Pendiente
684	Publicación Segura de aplicaciones y escritorios virtuales con Citrix Secure publishing of virtual applications and desktops with Citrix	Pendiente
691	Oracle Application Server 10gR2 para Red Hat 3 y 4 Security in Oracle Application Server 10gR2 for Red Hat 3 y 4	DIC 07
692	Oracle Application Server 10gR2 para Solaris 9 y 10 Security in Oracle Application Server 10gR2 for Solaris 9 y 10	DIC 07
693	Oracle Application Server 10gR2 para HP-UX 11i Security in Oracle Application Server 10gR2 for HP-UX 11i	DIC 07

Serie 800: Esquema Nacional de Seguridad
SERIE 800: NATIONAL SECURITY SCHEME

800	Glosario de Términos y Abreviaturas Glossary of Terms and Abbreviations	MAR 11
801	Responsabilidades en el ENS Responsibilities in the National Security Scheme	ABR 19
802	Auditoría del Esquema Nacional de Seguridad Audit for the National Security Scheme	ABR 17
803	Valoración de Sistemas en el ENS Systems Evaluation in the National Security Scheme	NOV 17
804	Medias de Implementación en el ENS Implementation Measures in the National Security Scheme	JUN 17
805	Política de Seguridad de la Información Information Security Policy	SEP 11
806	Plan de Adecuación del ENS Adaptation Plan in the National Security Scheme	ENE 11
807	Criptología de Empleo en el ENS Encryption in the National Security Scheme	ABR 17
808	Verificación del Cumplimiento de las Medidas en el ENS Verification of Compliance with Measures Established by the National Security Scheme	JUN 17
809	Declaración de conformidad del ENS ENS declaration of conformity	MAR 18
810	Guía de creación de un CERT/CSIRT Cert/CSIRT construction guide	SEP 11
811	Interconexión en el ENS ENS interconnection	OCT 17
812	Seguridad en entornos y aplicaciones Web Security in web applications and enviroments	OCT 11
813	Componentes certificados en el ENS ENS components certificates	FEB 12
814	Seguridad en corro electrónico Security in email	AGO 11
815	Indicadores y métricas en el ENS Indicators and metrics ENS	FEB 14
816	Seguridad en Redes Inalámbricas en el ENS Wireless Network Security ENS	JUL 17
817	Gestión de Ciberincidentes en el ENS Cyberincident Management	JUN 18
818	Herramientas de seguridad en el ENS Security Tools National Security Scheme	OCT 12
819	Medidas compensatorias en el ENS ENS compensatory measures	OCT 18

Fuera de soporte
Out of support

* **Difusión limitada**
Limited difussion

** **Confidencial**
Confidential

820	Guía de protección contra Denegación de Servicio DDoS protection guide	JUN 13
821	ENS. Normas de seguridad Security rules Apéndice I. NG 00 Utilización de recursos y sistemas Resources and systems Apéndice II. NP 10 Acceso a Internet Internet access Apéndice III. NP 20 Correo Electrónico E-mail Apéndice IV. NP 30 Trabajar fuera de instalaciones del organismo Work outside the body´s facilities Apéndice V. NP 40 Creación y uso de contraseñas Passwords Apéndice VI. NP 50 Acuerdo confidencialidad terceros Confidetiality with third parties Apéndice VII. NP 60 Modelo de buenas prácticas para terceros Good practices with third parties Apéndice VIII. NP 70 Normativa de uso de redes sociales Regulations for the use of social networks	FEB 18
822	Esquema Nacional de Seguridad. Procedimientos de Seguridad National Security Framework. Security Procedures Anexo I .PR 10 Procedimiento de gestión de usuarios User Management Anexo II. PR 20 Procedimiento de clasificación y tratamiento de la información clasificada Classification and treatment of classified information Anexo III. PR 30 Procedimiento de generación de copias de respaldo y recuperación de la información Backup and recovery information	OCT 12
823	Utilización de servicios en la nube Security requirements cloud environments	DIC 14
824	Informe del estado de seguridad Security Status Report	OCT 18
825	Certificaciones 27001 27001 certificates	NOV 13
826	Esquema de certificación de personas Person certification schemes	Pendiente
827	Gestión y uso de dispositivos móviles Management and use of mobile devices	MAY 14
829	Seguridad en VPN en el marco del ENS VPN security in ENS	Pendiente
830	Ámbito de aplicación del Esquema Nacional de Seguridad Scope of the National Security Scheme	SEP 16
831	Registro de actividad de usuario User activity log	MAR 18
834	Protección ante código dañino en el ENS Protection against malicious code in the ENS	SEP 18
835	Borrado de metadatos en el marco del ENS Deleting metadata	MAR 17
836	Seguridad en VPN en el marco del ENS VPN security	JUN 17
837	Seguridad en Bluetooth en el marco del ENS Bluetooth security	FEB 18
844	INES – Informe Nacional del Estado de Seguridad. Manual de usuario INES, Status report on security. Handbook INES – Anexo-I. Preguntas más frecuentes (FAQ) INES – Anexo-II. Recopilación de datos Data collection INES – Anexo-III. Formato para la creación del XML de incidentes propios en caso de no disponer de instancia propia de LUCIA Format for the creation of XML of own incidents in case of non-dispense of own LUCIA´s instance	OCT 18
845A	LUCIA. Manual de usuario LUCIA. Handbook	ABR 16
845B	LUCIA. Manual de usuario con Sistema de Alerta Temprana (SAT) LUCIA. User Manual with Early Warning System (EWS)	FEB 16
845C	LUCIA. Manual de instalación. Organismo LUCIA. Installation manual. Organism	FEB 17
845D	LUCIA. Manual de administrador LUCIA. Administrator's Manual	NOV 16
850A	Seguridad en Windows 7 en el ENS (cliente en dominio) Windows 7 security in ENS (client within a domain)	AGO 14
850B	Seguridad en Windows 7 (cliente independiente) Windows 7 security in ENS (independent client)	OCT 14
851A	Seguridad en Windows 2008 Server R2 (controlador de dominio) Windows 2008 Server R2 security in ENS (domain controller)	AGO 14
851B	Seguridad en Windows 2008 Server R2 (servidor independiente) Windows 2008 Server R2 security in ENS (independent server)	SEP 14
859	Recolección y consolidación de eventos con Windows Server 2008R2 Collections and consolidation of events in Windows Server 2008 R2	ENE 15

860	Seguridad en el servicio de Outlook Web App del Microsoft Exchange Server 2010 Outlook Web App of Microsoft Exchange Server 2010 security	AGO 15
865	Punto final en ENS Endpoint in ENS	
869	Implementación de AppLocker en el ENS ENS AppLocker	OCT 15
870A	Implementación del ENS en Windows Server 2012 R2 Windows 2012 Server R2 security in ENS	JUL 15
870B	Implementación del Esquema Nacional de Seguridad en Windows Server 2012 R2 Servidor independiente Windows 2012 Server R2 security (independent server)	AGO 15
871	Implementación del ENS en servidor de impresión sobre Microsoft Windows Server 2012 R2 Windows Server 2012 R2 (print server)	FEB 17
872	Implementación del ENS en servidor de ficheros sobre Microsoft Windows Server 2012 R2 MS Windows Server 2012 R2 File server	FEB 17
873	Implementación ENS en MS Windows Internet Informations Server 8.5 MS Windows Internet Informations Server 8,5	DIC 16
874	Implementación del ENS en Cluster de conmutación por error en Windows Server 2012 R2 Implementing ENS in Failover Cluster on Windows Server 2012 R2	AGO 17
875	Implementación del ENS en MS System Center configuration manager 2012 R2 Implementation of ENS in MS System Center configuration manager 2012 R2	JUL 17
880	Implementación del ENS en Exchange Server 2013 sobre Windows Server 2012 R2 Implementation of ENS in Exchange Server 2013 on Windows Server 2012 R2	NOV 16
881	Impacto del RGPD en el ENS Impact of the RGPD on the ENS	
882	Análisis de Riesgos para Entidades Locales Risk Analysis for Local Entities	ABR 19
883	Implantación del ENS para Entidades Locales Implementation of the ENS for Local Entities	MAY 19

Serie 900: Informes técnicos
SERIE 900: TECHNICAL REPORTS

903	Configuración segura de asistente personal digital HP-IPAQ 6340 HP-IPAQ Secure Configuration	DIC 05
911A	Ciclo de una APT Cycle of an APT	JUN 13
911B	Recomendaciones generales ante un APT APT general recommendations	JUL 13
912	Procedimiento de investigación de código dañino Malware investigation procedure	JUN 13
920	Análisis de malware con Cuckoo Sandbox Malware analysis with Cuckoo Sandbox	MAR 14
950	Recomendaciones de empleo de la herramienta EMET Recommendations for the use of the EMET tool	ABR 17
951	Manual de Ethereal/Wireshark Using Ethereal/ Wireshark Tool	DIC 06
952	Empleo de la Herramienta Nessus Usage Recommendations for Nessus Tool	AGO 11
953	Recomendaciones de Empleo de la Herramienta Snort Usage Recommendations for Snort Tool	JUN 09
954	Recomendaciones de Empleo de la Herramienta Nmap Usage Recommendations for Nmap Tool	AGO 12
955	Recomendaciones de Empleo de GnuPG v.1.4.7 Usage Recommendations for GnuPG v.1.4.7 Tool	DIC 07
955B	Recomendaciones de Empleo de GPG Usage Recommendations for GnuPG	DIC 16
956	Seguridad (Identificación y escape) de entornos de computación virtuales (virtualización de sistemas) Security (Identification and escape) of virtual computing environments (systems virtualization)	DIC 07
957	Recomendaciones de empleo de TrueCrypt TrueCrypt recommendations	ENE 13
970**	Uso de Cifradores IP en Redes Públicas Use of IP cyphers in public networks	SEP 13

Serie 1000: Procedimientos de empleo seguro
SERIE 1000: SAFE USE PROCEDURES

1401	Configuración segura de pasarelas de Autek Secure configuration of Autek gateways	JUN 18
1408	Procedimiento de empleo seguro DIODO Autek Ingeniería Safe use procedure DIODO Autek Ingeniería	ABR 19
1501	Configuración segura de ERASE IT Safe configuration of ERASE IT	OCT 18
1601	Configuración segura de Samsung Galaxy S7 Samsung Galaxy S7 Secure Configuration	JUN 18
1605	Configuración y empleo seguro de la tableta GETAC F110G4 Safe configuration and use of the GETAC F110G4 tablet	ABR 19

AUDITORÍAS e implementación de SEGURIDAD

AUDITS and SECURITY Implementation

En el campo de la auditoría, el CCN-CERT realizó en 2017 una importante campaña para impulsar la **implantación de HTTPS** en las sedes electrónicas del Sector Público. Para ello realizó informes periódicos, un documento de buenas prácticas que ayudara a los organismos a establecer este protocolo seguro de transferencia de datos y diversos **cursos** de formación. Además, realizó un análisis de los **dominios**, **servidores** y **aplicaciones web** de todos aquellos organismos y entidades que así lo solicitaron.

Asimismo, se llevó a cabo un análisis preliminar, a través del sistema de auditoría continua (ANA), para detectar vulnerabilidades importantes en recursos web pertenecientes a diferentes Ministerios.

El fin último de la función de auditoría es la necesidad de evaluación continua, tener la capacidad de gestionar y medir de manera constante la evolución de los activos respecto a niveles de seguridad y riesgo definidos.

En total, se analizaron 635 dominios, pertenecientes a 226 organismos del Sector Público, incluida la Administración General del Estado, las Comunidades Autónomas, Entidades Locales y Universidades.

In the field of auditing, the CCN-CERT carried out an important campaign in 2017 to promote the **implementation of HTTPS** in the Public Sector's electronic headquarters. For this purpose, it prepared periodic reports, a document of best practices that would help the organizations to establish this secure data transfer protocol and several training **courses**. In addition, it conducted an analysis of the **domains, servers and web applications** of all those organizations and entities that requested it. Likewise, a preliminary analysis was carried out, through the continuous audit system (ANA), to detect important vulnerabilities in web resources belonging to different Ministries

En 2018 se analizaron 635 dominios de 226 organismos

In 2018, 635 domains from 226 organizations were analysed

The ultimate goal of the audit function is the need for continuous evaluation, the ability to manage and constantly measure the evolution of assets against defined levels of security and risk.

In total, 635 domains were analysed, belonging to 226 bodies in the Public Sector, including the General State Administration, Regional Goverments, Local Bodies and Universities. The ultimate goal of the audit function is the need for continuous evaluation, the ability to manage and constantly measure the evolution of assets against defined levels of security and risk.

In total, 635 domains were analysed, belonging to 226 bodies in the Public Sector, including the General State Administration, Autonomous Communities, Local Bodies and Universities..

Implementación de seguridad
Security Implementation

Dada la importancia que tiene la información que manejan los sistemas TIC, es de vital importancia que las organizaciones se aseguren de que están protegidos.

Como desarrollo de la **Ley 11/2002 de 6 de mayo**, reguladora del CNI y del R.D. 421/2004, de 12 de marzo, por el que se regula el CCN, se establece una Política de Seguridad de las TIC (CCN-STIC-001) donde se recoge la necesidad de la **Acreditación** de los sistemas que manejan **información clasificada**. Estos sistemas deben trabajar en unos modos seguros de operación y una de las condiciones para la acreditación de un sistema es el cumplimiento de los requisitos STIC. Estos requisitos constituyen el nivel mínimo de protección exigible que deberá ser completado con los obtenidos de un análisis de riesgos.

Hay sistemas que, por su origen y naturaleza, tienen grandes dificultades para cumplir con los requisitos de seguridad exigidos. En este sentido, durante 2018, ha sido clave implementar un procedimiento de mejora continua de los niveles de seguridad en base a la adopción de compromisos a corto, medio y largo plazo por parte del propietario del Sistema; junto con una evaluación continua basada en la determinación de vulnerabilidades y deficiencias de configuración de los sistemas.

El CCN y, concretamente, su equipo de **Acreditación e Inspecciones de Seguridad**, se encargó de realizar inspecciones de seguridad para verificar la seguridad implementada en un sistema y comprobar que los servicios y recursos utilizados cumplían con el mínimo especificado y requerido. Durante los años 2017 y 2018, este equipo realizó 40 inspecciones de seguridad.

Inspecciones de seguridad durante los años 2017 y 2018

Security inspections during 2017 and 2018

Given the importance of the information handled by ICT systems, it is vitally important that organizations ensure that they are protected. As a development of **Law 11/2002, dated 6th May**, regulating the CNI and R.D. 421/2004 of 12 March, which regulates the CCN, an ICT Security Policy (CCN-STIC-001) is established, which includes the need for **Accreditation** of systems that handle **classified information**. These systems must work in safe modes of operation and one of the conditions for the accreditation of a system is compliance with the STIC requirements. These requirements constitute the minimum level of protection that must be completed with those obtained from a risk analysis. There are systems that, due to their origin and nature, have great difficulties in complying with the security requirements demanded. In this sense, during 2018, it has been key to implement a procedure of continuous improvement of security levels based on the adoption of short, medium and long term commitments by the owner of the System, together with a continuous assessment based on the determination of vulnerabilities and deficiencies in the configuration of the systems. The CCN, and specifically its **Accreditation and Security Inspections** team, was in charge of conducting security inspections to verify the security implemented in a system and to verify that the services and resources used complied with the specified and required minimum. During 2017 and 2018, this team conducted 40 security inspections.

GESTIÓN y Respuesta a CIBERINCIDENTES

CYBER INCIDENT MANAGEMENT and Response

El **CCN-CERT** es la Capacidad de Respuesta a incidentes de Seguridad de la Información del CCN. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo 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 (CERT/CSIRT) o Centros de Operaciones de Ciberseguridad (SOC) existentes.

Todo ello, con el fin último de conseguir **un ciberespacio más seguro y confiable**, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) 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.

The **CCN-CERT** is the CCN's Computer Emergency Response Team. This service was created in 2006 as the Spanish National Governmental CERT and its functions are included in Law 11/2002 regulating the CNI, RD 421/2004 regulating the CCN and RD 3/2010, dated 8th January, regulating the National Security Framework (ENS), modified by RD 951/2015 of 23rd October.

Its mission, therefore, is to contribute to the improvement of Spanish cybersecurity, being the **national alert and response centre** that cooperates and helps to respond quickly and efficiently to cyberattacks and to actively confront cyber threats, including the coordination at the national public level of the Computer Emergency Response Teams (CERT), Computer Security Incident Response Teams (CSIRT) or Security Operations Centres (SOC).

All this, with the ultimate aim of achieving a **safer and more reliable cyberspace**, preserving classified information (as stated in Article 4. F of Law 11/2002) and sensitive information, defending the Spanish Technological Heritage, training expert personnel, applying security policies and procedures and employing and developing the most appropriate technologies for this purpose.

De acuerdo con esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público, 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 se realizará en coordinación con el CNPIC.

In accordance with these regulations and Law 40/2015 on the Legal System for the Public Sector, the CCN-CERT is responsible for the management of cyberincidents that affect any public body or company. In the case of critical operators in the public sector, the management of cyber incidents will be carried out in coordination with the CNPIC.

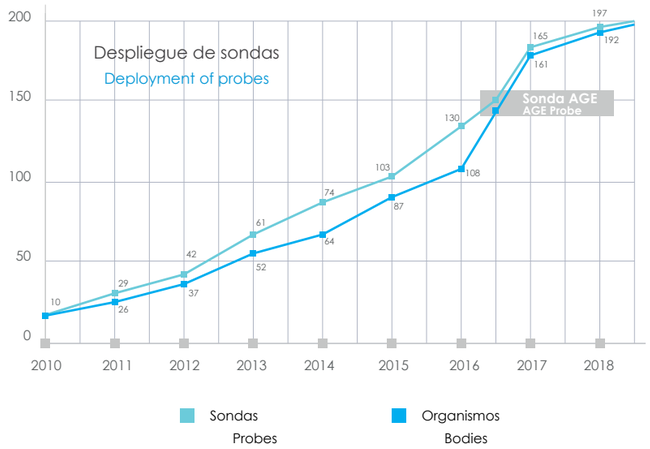
8.1 Sistema de ALERTA Temprana (SAT)

Early WARNING System (SAT)

Sistema desarrollado por el CCN-CERT desde el año 2008 que busca actuar antes de que se produzca un incidente o, por lo menos, detectarlo en un primer momento para reducir su impacto y alcance. Este **Sistema de Alerta Temprana (SAT)** para la **detección rápida de incidentes y anomalías** dentro de la Administración y de las empresas de interés estratégico, se enmarca dentro de las acciones preventivas, correctivas y de contención realizadas por el CERT Gubernamental Nacional.

El SAT cuenta con tres vertientes con un denominador común: la detección temprana de intrusiones. Dichas vertientes son **SAT-SARA**, para la monitorización de la Intranet de la Administración; **SAT-INET**, para la monitorización de las salidas de Internet de los organismos adscritos al servicio y **SAT-ICS,** para los Sistemas de Control Industrial.

Anualmente, el CCN-CERT organiza una jornada de puesta en común con todas las organizaciones implicadas en este servicio (o aquellas que pueden estarlo en un futuro), con el fin de realizar un balance del año y compartir los conocimientos del mismo (*véase apartado correspondiente*).



System developed by the CCN-CERT since 2008 that seeks to act before an incident occurs or, at least, detect it at an early stage to reduce its impact and scope. This **Early Warning System (SAT)** for the **rapid detection of incidents and anomalies** within the Administration and companies of strategic interest, is framed within the preventive, corrective and containment actions carried out by the National Governmental CERT.

The SAT has three aspects with a common denominator: early detection of intrusions. These aspects are **SAT-SARA**, for monitoring the Administration Intranet; **SAT-INET**, for the Internet outputs of the bodies attached to the service; and **SAT-ICS** for Industrial Control Systems.

Every year, the CCN-CERT organises a meeting with all the organizations involved in this service (or those that may be in the future), in order to take stock of the year and share the knowledge of it (*see the corresponding section*).

SAT-INET / SAT-ICS

SAT-INET

SONDAS DESPLEGADAS: 197
/ Probes deployed

ORGANISMOS: 192
/ Organizations

- Ministerios y organismos AGE / Ministries and AGE organizations
- Comunidades Autónomas / Regional Goverments
- Diputaciones provinciales / Provincial Goverments
- Mancomunidades /
- Ayuntamientos / Town Councils
- Confederaciones Hidrográficas / Hydrographic Confederations
- Puertos / Ports
- Universidades / Universities
- Empresas de interés estratégico / Strategic interest companies

SAT-ICS

SONDAS DESPLEGADAS: 8
/ Probes deployed

ORGANISMOS: 8

- Confederaciones Hidrográficas / Hydrographic Confederations
- Puertos / Ports
- Servicios sanitarios / Health services
- Energía nuclear / Nuclear energy

SAT-SARA

50 ÁREAS DE CONEXIÓN / 50 CONNECTION AREAS

- Ministerios y organismos AGE / Ministeries and AGE organizations
- Comunidades Autónomas / Regional Goverments
- Órganos constitucionales / Constitutional Bodies
- Organismos independientes / Independent Organizations

8.2 Respuesta a CIBERINCIDENTES

CYBER INCIDENT Response

El CCN-CERT, como CERT Gubernamental Nacional, colabora con todos los organismos públicos y empresas de interés estratégico para el país en la detección, notificación, evaluación, respuesta, tratamiento y aprendizaje de incidentes de seguridad de información o ciberincidentes que puedan sufrir sus sistemas.

El número de incidentes gestionados por este organismo durante los dos últimos años sumaron un total de 64.664.

The number of incidents managed by this body during the last two years was 64,664.

En este proceso, realizado siempre en la más absoluta confidencialidad entre ambas partes, el CCN-CERT brinda **apoyo técnico y operativo**, tanto en las etapas de detección, como reacción, contención y eliminación. A ello se une una política preventiva, en la que trabaja un equipo de expertos destinados a investigar sobre técnicas empleadas, tendencias, soluciones y procedimientos más adecuados para hacerles frente, incluyendo metodologías para recopilar y analizar datos y eventos, procedimientos de tipificación de su peligrosidad y priorización de los mismos.

Actúa, además, como **Nodo de Intercambio de Información** de Ciberincidentes en los Sistemas de Información de las Administraciones Públicas y como principal coordinador con los organismos adecuados en dicho intercambio.

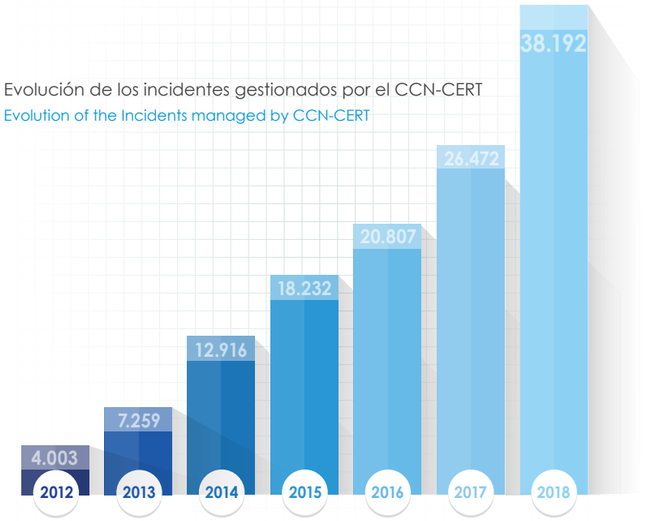
The CCN-CERT, as a National Governmental CERT, collaborates with all public organizations and companies of strategic interest for the country in the detection, notification, evaluation, response, treatment and learning of information security incidents or cyber incidents that may suffer their systems.

In this process, always carried out in the most absolute confidentiality between both parties, the CCN-CERT provides **technical and operational support**, both in the stages of detection, reaction, containment and elimination. In addition to this, there is a prevention policy, in which a team of experts work to investigate the techniques used, trends, solutions and procedures most suitable for dealing with them, including methodologies for collecting and analysing data and events, procedures for classifying their dangerousness and prioritising them.

It also acts as an **Information Exchange Node** for Cyber incidents in Public Administration Information Systems and as the main coordinator with the appropriate bodies in such exchange.

Evolución de los incidentes gestionados por el CCN-CERT

Evolution of the Incidents managed by CCN-CERT

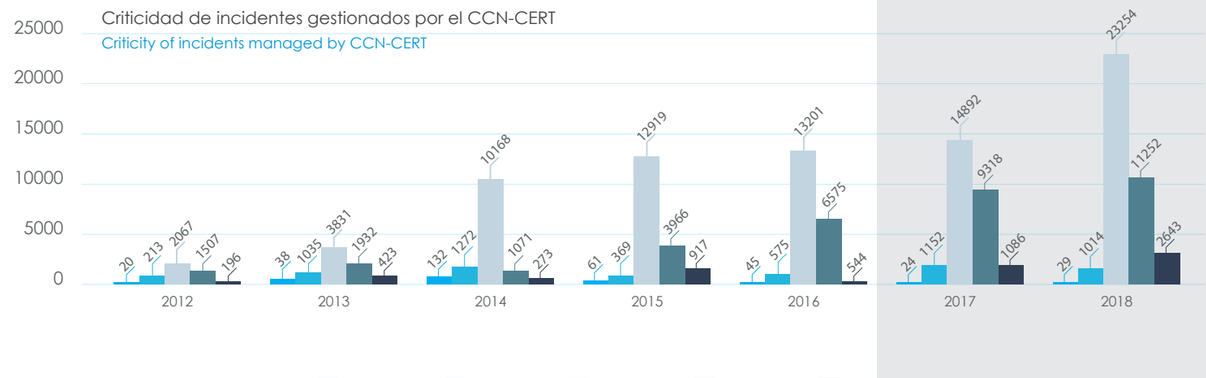


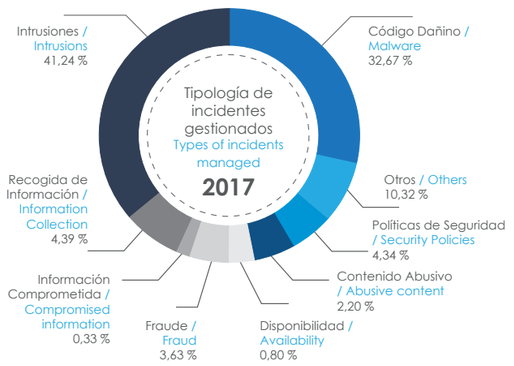
Prueba de ello es el número de incidentes gestionados por este organismo durante los dos últimos años que sumaron un total de **64.664**; es decir casi 89 incidentes diarios durante el período de 2017 y 2018.

Proof of this is the number of incidents managed by this body during the last two years: **64,664**, that is, almost 89 incidents per day during 2017 and 2018.

Criticidad de incidentes gestionados por el CCN-CERT

Criticity of incidents managed by CCN-CERT





Tipología de incidentes gestionados por el CCN-CERT

Typology of incidents managed by CCN-CERT

El impacto de WannaCry
The impact of WannaCry

Mención especial requiere la campaña de ransomware WannaCry, detectada el 12 de mayo de 2017 y que alcanzó en todo el mundo una repercusión mediática inusitada hasta el momento. Puede decirse que la ciberseguirdad vivió un antes y un después de este ataque. La campaña utilizó el exploit que aprovechaba la vulnerabilidad de Microsoft (MS17-010) y cuyo parche había sido publicado por la compañía el 14 de marzo.

En nuestro país, el CCN-CERT lanzó en 24 horas la **primera vacuna** frente a este código dañino (**NoMoreCry**), que fue utilizada 300.000 veces en tan solo cinco días, lo que permitió a empresas y organismos públicos en España y en otros países frenar los efectos nocivos sobre sus actividades.

Al finalizar la campaña, el CERT Gubernamental Nacional había detectado en nuestro país 239 direcciones IP que habían intentado contactar con uno de los dominios dañinos identificados. Del mismo modo, y a pesar de las medidas de mitigación publicadas, cinco días después se tenía constancia de la existencia de 2.774 direcciones IP, con origen en España, vulnerables todavía al exploit utilizado.

Special mention must be made of the WannaCry ransomware campaign, which was detected on 12nd May 2017 and reached an unprecedented level of media coverage throughout the world. It can be said that this attack has been a milestone in cybersecurity. The campaign used the exploit that exploited Microsoft's vulnerability (MS17-010) and whose patch had been released by the company on 14th March.

In our country, CCN-CERT launched in 24 hours the **first vaccine** against this malware (**NoMoreCry**), which was used 300,000 times in just five days, allowing companies and public agencies in Spain and other countries to curb the harmful effects on their activities.

La vacuna desarrollada por el CCN-CERT fue utilizada 300.000 veces en 5 días

The vaccine developed by CCN-CERT was used 300,000 times in 5 days.

At the end of the campaign, the National Governmental CERT had detected 239 IP addresses in our country that had tried to contact one of the identified harmful domains. In the same way, and despite the mitigation measures published, five days later there was evidence of the existence of 2,774 IP addresses, originating in Spain, still vulnerable to the exploit used. The vaccine developed by the CCN-CERT was used 300,000 times in five days.

El CCN-CERT, dentro de su labor de investigación de incidentes, realiza una importante tarea en materia de **ingeniería inversa** y **análisis forense**. Todo ello con el fin de averiguar el procedimiento de actuación llevado a cabo en un ataque, su funcionalidad y su modus operandi. Asimismo, y gracias al análisis forense, se llevan a cabo distintas técnicas destinadas a extraer la información valiosa de discos, sin alterar su estado. De este modo, es posible encontrar patrones de comportamiento o descubrir información oculta en el transcurso de la investigación del incidente.

En este sentido, el CCN-CERT, en apoyo a las Fuerzas y Cuerpos de Seguridad del Estado, ha realizado 50 análisis de evidencias desde 2018.

The CCN-CERT, as part of its incident investigation work, performs an important task in **reverse engineering** and **forensic analysis**. All this in order to find out the procedure of action carried out in an attack, its functionality and its modus operandi. Likewise, and thanks to forensic analysis, different techniques are carried out to extract valuable information from disks, without altering their state.

In this way, it is possible to find patterns of behaviour or to discover hidden information in the course of the investigation of the incident.

In this sense, the CCN-CERT, in support of the State Security Forces and Corps, has carried out 50 analyses of evidence since 2018.

8.3 SOLUCIONES propias
CCN's own SOLUTIONS

Co-financed by the Connecting Europe Facility of the European Union

La coordinación, promoción y desarrollo de soluciones que garanticen la seguridad de los sistemas y contribuyan a una mejor gestión de la ciberseguridad en cualquier organización es otra de las funciones del CCN.

Para ello, además de mantener acuerdos con diferentes empresas del sector, el CCN ha contado con ayudas de la **Unión Europea**; a través del **CEF (*Connecting Europe Facility*)**, un instrumento financiero para promover el crecimiento, el empleo y la competitividad a través de inversiones específicas en tres grandes áreas: energía, telecomunicaciones (incluida la ciberseguridad) y transporte.

Los proyectos seleccionados de entre numerosas peticiones de todos los países de la UE pretenden fomentar la tecnología europea, en este caso la española, y mejorar las capacidades nacionales de ciberseguridad e intercambio de información. En concreto, sus soluciones **CARMEN, GLORIA, MARTA, LUCIA y REYES** contaron con estas ayudas.

The coordination, promotion and development of solutions that guarantee the security of the systems and contribute to a better management of cybersecurity in any organization is another one of the CCN's functions.

To this end, in addition to maintaining agreements with different companies in the sector, the CCN has received aid from the **European Union** through the **CEF (Connecting Europe Facility)**, a key financial instrument to promote growth, employment and competitiveness through specific investments in three major areas: energy, telecommunications (including cybersecurity) and transport.

The projects selected from among numerous requests from all EU countries aim to promote European technology, in this case Spanish technology, and to improve national capacities for cybersecurity and information exchange. In particular, their solutions **CARMEN, GLORIA, MARTA, LUCIA and REYES** were supported.

Automatización y Normalización de Auditorías
Automation and Standardization of Audits

Aplicación para la gestión y evolución de los niveles de exposición a los que se encuentra sometida una entidad. ANA proporciona la capacidad de medir estos niveles, ayudando a reducir las probabilidades de aprovechamiento de vulnerabilidades por un agente externo.

Application for the management and evolution of an entity's exposure levels. ANA provides the ability to measure them, helping to reduce the likelihood of vulnerabilities being exploited by an external agent.

Defensa de ataques avanzados/APT

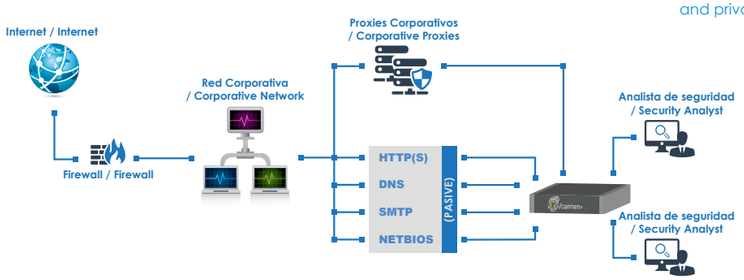
Advanced attack defense/APT

Solución desarrollada con el objetivo de identificar el compromiso de la red de una organización por parte de una APT. Esta solución adquiere, procesa y analiza información para la elaboración de inteligencia a partir del tráfico de una red interna. Es capaz de detectar anomalías y movimientos laterales y externos dentro de la red, así como de analizar malware mediante sandboxing avanzado.

Solution developed with the objective of identifying the commitment of an organization's network by APT. This solution acquires, processes and analyzes information for the elaboration of intelligence from the traffic of an internal network. It is capable of detecting anomalies and lateral and external movements within the network, as well as analyzing malware using advanced sandboxing.

57 implantaciones de CARMEN repartidas en Administración Pública y sector privado

57 CARMEN implementations spread over Public Administration and private sector



Solución de punto final

Endpoint Solution

Solución de endpoint integrada con la herramienta CARMEN que permite tener una visión más completa de lo que ocurre dentro de una red, siendo su objetivo principal la detección de malware complejo y su movimiento lateral relacionado con APT.

La flexibilidad de los denominados "sensores" permite tener un control total de la red, aumentando de manera considerable la rapidez y eficiencia en la resolución de un incidente de seguridad.

Endpoint solution integrated with the CARMEN tool that allows to have a more complete vision of what happens inside a network, being the detection of complex malware and its lateral movement related to APT its main objective.

The flexibility of the so-called "sensors" allows total control of the network, considerably increasing the speed and efficiency in the resolution of a security incident.

Verificación de cumplimiento

Compliance Verification

Solución para analizar las características de seguridad técnicas definidas a través del R.D. 3/2010 por el que se regula el ENS en el ámbito de la Administración Electrónica. El análisis del cumplimiento está basado en las normas proporcionadas a través de las plantillas de seguridad de las Guías CCN-STIC 850A, 850B, 851B, 870A, 870B, 570A, 570B,599A18 y 599B18.

Solution for analysing the technical security characteristics defined by Royal Decree 3/2010 regulating the ENS in the field of the Electronic Administration. The compliance analysis is based on the standards provided through the CCN-STIC 850A, 850B, 851B, 870A, 870B, 570A, 570B, 599A18 and 599B18 security templates.

Gestor de logs en respuesta a incidentes/amenazas

Log manager for incidents and threats response

Plataforma para la gestión de incidentes y amenazas de ciberseguridad a través de técnicas de correlación compleja de eventos. Basado en los sistemas SIEM, va un paso más allá de las capacidades de monitorización, almacenamiento e interpretación de los datos relevantes. Permite una orientación muy flexible hacia la vigilancia del mundo IP.

Platform for the management of cybersecurity incidents and threats through complex event correlation techniques. Based on SIEM systems, it goes one step beyond the capabilities of monitoring, storing and interpreting the relevant data. It allows a very flexible orientation towards the surveillance of the IP world.

Informe Nacional del Estado de Seguridad en el ENS

National Report on the ENS Security Status

Proyecto que tiene por objetivo facilitar la labor de todos los organismos en su obligación de evaluar regularmente el estado de la seguridad de sus sistemas *(véase apartado del ENS)*.

This project aims to facilitate the work of all bodies in their obligation to regularly assess the security status of their systems *(see section of the ENS)*.

Almacenamiento en la nube

Cloud Storage

Servicio de uso compartido en la nube para el almacenamiento virtual de información (archivos, muestras, aplicaciones, etc.) que permite el intercambio de la misma con colaboradores y partners.

Cloud sharing service for the virtual storage of information (files, samples, applications, etc.) that allows its exchange with collaborators and partners.

Sistema de Gestión Federada de Tickets

Federated Ticket Management System

Sistema para la Gestión de Ciberincidentes en las entidades del ámbito de aplicación del ENS. Con ella se pretende mejorar la coordinación entre el CERT Gubernamental Nacional y los distintos organismos y organizaciones con las que colabora.

A finales de 2018, se encontraba operativa la versión 3.1 y a ella estaban inscritas 265 organizaciones. En su mayoría, el 73% conectados a LUCIA central (la instancia del CCN-CERT desde la que se gestionan los ciberincidentes).

49 organismos se encontraban federados. Estos comparten incidentes detectados diariamente y constituyen el 27% de los incidentes gestionados por el CCN-CERT.

269
Organismos en LUCIA Central / Organizations in LUCIA Central

49
Organismos federados / Federated Organizations

System for cyber Incident Management in ENS entities. It aims to improve the coordination between the National Governmental CERT and the various agencies and organizations with which it collaborates.

By the end of 2018, version 3.1 was operational and 265 organizations were registered. For the most part, 73 % connected to central LUCIA (the CCN-CERT instance from which cyber incidents are managed). There were 49 federated organizations. These share incidents on a daily basis and constitute 27 % of the incidents managed by CCN-CERT.

Plataforma Multiantivirus en tiempo real

Platform Multiantivirus in real time

Herramienta de detección desarrollada para el análisis estático de código dañino a través de múltiples motores antivirus y antimalware para plataformas Windows y Linux. Una de sus principales ventajas es que analiza cualquiera de los ficheros subidos de forma aislada, lo que garantiza que dicho fichero no es trasladado a ninguna otra organización, ni empresa antivirus.

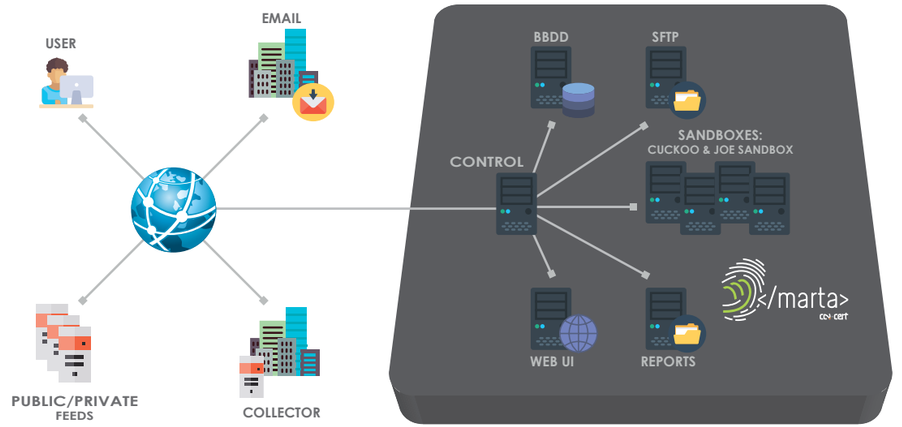
Detection tool developed for malware static analysis through multiple antivirus and antimalware engines for Windows and Linux platforms. One of its main advantages is that it analyzes any of the uploaded files in isolation, which guarantees that the file is not transferred to any other organization or antivirus company.

Análisis avanzados de ficheros

Advanced file analysis

Plataforma avanzada de **multi-sandboxing** dedicada al análisis automatizado de múltiples tipos de ficheros que pudieran tener un comportamiento malicioso. A partir de la información que recoge, un analista podrá determinar qué tipo de funcionalidad y qué implicaciones tiene para su organización.

Advanced **multi-sandboxing** platform dedicated to the automated analysis of multiple file types that could have malicious behavior. From the information it collects, an analyst will be able to determine what kind of functionality and what implications it has for the organization.



Análisis y Gestión de riesgos

Analysis and Risk Management

Las herramientas EAR (Entorno de Análisis de Riesgos) soportan el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) y está desarrollada y financiada parcialmente por el CCN. Se actualizan periódicamente y existen diversas variantes:

The ERA (Environmental Risk Analysis) tools support the analysis and risk management of an information system following the Magerit methodology (Information Systems Analysis and Risk Management Methodology) and is developed and partially financed by the CCN. They are maintained periodically and there are several variants:

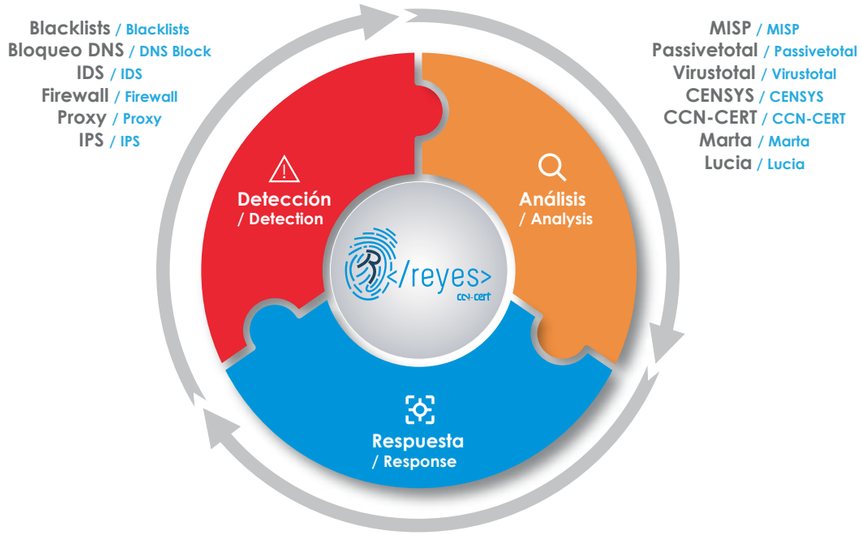
- **PILAR:** versión íntegra de la herramienta.
  / full version of the tool.
- **PILAR Basic:** versión sencilla para Pymes y Administración Local.
  / simple version for SMEs and Local Administration.
- **µPILAR:** versión de PILAR reducida, destinada a la realización de análisis de riesgos muy rápidos.
  / reduced version of PILAR, intended for very rapid risk analysis.
- **RMAT** (*Risk Management Additional Tools*): personalización de herramientas.
  / (Risk Management Additional Tools): customization of tools.

Intercambio de Información de Ciberamenazas

Cyber threats Information Exchange

Solución desarrollada para agilizar la labor de análisis de ciberincidentes y compartir información de ciberamenazas. A través de este **portal centralizado de información** puede realizarse cualquier investigación de forma rápida y sencilla, accediendo desde una única plataforma a la información más valiosa sobre ciberincidentes. Fue la página de la parte pública del portal del CCN-CERT más visitada durante 2018.

Solution created to streamline the cyber incidents analysis and share information on cyberthreats. Through this **centralized information site**, any investigation can be carried out quickly and easily, with access from a single platform to the most valuable information on cyber incidents. It was the section of the CCN-CERT website's public part most visited during 2018.



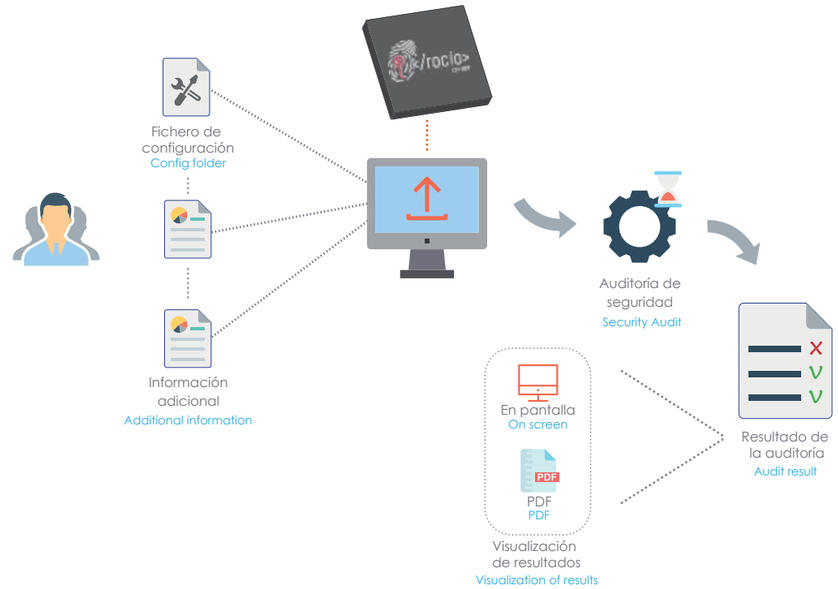
IOC / IOC
Reglas YARA / YARA Rules

Auditoría de configuraciones de dispositivos de red

Audit of network device configurations

Solución para la automatización de las tareas básicas realizadas por un auditor de seguridad sobre equipos de comunicaciones: enrutadores, conmutadores y cortafuegos. Ha sido desarrollada para verificar el nivel de seguridad de dichos equipos. Gracias a ella, los responsables de seguridad podrán comprobar, de un modo rápido y sencillo, si su dispositivo está configurado adecuadamente o no.

Solution for the automation of basic tasks performed by a security auditor on communications equipment: routers, switches and firewalls. It has been developed to verify the level of security of such equipment. It allows security officers to quickly and easily check whether or not their device is configured properly.



Grabaciones y emisiones de vídeo en streaming

Streaming video recordings and broadcasts

Herramienta para facilitar la tarea de formación y sensibilización con toda su comunidad de referencia (*véase apartado de Formación*).

Tool to facilitate the task of training and awareness-raising with the entire reference community (*see Training section*).

8.4 Informes, AVISOS y vulnerabilidades
Reports, WARNINGS and vulnerabilities

El CCN-CERT ofrece información sobre el estado de la ciberseguridad, con el fin de reducir tanto las vulnerabilidades técnicas (de hardware y software), como humanas y de organización.

Su principal público objetivo son los usuarios registrados de su portal, a los que notifica periódicamente avisos, alertas, vulnerabilidades y la publicación de informes de diferentes materias (un total de 286 a lo largo de los dos últimos años, de los cuales 217 se encuentran disponibles en el portal) elaborados por su grupo de expertos. Entre estos se encuentran informes de **código dañino**, informes de **buenas prácticas** o informes de **amenazas** (siendo estos últimos la página de la parte privada del portal del CCN-CERT más visitada durante 2018), todos ellos disponibles en el portal web del CCN-CERT, www.ccn-cert.cni.es.

The CCN-CERT provides information on the cybersecurity status, in order to reduce both technical vulnerabilities (hardware and software) and human and organizational vulnerabilities.

Its main target audience are users registered on the site, to whom it regularly notifies warnings, alerts, vulnerabilities and the publication of reports on different issues (286 over the last two years, of which 217 are available on the website) drawn up by its group of experts. These include **malware**, **best practices** or **threats reports** (being the latter the most visited section of the CCN-CERT website's private part during 2018). They all are available on the CCN-CERT site, www.ccn-cert.cni.es

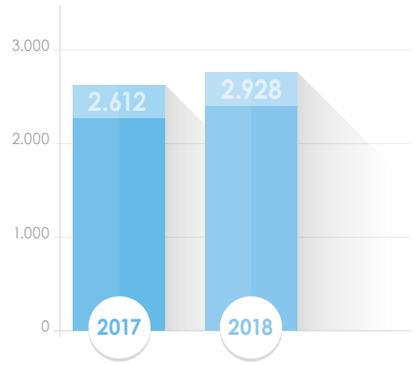
El CCN-CERT ha publicado un total de 286 informes de diferentes materias a lo largo de los dos últimos años
The CCN-CERT has published a total of 286 reports on different subjects over the last two years.

Vulnerabilidades
Vulnerabilities

Diariamente, el CCN-CERT publica las vulnerabilidades de los siguientes fabricantes: Microsoft, Red Hat, Cisco, Oracle, Adobe, Suse, Debian, IBM, Apple, Symantec, Joomla, Moodle, WordPress, Drupal, Juniper, VMWare, AmazonWS y F5. Entre 2017 y 2018 se publicaron un total de 5.540 vulnerabilidades (2.612 durante 2017 y 2.928 durante 2018).

Entre 2017 y 2018 se publicaron un total de 5.540 vulnerabilidades
A total of 5,540 vulnerabilities were released between 2017 and 2018

Every day the CCN-CERT publishes vulnerabilities for the following manufacturers: Microsoft, Red Hat, Cisco, Oracle, Adobe, Suse, Debian, IBM, Apple, Symantec, Joomla, Moodle, WordPress, Drupal, Juniper, VMWare, AmazonWS and F5. A total of 5,540 vulnerabilities were published between 2017 (2,612) and 2018 (2,928).



Vulnerabilidades publicadas por el CCN-CERT
Vulnerabilities published by CCN-CERT

Principales Informes elaborados por el CCN-CERT
CCN-CERT reports

Informes de Amenazas 2017: 28
Threat Reports 2017: 28

CCN-CERT IA-03/17 Medidas Seguridad Ransomware
CCN-CERT IA-03/17 Security Measures Ransomware
CCN-CERT IA-04/17 Ciberhacktivismo y Ciberyihadismo. Informe Resumen 2016
CCN-CERT IA-04/17 Hacktivism and Cyber-jihadism. Summary Report 2016
CCN-CERT IA-06/17 Dispositivos y Comunicaciones Móviles. Informe Resumen 2016
CCN-CERT IA-06/17 Mobile Devices and Communications. Summary Report 2016
CCN-CERT IA-09/17 Medidas Seguridad Vulnerabilidad Struts
CCN-CERT IA-09/17 Security Measures Struts Vulnerability
CCN-CERT IA-16/17 Ciberamenazas y Tendencias. Edición 2017. Resumen Ejecutivo
CCN-CERT IA-16/17 Cyber threats and Trends. 2017 Edition. Executive Summary
CCN-CERT IA-16/17 Ciberamenazas y Tendencias. Ed. 2017
CCN-CERT IA-16/17 Cyber threats and Trends. 2017 Edition
CCN-CERT IA-16/17 Cyberthreats-Trends 2017. Executive Summary
CCN-CERT IA-16/17 Cyber threats and Trends 2017. Executive Summary
CCN-CERT IA-17/17 Análisis de IMBox: riesgos de uso
CCN-CERT IA-17/17 IMBox analysis: risks of use
CCN-CERT IA-22/17 Medidas de Seguridad Vulnerabilidad de Struts
CCN-CERT IA-22/17 Security Measures Strut Vulnerability
CCN-CERT IA-23/17 Riesgos de uso de Telegram
CCN-CERT IA-23/17 Risks of using Telegram

Informes de Amenazas 2018: 30
Threat Reports 2018: 30

CCN-CERT IA-25/18 Cryptojacking

CCN-CERT IA-09/18 Cyberthreats and tendencies. Executive Summary 2018

CCN-CERT IA-13/18 Riesgos de uso de Line
CCN-CERT IA-13/18 Line Use Risks
CCN-CERT IA-11/18 Medidas de seguridad contra ransomware
CCN-CERT IA-11/18 Security measures against ransomware
CCN-CERT IA-07/18 Informe Anual 2017. Ciberhacktivismo y Ciberyihadismo
CCN-CERT IA-07/18 Annual Report 2017. Hacktivism and Cyber-jihadism
CCN-CERT IA-09/18 Ciberamenazas y Tendencias. Resumen Ejecutivo 2018

CCN-CERT IA-09/18 Ciberamenazas y Tendencias. Ed. 2018
CCN-CERT IA-09/18 Cyber threats and Trends. 2018 Edition
CCN-CERT IA-10/18 Informe de Ciberamenazas 2017 y Tendencias 2018 - Dispositivos y Comunicaciones Móviles
CCN-CERT IA-10/18 2017 Cyber threats Report and 2018 Trends - Mobile Devices and Communications

Informes de Código Dañino 2017: 29
Malware Code Reports 2017: 29

CCN-CERT ID-01/17 Ransom.VenusLocker
CCN-CERT ID-02/17 Ransom.Bart
CCN-CERT ID-04/17 Hajime
CCN-CERT ID-13/17 Necurs
CCN-CERT ID-17/17 Ransom.WannaCrypt0r_ENG
CCN-CERT ID-17/17 Codigo Dañino.WannaCrypt0r
CCN-CERT ID-21/16 Ransom.Cerber
CCN-CERT ID-07/17 Worm.Win32.Palevo.smah
CCN-CERT ID-20/17 Ransom.Petya/NotPetya
CCN-CERT ID-08/17 Ransom.Spora
CCN-CERT ID-18/17 Ransom.TorrentLocker
CCN-CERT ID-19/17 Trojan.Torpig
CCN-CERT ID-24/17 Trojan.Sharik
CCN-CERT ID-23/17 Downeks

Informes de Código Dañino 2018: 26
Malware Code Reports 2018: 26

CCN CERT ID-25/18 BackSwap
CCN-CERT ID-18/18 Kovter
CCN-CERT ID-13/18 CrossRat
CCN-CERT ID-12/18 TROJ_QUANT
CCN-CERT ID-10/18 Trojan.Shiotob
CCN-CERT ID-09/18 Trojan-Banker.Win32.ChePro
CCN-CERT ID-08/18 Trojan.Fleercivet
CCN-CERT ID-07/18 Trojan.BetaBot
CCN-CERT ID-05/18 Trj.NjW0rm
CCN-CERT ID-04/18 Refete
CCN-CERT ID-02/18 Shifu
CCN-CERT ID-01/18 Predator Pain

Informes de Buenas Prácticas 2017: 5
Best Practices Reports 2017: 5

CCN-CERT BP-04 Ransomware
CCN-CERT BP-04 Ransomware

CCN-CERT BP-07 Recomendaciones implementación HTTPS
CCN-CERT BP-01 HTTPS implementation recommendations

CCN-CERT BP-05 Internet de las Cosas
CCN-CERT BP-05 Internet of Things

CCN-CERT BP-01 Principios y recomendaciones básicas en Ciberseguridad
CCN-CERT BP-01 Basic Principles and Recommendations on Cybersecurity

CCN-CERT BP-09 Recomendaciones de protección DoS en cortafuegos
CCN-CERT BP-03 DoS protection recommendations for firewalls

Informes Técnicos 2017: 92
Technical Reports 2017: 92

Informes de Buenas Prácticas 2018: 4
Best Practices Reports 2018: 4

CCN-CERT BP/11 Recomendaciones redes WIFI corporativas
CCN-CERT BP/11 Recommendations on corporate WIFI networks

CCN-CERT BP/08 Redes Sociales
CCN-CERT BP/08 Social Networks

CCN-CERT BP/04 Ransomware
CCN-CERT BP/04 Ransomware

CCN-CERT BP/10 Recomendaciones de seguridad para CDN
CCN-CERT BP/10 CDN Security Recommendations

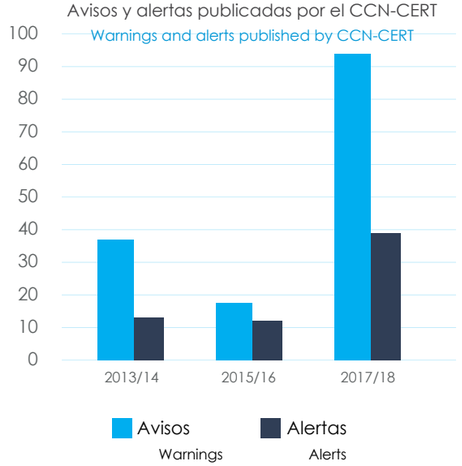
Informes Técnicos 2018: 72
Technical Reports 2018: 72

Avisos y alertas
Warnings and alerts

Todos los usuarios registrados en el portal del CCN-CERT reciben directamente los avisos y alertas de ciberseguridad en los que se informa de las nuevas amenazas detectadas (siendo las alertas las que representan una mayor criticidad). En concreto, en los dos últimos años se han notificado **94 avisos** (31 en 2017 y 63 en 2018) y **38 alertas** (21 en 2017 y 17 en 2018).

All users registered on the CCN-CERT website receive cybersecurity notifications and warnings directly, informing them of threats newly detected (being one or the other depending on their criticality). In particular, **94 notifications** (31 in 2017 and 63 in 2018) **and 38 warnings** (21 in 2017 and 17 in 2018) have been notified in the last two years.

Avisos y alertas publicadas por el CCN-CERT
Warnings and alerts published by CCN-CERT



En los dos últimos años se han notificado 94 avisos y 38 alertas
94 notices and 38 alerts have been notified in the last two years

Centros de Operaciones de SEGURIDAD (SOC)

SECURITY Operations Centres (SOC)

El incesante incremento de los ciberataques que está sufriendo el Sector Público, junto con los riesgos que ello puede suponer para la posición estratégica, económica y social del país, hace prioritario reforzar la capacidad de prevención, monitorización, vigilancia y respuesta a incidentes, a través de distintos **Centros de Operaciones de Ciberseguridad (SOC)**.

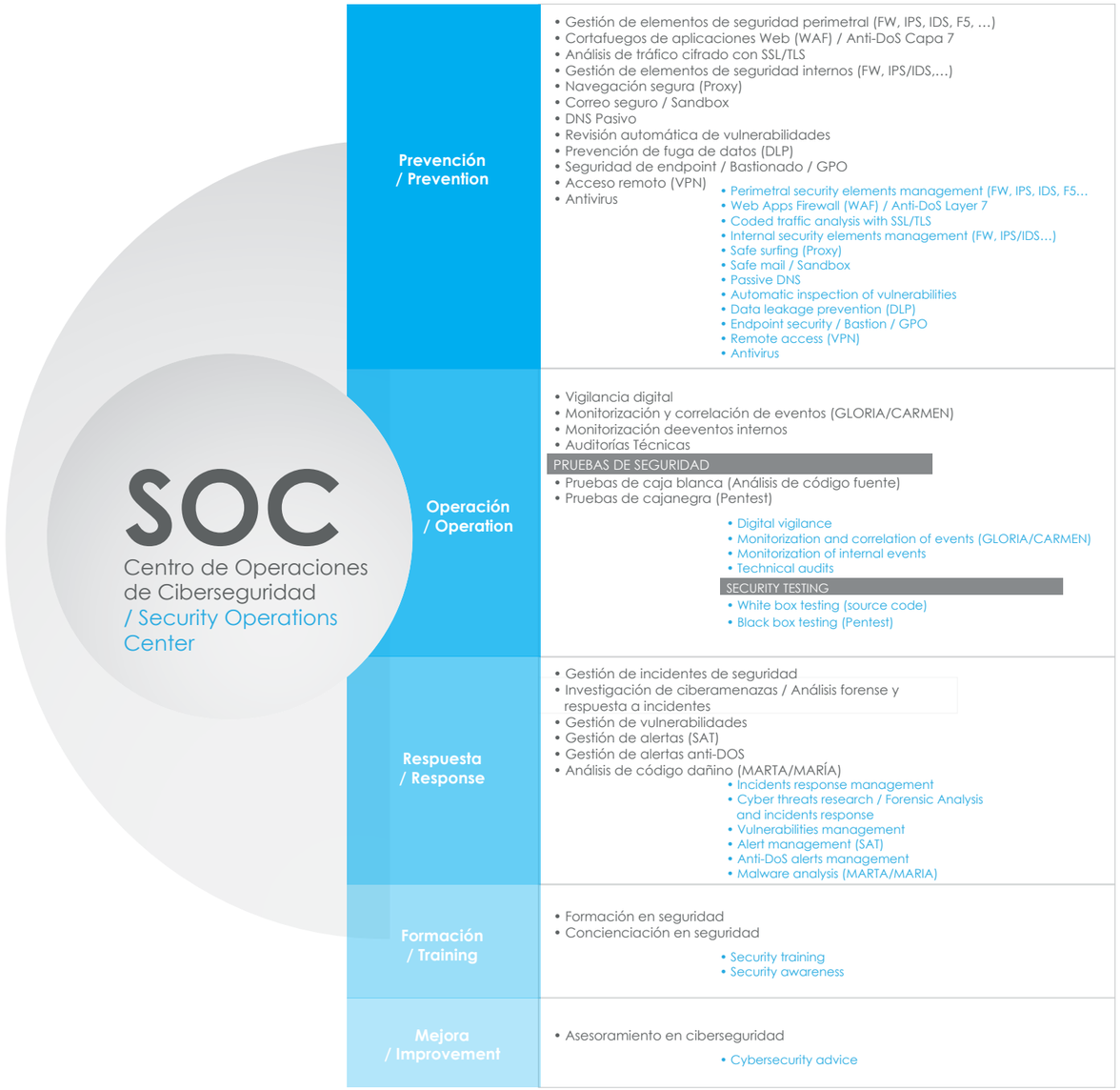
A través de un **SOC** se realizan tareas de prevención, detección y vigilancia, supervisando a las personas, los procesos y la tecnología que intervienen en todos los aspectos operativos de la ciberseguridad.

El CCN-CERT ha ofrecido servicios de vigilancia, sin coste asociado, a diversos organismos de la Administración Pública, promocionando la creación de este tipo de Centros con el fin de optimizar este tipo de recursos que son críticos. Los primeros en desarrollarse fueron en 2018 el **SOC-Justicia** y el **SOC de la Administración General del Estado (AGE)** y sus organismos públicos.

The incessant increase in cyberattacks that the Public Sector is suffering, together with the risks that this may pose to the strategic, economic and social position of the country, makes it a priority to reinforce the capacity for prevention, monitoring, surveillance and response to incidents, through different **Security Operations Centres (SOC)**.

In a **SOC**, prevention, detection and surveillance tasks are carried out, supervising the people, processes and technology involved in all operational aspects of cybersecurity.

The CCN-CERT has offered surveillance services, at no associated cost, to various government agencies, promoting the creation of such centres in order to optimize this type of critical resources. The first to be developed in 2018 were the **SOC-Justice** and the **SOC of the General State Administration (AGE)** and its public bodies.

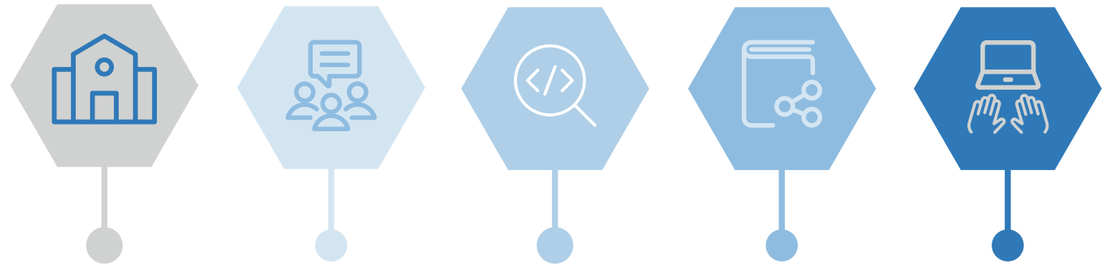


Centros de Operaciones de Seguridad (SOC)
Security Operations Centres (SOC)

vSOC

A ellos le seguirán, ya como un proyecto de 2019, los centros destinados a las entidades locales. A través del **vSOC**, ayuntamientos y diputaciones tendrán más visibilidad e información sobre vulnerabilidades, fallos de configuración e incidentes, capacidad de despliegue, protección y actuación. Al disponer de una gestión centralizada, aumentará el número de entidades adscritas a cada **vSOC**.

These will be followed, as a 2019 project, by centres for local entities. Through the **vSOC**, town councils and local governments will have more visibility and information on vulnerabilities, configuration and incident failures, greater capacity for deployment, protection and action. By having a centralised management, the number of entities attached to each **vSOC** will increase.



Departamento de PRODUCTOS y Tecnologías, PYTEC

PRODUCTS and Technologies Department, PYTEC

El Departamento de Productos y Tecnologías del CCN, PYTEC, desempeña las siguientes funciones:

- Promoción y desarrollo de productos de cifra y seguridad TIC: su objetivo es garantizar que los productos utilizados por la Administración cumplan con los niveles de seguridad exigidos.
- Evaluación y certificación: la evaluación y certificación de productos de seguridad TIC son el único medio objetivo que permite valorar y acreditar la capacidad de un producto para manejar información segura.
- Seguridad Productos TIC: el CCN elabora un Catálogo de Productos STIC en el que ofrece un listado de productos de seguridad TIC con unas garantías de seguridad contrastadas por el propio CCN.

The Products and Technologies Department of the CCN, PYTEC, performs the following functions:

- Promotion and development of ICT security and encryption products: its objective is to guarantee that the products used by the Administration comply with the required security levels.
- Evaluation and certification: The evaluation and certification of ICT security products are the only objective means to assess and accredit the ability of a product to handle secure information.
- Security ICT Products: the CCN prepares a Catalogue of ICT Products in which it offers a list of ICT security products with security guarantees contrasted by the CCN itself.

10.1 Promoción y DESARROLLO DE PRODUCTOS

PRODUCTS promotion and DEVELOPMENT

Una de las funciones del CCN es la de coordinar la promoción, desarrollo, obtención, adquisición, puesta en explotación y utilización de la tecnología de la seguridad de los sistemas TIC que incluyan cifra, para procesar, almacenar o transmitir información de forma segura. Durante los años 2017 y 2018 se han llevado a cabo los siguientes desarrollos y dado a conocer los siguientes productos:

One of the functions of the National Cryptologic Centre is to coordinate the promotion, development, obtaining, acquisition, start-up and use of security technology for ICT systems including encryption, in order to process, store or transmit information securely. During 2017 and 2018 the following developments have been carried out and promoted:

Cifrador IP europeo (EP430GU)
EP430GU European IP Crypto

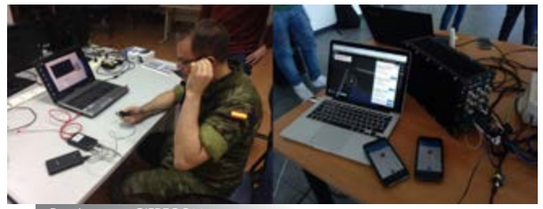
Este proyecto ha sido desarrollado desde 2014 por la empresa Epicom y financiado con fondos I+D del Programa Galileo. Durante este periodo se ha modificado la criptología y los mecanismos de seguridad de su predecesor, el cifrador NATO Secret EP430GN, adecuándolos a los requisitos de la Unión Europea con la finalidad de superar la segunda evaluación por parte de Francia. Una vez superada, supondrá la aprobación por parte del Consejo de la UE del primer cifrador IP nacional para proteger información hasta EU Secret.

This project has been developed since 2014 by the company Epicom and financed by Galileo Program R&D funds. During this period, the cryptology and the security mechanisms of its predecessor, the NATO Secret EP430GN encryption device, have been modified, adapting them to the European Union requirements in order to pass the second assessment by France. Once overcome, it will imply the approval by the Council of the EU of the first national IP encryption device to protect information up to EU Secret.

Cifrador Personal para el Combatiente (CIFPECOM) e integración con sistemas CIS de las FAS
Personal Combatant Encryption Device (CIFPECOM) and integration with CIS systems

Durante el año 2017 y 2018 se ha trabajado de forma conjunta con diferentes unidades del Ejército de Tierra en la integración de este cifrador con diferentes equipos de dotación (radios PR4G, terminales SECOMSAT, etc.). La Jefatura CIS del ET le ha incluido en su arquitectura de referencia para la protección de las comunicaciones de su gestor de comunicaciones (GESCOMET) entre puestos de mando de brigada y puestos de mando de batallón.

Por su parte, la empresa Tecnobit ha continuado trabajando con financiación propia en la evolución de este prototipo.



Pruebas con CIFPECOM

During 2017 and 2018, the integration of this encryption device with some equipment (PR4G radios, SECOMSAT terminals, etc.) has been developed jointly with different units of the Army. The CIS Headquarters of the ET has included it in its reference architecture for the protection of the communications in its communications manager (GESCOMET) between brigade and battalion command posts.

For its part, the company Tecnobit has continued working with its own financing on the evolution of this prototype.

Evolución de COMSec Admin.
Evolution of COMSec Admin.

COMSEC Admin es un sistema de comunicaciones móviles seguras creado por la empresa española INDRA SCS para su uso en la Administración Española, con el objetivo de asegurar la confidencialidad de las comunicaciones de voz y mensajería. Durante 2017 el CCN ha trabajado en la evaluación funcional y criptológica de la nueva versión de esta solución (COMSec Admin+) y durante 2018 el CCN ha trabajado en la mejora de las herramientas auxiliares de la solución con el fin de mejorar su operatividad.

COMSEC Admin is a secure mobile communications system created by the Spanish company INDRA SCS for use in the Spanish Administration, with the aim of ensuring the confidentiality of voice communications and messaging. During 2017 the CCN has worked on the functional and cryptological evaluation of the new version of this solution (COMSec Admin+) and during 2018 the CCN has worked on the improvement of the auxiliary tools of the solution in order to improve its operability.

Programa GALILEO
GALILEO Program

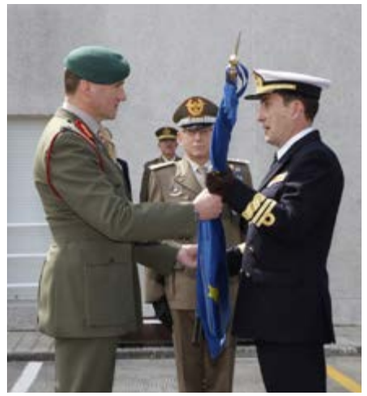
Durante 2017 se ha apoyado la labor del INTA en el programa GALILEO mediante la validación de las arquitecturas de seguridad propuestas por los desarrolladores implicados en el programa. También se ha dado formación a los mismos de cara a que los productos que se están desarrollando dentro del programa, puedan superar en el futuro los procesos de evaluación y certificación.

During 2017, INTA's work in the GALILEO programme was supported through the validation of the security architectures proposed by the developers involved in the programme. They have also been trained to ensure that the products being developed within the programme will be able to pass the evaluation and certification processes in the future.

Apoyo al despliegue español de la Operación ATALANTA
Support for the Spanish deployment of Operation ATALANTA

En 2018 el CCN ha realizado un gran esfuerzo para permitir dotar a la Armada de los equipos de cifra necesarios para el despliegue de la ACMN. Dentro de este esfuerzo, se ha realizado la dirección técnica para la adaptación de los equipos EP430DIC y EP960IC a las necesidades de seguridad de la Operación

In 2018, the CCN made a great effort to provide the Navy with the equipment necessary for the deployment of the HCNM. As part of this effort, the technical management for the adaptation of equipment EP430DIC and EP960IC to the security needs of the Operation has been carried out.



Bittium Tough Mobile
Bittium Tough Mobile

En 2017 se retomó la relación con la empresa finlandesa Bittium (antigua Electrobit) para finalizar el desarrollo y certificación finlandesa de su dispositivo y su interés para realizar una aprobación a nivel nacional.

En 2018, comenzó la evaluación funcional y criptológica del dispositivo. De esta manera, una vez superadas las evaluaciones se ampliará la oferta de terminales móviles aprobados para el manejo de información nacional clasificada.

In 2017 the relationship with the Finnish company Bittium (former Electrobit) was resumed in order to complete the development and Finnish certification of its device and interest to make a national approval.

In 2018, the functional and cryptologic evaluation of the device started. Thus, once the evaluations have been completed, the supply of mobile terminals approved for the handling of classified information will be increased.

Samsung
Samsung

En 2017 se finalizó el proceso de cualificación del Samsung Galaxy S8. Su dispositivo móvil se ha convertido en el primer terminal móvil cualificado y, por tanto, apto para su uso en el ENS categoría Alta.

En 2018 se ha continuado la colaboración con la empresa trabajando en la cualificación de varios de sus productos de gama alta (S9, S9+, Note8).

Samsung S8 / Samsung S9

The Samsung Galaxy S8 qualification process was completed in 2017. This mobile device has become the first qualified mobile terminal and therefore suitable for use in the ENS High category.

In 2018 the collaboration with the company has continued for the qualification of several of its high-end products (S9, S9+, Note8).

Prototipo de pasarela de intercambio seguro para el canal secundario del Sistema Galileo
Prototype of a secure exchange gateway for the secondary channel of the Galileo System

Esta pasarela garantizará el aislamiento y la protección de los nodos de comunicaciones del canal secundario de Galileo frente al flujo de información proveniente o con destino a terminales de usuario. Todo ello independientemente del nivel de clasificación, dominio de seguridad o autoridad operativa que tengan, minimizando las amenazas provenientes de dichas interconexiones.

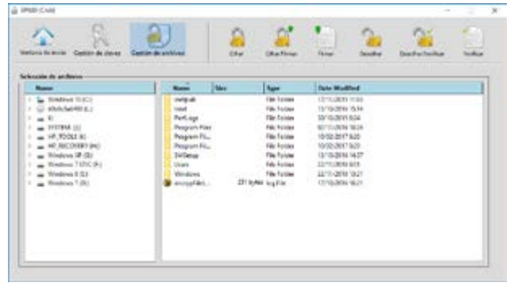
Este proyecto, desarrollado por la empresa Autek, ha sido financiado con fondos del programa Galileo.

This gateway will ensure the isolation and protection of the communications nodes of Galileo's secondary channel against the flow of information from or to user terminals. All this regardless of the classification, security domain or operational authority level they have, minimizing threats from these interconnections.

This project, developed by the company Autek, has been financed with funds from the Galileo program.

Software de Cifrado Offline – EP880
Offline Encryption Software - EP880

El EP880 es un software de cifrado offline que, mediante el uso de certificados y mecanismos de cifrado simétrico y firma asimétrica, permite cifrar y firmar archivos para su posterior envío de forma segura por redes abiertas. El sistema posibilita el cifrado para múltiples usuarios, utilizando para cada uno de ellos una clave distinta, protegiendo la confidencialidad y la autenticidad de los archivos.



The EP880 is an offline encryption software that, through the use of certificates and mechanisms of symmetric encryption and asymmetric signature, allows the encryption and signing of files for secure delivery through open networks. The system makes it possible to encrypt for multiple users, using a different key for each of them, protecting the confidentiality and authenticity of the files.

Crypto Token EP852 y EP585
Crypto Token EP852 & EP585

Durante 2017-2018 Epicom ha desarrollado bajo la supervisión del CCN, el cifrador offline EP852, evolución del crypto token EP851. Esta nueva versión implementa funcionalidades mejoradas de seguridad, así como un nuevo diseño del dispositivo. Es compatible con las versiones anteriores.

During 2017-2018 Epicom has developed, under the supervision of the CCN, the device for offline encryption EP852, evolution of the crypto token EP851. This new version implements enhanced security features as well as a new device design. It is compatible with previous versions.

Para facilitar su gestión, junto con la del EP851v1 y EP851v2, se desarrolló el centro de gestión de equipos EP585. Este sistema permite agilizar las labores de administración y gestión, además de incluir funcionalidades extendidas de cifrado.

To facilitate its management, together with the EP851v1 and EP851v2, the EP585 equipment management centre was developed. This system allows to speed up the administration and management tasks as well as include extended encryption functionalities.

Cifrador IP personal EP960+
Personal IP Encryption Device EP960+

Este cifrador personal de alto nivel de seguridad, desarrollado por Epicom, está basado en una arquitectura que permite la separación lógica rojo-negro. Ha sido diseñado para satisfacer las necesidades operacionales de los organismos del despliegue, ya que con su reducido tamaño permite un fácil transporte y establecer enlaces seguros a través de conexiones a redes LAN, inalámbricas, y redes móviles.

This high-level personal security encryption device, developed by Epicom, is based on an architecture that allows logical red-black separation. It has been designed to meet the operational needs of deployment agencies, since its small size allows easy transport and establish secure links through connections to LAN, wireless, and mobile networks.

Cifrador concentrador confidencial de alta velocidad: EP430AVC
High Speed Confidential Concentrator Encryption device: EP430AVC

El prototipo de cifrador 430AVC se ha desarrollado para servir de equipo concentrador para las redes de EP960+.
Este desarrollo ha sido financiado por el CNI, y se ha desarrollado con la nueva arquitectura exigible para equipos para procesar información confidencial.

The 430AVC encryption device prototype has been developed to serve as a concentrator equipment for EP960+ networks. It has been funded by the CNI and has been developed with the new architecture required for equipment to process confidential information.

Cifrador de alta velocidad IP: MAVIP-R y MAVIP-S
High-speed IP Encryption Device: MAVIP-R and MAVIP-S

Esta nueva familia de cifradores IP de alta velocidad, 10Gbps, ha sido diseñada para cubrir los requisitos de protección de los enlaces troncales de las redes de la Administración. Ambos desarrollados por Epicom y financiados por la DGAM (MAVIP-R) y el CNI (MAVIP-S). El primero de ellos conforme a los estándares establecidos para la protección de información nacional clasificada hasta Difusión Limitada (Restricted).

This new family of high-speed IP encryption devices, 10Gbps, has been designed to meet the protection requirements of the backbones of the Administration's networks. Both developed by Epicom and funded by DGAM (MAVIP-R) and the CNI (MAVIP-S). The first of them as stated by the standards established for the protection of classified information up to Restricted Diffusion.

Desarrollo de un software de cifrado de disco duro
Development of a hard disk Encryption software

Se ha trabajado con la empresa francesa PrimX y la empresa nacional Epicom para personalizar con un algoritmo nacional el software de cifrado de disco duro que ya tiene desarrollado la empresa PrimX.

The CCN has worked with the French company PrimX and the national company Epicom to personalize with a national algorithm the hard disk encryption software which has already developed PrimX.

MAVLINK, prototipo de cifrador de enlace 100 GBPS
MAVLINK, prototype of 100 GBPS link encryption device

Este prototipo surge de la necesidad de conectar Centros de Procesado de Datos (CPD) garantizando la velocidad suficiente. Su finalidad es conectar distintas sedes de la Administración a una velocidad media de 100Gbps agregados.

This prototype arises from the need to connect Data Processing Centers (DPC) ensuring sufficient speed. Its purpose is to connect different offices of the Administration to an average speed of 100Gbps aggregated.

10.2 EVALUACIÓN
EVALUATION

La evaluación es el proceso en el que se contrasta la seguridad de un producto o sistema de acuerdo a unos determinados criterios o normativa, en función de la información que manejan. Una vez son confirmados los resultados de la citada evaluación se inicia el proceso de certificación; es decir la confirmación de los resultados de la evaluación por la que el producto o sistema tiene la capacidad de proteger la información hasta el nivel de seguridad otorgado o de aseguramiento declarado.

El CCN realiza cuatro tipos de certificaciones: **certificación funcional**, **cualificación de productos y servicios**, **aprobaciones** (en el caso de que manejen información nacional clasificada) y **certificación TEMPEST** (si manejan información clasificada de grado Confidencial o superior). *Véase apartado del Organismo de Certificación.*

Evaluation is the process in which the security of a product or system is contrasted according to certain criteria or normative, depending on the information they handle. Once the results of the aforementioned evaluation are confirmed, the certification process begins; that is, the confirmation of the results of the evaluation by which the product or system has the ability to protect the information up to the level of security granted or assurance declared.

The CCN performs four types of certifications: **functional certification, qualification of products and services, approvals** (in the case that they handle classified information) and **TEMPEST certification** (if they handle classified information of Confidential or superior degree). *See section on Certification Body.*

Tipo de Certificación Type of certification	**Requisito previo** Previous requirement
Certificación Funcional Functional Certification	**Evaluación Funcional (Common Criteria, ITSEC, ISO19790, LINCE)** Functional Evaluation (Common Criteria, ITSEC, ISO19790, LINCE)
Cualificación Qualification	**Certificación Funcional con requisitos fundamentales de seguridad (CCN-STIC 140)** Functional Certification with basic security requirements (CCN-STIC 140)
Aprobación Approval	**Certificación Funcional con requisitos fundamentales de seguridad (CCN-STIC 140)** **Evaluación criptológica** Functional Certification with basic security requirements (CCN-STIC 140) Cryptologic Evaluation
TEMPEST TEMPEST	**Evaluación TEMPEST / Evaluación Zoning** TEMPEST Evaluation / Zoning Evaluation

Evaluación y Certificación de Productos STIC
Evaluation and Certification of STIC Products

El Director del Centro Criptológico Nacional es la Autoridad de Certificación de la seguridad de las Tecnologías de la Información y Autoridad de Certificación Criptológica. El departamento CCN-PYTEC realiza los siguientes tipos de certificaciones a los productos de seguridad TIC:

The Director of the National Cryptologic Centre is the Certification Authority for the security of Information and Communication Technologies and Cryptologic Certification Authority. The CCN-PYTEC Department performs the following types of certifications for ICT security products:

Cualificado
Qualified

Productos aptos para su utilización en el Esquema Nacional de Seguridad (ENS)

Products suitable for their use in the National Security Framework (ENS).

Aprobado
Approved

Productos aptos para su utilización para el manejo de Información Clasificada Nacional.

Products suitable for their use in the manage of National Classified Information.

Certificación TEMPEST
TEMPEST Certification

Evaluación de equipos y plataformas para determinar el nivel de emanaciones en canales secundarios.

Evaluation of equipment and platforms to determine the level of emanations on secondary channels.

Certificación Zoning
Zoning Certification

Evaluación de equipos e instalaciones para clasificar el nivel de seguridad de emanaciones.

Evaluation of channels and facilities to classify the security level of emanations.

10.3 PRODUCTOS y SERVICIOS de Seguridad de las TIC
ICT Security PRODUCTS and SERVICES

Con el objetivo de facilitar la adquisición de productos y servicios de seguridad TIC que dispongan de un nivel mínimo de confianza para la Administración Pública, es decir cuyas funcionalidades de seguridad relacionadas con el objeto de su adquisición han sido certificadas; el Departamento de Productos y Tecnologías del CCN, CCN-PYTEC, publica el **Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación** (CPSTIC), tanto en formato web (https://oc.ccn.cni.es) cómo en forma de guía (CCN-STIC 105).

El CPSTIC tiene como finalidad ofrecer a los organismos de la Administración un conjunto de productos STIC de referencia cuyas funcionalidades de seguridad relacionadas con el objeto de su adquisición han sido certificadas. Este proceso de certificación permite proporcionar un nivel mínimo de confianza al usuario final en los productos adquiridos, en base a las mejoras de seguridad derivadas del proceso de evaluación y certificación y a un procedimiento de empleo seguro.

Consta de dos partes: **Productos Aprobados** y **Productos Cualificados**. En el apartado de **Aprobados** se recogen aquellos productos que se consideran adecuados para el manejo de información clasificada, mientras que en el de **Cualificados** se incluyen aquellos que cumplen los requisitos de seguridad exigidos para el manejo de información sensible en el ENS, en cualquiera de sus categorías (Alta, Media y Básica).

With the aim of facilitating the acquisition of ICT security products and services with a minimum level of confidence for the Public Administration, that is to say, whose security functionalities related to the object of their acquisition have been certified: the CCN's Products and Technologies Department, CCN-PYTEC, publishes the **Information and Communication Technologies Security Product Catalogue** (CPSTIC), both in web format (https://oc.ccn.cni.es) and as a guide (CCN-STIC 105).

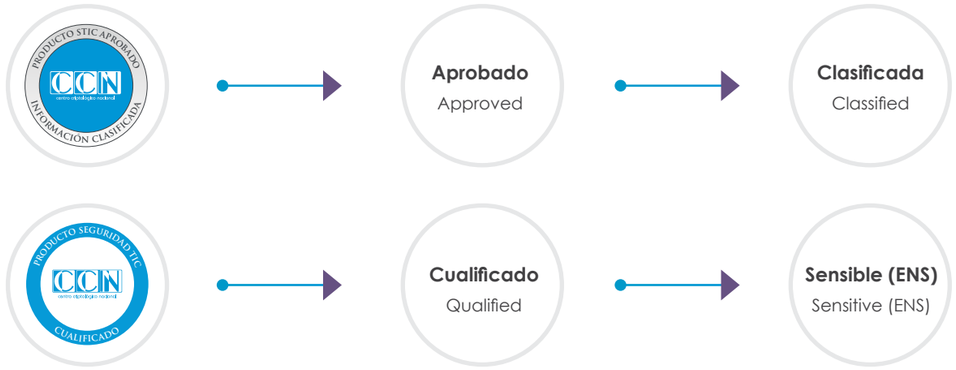
The purpose of the CPSTIC is to provide government agencies with a set of reference STIC products whose security features related to the object of their acquisition have been certified. This certification process provides a minimum level of end-user confidence in purchased products, based on security enhancements and certification process and to a safe employment procedure.

It consists of two parts: **Approved Products** and **Qualified Products.** The section on **Approved** products includes those which are considered suitable for the management of classified information, while the **Qualified** products category includes those that meet the security requirements for the handling of sensitive information in the ENS, in any of its categories (High, Medium and Basic).

1 SELLO / STAMP

2 TIPO DE PRODUCTO / TYPE OF PRODUCT

3 INFORMACIÓN QUE MANEJA / INFORMATION MANAGED



Tipos de productos incluidos en el CPSTIC
Types of products included in the CPSTIC

A finales de 2018 había 191 productos incluídos en el CPSTIC
At the end of 2018 there were 191 products included in the CPSTIC

El catálogo recoge **seis categorías** (Control de Acceso, Seguridad en la Explotación, Monitorización de la Seguridad, Protección de las Comunicaciones, Protección de la Información y Soportes de Información, Protección de equipos y servicios) y **33 familias**, como sistemas operativos, herramientas anti-spam, tarjetas inteligentes, dispositivos biométricos o sistemas Honeypot.

The catalogue includes **six categories** (Access Control, Operational Security, Security Monitoring, Communications Protection, Information Protection and Information Supports, Protection of equipment and services) and **33 families**, such as operating systems, anti-spam tools, smart cards, biometric devices or Honeypot systems.

Productos incluidos / Products included	Cualificados / Qualified	Aprobados / Approved	Total / Total
2017	76	20	96
2018	88	7	95
Total 2017-2018	164	27	191

Evolución nº productos incluidos en CPSTIC
Evolution in the number of products included in CPSTIC

Organismo de CERTIFICACIÓN (OC)

CERTIFICATION Body (OC)

La evaluación y certificación de un producto de seguridad TIC es el único medio objetivo que permite valorar y acreditar la capacidad de un producto para manejar información de forma segura. En España, esta responsabilidad está asignada al CCN a través del RD 421/2004 de 12 de marzo, en su Artículo 1 y en su Artículo 2.1, el cual establece entre sus funciones la de «constituir el organismo de certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI), de aplicación a productos y sistemas en su ámbito».

Concretamente, el **Organismo de Certificación** (OC) realiza **tres tipos de certificaciones** en función de los aspectos de seguridad que se evalúen, pero siempre referidos a productos y sistemas y servicios de seguridad TIC:

- Certificación funcional
- Certificación criptológica
- Certificación TEMPEST

En lo relativo al **ENECSTI**, se articula mediante el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, aprobado por Orden PRE/2740/2007, de 19 de septiembre, completado por su propia normativa interna y haciendo uso de los documentos de soporte que se generan en los grupos internacionales, **CCRA (Common Criteria Recognition Arrangement)** y **SOGIS-MRA**, a los cuales pertenecen.

OC-CCN

The evaluation and certification of an ICT security product is the only objective means of assessing and accrediting the ability of a product to handle information securely. In Spain, this responsibility is assigned to the CCN through RD 421/2004, dated 12th March, in its Article 1 and Article 2.1, which establishes among its functions that of "constituting the certification body of the National Framework for the Evaluation and Certification of Information Technology Security (ENECSTI), applicable to products and systems within its scope".

Specifically, the **OC** carries out **three types of certification** depending on the security aspects being assessed, but always referring to SICT products and systems:

- Functional Certification
- Cryptologic Certification
- TEMPEST Certification

With regard to the **ENECSTI**, it is articulated through the Regulation for the Evaluation and Certification of Information Technology Security, approved by Order PRE/2740/2007, dated 19th September, completed by its own internal regulations and making use of the support documents generated in the international groups, **CCRA (Common Criteria Recognition Arrangement)** and **SOGIS-MRA**, to which they belong.

En 2018, el Organismo de Certificación desarrolló una nueva metodología nacional con la que evaluar los productos de seguridad TIC. Esta nueva certificación nacional, denominada **LINCE**, está orientada al analisis de vulnerabilidades y pruebas de penetración de tipo caja negra en la que el esfuerzo documental del desarrollador se minimiza y se acota el esfuerzo de evaluacion realizado por los laboratorios acreditados a 25 jornadas en un periodo máximo de dos meses.

In 2018, the Certification Body developed a new national methodology to evaluate ICT security products. This new national certification, called **LINCE**, is oriented to the analysis of vulnerabilities and black box penetration testing in which the documentary effort of the developer is minimized and the effort of evaluation made by the laboratories accredited is limited to 25 days in a maximum period of two months.

Laboratorios acreditados o en proceso bajo su correspondiente metodología
Laboratories accredited or in process under their corresponding methodology

El OC, además, presentó en febrero de 2018 su nuevo portal web como herramienta imprescindible para fabricantes y usuarios de productos con unos requisitos mínimos de seguridad.

In February 2018, the OC presented its new webpage as an essential tool for manufacturers and users of products with minimum security requirements.

11.1 Certificación FUNCIONAL

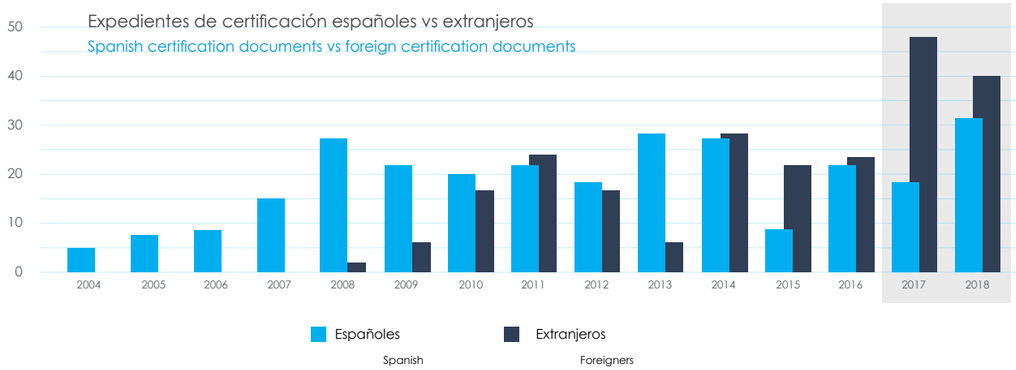
FUNCTIONAL certification

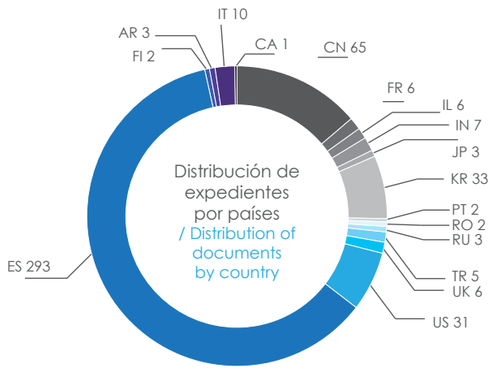
En **2017** se iniciaron **65 expedientes**: 3 de seguimiento de la acreditación de laboratorios y 62 de certificación de productos. De ellos, 35 han sido solicitudes de certificación de nuevos productos, 4 mantenimientos de la certificación, 21 revisiones de vigencia abiertas de oficio y 2 renovaciones de certificado.

En **2018** fueron **71 expedientes**: 8 de nuevas acreditaciones de laboratorios y 62 de certificación de productos. De ellos, 38 han sido solicitudes de certificación de nuevos productos, 4 mantenimientos de la certificación, 8 recertificaciones,12 revisiones de vigencia abiertas de oficio y 1 renovación de certificado.

In **2017**, **65 dossiers** were initiated: 3 for laboratory accreditation follow-up and 62 for product certification. Of these, 35 have been applications for certification of new products, 4 for certification maintenance, 21 reviews of open legal validity and 2 for certificate renewals.

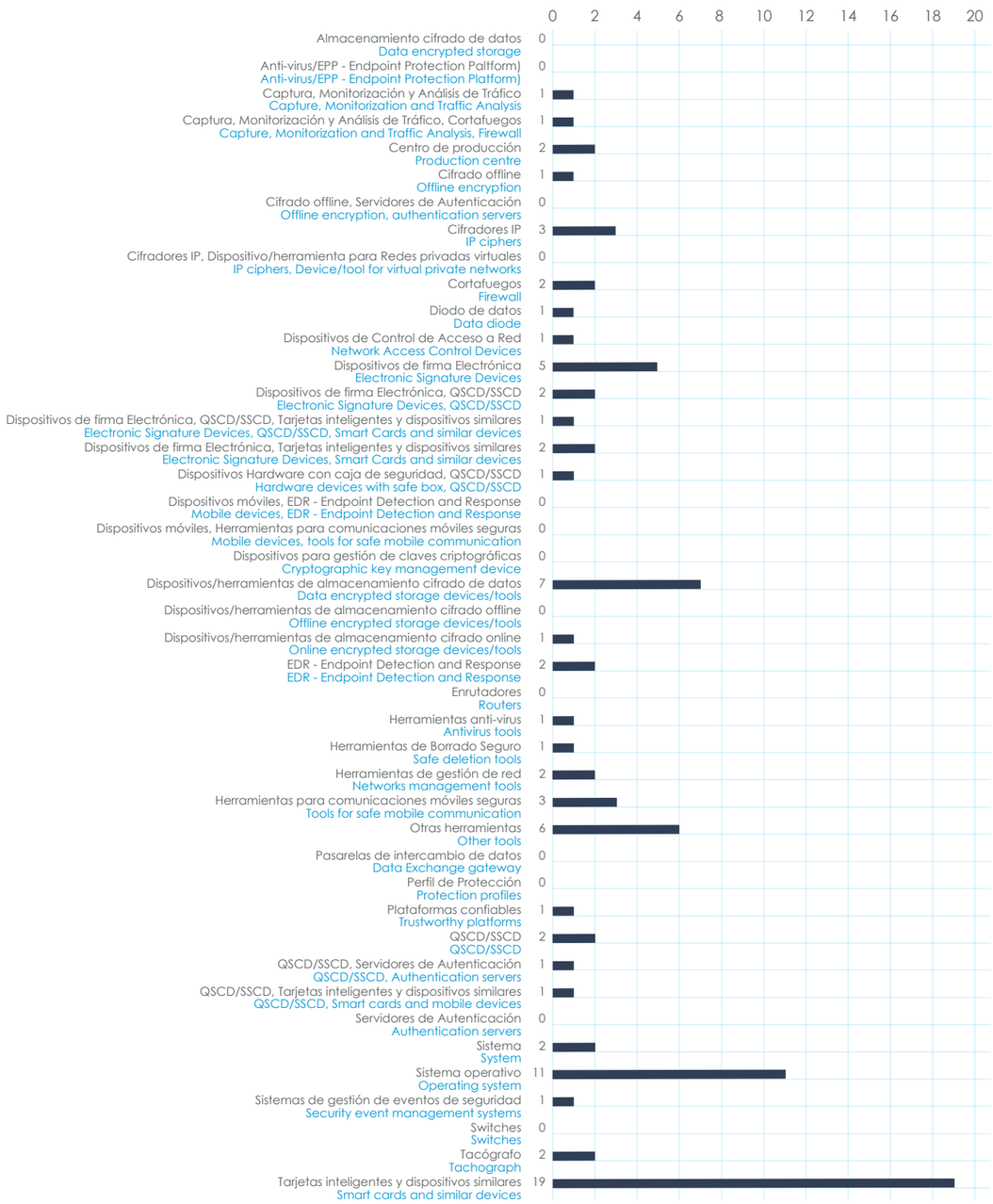
In **2018** there were **71 dossiers**: 8 for new laboratory accreditations and 62 for product certification. Of these, 38 have been applications for certification of new products, 4 certification maintenance, 8 recertifications, 12 reviews of open legal validity and 1 renewal of certificate.





Distribución de expedientes por países

Distribution of documents, by country



Expedientes de certificación por categoría (2017-2018)

Certification files by category (2017-2018)

Durante **2017**, se publicaron en el Boletín Oficial del Estado, BOE, **23 resoluciones**, de las cuales 17 son de certificación de productos STIC; 4 de certificación de centros de desarrollo; 1 de certificación de sistema y 1 de certificación de perfil de protección.

During **2017**, **23 resolutions** were published in the Spanish Official State Gazette (BOE), of which 17 were for certification of STIC products; 4 for certification of development centres; 1 for system certification and 1 for protection profile certification.

OBJETO A EVALUAR / OBJECT TO BE EVALUATED	PATROCINADOR / SPONSORSHIP	ID BOE / ID BOE	FECHA / DATE
Microsoft Windows 10 Anniversary update & Windows Server 2016	Microsoft Corporation	BOE-A-2017-1095	02/02/2017
DNIe	Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda	BOE-A-2017-1097	02/02/2017
Varonis Data Governance Suite including DataPrivilege version 6.2.38.0 for Data Governance Suite and 6.0.113 for DataPrivilege	Varonis Systems, Inc.	BOE-A-2017-1097	02/02/2017
Samsung S3FW9FJ/FL/FH/FU	Samsung Electronics Co., Ltd.	BOE-A-2017-1098	02/02/2017
Varonis Data Governance Suite including DataPrivilege version 6.2.38.0 for Data Governance Suite and 6.0.113 for DataPrivilege	Varonis Systems, Inc.	BOE-A-2017-3172	24/03/2017
Protection Profile for Trusted Platform for secure communications. EAL2+	Centro Criptológico Nacional	BOE-A-2017-3173	24/03/2017
G&D Development Center India (DCI)	Giesecke & Devrient Pvt. Ltd.	BOE-A-2017-3406	29/03/2017
Winbond Secure Serial Flash Memory W75F32W version D	Winbond Electronics Corporation	BOE-A-2017-5385	15/05/2017
HPE Network Node Manager i Premium Edition	Hewlett Packard Enterprise Development LP.	BOE-A-2017-8023	08/07/2017
Winbond TrustME? Secure Element W76S(2/4)MR(KD/DN/D1/Q1/Q3/4F) version A	Winbond Electronics Corporation	BOE-A-2017-9863	18/08/2017
Giesecke+Devrient Development Center China (DCC)	Giesecke & Devrient China Pvt. Ltd.	BOE-A-2017-9864	18/08/2017
SolarWinds Orion Suite for Federal Government V2.0	NetApp, Inc.	BOE-A-2017-9865	18/08/2017
Eternal Production Centre Shanghai	Shanghai Eternal Group Co. Ltd.	BOE-A-2017-11680	11/10/2017
Samsung S3M228A/192A/176A/132A revision 0	Samsung Electronics Co., Ltd.	BOE-A-2017-12127	23/10/2017
Huawei Eudemon8000E-X/USG9500 Series Firewall, version V300R001C01SPC300B113	Huawei Technologies Co. Ltd.	BOE-A-2017-11219	02/10/2017
Huawei 3900 Series LTE eNodeB Software (a.k.a. eNodeB)	Huawei Technologies Co. Ltd.	BOE-A-2017-12965	10/11/2017
A400M MDS v4 B3.3	Airbus Defence and Space	BOE-A-2017-13733	27/11/2017
SOMA-c007 Machine Readable Electronic Document Basic Access Control (SOMA-c007_2)	HID Global / Arjo Systems	BOE-A-2017-13821	28/11/2017
SOMA-c007 Machine Readable Electronic Document EAC-PACE-AA version 2 (SOMA-c007_2)	HID Global / Arjo Systems	BOE-A-2017-13886	29/11/2017
SOMA-c007 Machine Readable Electronic Document SSCD Application (SOMA-c007_2) version 2	HID Global / Arjo Systems	BOE-A-2017-13977	30/11/2017
Veridos Matsoukis S.A. Production Center	Veridos Matsoukis S.A.	BOE-A-2017-14099	01/12/2017
Huawei WLAN AC Series Product, version V200R007C10SPC200	Huawei Technologies Co. Ltd.	BOE-A-2017-14154	02/12/2017
Huawei WLAN AP Series Product V200R007C10SPC200	Huawei Technologies Co. Ltd.	BOE-A-2017-14258	04/12/2017

Resoluciones publicadas 2017 / Published resolutions 2017

En **2018 fueron 31 resoluciones**, de las cuales 28 eran de certificación de productos STIC, 2 de certificación de centros de desarrollo o producción y 1 de certificación de sistema.

In **2018 there were 31 resolutions**, of which 28 were for certification of STIC products, 2 for certification of development or production centres and 1 for system certification.

OBJETO A EVALUAR / OBJECT TO BE EVALUATED	PATROCINADOR / SPONSORSHIP	ID BOE / ID BOE	FECHA / DATE
Core @Firma version 5.3	Ministerio de Hacienda y Administraciones Públicas	BOE-A-2018-322	10/01/2018
SIAVAL SafeCert Appliance v2.4	Sistemas Informáticos Abiertos, S.A.	BOE-A-2018-323	09/01/2018
HPE Operations Bridge Premium v2016.05	Hewlett-Packard Enterprise Development L.P.	BOE-A-2018-324	09/01/2018
Nimble Storage, Inc. NimbleOS, version 4.2.0.1-499435-opt	Nimble Storage, Inc.	BOE-A-2018-1264	30/01/2018
Windows 10: build 10.0.15063 (also known as version 1703)	Microsoft Corp.	BOE-A-2018-4678	05/04/2018
ANCERT Server Signing Application version 1.1.7	Agencia Notarial de Certificación	BOE-A-2018-4304	27/03/2018
EulerOS v2.0 build 3.10.0-327.59.59.46.h34.x86_64	Huawei Technologies Co., Ltd.	BOE-A-2018-4741	06/04/2018
S3FW9FV/FT/F9/F8 Revision 2	Samsung Electronics Co., Ltd.	BOE-A-2018-4783	07/04/2018
Kaspersky Endpoint Security 10 for Windows with Kaspersky Full Disk Encryption 3.0 version 10.3.0.6294 AES256	Kaspersky Lab UK Ltd.	BOE-A-2018-5511	23/04/2018
vinCERTcore v.4.0.5.5733	VINTEGRIS S.L.	BOE-A-2018-5512	23/04/2018
SIAVAL SafeCert Manager 2.4	Sistemas Informáticos Abiertos, S.A.	BOE-A-2018-5382	05/06/2018
Panda Adaptive Defense Protection Agent v8.0	Panda Security SL	BOE-A-2018-6640	18/05/2018
Windows 10: build 10.0.16299 (also known as version 1709)	Microsoft Corp.	BOE-A-2018-6641	18/05/2018
Dell EMC VxRail Appliance with VxRail 4.0.400-6628128 on 160 and Dell EMC VxRail Appliance with VxRail 4.0.400-6628128 on 160F	Dell Technologies, Inc.	BOE-A-2018-6990	25/05/2018
Giesecke & Devrient Ibérica	Giesecke + Devrient Mobile Security Iberia	BOE-A-2018-6991	25/05/2018
Aselsan STC-8250A v1.1	Aselsan A.S.	BOE-A-2018-7693	08/06/2018
IS101 v1.01	ISTRIA Soluciones de Criptografía	BOE-A-2018-9209	02/07/2018
Certus Erasure Engine	Certus Software S.R.L.	BOE-A-2018-9210	02/07/2018
DNIe-DSCF (dispositivo seguro de creación de firma), version 2.0	Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda	BOE-A-2018-9672	11/07/2018
DNIe-DSCF (dispositivo seguro de creación de firma), version 3.0	Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda	BOE-A-2018-9673	11/07/2018
DNIe-DCCF (dispositivo cualificado de creación de firma), version 3.0	Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda	BOE-A-2018-9674	11/07/2018
Módulo de Firma Electrónica de Documentos v3.5	RCI Banque, S.A., Sucursal en España	BOE-A-2018-11567	14/08/2018
EP430GU version 1.04 revisión 16	Epicom S.A.	BOE-A-2018-11510	13/08/2018
THD89 Secure Microcontroller version 1.0 with Crypto Library version 1.01	Tongxin Microelectronics Co., Ltd.	BOE-A-2018-14455	22/10/2018
Fusion Access Software version V100R006C20	Huawei Technologies Co. Ltd.	BOE-A-2018-15895	21/11/2018
Savvy M2C Communications version 1.3	Savvy Data Systems S.L.	BOE-A-2018-15896	21/11/2018
Giesecke+Devrient Development Center Spain (DCS)	Giesecke + Devrient Mobile Security Iberia	BOE-A-2018-15897	21/11/2018
MPRS_TOE_Std_C version 3.6	Airbus Defence and Space	BOE-A_2018-17267	17/12/2018
KONA2 D2320N ePassport [BAC Configuration] version 02 revision 10 update 00	KONA I Co. Ltd.	BOE-A-2018-17268	18/12/2018
KONA2 D2320N ePassport [EAC with PACE configuration] version 02 revision 10 update 00	KONA I Co. Ltd.	BOE-A-2018-17269	17/12/2018

Resoluciones publicadas 2018 / Published resolutions 2018

11.2 Certificación CRIPTOLÓGICA
CRYPTOLOGIC certification

El CCN es el organismo responsable de la **evaluación**, **certificación** y **aprobación** de los productos que protegen información nacional clasificada. Tiene la consideración de equipo de cifra con certificación criptológica, aquel equipo que ha sido evaluado y ha obtenido dicha certificación del CCN. Existen distintos tipos: cifradores IP, cifradores de datos, telefonía movil cifrada, cifradores de voz, cifradores de fax, PKI (Public Key Infraestructure), generadores de números aleatorios, centros de gestión, etc.

Los productos aprobados para el manejo de información nacional clasificada o que legalmente requiera protección se incluyen en el ya citado CPSTIC, dentro de productos aprobados.

Con el fin de explicar el Procedimiento para la Aprobación de Productos de Seguridad TIC para manejar Información Clasificada se ha publicado la **guía CCN-STIC 102**, que se complementa con la CCN-STIC-130 Requisitos de los Productos de Cifra para Superar la Evaluación Criptológica.

The CCN is the Organization in charge of the **evaluation**, **certification** and **approval** of those products which protect classified information in Spain. A device is considered as cryptographic equipment with cryptologic certification if it has been assessed and has obtained this certification from the CCN. There are different types of cryptographic equipment: IP, data, mobile telephony, voice, fax, PKI (Public Key Infrastructure), random number generators, management centres, etc.

Products that have been approved for handling classified information or that legally requires protection are included in the aforementioned CPSTIC, within approved products.

The guide **CCN-STIC 102**, which complements the CCN-STIC-130 Requirements of Crypto Products to Pass the Cryptologic Evaluation, was published in order to explain the Procedure for the Approval of ICT Security Products to handle Classified Information.

CCN-STIC 102

Procedimiento para la Aprobación de Productos de Seguridad TIC

Procedure for the Approval of ICT Security Products

CCN-STIC 130

Requisitos de los Productos de Cifra para Superar la Evaluación Criptológica

Requirements of the code products to pass the cryptological evaluation

11.3 Certificación TEMPEST
TEMPEST certification

Todo dispositivo electrónico, y entre ellos los sistemas de las TIC, generan un campo electromagnético más o menos intenso que puede contener o estar relacionado con la información procesada en ese momento. Estas emanaciones pueden comprometer la seguridad, ya que afectan directamente a la confidencialidad de la información. Esta vulnerabilidad, asociada a la posibilidad de detectar la radiación y reconstruir la información original, es conocida como TEMPEST. Este mismo término se emplea también con los ataques y las contramedidas aplicadas para la protección ante dichas emanaciones comprometedoras.

El CCN, como **autoridad de certificación de seguridad TIC** en el **ámbito EMSEC** (Seguridad de las Emanaciones), es responsable del desarrollo de normativa nacional en este campo, la evaluación y certificación de equipos, sistemas, plataformas e instalaciones, así como la participación y asesoramiento tanto a administraciones públicas como a empresas privadas, actuando en todos ellos como Autoridad TEMPEST Nacional (NTA).

Con este mismo perfil, el CCN participa activamente en diversos **grupos de trabajo internacionales** para la definición de estándares de medida así como en simposios y foros de formación.

El CCN se apoya para esta actividad en las evaluaciones llevadas a cabo por el Laboratorio de Ingenieros del Ejército (LABINGE-INTA) y el Grupo de Transmisiones del Ejército del Aire (GRUTRA). Ambos laboratorios pertenecientes al Ministerio de Defensa están autorizados para la realización de este tipo de medidas en instalaciones de Defensa. En el periodo 2017-2018, estos laboratorios han llevado a cabo la evaluación de hasta **94 emplazamientos** repartidos por toda la geografía nacional.

All electronic devices, including ICT systems, generate a more or less intense electromagnetic field that may contain or be related to the information processed at that moment. These emanations can compromise security as they directly affect the confidentiality of information. This vulnerability, associated with the possibility of detecting radiation and reconstructing the original information, is known as TEMPEST. This term also refers to the attacks and countermeasures applied to guard against these compromising emanations.

The CCN's many assignments, as the **Certification Authority for ICT security** in the **EMSEC field** (Emanations Security), include developing a national standard in this field, evaluation and certification of equipment, systems and facilities, plus participation and consultancy to both public administrations and private companies, acting in all of them as the National TEMPEST Authority (NTA).

With this same profile, the CCN actively participates in various **international working groups** for the definition of measurement standards as well as in symposiums and training forums.

The CCN relies for this activity on evaluations carried out by the Army Engineers Laboratory (LABINGE-INTA) and the Air Force Transmissions Group (GRUTRA). Both laboratories belonging to the Ministry of Defence are authorised to carry out this type of measure in defence facilities. In the period 2017-2018, these laboratories have carried out the evaluation of up to **94 sites** throughout the country.

74 EVALUACIONES ZONING
74 ZONING EVALUATIONS

Efectuadas por el CCN a instalaciones, pertenecientes a otras administraciones y empresas públicas y privadas

Carried out by the CCN to installations belonging to other administrations and public and private companies.

200 MODELOS
200 MODELS

Diferentes de equipos y sistemas que han pasado por el laboratorio del CCN para obtener su clasificación ZONING.

Of different equipment and systems that have passed through the CCN laboratory to obtain their ZONING classification.

115 RENOVACIONES
115 RENEWALS

De expedientes ZONING solicitados durante 2017 y 2018

Of ZONING files requested during 2017 and 2018

31 EQUIPOS
31 PIECES OF EQUITMENT

Y Sistemas certificados TEMPEST por el CCN

And Systems certified TEMPEST by the CCN

El CCN actualiza dos veces al año la **guía CCN-STIC-104** con un listado de equipos y sistemas que han sido evaluados ZONING y que sirve como referencia para la selección de equipamiento, si bien el resultado final siempre dependerá de la evaluación del sistema seleccionado.

En el ámbito nacional, el CCN ha alentado la **fabricación de productos TEMPEST** nacionales. Entre estos equipos figuran distintos cifradores de la empresa Epicom, el CIFPECOM de Tecnobit o sistemas de la empresa Consuegra. Y en el internacional ha participado en 2017 y 2018 en diversos programas para la certificación TEMPEST de plataformas como son el EF2000 o el A400M y ha certificado diversos vehículos para el Ejército del Aire, con el apoyo del GRUTRA y para la Unidad Militar de Emergencias (UME). Además, ha iniciado el estudio de plataformas de la Armada para poder acometer a medio plazo la certificación TEMPEST de las fragatas F-100.

Por último, y a petición de Airbus Defence & Space y del Gobierno australiano, el grupo EMSEC del CCN ha llevado a cabo la evaluación y certificación TEMPEST de la última versión de la plataforma MRTT (KC-30A).

The CCN updates twice a year the guide **CCN-STIC-104** with a list of equipment and systems that have been evaluated Zoning, and that serves as a reference for the selection of equipment, although the final result will always depend on the evaluation of the selected system.

At the national level, the CCN has encouraged the manufacture of national TEMPEST products. Amongst these pieces of equipment there are different encryption devices of the company Epicom, the CIFPECOM of Tecnobit or systems of the company Consuegra.

And at the international level it has participated, during 2017 and 2018, in various international programs for the TEMPEST certification of platforms such as the EF2000 or the A400M and has certified various vehicles for the Air Force, with the support of GRUTRA, and for the Military Emergency Unit (UME). In addition, it has initiated the study of Navy platforms in order to undertake in the medium term the TEMPEST certification of the F-100 frigates.

Finally, at the request of Airbus Defence & Space and the Australian Government, CCN's EMSEC group has carried out the TEMPEST evaluation and certification of the latest version of the MRTT platform (KC-30A).

CULTURA de la Ciberseguridad

Cybersecurity CULTURE

El CCN tiene entre sus funciones la promoción en nuestro país de la cultura de la ciberseguridad, a través de iniciativas de intercambio de conocimientos entre todos los actores implicados. Para ello, acomete un gran número de **acciones de información y sensibilización**, al tiempo que promueve y participa en diferentes jornadas de ciberseguridad. Del mismo modo, mantiene una fuerte presencia en medios de comunicación y una actividad importante en distintas redes sociales: LinkedIn, YouTube y Twitter.

One of the CCN's functions is to promote cybersecurity culture nationwide through initiatives involving knowledge exchange among all stakeholders. To this end, the CCN performs a large number of information and awareness-raising actions, and promotes and participates in different cybersecurity events. It also maintains a strong media presence with significant activity on social media: LinkedIn, YouTube and Twitter.

En 2018 el CCN presento su nuevo portal, adaptado para todos los dispositivos.

In 2018 CCN presented its new portal, adapted for all devices.

- Seguidores / Followers: 9.130
- Media de impresiones / Average impressions: 118.107

- Seguidores / Followers: 10.792
- Visitas al perfil / Profile visits: 128.307
- Menciones / Mentions: 4.663

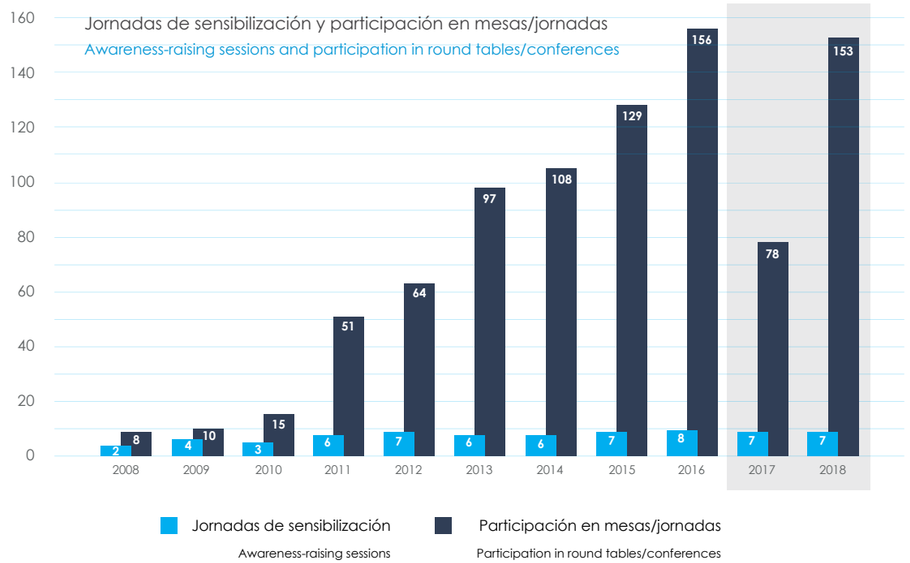
- Suscriptores / Subscribers: 985
- Visualizaciones / Views: 30.016
- Impresiones y clics / Impressions and clicks: 227.211

- Seguidores / Followers: 108
- Impresiones y clics / Impressions and clicks: 206

- Seguidores / Followers: 625
- Visitas al perfil / Profile visits: 2980
- Menciones / Mentions: 221

El Departamento de Productos y Tecnologías del CCN comenzó su andadura por las redes sociales en diciembre de 2017.

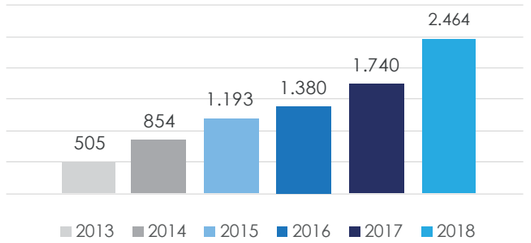
The CCN's Products and Technologies Department began its activity on social networks in december 2017.



Jornadas STIC CCN-CERT
CCN-CERT STIC Conference

El CCN-CERT organiza, desde el año 2007, las **Jornadas STIC CCN-CERT**, las cuales se han convertido en el principal encuentro de expertos en ciberseguridad del país y donde se dan cita los principales responsables de seguridad de las AAPP y de empresas de interés estratégico.

Con un total de 12 ediciones hasta la fecha, la última celebrada, que llevaba el lema *"Ciberseguridad, hacia una respuesta y disuasión efectiva"*, fueron inauguradas por Su Majestad el Rey Felipe VI. Las **XII Jornadas CCN-STIC** fueron, además, las que más asistentes han recibido hasta el momento: **más de 2.400** profesionales del sector se dieron cita en Madrid.



Asistentes Jornadas STIC CCN-CERT
Attendees of the CCN-CERT Conference

Since 2007, the CCN-CERT has been organising the **STIC CCN-CERT Conference**, which has become the main meeting of cybersecurity experts in Spain and brings together the main security officers of the Public Administrations and companies of strategic interest.

With a total of 12 editions to date, the last one, held under the slogan "Cybersecurity, for an effective response and deterrence", was inaugurated by His Majesty King Felipe VI. The XII CCN-STIC Conference was also the most attended so far: **more than 2,400** professionals from the sector met in Madrid.

Otra Jornada organizada por el CCN-CERT es la del **Sistema de Alerta Temprana (SAT)**. Durante este evento, que ya ha celebrado nueve ediciones, se ofrece una instantánea del proyecto, de su evolución futura y se intercambiaron impresiones con todas las organizaciones adheridas a este sistema.

Además, el 19 de junio de 2018 se celebró en Madrid el **encuentro "Ciberseguridad en el Sector Salud"**, organizado por el CCN-CERT junto a Entelgy Innotec Security. A la cita acudieron diversos actores de un sector especialmente sensible.

Asimismo, el CCN mantiene su compromiso con los principales eventos en los que se promueve el intercambio de conocimiento entre los miembros de la comunidad de seguridad y patrocinó los principales eventos de ciberseguriad celebrados en España (RootedCon, CONPilar, TomatinaCON, Sec/Admin, Sedian Day,etc).

Another event organized by the CCN-CERT is the **Early Warning System Sessions (CCN-CERT SAT)**. During this event, which has already celebrated nine editions, a snapshot of the project and its future evolution is offered and all the organizations adhered to it exchange impressions.

In addition, on June 19 it was held in Madrid the **meeting 'Cybersecurity in the Health Sector'**, organized by the CCN-CERT together with Entelgy InnoTec Security. The event was attended by several agents from a particularly sensitive sector.

In addition, CCN maintains its commitment to major events promoting knowledge sharing among members of the security community and sponsored major cybersecurity events held in Spain (RootedCon, CONPilar, TomatinaCON, Sec/Admin, Sedian Day).

Desayunos Tecnológicos
Technological Breakfasts

En 2018, CCN-PYTEC comenzó a desarrollar sus *Desayunos Tecnológicos* como punto de encuentro e intercambio de información y conocimientos entre el CCN, la Administración y la Industria y fabricantes de productos de Seguridad TIC.

Así, durante ese año se celebraron dos encuentros en la Escuela de Organización Industrial (EOI) de Madrid, cuya temática fue el Catálogo de Productos de Seguridad de las Tecnologías de la Información y Comunicaciones (CPSTIC). En ellos se presentó el Catálogo como herramienta de selección y adquisición de productos de seguridad TIC en los distintos entornos de aplicación dentro de la Administración: Esquema Nacional de Seguridad (ENS) y protección de Información Clasificada.

In 2018, CCN-PYTEC began to develop the *Technological Breakfasts* as a meeting point and exchange of information and knowledge between the CCN, the Administration and Industry and manufacturers of ICT Security products.

Thus, during that year two meetings were held at the Escuela de Organización Industrial (EOI) in Madrid, both focused on the Information and Communication Technologies Security Products Catalogue (CPSTIC). The Catalogue was presented as a tool for selecting and acquiring ICT security products in the different application environments within the Administration: National Security Framework (ENS) and protection of Classified Information.

Grupos de trabajo y acuerdos de colaboración

WORKING GROUPS AND COLLABORATION AGREEMENTS

En el plano nacional, la división de **ciberseguridad** del Centro Criptológico Nacional participa de los siguientes grupos de trabajo o foros:

At the national level, the **cybersecurity** division of the National Cryptologic Centre participates in the following working groups or forums:

- **Consejo Nacional de Ciberseguridad**, donde el CNI ocupa la presidencia y el CCN mantiene un puesto permanente. **National Cybersecurity Council**, where the CNI holds the presidency and the CCN holds a permanent seat.
- **CSIRT.es:** Grupo de Equipos de Respuesta a Incidentes español, con más de 30 organizaciones adscritas a él. **CSIRT.es**: Spanish group of Incident Response Teams, with more than 30 organizations attached to it.
- **Consejo de Certificación del Esquema Nacional de Seguridad, CoCENS.** Primera reunión celebrada el 17 de septiembre de 2018 **Certification Council of the National Security Framework, CoCENS**. First meeting held on 17 September 2018
- **Grupo de Trabajo de comunicaciones electrónicas seguras. Working Groups on secure electronic communications.**
- **Grupo de Trabajo del Esquema Nacional Seguridad. National Security Framework Working Group.**
- **Grupo de Trabajo de Seguridad del Comité Sectorial de la Administración Electrónica (CSAE). Security Working Group for the Electronic Administration Sector Committee (CSAE).**
- **AENOR:** Subcomités de seguridad TIC e identificación biométrica. **AENOR**: subcommittees on ICT security and biometric identification.
- **Foro ABUSES:** Grupo de Trabajo con Proveedores de Servicio de Internet (ISP). **ABUSES Forum** Working Group with Internet Service Providers (ISPs).
- **Ministerio de Defensa. Ministry of Defence**
- **Ministerio de Industria Turismo y Comercio:** Grupos de trabajo de los proyectos Rescata, Seguridad y Confianza, usabilidad del DNIe. **Ministry of Industry, Tourism and Commerce**: Working groups of the projects Rescata, Seguridad y Confianza, usabilidad del DNIe.
- **Ministerio del Interior**: Grupo de Trabajo sobre DNI electrónico con la Dirección General de la Policía; y Grupo de Trabajo de Infraestructuras Críticas con la Secretaría de Estado de Seguridad. **Ministry of the Interior**: Working group on electronic ID with the General Police Board; Working group on Critical Infrastructures with the Secretary of State for Security.
- **Federación Española de Municipios y Provincias. Spanish Federation of Towns and Provinces**

Acuerdos y convenios
Memorandums of agreements

- **Generalitat Valenciana:** Convenio firmado y apoyo al CSIRT-CV. Prorrogado el 6 de septiembre de 2017. **Generalitat Valenciana**: Convention signed and support for CSIRT-CV. Extended on 6 September 2017.
- **Junta de Andalucía:** Convenio de colaboración para el Impulso de la Sociedad de la Información y apoyo al AndalucíaCERT. **Junta de Andalucía**: Collaboration Agreement for the Promotion of the Information Society and support for AndalucíaCERT.
- **Región de Murcia:** Convenio firmado el 20 de abril de 2017. **Región de Murcia**: Collaboration agreement signed on 20th April 2017
- **Consejo General del Poder Judicial:** Convenio en materia de ciberseguridad, el 3 de octubre de 2017. **General Council of the Judiciary**: Collaboration Agreement on Cybersecurity, 3rd October 2017.
- **Gobierno de Aragón:** Convenio de colaboración en materia de ciberseguridad, **Gobierno de Aragón**: Collaboration Agreement on Cybersecurity, signed on 3rd July 2018.
- **Microsoft:** Acuerdo de colaboración en seguridad, renovado el 27 de junio de 2018. **Microsoft**: Security Collaboration Agreement, renewed 27th June 2018.
- **Universidad San Pablo-CEU:** Convenio de colaboración en materia de ciberseguridad, firmado el 15 de junio de 2018. **San Pablo-CEU University**: Collaboration Agreement on Cybersecurity, signed on 15th June 2018.
- **Ministerio de Justicia:** Convenio de colaboración en materia de ciberserguridad, firmado el 31 de julio de 2018. **Ministry of Justice**. Collaboration Agreement on Cybersecurity, signed on 31st July 2018.

Convenio con la Región de Murcia
Agreement with the Region of Murcia

Convenio con Microsoft
Agreement with Microsoft

En el plano internacional, la división de **ciberseguridad** del Centro Criptológico Nacional participa en los siguientes grupos de trabajo o foros:
At the international level, the CCN's cybersecurity division participates in the following meetings and working groups:

- **NCIRC de la OTAN** (NATO Computer Incident Response Capability), en las que los distintos CERTs de los países miembros de esta Organización analizan y comparten información sobre seguridad de la información. **NATO NCIRC** (NATO Computer Incident Response Capability), in which the different CERT of member countries analyze and share information on information security.
- **Agencia Europea de la Seguridad de las Redes y la Información** (ENISA -European Network & Information Security Agency-) de la Unión Europea. **ENISA - European Network & Information Security Agency of the European Union**.
- **APWG (Anti-Phishing Working Group)**, un programa del Consejo de Europa enfocado a eliminar todo tipo de fraude y robo de identidad a través de phishing, pharming o correos fantasmas. **APWG (Anti-Phishing Working Group)**, European Council Program aimimg to eradicate all types of fraud and identity theft through phishing, pharming or ghost mail.
- **Fórum de Respuesta a 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. **Forum of Incident Response and Security Teams (FIRST)**, the first and most important of the existing international organizations with members in Europe, America, Asia and Oceania, coming from the governmental, economic, educational, business and financial environment.
- **Trusted Introducer**, principal foro europeo de CERTs en el que colaboran, innovan y comparten información los CERTs más destacados del continente, y que forma parte de TERENA, la Asociación Transeuropea de Investigación y Educación de Redes. **Trusted Introducer**, the main European forum for CERT where the most outstanding CERT on the continent work together, innovate and share information, and which is part of TERENA, the Trans-European Research and Education Networking Association.
- **EGC** (European Government CERTs) group. Organización que reúne a los principales CERTs gubernamentales en Europa. **EGC** (European Government CERTs) group. Organization that brings together the main governmental CERTs in Europe.
- **Grupo de Cooperación de la Unión Europea.** European Union cooperation group.
- **CSIRT-Networks.** CSIRT Network
- **Intercambio con Servicios:** más de 28 encuentros anuales. Exchange with Services (more than 28 meetings per year)
- **Intercambios bilaterales con otros CERT.** Bilateral exchanges with other CERTs.

En estos foros se comparten objetivos, ideas e información sobre vulnerabilidades y ataques a nivel global.

Asimismo, esta presencia permite al CCN-CERT mantener un **contacto directo con otros equipos del resto del mundo** para, en caso de ataque, asegurarse de qué fuentes de información son fiables, así como para divulgar medidas tecnológicas que mitiguen el riesgo de ataques a sistemas y usuarios conectados a Internet, que dan servicio a sus respectivas comunidades.

During these forums objectives, ideas, and information about vulnerabilities and attacks globally are shared.

Likewise, this presence allows the CCN-CERT to maintain **direct contact with other teams from the rest of the world** in order, in the event of an attack, to make sure which sources of information are reliable, as well as to disseminate technological measures that mitigate the risk of attacks on systems and users connected to the Internet, which provide service to their respective communities.

Programa EF2000
EF2000 Program

- Grupo de Trabajo TEMPEST COMSEC Group (TCG) del Programa EF2000.
- Grupo de Trabajo INFOSEC Working Group (IWG).
  - TEMPEST COMSEC Group (TCG) of the EF2000 Program.
  - INFOSEC Working Group Group (IWG).

Programa A-400M
A-400M Program

Colaboración en el desarrollo del programa A400M, con el objeto de defender los intereses españoles en dicho programa.

- Comité Conjunto de Acreditación, JAB (Joint Accreditation Board), siguiendo la evolución de la acreditación de los sistemas, tanto embarcados como de apoyo en tierra.
- JCP (Joint Certification Panel), siguiendo la evolución de la certificación de los sistemas.
- TCP (TEMPEST Control Panel), siguiendo la evolución de la certificación TEMPEST de los equipos.
- Panel COMSEC, siguiendo la correcta implementación de la seguridad de las comunicaciones en los sistemas.
- Talleres de Análisis de Riesgos del Equipamiento Común a todas las naciones implicadas en el Programa.
- Panel Conjunto de Acreditación de la red corporativa del Grupo AIRBUS para los programas en los que está involucrado (A400M, TIGER).

Collaboration in the development of the A400M program, with the aim of defending Spanish interests in this program.

- JAB (Joint Accreditation Board), following the evolution of the accreditation of both on-board and ground support systems.
- JCP (Joint Certification Panel), following the evolution of system certification.
- TCP (TEMPEST Control Panel), following the evolution of the TEMPEST certification of the equipment.
- COMSEC Panel, following the correct implementation of communications security in the systems.
- Common Equipment Risk Analysis to all nations involved in the Program.
- Joint Accreditation Panel of the AIRBUS Group corporate network for the programs in which it is involved (A400M, TIGER).

Programa ESSOR (European Secure Software defined Radio)
ESSOR Program (European Secure Software defined Radio)

- Representante español en el "Security Technical Working Group" (STWG) del programa ESSOR (la iniciativa europea más importante en materia de radio definida por software -SDR-). Su principal cometido es abordar todas las cuestiones relacionadas con seguridad criptográfica dentro del programa (COMSEC, TRANSEC, gestión de claves, etc.). En este programa participan España, Finlandia, Francia, Italia, Polonia y Suecia (Alemania se sumará próximamente)
  - Spanish representative in the "Security Technical Working Group" (STWG) of the ESSOR program (the most important European initiative in radio defined by software -SDR-). Its main task is to address all issues related to cryptographic security within the program (COMSEC, TRANSEC, key management, etc.). This program involves Spain, Finland, France, Italy, Poland and Sweden (Germany will join soon).

Programa MALE RPAS
MALE RPAS Program

- Representante español en el grupo de trabajo INFOSEC de este programa gestionado que aborda el desarrollo europeo (Alemania, España, Francia e Italia) de un sistema aéreo remotamente pilotado de gran resistencia y preparado para operar a media altura (MALE RPAS).
  - Spanish representative in the INFOSEC working group of this program which deals with the European development (Germany, Spain, France and Italy) of a remotely controlled air system of great resistance and prepared to operate at medium altitude (MALE RPAS).

Grupo COMSEC del programa MIDS[1] (MICWG[2])
COMSEC group of the MIDS[1] program (MICWG[2])

- Representante español en este grupo de trabajo del programa MIDS (gestionado y dirigido nacionalmente por la DGAM el Ministerio de Defensa), en los que se abordan los nuevos desarrollos cripto correspondientes al BU2 ("Block Update 2") y la gestión de claves.
  - Spanish representative in this working group of the MIDS program (managed and directed nationally by the DGAM and the Ministry of Defence), in which the new encryption developments for BU2 ("Block Update 2") and key management are addressed.

Programa Galileo
Galileo Program

- Apoyo al desarrollo de este programa de radionavegación por satélite (similar al GPS norteamericano), representando los intereses españoles en el Comité de Acreditación de Seguridad, y en los distintos paneles y grupos de trabajo que desempeñan tareas de asesoramiento técnico de seguridad de las tecnologías de la información y las comunicaciones (WGNET, GSAP).
  - Support for the development of this satellite radio navigation program (similar to the North American GPS), representing Spanish interests in the Security Accreditation Committee, and in the various panels and working groups which carry out technical advisory tasks on information and communications technology security (WGNET, GSAP).

[1] Multifunctional Information Distribution System.
[2] MIDS International COMSEC Working Group.

Edita: Centro Criptológico Nacional
Edit: National Cryptologic Centre

Fotografía / photography: Centro Criptológico Nacional
Imprime / print: AINERGESA Services S.L. (Langayo)

D.L. M-28374-2019

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2019.10.09 21:55:46 +02'00'

Centro Criptológico Nacional
Argentona, 30 - 28023 Madrid

www.ccn.cni.es
www.ccn-cert.cni.es
www.oc.ccn.cni.es

centro criptológico nacional

2017 / 2018

Informe de Actividades
Activity report