MEMORIA ANUAL

ANNUAL REPORT 2019

CCN
centro criptológico nacional

Carta de la Secretaria de Estado Directora del CNI
Letter from the Secretary of State Director of the CNI

Querido/a lector/a

En el seno de esta casa, a principios de los años 80, un grupo reducido de profesionales y expertos comenzaron a prever las vulnerabilidades y los riesgos asociados al uso y aplicación de las nuevas tecnologías.

Su vocación de servicio y su capacidad de vislumbrar las amenazas en un espacio aún por definir, el ciberespacio, los llevó a formar y capacitar al personal de la Administración Pública y compartir su conocimiento con todos ellos. Un trabajo que realizaron con visión de futuro para constituir, en 2004, el **Centro Criptológico Nacional (CCN)**, cuya **Memoria Anual** 2019 tengo el placer de presentar en estas páginas.

Unas páginas que hablan de un año muy especial para todos nosotros. Un año en el que hemos celebrado el **decimoquinto aniversario** del **CCN**, adscrito al **Centro Nacional de Inteligencia (CNI)**. Quince años han transcurrido ya desde la publicación en el Boletín Oficial del Estado (BOE) del Real Decreto 421/2004, de 12 de marzo, que regulaba este Organismo.

Durante todo este tiempo, el CCN siempre ha tenido el firme propósito de fortalecer la ciberseguridad nacional, promoviendo el desarrollo, certificación y uso de productos y tecnologías seguras y velando por la protección de la información clasificada. Dando respuesta a la demanda por parte de la sociedad española de "unos servicios de inteligencia eficaces, especializados y modernos, capaces de afrontar los nuevos retos del actual escenario nacional e internacional", tal y como recoge el citado Real Decreto.

Desde su creación, el CCN ha ido adecuándose a una realidad cambiante, potenciando las acciones de prevención, detección y respuesta a los ciberataques. Así, en el año 2006 se creó el CCN-CERT o Capacidad de Respuesta a Incidentes de Seguridad, con responsabilidad en ciberataques sobre sistemas clasificados y sobre sistemas del sector público y de empresas y organizaciones de interés estratégico para el país (durante 2019 gestionó 42.997 incidentes de seguridad, de los cuales, el 7,46% fueron de peligrosidad muy alta o crítica).

Dear Reader

Within this house, in the early 1980s, a small group of professionals and experts began to anticipate the vulnerabilities and risks associated with the use and application of new technologies.

Their vocation of service and their ability to foresee the threats in a space yet to be defined, cyberspace, led them to train and capacitate the personnel of the Public Administration and to share their knowledge with all of them. This work was carried out with a vision of the future to constitute, in 2004, the **National Cryptologic Centre (CCN)**, whose **2019 Annual Report** I am pleased to present in these pages.

A few pages that speak of a very special year for all of us. A year in which we have celebrated the **fifteenth anniversary** of the **CCN**, which is attached to the **National Intelligence Center (CNI)**. Fifteen years have already passed since the publication in the Official State Gazette (BOE) of the Royal Decree 421/2004, of March 12, which regulated this Organisation.

Throughout this time, the CCN has always been committed to strengthening national cybersecurity, promoting the development, certification and use of secure products and technologies and ensuring the protection of classified information. In response to the demand of the Spanish society for "efficient, specialised and modern intelligence services, capable of meeting the new challenges of the current national and international scenario", as stated in the aforementioned Royal Decree.

Since its creation, the CCN has been adapting to a changing reality, strengthening prevention, detection and response actions to cyber attacks. Thus, in 2006 the CCN-CERT or Security Incident Response Capacity was created, with responsibility for cyber-attacks on classified systems and on systems of the public sector and of companies and organisations of strategic interest to the country (in 2019 it managed 42,997 security incidents, of which 7.46% were of a very high or critical nature).

Los hombres y mujeres del CCN han recorrido España explicando sus servicios a todas las Comunidades Autónomas, diputaciones, ayuntamientos y universidades. Han firmado convenios y acuerdos de colaboración con instituciones públicas y privadas. Todo ello hasta convertirse en punto de referencia imprescindible para todos los profesionales de la ciberseguridad de este país y situando a España en una destacada posición a nivel internacional.

Han afianzado, además, la respuesta a incidentes, promoviendo y facilitado la creación de los SOC, Centros de Operaciones de Ciberseguridad en todas las Administraciones Públicas, siendo pioneros en la concepción del ciberespacio como un vector de comunicación estratégica.

Importante ha sido también, y sigue siendo, el papel del CCN en el desarrollo, implantación y seguimiento del **Esquema Nacional de Seguridad (ENS)**, en colaboración con el Ministerio de Política Territorial y Función Pública, así como en la nueva **Estrategia Nacional de Ciberseguridad**, publicada en abril de 2019.

Cuando escribo estas líneas, nos enfrentamos a uno de los mayores desafíos a los que como Sociedad nos hemos tenido que enfrentar. La situación provocada por la pandemia del COVID-19 ha exigido de todos un esfuerzo aún mayor de resiliencia y adaptabilidad a unas circunstancias muy difíciles en todos los ámbitos de la vida.

Desde el CCN, y con la experiencia de 15 años de intenso trabajo en un marco lleno de desafíos y en continua evolución como es el de la ciberseguridad, hemos mantenido, y lo seguiremos haciendo, el mismo espíritu que nos ha guiado desde nuestros orígenes: aportar todo lo que esté en nuestras manos para garantizar un ciberespacio más seguro y confiable.

Y lo haremos con el firme propósito de superar este reto colectivo que precisa de la implicación de todos (sector público, empresas y ciudadanos) y que seguirá guiando nuestros pasos. El CCN mantendrá todos sus esfuerzos, energías y recursos en fortalecer la ciberseguridad en España y con ella las bases de su desarrollo futuro.

The men and women of the CCN have travelled around Spain explaining their services to all the Autonomous Communities, councils and universities. They have signed agreements and collaboration agreements with public and private institutions. All of this has made the CCN an essential point of reference for all the cybersecurity professionals in this country, and has placed Spain in an outstanding position at the international level.
They have also strengthened the response to incidents, promoting and facilitating the creation of SOCs, Cybersecurity Operations Centres in all Public Administrations, being pioneers in the concept of cyberspace as a strategic communication vector.

The role of the CCN in the development, implementation and monitoring of the **National Security Framework (ENS)**, in collaboration with the Ministry of Territorial Policy and the Civil Service, and in the new **National Cybersecurity Strategy**, published in April 2019, has been and continues to be important.

As I write these lines, we face one of the greatest challenges that we, as a Society, have ever had to face. The situation caused by the COVID-19 pandemic has demanded from all of us an even greater effort of resilience and adaptability to very difficult circumstances in all areas of life.

From the CCN, and with the experience of 15 years of intense work in a framework full of challenges and in continuous evolution such as cybersecurity, we have maintained, and will continue to do so, the same spirit that has guided us since our origins: to provide everything in our hands to ensure a safer and more reliable cyberspace.

And we will do so with the firm intention of overcoming this collective challenge that requires the involvement of everyone (public sector, companies and citizens) and that will continue to guide our steps. The CCN will maintain all its efforts, energy and resources to strengthen cybersecurity in Spain and with it the basis for its future development.

Paz Esteban López
Secretaria de Estado Directora del CNI
Secretary of State Director of the CNI

Índice
Index

Quince años fortaleciendo la ciberseguridad nacional
Fifteen years of Strengthening National Cybersecurity

Dña. Paz Esteban, Secretaria de Estado Directora del CNI y del CCN
Secretary of State Director of the CNI

"En el aniversario de la constitución del Centro Criptológico Nacional, resulta inevitable volver la vista atrás y recordar todos los retos a los que nos hemos enfrentado durante estos años. Nos invaden los recuerdos de nuestros inicios, en los que ya comenzábamos a advertir y a prever las vulnerabilidades y riesgos asociados a las tecnologías.

Hace 15 años se constituyó el Centro Criptológico Nacional, sobre los cimientos de un departamento que surgió en los años 80, en el seno del propio Centro Nacional de Inteligencia, y que por entonces ya había alcanzado un profundo conocimiento de las amenazas y vulnerabilidades de los sistemas de información y comunicaciones.

Pero he de confesar que, al volver la vista atrás, el primer recuerdo que se dibuja es el de las personas que durante estos 15 años han contribuido a la evolución de este organismo, cuya actividad ha ido adecuándose a una realidad cambiante como pocas.

Por ello, estas palabras pretenden servir de homenaje a todos los hombres y mujeres que han formado parte del Centro Criptológico Nacional. Su trabajo y vocación de servicio han sido elementos clave para el fortalecimiento de la ciberseguridad nacional. Gracias a ellos, el CCN es hoy una institución de referencia en el ámbito de la ciberseguridad."

"On the anniversary of the establishment of the National Cryptologic Centre, it is inevitable to look back and remember all the challenges we have faced over the years. We are invaded by memories of our beginnings, when we were already starting to detect and anticipate the vulnerabilities and risks associated with technologies.

Fifteen years ago, the National Cryptologic Centre was set up on the foundations of a department that emerged in the 1980s, within the National Intelligence Centre itself, and which by then had already achieved a thorough understanding of the threats to and vulnerabilities of information and communications systems.

But I must confess that, when looking back, the first memory that comes to mind is that of the people who, during these 15 years, have contributed to the evolution of this institution, whose activity has been adapting to a changing reality like few others.

Therefore, these words are intended to serve as a tribute to all the men and women who have been part of the National Cryptologic Centre. Their work and vocation of service have been key elements in the strengthening of national cybersecurity. Thanks to them, the CCN is today a reference institution in the field of cybersecurity."

D. Luis Jiménez, Subdirector General del CCN Assistant Director-General of the CCN

"Hace ahora 15 años un número reducido de personas comenzábamos a prevenir y detectar las amenazas del ciberespacio. Emprendíamos un nuevo camino, con ilusión y con la vista puesta en el futuro, pues ya éramos conscientes de que la protección y defensa del ciberespacio español era un reto prioritario.

La historia del CCN nos sirve a todas las personas que formamos parte de este organismo como ejemplo a seguir, pues da muestra de cómo en 15 años el trabajo incesante de todos sus miembros ha logrado convertir a este organismo en un referente nacional e internacional.

Hoy recordamos todo lo que hemos logrado en estos 15 años y, con la misma ilusión con la que emprendíamos este camino, seguimos mirando hacia el futuro. Y lo hacemos con el compromiso y la vocación de hacer del ciberespacio español un lugar más seguro y confiable."

"Fifteen years ago, a small number of people began to prevent and detect threats from cyberspace. We were embarking on a new path, with enthusiasm and with an eye toward the future, as we were already aware that the protection and defense of Spanish cyberspace was a priority challenge.

The history of the CCN serves all of us who are part of this body as an example to follow, as it shows how in 15 years the incessant work of all its members has managed to make this body a national and international benchmark.

Today we remember everything we have achieved in these 15 years and, with the same enthusiasm with which we started this path, we continue to look to the future. And we do it with the commitment and vocation to make Spanish cyberspace a safer and more reliable place."

D. Javier Candau, Jefe del Departamento de Ciberseguridad del CCN
Head of the Cybersecurity Department of the CCN

"Se cumplen 15 años de intenso trabajo para proteger el patrimonio tecnológico español, de esfuerzo para situar a España en una posición destacada a nivel internacional en materia de ciberseguridad; quince años de aprendizaje continuo, de trabajo en equipo. El Centro Criptológico ha sido capaz de evolucionar en la medida que lo han hecha las amenazas a las que nos enfrentamos día a día.

En esta evolución, de la que todos hemos sido testigo, solo hay un aspecto que se ha conservado intacto, una cualidad inherente a las personas que conforman este organismo: la dedicación con la que seguimos desempeñando nuestro trabajo. El esfuerzo, el compromiso y la proactividad han guiado nuestros pasos en estos quince años y lo seguirán haciendo en el futuro. Con estos principios por bandera, continuaremos fortaleciendo la ciberseguridad nacional."

"It is 15 years of intense work to protect Spain's technological heritage, of effort to place Spain in a leading position internationally in cybersecurity; 15 years of continuous learning, of teamwork. The Cryptologic Centre has been able to evolve in line with the threats we face every day.

In this evolution, which we have all witnessed, there is only one aspect that has remained intact, a quality inherent to the people who make up this institution: the dedication with which we continue to carry out our work. Effort, commitment and proactivity have guided our steps over these fifteen years and will continue to do so in the future. With these principles as our banner, we will continue to strengthen national cybersecurity."

D. Miguel Loste, Jefe del Departamento de Productos y Tecnologías del CCN
Head of the Products and Technologies Department od the CCN

"Ya han pasado 15 años desde que unas pocas personas comenzamos esta nueva andadura del CCN. Desgraciadamente, el tiempo pasa muy rápidamente (como bien dijo Ovidio, los días huyen sin que freno alguno los detenga), pero siempre queda la obra que se ha realizado con entusiasmo y dedicación, que puede no ser perfecta pero de la que nadie podrá objetar que se trató de hacer lo mejor posible. En mi opinión, el personal del CCN durante estos años ha hecho una importante contribución en la mejora de nuestras capacidades de ciberseguridad y en la defensa del ciberespacio español. Además, a pesar de las limitaciones existentes, muchas veces compensadas con la ilusión y entrega del personal del CCN, se ha conseguido situar al Centro en una posición impensable hace 15 años y alcanzar un merecido reconocimiento tanto a nivel nacional como internacional.

El mundo actual, al menos desde el punto de vista de la tecnología, no tiene mucho que ver con el de hace 15 años, y es evidente que las amenazas actuales son infinitamente mayores que hace unos años. Sin embargo, conceptualmente seguimos haciendo lo mismo que durante estos últimos años y es buscar soluciones confiables que proporcionen una seguridad adecuada y permitan al usuario hacer uso de la tecnología con ciertas garantías de seguridad. Y así seguiremos durante los próximos años, con el mismo entusiasmo y dedicación que al principio, defendiendo los intereses nacionales y a nuestros conciudadanos en esta nueva dimensión que hemos venido en llamar el ciberespacio."

"It has been 15 years since a few people started this new venture of the CCN. Unfortunately, time goes by very quickly (as Ovid said, days flee without any stop), but there is always the work that has been done with enthusiasm and dedication, which may not be perfect but nobody will be able to object that we tried to do our best. In my opinion, the staff of the CCN during these years has made an important contribution to improving our cybersecurity capabilities and to the defense of Spanish cyberspace.

Furthermore, despite the existing limitations, often compensated by the enthusiasm and dedication of the CCN staff, the Centre has managed to place itself in a position unthinkable 15 years ago and to achieve well-deserved recognition both nationally and internationally.

Nowadays, at least from the point of view of technology, it has little to do with that of 15 years ago, and it is clear that the threats today are infinitely greater than they were a few years ago. However, conceptually we are still doing the same thing as during the last few years and that is to look for reliable solutions that provide adequate security and allow the user to make use of the technology with certain security guarantees. And so we will continue over the coming years, with the same enthusiasm and dedication as at the beginning, to defend national interests and our fellow citizens in this new dimension that we have come to call cyberspace"

D. José Antonio Mira, primer Subdirector General del CCN
Responsable de Transformación Digital del CNI
First Deputy Director General CCN & Head of Digital Transformation CNI

"Es difícil ser conciso y breve cuando se agolpan las imágenes, compitiendo unas con otras, y es difícil no sucumbir a la nostalgia por la tremenda suerte de haber podido compartir sueños con los hombres y mujeres del Centro Criptológico Nacional (CCN) que hoy, como ayer, nos defienden, de manera anónima, a todos los españoles también en el ciberespacio.

El Centro Nacional de Inteligencia ya disponía en los años 80 de una unidad criptológica precursora del actual CCN que con la Ley de 2002 del CNI amplió su ámbito de actuación a escala nacional gracias al convencimiento de sus dirigentes, con los que tuve el honor de compartir responsabilidades, de que había que prepararse contra las amenazas emergentes que ya estaban surgiendo.

No es hasta dos años más tarde que se publica el Real Decreto que desarrolla sus misiones y cometidos y del que, recientemente, celebramos su decimoquinto aniversario.

La ilusión, la vocación, la actitud de servicio y la visión de futuro han sido, son y serán, entre otras muchas cualidades, el motor que consigue aglutinar experiencia y nuevas habilidades para seguir enfrentándose, con la excelencia que os adorna, a los retos que día a día se van presentando.

Deseo que sirvan estas líneas de reconocimiento a vuestra extraordinaria y callada labor, no siempre comprendida y compartida, de la que, si me lo permitís, me siento también orgulloso. Enhorabuena, lo habéis conseguido."

"It is difficult to be concise and brief when the images are crowded together, competing with each other, and it is difficult not to succumb to nostalgia for the tremendous luck of having been able to share dreams with the men and women of the National Cryptologic Centre (CCN) who today, as yesterday, defend us, all Spanish people, anonymously, in cyberspace.

The National Centre of Intelligence already had in the 80's a cryptologic unit that was the precursor of the current CCN, which with the 2002 Law of the CNI expanded its scope of action to a national level thanks to the conviction of its leaders, with whom I had the honour of sharing responsibilities, that it was necessary to prepare against the emerging threats that were already emerging.

It was not until two years later that the Royal Decree was published which developed its missions and tasks and of which we recently celebrated its fifteenth anniversary.

The enthusiasm, the vocation, the attitude of service and the vision of the future have been, are and will be, among many other qualities, the driving force that manages to bring together experience and new skills to continue facing, with the excellence that adorns you, the challenges that arise every day.

I would like these lines to serve as recognition of your extraordinary and quiet work, not always understood and shared, of which, if you allow me, I also feel proud. Congratulations, you have succeeded."

"Es increíble haber podido formar parte del CCN y verlo crecer y evolucionar hasta convertirse en el referente que es hoy en día, tanto a nivel nacional como internacional. Aunque lo mejor, sin duda, es el capital humano y la ilusión de su personal, sin el que nada de esto hubiera sido posible. Con el orgullo de haber formado parte de esta historia escribo estas líneas, deseando que en el futuro sigan aumentando todos los logros, hazañas y éxitos que aún quedan por conseguir."

"It is incredible to have been able to be part of the CCN and see it growing and evolving to become the benchmark it is today, both nationally and internationally. Although the best thing, without a doubt, is the human capital and the illusion of its staff, without which none of this would have been possible. With the pride of having been part of this history I write these lines, wishing that in the future all the achievements, feats and successes that are still to be achieved will continue to increase."

"Lo que en un principio empezó siendo un pequeño grupo de personas se ha convertido en un organismo de referencia nacional e internacional. Al igual que el CCN ha ido creciendo y evolucionando hasta convertirse en el gran organismo que es, también lo hemos hecho las personas que hemos estado trabajando en este organismo desde el principio, caminando juntos hacia el futuro. Así seguiremos trabajando, de la mejor forma que sabemos hacerlo."

"What started out as a small group of people has become a national and international reference institution. Just as the CCN has grown and evolved to become the great organism that it is, so have the people who have been working in this organism from the beginning, walking together towards the future. This is how we will continue to work, in the best way we know how."

"Desde que me incorporé a este proyecto la tecnología ha evolucionado enormemente, extendiendo su uso a todos los ámbitos de la vida cotidiana. Pero las amenazas que pueden comprometer la seguridad de la tecnología han cambiado mucho más rápido de lo que nadie podría imaginar, y esto ha hecho que la ciberseguridad se haya convertido en uno de los pilares fundamentales de la evolución tecnológica. Hoy en día la sociedad no entiende una tecnología como buena si no es segura y eso, estoy convencido, es gracias a la labor de concienciación que desde organismos como el CCN hemos realizado durante estos 15 años. Este es, sin duda, uno de sus mayores logros."

"Since I joined this project the technology has evolved enormously, extending its use to all areas of daily life. But the threats that can compromise the security of technology have changed much faster than anyone could have imagined, and this has made cybersecurity one of the fundamental pillars of technological evolution. Today society does not understand a technology as good if it is not secure and that, I am convinced, is thanks to the work of institutions such as CCN to raise awareness during these 15 years. This is, without a doubt, one of its greatest achievements."

"Desde su creación, el CCN ha abierto líneas de trabajo pioneras en muchos ámbitos nacionales e internacionales, y su personal nunca dudó ni por un momento en poner el máximo de su capacidad en la tarea encomendada, independientemente de lo sufrida que pudiera resultar, a cambio de saber que prestaba un servicio de primer nivel a España y a los intereses de la ciudadanía en general. Es un hecho que el CCN ha quedado ya grabado a fuego como uno de los grandes actores clave de la historia de la evolución digital en nuestra sociedad actual."

"Since its creation, the CCN has opened up pioneering lines of work in many national and international spheres, and its staff never hesitated for a moment to put their maximum capacity into the task entrusted to them, regardless of how much they suffered in return for knowing that they were providing a first-class service to Spain and to the interests of citizens in general. It is a fact that the CCN has already been recorded by fire as one of the great key players in the history of digital evolution in our current society."

"Tener como objetivo velar por la seguridad de las tecnologías TIC, supervisar y asesorar a organismos sobre el nivel de seguridad de sus sistemas y apoyar en todo lo posible para mejorarlos, para eso ha hecho falta mucho conocimiento y formación. Siempre fue un gran reto estar a la altura. Hoy veo con gran orgullo y admiración el gran organismo en el que se ha convertido el Centro Criptológico Nacional. Nunca dejaré de estar agradecida por haber formado parte de él."

"Aiming to ensure the security of ICT technologies, supervising and advising agencies on the level of security of their systems and supporting them in every possible way to improve them, this has required a lot of knowledge and training. It has always been a great challenge to keep up. Today I see with great pride and admiration the great body that the National Cryptologic Center has become. I will never cease to be grateful for having been part of itl."

"He tenido la suerte de poder desarrollar los últimos 14 años de mi carrera profesional en el CCN. En este tiempo he visto crecer la familia del CCN, siempre dispuesta a afrontar nuevos retos y en continua formación con el objetivo de estar a la vanguardia para fortalecer y mejorar la ciberseguridad de nuestras instituciones y sus servicios a los ciudadanos. Seguiremos en esta línea muchos años más."

"I have been lucky to be able to spend the last 14 years of my professional career at CCN. During this time I have seen the CCN family grow, always ready to face new challenges and in continuous training with the aim of being at the forefront to strengthen and improve the cybersecurity of our institutions and their services to citizens. We will continue in this line for many years to come."

"Hace 18 años que comencé a trabajar en un mini grupo, ya que por aquel entonces éramos muy pocos los afortunados que integrábamos el Centro Criptológico Nacional. Personal altamente cualificado en diversos campos. Me gustaría destacar el honor de haber podido compartir muchos momentos con personal de toda la Administración Pública, junto a los cuales, con esfuerzo y dedicación, hemos conseguido que los sistemas TIC sean más seguros."

"I started working in a small group 18 years ago, as there were very few of us lucky enough to be part of the National Cryptologic Centre before that. Highly qualified professionals in various fields. I would like to highlight the honour of having been able to share many moments with staff from all over the Public Administration, together with whom, with effort and dedication, we have managed to make ICT systems more secure."

centro criptológico nacional

Quince años fortaleciendo la ciberseguridad nacional

Fifteen years of Strengthening National Cybersecurity

4

Centro Criptológico Nacional

National Cryptologic Centre

El Centro Criptológico Nacional (CCN) está organizado de tal forma que se puedan cumplir las misiones que le fueron encomendadas a través del **RD 421/2004, de 12 de marzo**. Este Real Decreto asigna al CCN unas funciones que tienen por objetivo velar por la seguridad de las TIC en la Administración que procesan, almacenan o transmiten información en formato electrónico, que normativamente requieren protección, y que incluyen medios de cifra, así de aquellas tecnologías que procesan, almacenan o transmiten información clasificada.

De esta forma, el CCN se articula en dos departamentos: **Ciberseguridad (CCN-CERT) y Productos** y **Tecnologías (CCN-PYTEC)**, junto con la **Unidad de Certificación (OC)**.

Las **funciones** concretas del CCN, planteadas en el Real Decreto 421/2004, de 12 de marzo, son las siguientes:

The National Cryptologic Centre (CCN) is organised in such a way as to be able to fulfil the missions entrusted to it through **RD 421/2004, 12 March**. This Royal Decree assigns to the CCN some functions that have the objective of watching over the security of the ICTs in the Administration that process, store or transmit information in electronic format, that normatively require protection, and that include means of encryption, as well as those technologies that process, store or transmit classified information.

In this way, the CCN is articulated in two departments: **Cybersecurity (CCN-CERT)** and **Products and Technologies (CCN-PYTEC),** together with the **Certification Unit (OC)**.
The specific **functions of** the CCN, set out in Royal Decree 421/2004, 12 March, are:

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.
To contribute to the improvement of Spanish cyber security, through the CCN-CERT, by actively addressing threats affecting Public Sector systems, companies and organizations of strategic interest to the country.

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.

Desarrollo reglamentario. ENS

Regulatory development. ENS

El pasado 8 de enero de 2010, hace ya 10 años, se aprobaba el **Real Decreto 3/2010 por el que se regulaba el Esquema Nacional de Seguridad (ENS)** en el ámbito de la Administración Electrónica. Veintiún días después, el 29 de enero, se publicaba en el Boletín Oficial del Estado (BOE), estableciendo los principios básicos y los requisitos mínimos que, de acuerdo con el interés general, permitían una protección adecuada de la información, las comunicaciones y los servicios de las Administraciones Públicas.

On 8 January 2010, 10 years ago, **Royal Decree 3/2010** was approved, **regulating the National Security Framework (ENS)** in the field of Electronic Administration. Twenty-one days later, on 29 January, it was published in the Official State Gazette (BOE), establishing the basic principles and minimum requirements that, in accordance with the general interest, allowed for adequate protection of information, communications and services of the Public Administrations.

A lo largo de esta década, el ENS se ha convertido en la principal herramienta para fortalecer la ciberseguridad en el Sector Público, acompañada de **71 Guías CCN-STIC** (Serie 800). Para confeccionar este informe y poder establecer un sistema de medición de la seguridad del Sector Público, el CCN desarrolló la **solución INES** (Informe Nacional del Estado de Seguridad) para facilitar de un modo más rápido e intuitivo su nivel de adecuación al ENS[1].

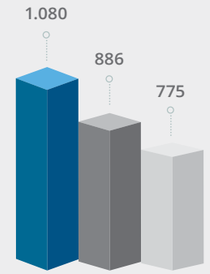
> **El ENS se ha convertido en la principal herramienta para fortalecer la ciberseguridad en el Sector Público**
>
> **The ENS has become the main tool for strengthening cybersecurity in the Public Sector**

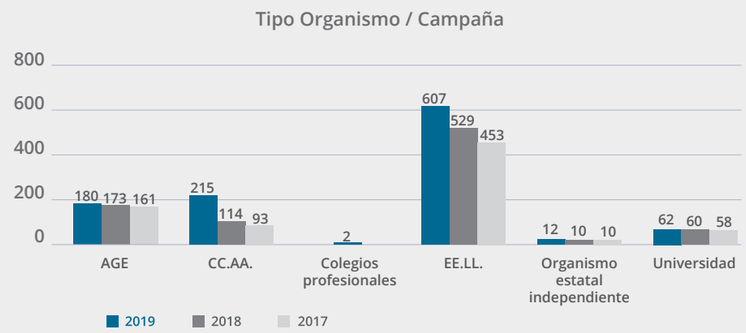
En este 2019, 1.080 entidades habían cargado aquí sus datos, frente a las 886 de un año antes. La valoración general que se desprende del informe INES es que se ha de mantener el esfuerzo de implantación del ENS, máxime cuando se demuestra que su aplicación ayuda a una mejor protección frente a las ciberamenazas.

Throughout this decade, the ENS has become the main tool for strengthening cybersecurity in the Public Sector, accompanied by **71 CCN-STIC Guidelines** (800 Series). In order to prepare this report and establish a system to measure the security of the Public Sector, the CCN developed the **INES solution** (National Report of the State of Security) to facilitate in a faster and more intuitive way its level of adaptation to the ENS[1].

By 2019, 1006 entities had uploaded their data here, compared to 799 a year earlier. The general assessment that emerges from the INES report is that the effort to implement the ENS must be maintained, especially when it is shown that its application helps to improve protection against cyberthreats.

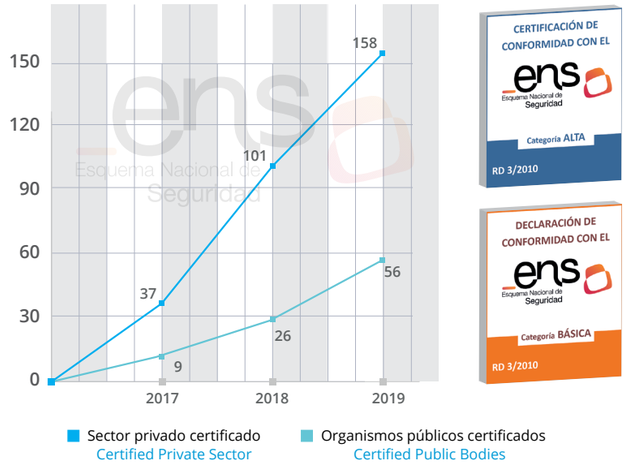
Entidades que han cargado sus datos en INES
Entities that have uploaded their data to INES





Evolución de la campaña INES
Evolution of the INES campaign

[1]EVENS: Entorno de Validación del ENS (https://www.ccn-cert.cni.es/evens)
[1]EVENS: ENS Validation Environment (https://www.ccn-cert.cni.es/evens)



Entidades de certificación acreditadas
Accredited certification entities

ENS en revisión
ENS under review

El Centro Criptológico Nacional, en colaboración con el Ministerio de Política Territorial y Función Pública, ha trabajado en 2019 en la revisión del alcance del Esquema Nacional de Ciberseguridad (ENS), con el objetivo de **adaptar el citado texto a las nuevas normativas** publicadas en materia de Seguridad de las Tecnologías de la Información y la Comunicación.

Este trabajo de revisión tiene por objeto la actualización del Esquema Nacional de Seguridad, de manera que se facilite una mejor respuesta a tendencias y necesidades de ciberseguridad, se reduzcan las vulnerabilidades y se promueva la defensa activa.

The National Cryptologic Centre, in collaboration with the Ministry of Territorial Policy and Public Function, has worked in 2019 on the revision of the scope of the National Cybersecurity Framework (ENS), with the aim of **adapting the aforementioned text to the new regulations** published on Information and Communication Technology Security.

The purpose of this review is to update the National Security Framework in order to facilitate a better response to cybersecurity trends and needs, reduce vulnerabilities and promote active defence.

6

Servicios de ciberseguridad

Cybersecurity services

6.1 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.

To achieve a safe cyberspace, where risks can be mitigated to an acceptable extent, it is essential to raise awareness among society, because only through continuous training can cybersecurity incidents be prevented and dealt with in a timely manner. In view of the need to promote and develop qualified professional profiles for the Public Sector, the CCN offers an **extensive programme of training courses,** adapted to the needs of its community of reference.

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.

This Training Plan, with a **flexible curricular design,** has been transformed as technologies have done so, thus adapting to the new scenario presented by cyberspace. The CCN's training offer has been drawn up 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 makes its knowledge and experience in the training of personnel in the field of cybersecurity available to the Public Sector, the private sector and even to other States. In addition, as a guarantee of successful completion of the training, the CCN grants those who have successfully completed the training a **certificate** specifying the associated subjects and credits.

El CCN otorga, a los concurrentes que la hayan superado con aprovechamiento, un certificado que especifica las materias y créditos asociados

The CCN gives, to those who have successfully passed the course, a certificate indicating the subjects and credits associated

6.1.1. 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).

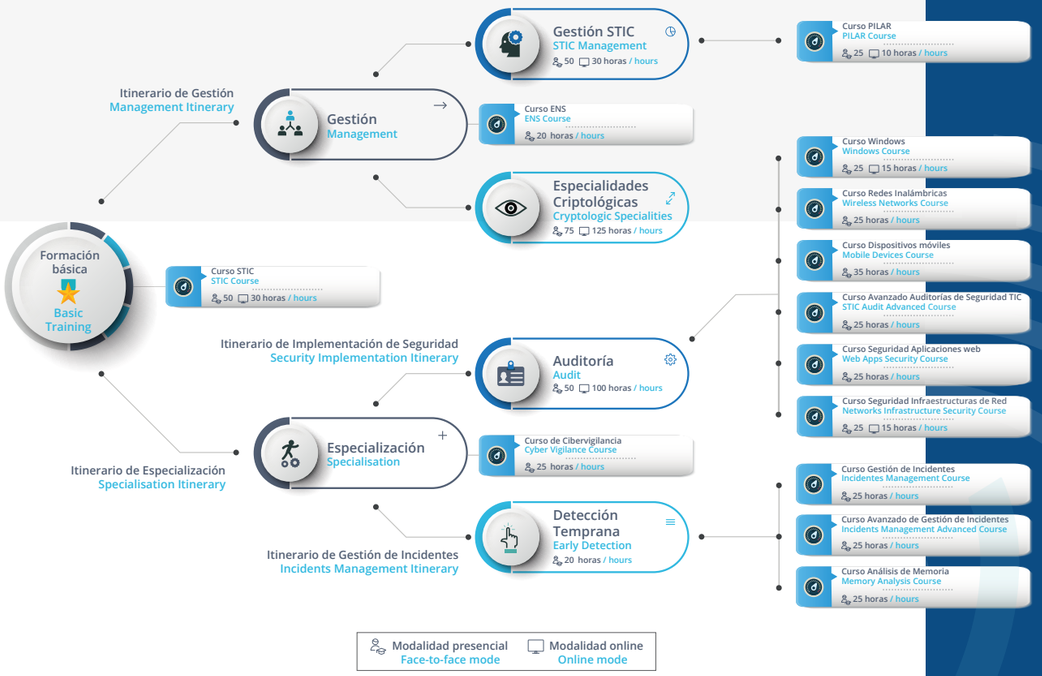
Igualmente, en 2019 el Centro Criptológico Nacional ha continuado mejorando sus relaciones con los países de América Latina e impulsando la capacitación y formación en ciberseguridad, impartiendo diversos cursos de Seguridad de las Tecnologías de la Información y la Comunicación en países como Perú, Colombia o México.

The CCN Training Plan has been designed to meet the need to train, both in person and by distance learning, 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 Information and Communication Technology Security. Once this is completed, the professional can choose between two itineraries**: management** or **specialisation** (aimed at more technical staff).

Likewise, in 2019 the National Cryptologic Centre has continued to improve its relations with Latin American countries and to promote training and education in cybersecurity, giving various courses on Information and Communication Technology Security in countries such as Peru, Colombia and Mexico.

En 2019 el Centro Criptológico Nacional ha continuado impartiendo diversos cursos de Seguridad en países como Perú, Colombia o México

In 2019 the National Cryptologic Centre has continued to give various safety courses in countries such as Peru, Colombia and Mexico



Formación presencial
Face-to-face training

26 cursos presenciales + cursos ad hoc / 26 face-to-face courses + ad hoc courses

Nuevos cursos:
- I Curso TIC de Análisis de Memoria
- I Curso Básico de Auditorías de Seguridad TIC
- I Curso Avanzado de Auditorías de Seguridad TIC

Más de 3.400 solicitudes de asistencia a cursos
Más de 400 alumnos en formación presencial

New courses:
- I STIC Memory Analysis Course
- I Basic Course on ICT Security Audits
- I Advanced Course on ICT Security Audits

More than 3,400 courses attendance requests
More than 400 students in face-to-face training

6.1.2. Formación online
Online training

El CCN ha continuado ampliando su oferta formativa durante 2019 a través de métodos de enseñanza que incluyen tanto cursos a distancia como de e-learning. El pasado año un total de 10.194 personas realizaron los cursos online.

The CCN has continued to expand its training offerings during 2019 through teaching methods that include both distance and e-learning courses. Last year a total of 10,194 people took the online courses.

10.194 personas realizaron los cursos online del CCN en 2019

10,194 people took the CCN online courses in 2019

6.1.3. 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 2019 se realizaron 21 sesiones formativas en las que se recibieron más de 7.000 solicitudes. Más de 4.000 alumnos se inscribieron en cursos de diversas temáticas, entre las que destacaron: Análisis de malware, Soluciones CCN-CERT, Gestiones de la Seguridad de la Información en dispositivos móviles, Catálogo de Productos STIC, Inyecciones en aplicaciones web y Auditoría de aplicaciones móviles Android.

The CCN-CERT's VANESA solution is a live training session **broadcasting** platform, which allows hundreds of people to attend from anywhere in the world. In addition, it preserves the recordings and the material used, so that they can be viewed later.
During 2019, 21 training sessions were held in which more than 7,000 applications were received. More than 4,000 students registered for courses on various topics, including: Malware Analysis, CCN-CERT solutions, Information Security Management on mobile devices, STIC Product Catalogue, Injections in web applications and Auditing of Android mobile applications.

6.1.4 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.

ATENEA
Plataforma de desafíos de seguridad

En 2019 se publicaron un total de 30 nuevos retos, lo que hace un total de 107 desde la puesta en marcha de la plataforma. Asimismo, a finales de este año las personas inscritas ascendían a 9.800, mientras que en 2018 sumaban 7.694.

A finales de este año las personas inscritas en ATENEA ascendían a 9.800

By the end of this year, 9,800 people were registered in ATENEA

In December 2017 Atenea, the CCN-CERT **challenge platform**, was launched. Through a series of challenges of different difficulty and very diverse topics (cryptography and steganography, exploiting, forensics, traffic analysis, reversing, etc.), this platform allows users to demonstrate their knowledge and skills. It was developed so that anyone with concerns in the field of cybersecurity can test their knowledge. Among its main objectives are:

- To raise awareness among ICT staff about the risks in this field.
- To involve experienced cybersecurity professionals to demonstrate their ingenuity and ability.
- To show people with less experience that challenges are fun and that security is not a secret science that they will never understand.

A total of 30 new challenges were published in 2019, making a total of 107 since the platform was launched. Also, by the end of this year, the number of people registered was 9,800, while in 2018 it was 7,694.

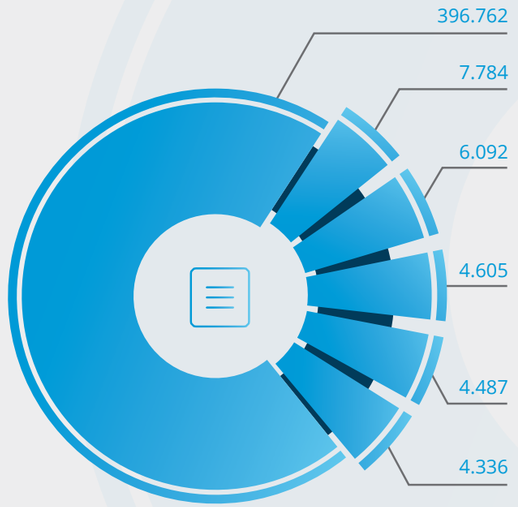
6.2 Normativa – Guías CCN-STIC
Regulations - CCN-STIC Guidelines

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. A lo largo de 2019 se llegaron a publicar 31 nuevas guías. Asimismo, un total de 10 guías fueron actualizadas. Estas cifras hacen que el total de guías disponibles a finales de 2019 fuera de 387 (356 al término de 2018). El éxito de estas guías se muestra en el número de descargas realizadas: un total de 443.650 veces (295.371 en 2018)

The **CCN-STIC Series** are standards, instructions, guides and recommendations developed by the CCN, in order to improve the degree of cybersecurity of organisations. They are periodically updated and completed with new ones, depending on the threats and vulnerabilities detected by the CCN-CERT. Throughout 2019, 31 new guides were published. Likewise, a total of 10 guides were updated. These figures bring the total number of guides available at the end of 2019 to 387 (356 at the end of 2018). The success of these guides is shown by the number of downloads made: a total of 443,650 times (295,371 in 2018).

El Centro Criptológico Nacional comenzó a desarrollar en 2019 las guías de configuración segura de la nube, conscientes de que el empleo de este tipo de servicios se ha convertido en una realidad de uso extendido

In 2019, the National Cryptologic Centre began to develop the guides for secure configuration of the cloud, aware that the use of this type of service has become a widespread reality



Top 5 Guías de acceso público descargadas en 2019
Top 5 Public Access Guides downloaded in 2019

6.3 Implementación de ciberseguridad
Implementation of cybersecurity

La protección de la información que manejan las organizaciones en sus sistemas se considera una actividad clave y de vital importancia, a través de la cual incrementa la garantía de protección.

Como desarrollo de la Ley 11/2002 de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI) y del Real Decreto 421/2004, 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.

Durante el año 2019 se ha afianzado como caso de éxito el modelo de mejora continua para aquellos sistemas que, por su origen y naturaleza, tienen grandes dificultades para cumplir con los requisitos de seguridad exigidos.

The protection of the information handled by organisations in their systems is considered a key and vitally important activity, through which the guarantee of protection is increased.

As a development of the Law 11/2002, 6 May, regulating the National Intelligence Centre (CNI) and the Royal Decree 421/2004, it is established a **Security Policy for ICT (CCN-STIC-001)** which includes the need for accreditation of systems that handle classified information.

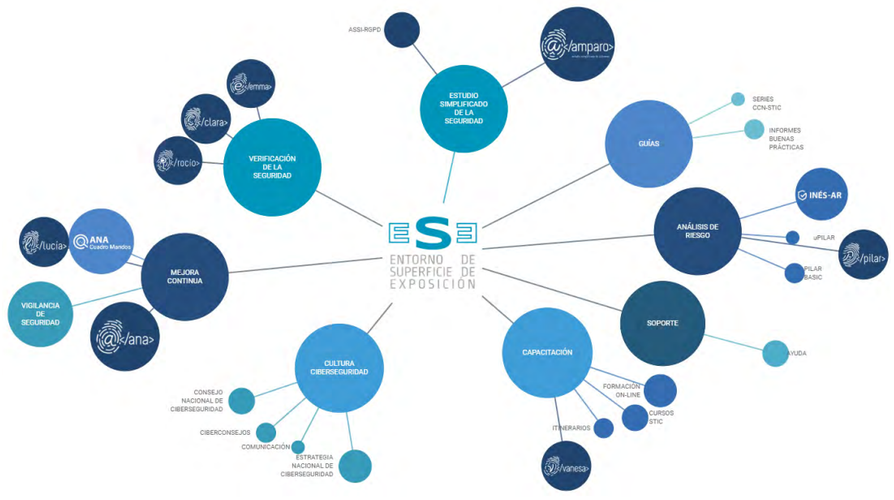
During 2019, the model of continuous improvement has been consolidated as a success story for those systems that, due to their origin and nature, have great difficulties in meeting the required security requirements.
Complementing the continuous improvement model, all security solutions included in the Exhibition Surface Environment (ESE) are available to optimize and facilitate the complex process of handling classified information in ICT systems.

The CCN, and specifically its Classified Systems Security Implementation teams, have carried out ICT security inspections with the aim of verifying the degree of compliance of the services provided and resources used, placing them within the security baseline established in the applicable regulations.

> **El CCN ha realizado un total de 150 inspecciones de seguridad TIC durante el año 2019**
>
> **The CCN has carried out a total of 150 ICT security inspections during 2019**

Complementando al modelo de mejora continua, se cuenta con todas las soluciones de seguridad incluidas en el Entorno de Superficie de Exposición (ESE) de manera que se optimiza y facilita el complejo proceso de manejar información clasificada en sistemas TIC.

El CCN, y concretamente sus equipos de Implementación de Seguridad sobre Sistemas Clasificados, ha llevado a cabo la realización de inspecciones de seguridad TIC con el objetivo de verificar el grado de cumplimiento de los servicios prestados y recursos utilizados encuadrándolos dentro de la línea base de seguridad establecida en la normativa de aplicación.



6.4 Auditorías
Audits

En 2019, el Centro Criptológico Nacional ha llevado a cabo auditorías de seguridad en organizaciones críticas mediante el uso de metodologías reconocidas. Ha sido capaz de gestionar y medir de manera continua la evolución de los activos auditados respecto a niveles de seguridad y riesgos definidos, posibilitando la capacidad de reacción y mitigación ante posibles defectos de configuración y vulnerabilidades detectadas.

De esta manera, en el periodo de tiempo establecido, el CCN-CERT ha realizado **24 auditorías de seguridad** en diferentes organismos y universidades, detectando vulnerabilidades, notificando alertas y recomendando el tratamiento oportuno de las mismas.

Asimismo, se han llevado a cabo análisis preliminares a través del sistema de Auditoría Continua, **ANA** (Automatización y Normalización de Auditorías), para detectar vulnerabilidades importantes en recursos web pertenecientes a diferentes ministerios.
En 2019, esta solución desarrollada por el CCN-CERT se ha instalado en nueve organismos y otros 19 se han adscrito al servicio **ANA CENTRAL**, que permite, entre otras cuestiones, el despliegue automático de nuevas capacidades para la gestión de las vulnerabilidades, la custodia de los datos de las auditorías realizadas por el CCN-CERT, y el establecimiento de un canal de comunicación con el equipo de soporte, reduciendo los tiempos de respuesta y resolución de incidencias.

En este sentido, en 2019 se ha comenzado a desarrollar el **Entorno de Superficie de Exposición**, que permite la elaboración del mapa de activos de la organización, así como la gestión tanto de las vulnerabilidades técnicas como de deficiencias de implementación. Todo ello, con el objetivo de lograr incrementar la capacidad de vigilancia y conocer la superficie de exposición.

In 2019, the National Cryptologic Centre has carried out security audits in critical organisations using recognized methodologies. It has been able to continuously manage and measure the evolution of the audited assets with respect to defined security and risk levels, enabling the capacity to react and mitigate against possible configuration defects and detected vulnerabilities.

In this way, in the period of time established, the CCN-CERT has carried out **24 security audits** in different organisations and universities, detecting vulnerabilities, notifying alerts and recommending timely treatment.

Likewise, preliminary analyses have been carried out through the Continuous Audit system, **ANA** (Automation and Standardisation of Audits), to detect important vulnerabilities in web resources belonging to different ministries. In 2019, this solution developed by the CCN-CERT has been installed in nine organisations and another 19 have been assigned to the **ANA CENTRAL** service, which allows, among other things, the automatic deployment of new capacities for the management of vulnerabilities, the custody of data from audits carried out by the CCN-CERT, and the establishment of a communication channel with the support team, reducing response and incident resolution times.

In this regard, in 2019, work has begun on the development of the **Exhibition Surface Environment,** which allows the mapping of the organisation's assets, as well as the management of both technical vulnerabilities and implementation deficiencies. All of this, with the aim of increasing surveillance capacity and knowledge of the exhibition surface.

> **El CCN-CERT ha realizado 24 auditorías de seguridad en diferentes organismos y universidades**
>
> **The CCN-CERT has carried out 24 security audits in different organizations and universities**

7

Gestión y respuesta a incidentes

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.

The **CCN-CERT** is the Information Security Incident Response Capacity of the CCN. This service was created in 2006 as the Spanish National Governmental CERT and its functions are set out in Law 11/2002 regulating the CNI, RD 421/2004 regulating the CCN and RD 3/2010, 8 January, regulating the National Security Framework (ENS), modified by RD 951/2015, 23 October.

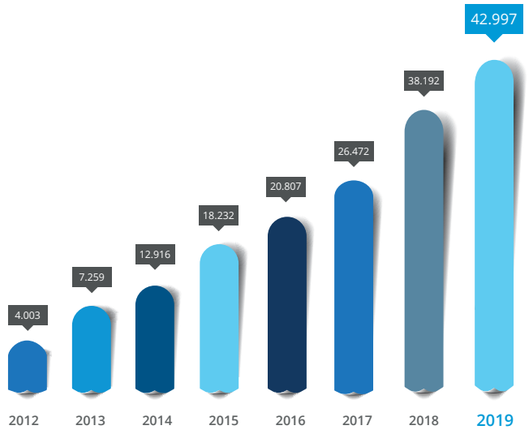
Its mission, therefore, is to contribute to the improvement of Spanish cybersecurity, being the **national alert and response centre** that cooperates and helps to respond quickly and efficiently to cyberattacks and to actively tackle cyberthreats, including the coordination at a state public level of the different Computer Emergency Response Teams (CERT), Computer Security Incident Response Teams (CSIRT) Security Operations Centers (SOC)

7.1 Respuesta a ciberincidentes
Response to cyber incidents

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.

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.



Incidentes gestionados por el CCN-CERT
Incidents managed by the CCN-CERT

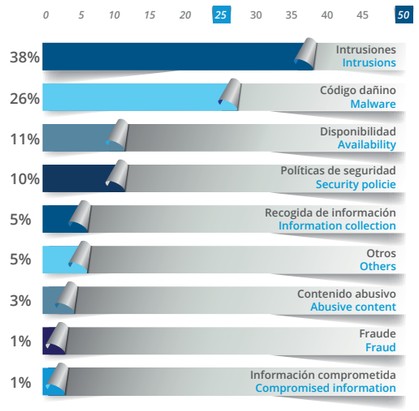
The CCN-CERT, as a National Governmental CERT, collaborates with all public bodies and companies of strategic interest to the country in the detection, notification, assessment, response, processing and learning of information security incidents or cyber incidents that may affect their systems.

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 detection, reaction, containment and elimination stages. In addition, a preventive policy is in place, in which a team of experts works to investigate the techniques used, trends, solutions and the most appropriate procedures for dealing with them, including methodologies for collecting and analysing data and events, procedures for classifying their dangerousness and prioritising them.

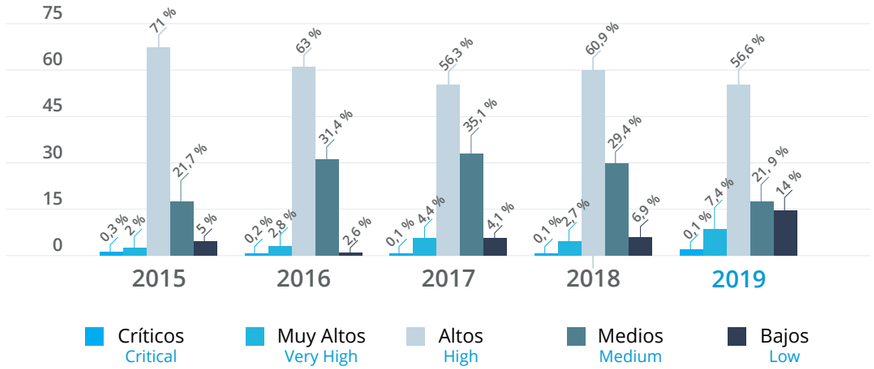
It also acts as a Cyber Incidents Information Exchange Node in the Information Systems of the Public Administrations and as the main coordinator with the appropriate bodies.

Prueba de ello es el número de incidentes gestionados por este organismo durante el último año: **42.997**, de los cuales 3.209 fueron de peligrosidad muy alta o crítica, es decir, un 7,46 %.

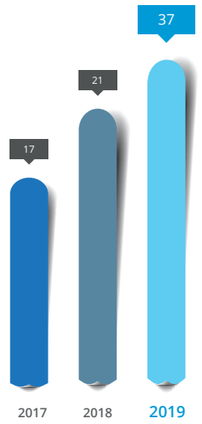
Proof of this is the number of incidents managed by this body over the last year: **42,997**, of which 3,209 were very dangerous or critical, i.e. 7.46%.



Tipología de incidentes gestionados 2019
Type of incidents managed 2019



Peligrosidad de los incidentes gestionados por el CCN-CERT
Danger of incidents managed by the CCN-CERT



El CCN-CERT ha gestionado los incidentes de seguridad a través de actuaciones en remoto y el despliegue de su equipo.

The CCN-CERT has managed security incidents through remote actions and the deployment of its team.

Nº de equipos desplegados in situ por el CCN-CERT para gestionar incidentes
Number of teams deployed on site by the CCN-CERT to manage incidents

EMOTET, el ransomware que protagonizó el año
EMOTET, the ransomware that starred in the year

En el año 2019, y muy especialmente el último trimestre, se detectaron diversas campañas muy agresivas de ataques del troyano EMOTET contra organismos públicos y empresas.

La campaña, que comenzó en septiembre de 2019 y tuvo una gran virulencia en todo el mundo, utilizaba diferentes métodos para conseguir infectar equipos que utilizan Sistemas Operativos de Microsoft Windows. Emotet posee módulos propios para realizar diversas acciones y despliega, además, diferentes códigos dañinos como, por ejemplo Trickbot.

Algunas de las consecuencias, una vez que la acción maliciosa se producía, eran el proceso de secuestro del sistema mediante el cifrado del contenido, el robo y exfiltración de contenido sensible o formar parte de una red de tipo "botnet". **Más de 30 organismos públicos y empresas sufrieron en un breve período de tiempo este tipo de ataques** para los que pidieron colaboración al CCN-CERT.

El CERT Gubernamental Nacional realizó una intensa actividad para hacer frente a esta campaña: desarrolló una vacuna, publicó **5 informes** (entre los que se incluía las familias de código dañino involucrados: Emotet, Trickbot y Ryuk) y emitió **3 avisos y alertas** a su Comunidad. Además, desplegó equipos propios en las sedes de algunos de los organismos aceptados

In 2019, and especially in the last quarter, several very aggressive campaigns of EMOTET Trojan attacks against public bodies and companies were detected.

The campaign, which began in September 2019 and was very virulent around the world, used different methods to infect computers using Microsoft Windows operating systems. Emotet has its own modules to perform various actions and also displays different malicious codes, such as Trickbot.

Some of the consequences, once the malicious action occurred, were the process of hijacking the system by encrypting the content, stealing and exfiltrating sensitive content or becoming part of a botnet. More than 30 public bodies and companies suffered this type of attack in a short period of time, for which they asked the CCN-CERT for collaboration.

The national governmental CERT carried out an intense activity to address this campaign: it developed a vaccine, published **5 reports** (including the malicious code families involved: Emotet, Trickbot and Ryuk) and issued **3 warnings and alerts** to its community. In addition, it deployed its own teams to the headquarters of some of the affected agencies.

Más de 30 organismos públicos y empresas sufrieron en un breve período de tiempo este tipo de ataques

More than 30 public bodies and companies suffered this type of attack in a short period of time

7.2 Sistema de Alerta temprana
Response to cyber incidents

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 (50 áreas de conexión); **SAT-INET**, para la monitorización de las salidas de Internet de los organismos adscritos al servicio (237 sondas y 228 organismos adscritos) y **SAT-ICS** (15 entidades), 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).

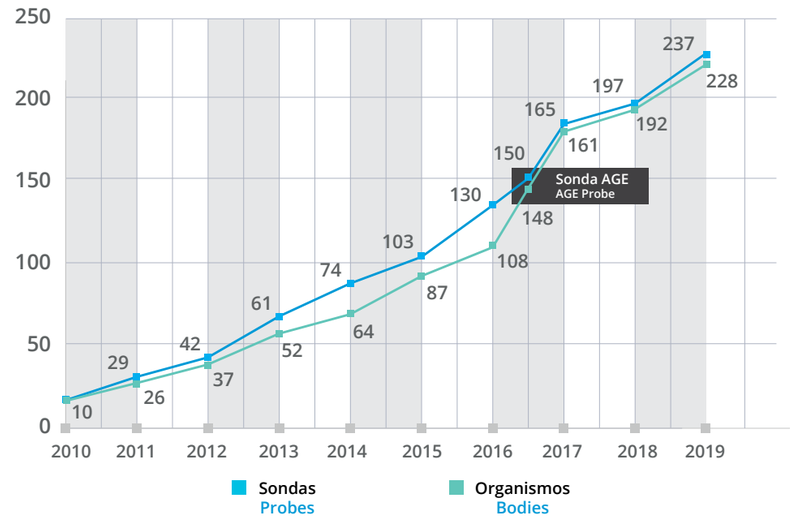
Durante 2019 la Capacidad de Respuesta a Incidentes del Centro Criptológico Nacional, CCN-CERT, ha incorporado importantes novedades en el portal del **SAT-ICS**. Entre otras, se incluye un nuevo apartado donde se puede visualizar de forma sencilla un mapa de los activos monitorizados. De esta forma se logra facilitar la interpretación y el análisis de los distintos incidentes de seguridad, así como mejorar la información disponible sobre las redes monitorizadas, proporcionando conocimiento sobre puertos y protocolos utilizados y características de los activos (marcas, modelo, rol o versión del sistema operativo).

A system developed by the CCN-CERT since 2008 which seeks to act before an incident occurs or, at least, to detect it in the first place in order 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 part of the preventive, corrective and containment actions carried out by the National Governmental CERT.

The SAT has three strands with a common denominator: early detection of intrusions. These are **SAT-SARA**, for monitoring the Administration Intranet (50 connection areas); **SAT-INET**, for monitoring the Internet outputs of the bodies assigned to the service (237 probes and 228 assigned bodies) and **SAT-ICS** (15 bodies), for the Industrial Control Systems.

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

During 2019, the Incident Response Capacity of the National Cryptologic Centre, CCN-CERT, has incorporated important new features to the **SAT-ICS** portal. Among others, it includes a new section where a map of the monitored assets can be easily visualized. This facilitates the interpretation and analysis of the different security incidents, as well as improving the information available on the monitored networks, providing knowledge about ports and protocols used and characteristics of the assets (brands, model, role or version of the operating system).



Nº de sondas y organismos adscritos a SAT-INET
Number of probes and bodies assigned to SAT-INET

7.3 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 de avisos, alertas, vulnerabilidades y la publicación de informes de diferentes materias (**un total de 186 en 2019**) elaborados por su grupo de expertos. Entre estos se encuentran informes de **código dañino**, informes de **buenas prácticas** o informes de **amenazas**.

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

Its main target audience is the registered users of its portal, to whom it periodically notifies of warnings, alerts, vulnerabilities and the publication of reports on different subjects (**a total of 186 in 2019**) prepared by its group of experts. These include reports of **malicious code,** reports of **good practices** or reports of **threats**.

Principales Informes elaborados por el CCN-CERT en 2019
Main Reports elaborated by the CCN-CERT in 2019

Informes de Amenazas: 73
Threat Reports: 73

Publicados en el portal
Published in the portal

CCN-CERT IA-76/19 Medidas de actuación frente al código dañino EMOTET
CCN-CERT IA-76/19 Action against the EMOTET malicious code
CCN-CERT IA-52/19 Implementación Segura de Microsoft Windows/Office frente a la Campaña EMOTET
CCN-CERT IA-52/19 Secure Implementation of Microsoft Windows/Office versus EMOTET Campaign
CCN-CERT IA-51/19 Prevención de la campaña de código dañino EMOTET con medidas técnicas de las guías CCN-STIC de ENS nivel ALTO
CCN-CERT IA-51/19 Prevention of the EMOTET malicious code campaign with technical measures of the CCN-STIC guidelines of ENS HIGH level
CCN-CERT IA-13/19 Ciberamenazas y Tendencias. Resumen Ejecutivo 2019
CCN-CERT IA-13/19 Threats and Trends Report. Executive Summary 2019
CCN-CERT IA-13/19 Ciberamenazas y Tendencias. Ed. 2019
CCN-CERT IA-13/19 Cyberthreats and Trends. Ed. 2019
CCN-CERT IA-03/19 Informe Anual 2018. Ciberhacktivismo y Ciberyihadismo
CCN-CERT IA-03/19 Annual Report 2018. Cyberhacktivism and Cyber Jihadism
CCN-CERT IA-04/19 Informe Anual 2018. Dispositivos Móviles
CCN-CERT IA-04/19 Annual Report 2018. Mobile Devices

Informes de Código Dañino: 26
Malicious Code Reports: 26

Publicados en el portal
Published in the portal

CCN-CERT ID-27/19 Sodinokibi
CCN-CERT ID-25/19 RACCOON STEALER
CCN-CERT ID-26/19 Ryuk
CCN-CERT ID-24/19 TrickBot
CCN-CERT ID-23/19 EMOTET
CCN-CERT ID-22/19 "Rarog"
CCN-CERT ID-21/19 "Megumin v2"
CCN-CERT ID-19/19 Qakbot
CCN-CERT ID-14/19 Red Alert 2.0
CCN-CERT ID-13/19 Godzilla Loader
CCN-CERT ID-12/19 Anubis II
CCN-CERT ID-11/19 W32.Revenge
CCN-CERT ID-10/19 ATMSpitter
CCN-CERT ID-09/19 JSDealer
CCN-CERT ID-08/19 Buhtrap
CCN-CERT ID-07/19 IcedID / Bokbot
CCN-CERT ID-06/19 JRat_Packer
CCN-CERT ID-01/19 Wapomi

Informes Técnicos: 81
Technical Reports: 81

Informes de Buenas Prácticas: 6
Good Practice Reports: 6

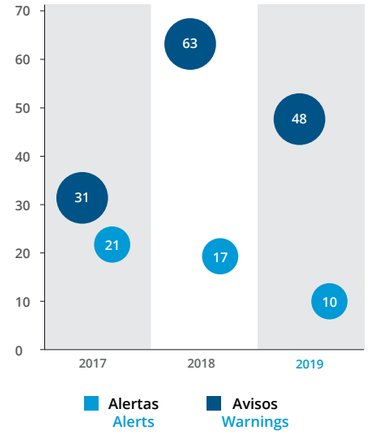
Publicados en el portal
Published in the portal

CCN-CERT BP/16 Recomendaciones de seguridad de Adobe Acrobat Reader DC
CCN-CERT BP/16 Adobe Acrobat Reader DC Security Recommendations
CCN-CERT BP/15 Buenas Prácticas en Virtualización
CCN-CERT BP/15 Good Practices in Virtualisation
CCN-CERT BP/14 Declaración de Aplicacibilidad ENS
CCN-CERT BP/14 ENS Statement of Applicability
CCN-CERT BP/13 Desinformación en el Ciberespacio
CCN-CERT BP/13 Disinformation in Cyberspace
CCN-CERT BP/12 Cryptojacking
CCN-CERT BP/12 Cryptojacking

Avisos y alertas
Warnings and alerts

El CCN-CERT informa, a través de avisos y alertas, de las nuevas amenazas que se van detectando. Estas notificaciones son publicadas en su portal web conforme son conocidas y, además, recibidas por todos los usuarios registrados en el mismo. En 2019 se publicaron un total de 48 avisos y 10 alertas.

The CCN-CERT informs, through warnings and alerts, of new threats that are detected. These notifications are published on its website as they become known and, furthermore, are received by all the users registered. In 2019 a total of 48 warnings and 10 alerts were published.



Vulnerabilidades
Vulnerabilities

En 2019 se publicaron 4.563 vulnerabilidades

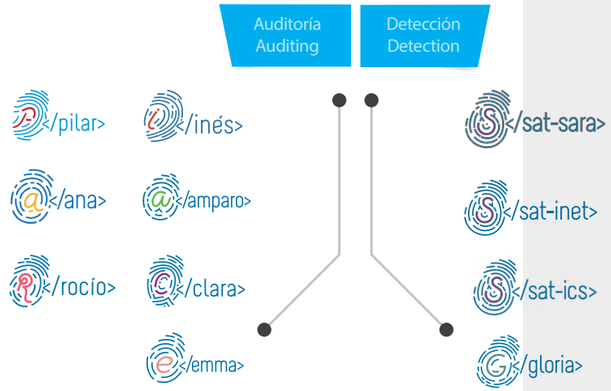
4,563 vulnerabilities were published in 2019

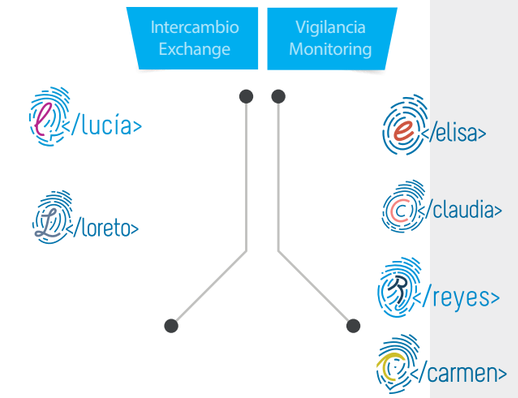
Diariamente, el CCN-CERT publica las vulnerabilidades de los siguientes fabricantes: Microsoft, Red Hat, Cisco, Oracle, Adobe, Suse, Debian, IBM, Apple, Symantec, Joomla, Moodle, WordPress, Drupal, Juniper, VMWare, AmazonWS y F5. En 2019 se publicaron 4.563 parches de sendas vulnerabilidades.

Every day, the CCN-CERT publishes the vulnerabilities of the following manufacturers: Microsoft, Red Hat, Cisco, Oracle, Adobe, Suse, Debian, IBM, Apple, Symantec, Joomla, Moodle, WordPress, Drupal, Juniper, VMWare, AmazonWS and F5. In 2019, 4,563 patches for each vulnerability were released.

Soluciones de ciberseguridad

Cybersecurity solutions





AMPARO. Estudio simplificado de sistemas
AMPARO. Simplified study of systems

AMPARO es la más reciente de las soluciones desarrolladas por el CCN-CERT. Presentada en **diciembre de 2019**, esta solución pretende facilitar y agilizar el proceso de acreditación de equipos aislados a todas aquellas empresas y organismos que así lo requieran. De este modo, AMPARO guía al usuario en todos los aspectos necesarios para la obtención de la acreditación que permita el manejo de información clasificada.

AMPARO is the most recent solution developed by the CCN-CERT. Presented in **December 2019**, this solution aims to facilitate and speed up the accreditation process for isolated equipment for all the companies and organisations that require it. In this way, AMPARO guides the user in all the necessary aspects to obtain the accreditation that allows the management of classified information.

ANA. Automatización y Normalización de Auditorías
ANA. Automation and Standardisation of Audits

Con el objetivo de reducir los tiempos en la gestión de la seguridad, el CCN-CERT desarrolló a **comienzos de 2019** la solución **ANA (Automatización y Normalización de Auditorías)**. Mediante una gestión eficiente de la detección de vulnerabilidades y de la notificación de alertas, así como ofreciendo recomendaciones para un tratamiento oportuno de las mismas, esta nueva solución incrementa la capacidad de vigilancia y permite conocer la superficie de exposición.

Además, se desarrolló el formato de nube privada **ANA Central** en la que cada organismo solicitante cuenta con un nuevo espacio de trabajo. Permite el despliegue automático de nuevas capacidades para la gestión de las vulnerabilidades, el mantenimiento de la infraestructura, copia de seguridad de la base de datos y custodia de los datos de las auditorías por parte del CCN-CERT, además de un canal de comunicación con el equipo de soporte.

With the aim of reducing time in security management, the CCN-CERT developed the **ANA** solution **(Automation and Standardisation of Audits)** at the **beginning of 2019**. Through an efficient management of vulnerability detection and alert notification, as well as offering recommendations for their treatment, this new solution increases the surveillance capacity and allows knowledge of the exposure area.

Moreover, the private cloud format **ANA Central** was developed, in which each applicant organisation is provided with a new workspace. It allows the automatic deployment of new capabilities for vulnerability management, infrastructure maintenance, database backup and custody of audit data by the CCN-CERT, as well as a communication channel with the support team.

CARMEN. Defensa de ataques avanzados/APT
CARMEN. 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.

Al término de 2019 eran 42 los organismos y empresas que contaban con esta solución, 27 de ellas integradas en CARMEN Central.

Solution developed with the objective of identifying the commitment of an organisation's network by ATP. This solution acquires, processes and analyses information for the elaboration of intelligence from the traffic of an internal network. It can detect anomalies and lateral and external movements within the network, as well as analysing malware through advanced sandboxing.

By the end of 2019 there were 42 agencies and companies that had this solution, 27 of them integrated into CARMEN Central.

CLAUDIA. Solución de punto final
CLAUDIA. 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. Son 12 los despliegues realizados en servidores y puestos de usuarios en 2019.

Endpoint solution, integrated with the CARMEN tool, which allows 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 a total control of the network, considerably increasing the speed and efficiency in the resolution of a security incident. There are 12 deployments performed in servers and user stations in 2019.

CLARA. Verificación de cumplimiento
CLARA. Verification of compliance

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 Electronic Administration. Compliance analysis is based on the standards provided through the CCN-STIC Guides 850A, 850B, 851B, 870A, 870B, 570A, 570B,599A18 and 599B18 security templates.

ELISA. Observatorio Digital
ELISA. Digital Observatory

El CCN-CERT presentó a finales de 2019 su nueva herramienta de cibervigilancia: ELISA. Esta solución, disponible exclusivamente para usuarios registrados del portal, facilita la monitorización de fuentes abiertas y el perfilado de medios y entidades de redes sociales. Además, ELISA permite realizar un seguimiento e interpretación de lo que sucede en el ciberespacio para efectuar una prospectiva digital, mejorando las capacidades de cibervigilancia.

The CCN-CERT presented at the end of 2019 its new cybersurveillance tool: ELISA. This solution, available exclusively to the portal's registered users, facilitates the monitoring of open sources and the profiling of media and social network entities. Moreover, ELISA allows the monitoring and interpretation of what is happening in the cyberspace to carry out a digital foresight, improving the cybersurveillance capabilities.

EMMA. Control de acceso a las infraestructuras de red
EMMA. Access control to network infrastructures

También **desarrollada en 2019**, su objetivo es el de agilizar la visualización de activos en una red, su autenticación y segregación, así como la automatización de auditorías de seguridad de la infraestructura. Con ella, el CCN pretende facilitar a las organizaciones una visibilidad completa de la capa de acceso a la red (routers, switches, puntos de acceso, controladores, etc.), un punto crucial para verificar quién o qué está conectado en una red.

The objective of this solution, also **developed in 2019**, is to streamline the visualisation of assets in a network, their authentication and segregation, as well as the automation of infrastructure security audits. With this solution, the CCN aims to provide organisations with complete visibility of the network access layer (routers, switches, access points, controllers, etc.), a crucial point to verify who or what is connected to a network.

GLORIA. Gestor de logs en respuesta a incidentes/amenazas
GLORIA. 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 relevant data. It allows a very flexible orientation towards the surveillance of the IP world.

INES. Informe Nacional del Estado de Seguridad en el ENS
INES. National Report on the ENS Security Status

Proyecto que tiene por objetivo facilitar, a través de una plataforma telemática a la que se accede desde el portal del CCN-CERT, 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, through a telematic platform accessed from the CCN-CERT portal, the work of all bodies in their obligation to regularly asses the security status of their systems (*see the ENS section*).

LORETO. Almacenamiento en la nube
LORETO. Cloud storage

Servicio de uso compartido en la nube para el almacenamiento virtual de información (archivos, muestras, aplicaciones, etc.) que permite su intercambio 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.

LUCIA. Sistema de gestión federada de tickets
LUCIA. 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 2019, 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 35% de los incidentes gestionados por el CCN-CERT.

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

By the end of 2019, **version 3.1** was operational and **265 organisations** were registered. Most of them are connected to the central LUCIA (the CCN-CERT instance from which cyberincidents are managed). Moreover, there were 49 federated organisations. These share incidents on a daily basis and constitute 35% of the incidents managed by the CCN-CERT.

MARIA. Plataforma Multiantivirus en tiempo real
MARIA. Real-time Multiantivirus Platform

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 analyses any of the uploaded files in isolation, which guarantees that the file is not transferred to any other organisation or antivirus company.

MARTA. Análisis avanzados de ficheros
MARTA. 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 your organisation.

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

REYES. Intercambio de Información de Ciberamenazas
REYES. Cyber threats Information Exchange

Solución desarrollada para agilizar la labor de análisis de ciberincidentes y compartir información de ciberamenazas y disponible para las organizaciones adscritas al SAT.

En marzo de 2019, el CCN-CERT presentó **REYES 3.0**, una nueva versión de la solución que agiliza la labor de análisis de incidentes al obtener información contextualizada y correlada con las principales fuentes de información existentes, tanto públicas como privadas. Dispone de un nuevo **motor de inteligencia** y gracias a ella puede realizarse cualquier investigación de forma rápida y sencilla, accediendo desde una única plataforma a la información más valiosa sobre ciberincidentes.

Al término de 2019, eran más de 600 los usuarios de esta solución y se habían realizado más de 3.800 investigaciones y más de 40.000 búsquedas.

Solution developed to streamline the work of analysing cyber-incidents and sharing information on cyber-threats and available to organisations attached to the SAT.

In March 2019, the CCN-CERT presented **REYES 3.0**, a new version of the solution that streamlines incident analysis work by obtaining contextualized and correlated information with the main existing information sources, both public and private. It has a new **intelligence engine** which allows any investigation to be carried out quickly and easily, accessing the most valuable information on cyberincidents from a single platform.

By the end of 2019, there were more than 600 users of this solution, more than 3,800 investigations had been carried out and more than 40,000 searches had been performed.

ROCÍO. Auditoría de configuraciones de dispositivos de red
ROCIO. Audit of network device configurations

ROCÍO, desarrollada por el CCN, agiliza el proceso de auditoría de seguridad sobre configuraciones de equipos de comunicaciones: enrutadores y conmutadores Cisco, cortafuegos Fortigate y, **desde 2019, conmutadores Aruba y Allied Telesis**. Gracias a esta solución, se automatizan las tareas básicas de auditoría, permitiendo que los responsables de seguridad puedan comprobar, de un modo rápido, si su dispositivo está configurado adecuadamente.

El análisis del cumplimiento está basado en las normas de seguridad recogidas en las Guías CCN-STIC 641, 643A, 644, 647C y 650.

ROCÍO, developed by CCN, streamlines the security audit process on communications equipment configurations: Cisco routers and switches, Fortigate firewalls and, **from 2019, Aruba and Allied Telesis switches**. This solution automates basic auditing tasks, allowing security officers to quickly and easily check whether or not their device is configured properly.

The analysis of compliance is based on the CCN-STIC Guides 641, 643A, 644, 647C and 650 security standards.

VANESA. Grabaciones y emisiones de vídeo en streaming
VANESA. Streaming video recordings and broadcasts

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

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

9

Centros de Operaciones de ciberseguridad

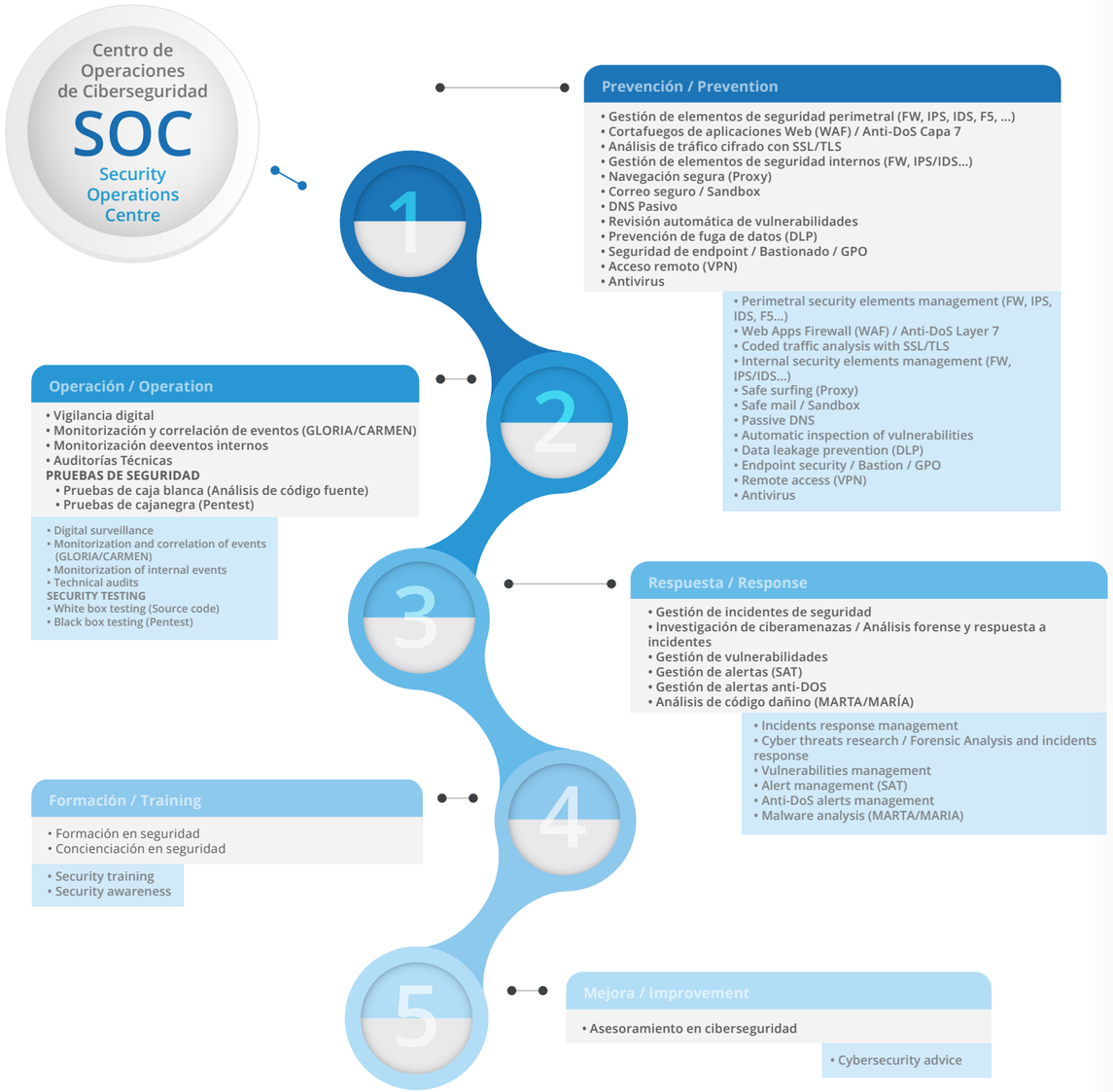
Cybersecurity Operations Centres

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

En este sentido, 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 objetivo de optimizar estos recursos tan críticos. El primero de ellos fue el **SOC-Justicia**, creado en 2018, seguido en 2019 por el **SOC de la Administración General del Estado (AGE)**, así como de sus organismos públicos.

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

The CCN-CERT has offered surveillance services, at no associated cost, to various government agencies, promoting the creation of such centers in order to optimize these types of critical resources. The first to be developed in 2018 was the **SOC-Justice**, followed in 2019 by the **SOC of the General State Administration (AGE),** as well as its public bodies.



9.1 vSOC
vSOC

Durante 2019 se trabajó en la implementación de **Centros de Operaciones de Seguridad virtuales (vSOC)**, un proyecto que nació con el objetivo de que ayuntamientos y diputaciones tengan más visibilidad e información sobre vulnerabilidades, fallos de configuración e incidentes, capacidad de despliegue, protección y actuación.

Para impulsar la implantación de los vSOC, la **Federación Española de Municipios y Provincias**, **FEMP**, en colaboración con el CCN, organizó en marzo de 2019 una jornada bajo el título "**Ciberseguridad en la Administración Local: Centros de Operaciones de Seguridad Virtuales**, **vSOC**".

During 2019, work was carried out on the implementation of **virtual Security Operations Centers (vSOC),** a project created in order to provide municipalities and councils with more visibility and information on vulnerabilities, configuration failures and incidents, deployment capacity, protection and action.

To promote the implementation of vSOCs, the **Spanish Federation of Municipalities and Provinces, FEMP,** in collaboration with the CCN, organized a conference in March 2019 under the title **"Cybersecurity in the Local Administration: Virtual Security Operations Centers, vSOC"**.

> ***En marzo de 2019 el CCN se reunió con la FEMP para impulsar la implantación de los vSOC en Entidades Locales***
>
> ***In March 2019 the CCN met with the FEMP to promote the implementation of vSOCs in Local Entities***

10

Promoción y desarrollo de productos de seguridad TIC

Promotion and development of ICT security products

En este apartado se recogen las diferentes actividades relacionadas con el desarrollo de productos de seguridad, con la definición de arquitecturas de seguridad y con la promoción de dichos productos y soluciones que ha abordado el Departamento de Productos y Tecnologías STIC, CCN-PYTEC, durante el año 2019.

This section includes the different activities related to the development of security products, the definition of security architectures and the promotion of these products and solutions undertaken by the STIC Products and Technologies Department, CCN-PYTEC, during 2019.

10.1 Productos y tecnologías STIC
ICT security products and technologies

10.1.1 Dispositivos de protección de perímetro
Perimeter protection devices

En 2019, el CCN ha desarrollado dispositivos de protección de perímetro para la interconexión de sistemas de diferentes niveles de clasificación, entre los que destacan:

In 2019, the CCN has developed perimeter protection devices for the interconnection of systems of different classification levels, among which the following ones stand out:

Pasarelas de intercambio seguro de información, diseñadas para controlar el intercambio de información entre diferentes dominios de seguridad y evitar la entrada y la salida de información no autorizada. Permite implementar mecanismos de defensa en profundidad y neutralizar o minimizar el efecto de las APT.

A lo largo de 2019 se han realizado desarrollos *ad hoc* para interconexión de sistemas específicos militares. Además, se han dotado de nuevas capacidades al conjunto de pasarelas existentes basadas en estándares o protocolos comúnmente utilizados: web services (REST y SOAP), SMTP, FTP, SFTP, SMB, FTPS, etc.

Secure information exchange gateways, designed to control the exchange of information between different security domains and prevent unauthorized information from entering and leaving. It allows the implementation of defense mechanisms in depth and neutralize or minimize the effect of APT.

Throughout 2019, *ad hoc* developments have been made for the interconnection of specific military systems. In addition, new capabilities have been added to the existing set of gateways based on commonly used standards or protocols: *web services* (REST and SOAP), SMTP, FTP, SFTP, SMB, FTPS, etc.

Diodos de datos hardware basados en TCP y UDP. Su aplicación principal es la introducción de información en una red aislada en entornos clasificados. También se puede aplicar para extraer información de una red de control industrial en entornos de infraestructuras críticas. El diodo desarrollado por la empresa AUTEK bajo la dirección de CCN-PYTEC obtuvo una certificación de seguridad Common Criteria EAL 4+ a lo largo del 2019.

Hardware data diodes based on TCP and UDP. Its main application is the introduction of information in an isolated network in classified environments. It can also be applied to extract information from an industrial control network in critical infrastructure environments. The diode developed by the company AUTEK under the direction of CCN-PYTEC obtained a Common Criteria EAL 4+ security certification during 2019.

10.1.2 Dispositivos de cifrado offline (EP852)
Offline Encryption Devices (EP852)

El EP852 es la evolución del Cripto Token USB (EP851), que incorpora las últimas medidas de seguridad que hacen al dispositivo menos vulnerable e implementa un cifrado de ficheros más robusto. Dispone de funcionalidades que mejoran la gestión del equipo, pudiendo actualizarse el FW y el SW en remoto de forma segura, así como un almacenamiento de claves más seguro y con mayor capacidad. El aspecto físico del equipo se ha modificado para adaptarlo al espacio estándar USB de los equipos informáticos.

The EP852 is the evolution of the USB Crypto Token (EP851), which incorporates the latest security measures that make the device less vulnerable and implements stronger file encryption. It has functionalities that improve the management of the device, being able to update the FW and SW in a secure way, as well as a more secure key storage with greater capacity. The physical aspect of the equipment has been modified to adapt it to the standard USB space of computer equipment.

10.1.3 Dispositivos móviles seguros
Secure mobile devices

En el año 2019 se ha continuado expandiendo la variedad de dispositivos móviles que el CCN pone a disposición de la Administración Española tras superar el proceso de cualificación o certificación. Entre los dispositivos móviles destaca el Samsung Galaxy S9, que entró en el Catálogo de Productos de Seguridad TIC (véase capítulo correspondiente) como cualificado para ENS Alto tras la realización de las correspondientes pruebas de evaluación por parte del CCN.

In 2019, the variety of mobile devices that the CCN makes available to the Spanish Administration after passing the qualification or certification process continued to expand. Among the mobile devices, the Samsung Galaxy S9 stands out, which entered the Catalogue of ICT Security Products (see corresponding chapter) as qualified for High ENS after the corresponding evaluation tests were carried out by the CCN.

10.1.4 Dispositivos de protección USB
USB protection devices

AuthUsb safeDoor es un dispositivo hardware que actúa como barrera entre las memorias USB y los equipos de una organización e identifica amenazas a tres niveles:

AuthUsb safeDoor is a hardware device that acts as a barrier between USB flash drives and computers in an organisation and identifies threats on three levels:

Eléctrico	Hardware	Software
deteniendo ataques de sobretensión.	desactivando ataques de la familia BadUsb, o HID, falsas tarjetas de red, interfaces compuestas, etc.	antivirus integrado que realiza un análisis previo a la descarga de cualquier contenido.
Stopping surge attacks.	disabling BadUsb family attacks, or HID, fake network cards, composite interfaces, etc.	integrated anti-virus that performs a pre-download scan of any content.

La utilización de este producto permite mejorar la seguridad del perímetro de un sistema mitigando las amenazas de ataques a través de memorias USB.

The use of this product allows to improve the security of the perimeter of a system by mitigating the threats of attacks through USB flash drives.

10.1.5 Dispositivos de Comunicaciones Tácticas Seguras
Tactical Secure Communications Devices

A lo largo de 2019, gracias a un expediente de I+D de la Subdirección General de Planificación, Tecnología e Innovación (SDGPLATIN), de la Dirección General Armamento y Material (DGAM) y bajo la **Dirección Técnica del CCN**, la empresa Tecnobit ha implementado nuevos modos de voz táctica segura ("Push-To-Talk"). Están definidos en las nuevas especificaciones criptográficas OTAN para interoperabilidad en este ámbito (STaC-IS y TSVCIS). Han sido implementados en el Cifrador Personal del Combatiente (CIFPECOM) y proporcionan soluciones de cifrado con diversos tipos de radios (HF, VHF, etc.), especialmente en aquellos casos en los que el canal es más hostil.

Nuevos modos de voz táctica segura en el cifrador CIFPECOM

Podrá ser una solución de cifrado para el Gestor de Comunicaciones del Ejército de Tierra (GESCOMET), así como servir de base para otras soluciones de cifra para la Red Radio de Combate.

Throughout 2019, thanks to an R&D file from the Subdirectorate General for Planning, Technology and Innovation (SDGPLATIN), the Directorate General for Armament and Material (DGAM) and under the **Technical Direction of the CCN,** the company Tecnobit has implemented new modes of secure tactical voice ("Push-To-Talk"). They are defined in the new NATO cryptographic specifications for interoperability in this field (STaC-IS and TSVCIS). They have been implemented in the Combatant Personal Encryptor (CIFPECOM) and provide encryption solutions with various types of radios (HF, VHF, etc.), especially in those cases where the channel is more hostile.

It could be an encryption solution for the Army Communications Manager (GESCOMET), as well as serve as a basis for other encryption solutions for the Combat Radio Network.

10.2 Arquitecturas y Soluciones STIC
Architectures and ICT Solutions

El objetivo fundamental es **proporcionar soluciones con las debidas garantías de seguridad** para su posible utilización por usuarios.

Como resultado de esta actividad durante el último año, cabe señalar la definición de arquitecturas de seguridad y posibles soluciones STIC para la protección de las comunicaciones móviles y de la información en puestos de mando inalámbricos.

The main objective is to **provide solutions with the appropriate security guarantees** for their possible use by users.

As a result of this activity during the last year, it is worth noting the definition of security architectures and possible ICT solutions for the protection of mobile communications and information in wireless command posts.

10.2.1 Comunicaciones inalámbricas seguras
Secure wireless communications

El año 2019 ha supuesto un salto cualitativo para el CCN en la definición de arquitecturas y la búsqueda de soluciones para proteger la información clasificada nacional cuando esta se transmite por medio de tecnologías inalámbricas como Wi-Fi o LTE.

Hay que destacar que las arquitecturas y soluciones identificadas por el CCN se han puesto en práctica junto con la **Sección de Arquitectura e Interoperabilidad (SECARQINT) de JCISAT/ SUBCIS**, dentro de los Planes de Experimentación que el Ejército de Tierra está llevando a cabo.

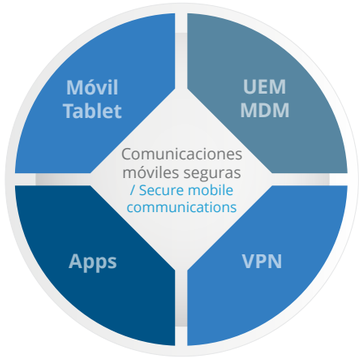
2019 has meant a qualitative leap for the CCN in the definition of architectures and the search for solutions to protect nationally classified information when it is transmitted via wireless technologies such as Wi-Fi or LTE.

It should be noted that the architectures and solutions identified by the CCN have been implemented together with the **Architecture and Interoperability Section (SECARQINT) of JCISAT/ SUBCIS,** within the Experimental Plans that the Spanish Army is carrying out.

10.2.2 Comunicaciones móviles seguras
Secure mobile communications

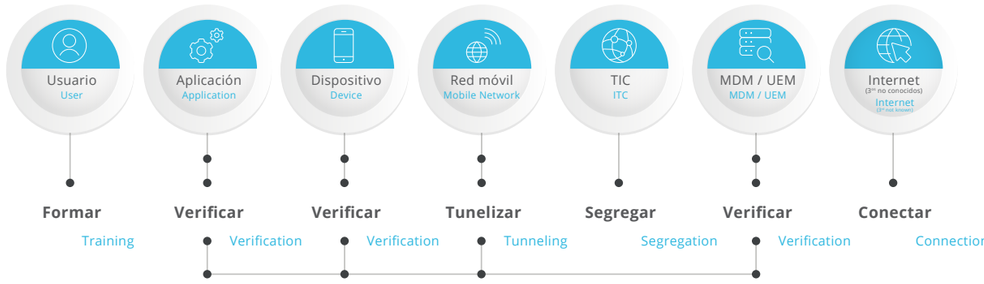
En el caso de las comunicaciones móviles, en octubre de 2019 se publicó el procedimiento de empleo de la aplicación **COMSec** (CCN-STIC-1407), que proporciona comunicaciones cifradas de voz, video y mensajería instantánea a usuarios móviles, a través de una aplicación instalada en una plataforma Android.

De esta forma, aplicaciones, terminales, VPN y dispositivos de gestión son verificados desde el punto de vista de la seguridad y, en consecuencia, están incluidos en el **catálogo de productos de seguridad del CCN, CPSTIC** (véase apartado correspondiente).



In the case of mobile communications, the procedure for using the **COMSec** application (CCN-STIC-1407) was published in October 2019. This application provides encrypted voice, video and instant messaging communications to mobile users, through an application installed on an Android platform.

In this way, applications, terminals, VPNs and management devices are verified from a security point of view and are therefore included in the **CCN's security product catalogue, CPSTIC** (*see corresponding section*).



Planteamiento para garantizar la seguridad de las comunicaciones móviles
Approach to ensure the security of mobile communications

Organismo de Certificación

Certification Body

La principal actividad del Organismo de Certificación (OC) es la **certificación de la seguridad de productos y sistemas TIC**, además de la **promoción de reuniones**, en el ámbito de su actuación, con otros actores involucrados en la certificación de la seguridad, como laboratorios de evaluación, desarrolladores, fabricantes y organizaciones.

Que un producto disponga de una certificación funcional significa que ha superado con éxito un proceso de evaluación en un laboratorio independiente acreditado, a partir del cual se puede afirmar que su Declaración de Seguridad es cierta, con un determinado nivel de confianza o "aseguramiento" (EAL, en sus siglas en inglés).

The main activity of the Certification Body (OC) is the **certification of the security of ICT products and systems,** in addition to the **promotion of meetings**, within the scope of its action, with other actors involved in security certification, such as evaluation laboratories, developers, manufacturers and organisations.

The fact that a product has a functional certification means that it has successfully passed an evaluation process in an independent accredited laboratory, from which it can be stated that its *Security Statement* is true, with a certain level of confidence or "assurance" (EAL).

11.1 Metodologías de evaluación
Evaluation methodologies

La página web del Organismo de Certificación (https://oc.ccn.cni.es) mantiene las metodologías de evaluación en las que el OC se encuentra acreditado para emitir certificados. Actualmente son:

The Certification Body website (https://oc.ccn.cni.es) maintains the evaluation methodologies in which the OC is accredited to issue certificates. Currently they are:

- Common Criteria
- ITSEC/ITSEM
- ISO 19790
- LINCE

11.1.1 Common Criteria
Common Criteria

La metodología común para la evaluación y certificación de productos de seguridad (*Common Criteria for Information Technology Security Evaluation*) es una norma internacional (ISO/IEC 15408) que permite verificar de forma objetiva la seguridad de un producto, con un determinado nivel de confianza (EAL), a partir de la comprobación de los requisitos funcionales de seguridad implementados en el producto y de las garantías proporcionadas por el fabricante.

The *Common Criteria for Information Technology Security Evaluation* is an international standard (ISO/IEC 15408) that allows the security of **a product** to be **objectively verified,** with a certain level of confidence (EAL), based on the verification of the functional security requirements implemented in the product and the guarantees provided by the manufacturer.

11.1.2 LINCE / LINCE

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

In 2018, the OC developed a new national methodology with which to evaluate ICT security products. This new national essential security certification, called LINCE, is oriented to the **analysis of vulnerabilities and black box type penetration tests** in which the developer's documentary effort is minimized and, in addition, the evaluation effort carried out by the accredited laboratories is limited to 25 days in a maximum period of two months.

11.1.3 Otras metodologías
Other methodologies

Asimismo, el OC certifica productos de seguridad de acuerdo a otras metodologías, como es la antigua norma europea para la evaluación de la seguridad de las tecnologías de la información y su correspondiente metodología (**ITSEC/ITSEM**), actualmente en desuso salvo en casos muy concretos (programas internacionales antiguos) y que dio lugar a los criterios comunes junto con las normas nacionales de Estados Unidos y Canadá, así como verificar la seguridad de módulos criptográficos (ISO 19790, similar a la norma norteamericana FIPS 140-2).

The OC also certifies security products according to other methodologies, such as the old European standard for information technology security assessment and its corresponding methodology (**ITSEC/ITSEM)**, which is now out of use except in very specific cases (old international programmes) and which gave rise to the common criteria together with the national standards of the United States and Canada, as well as verifying the security of cryptographic modules (ISO 19790, similar to the North American standard FIPS 140-2).

11.2 Laboratorios acreditados
Accredited laboratories

La actividad de evaluación la realizan laboratorios públicos o privados que han sido acreditados y autorizados para operar en el marco del Esquema Nacional de Evaluación y Certificación. Estos son los laboratorios que actualmente están **acreditados o en proceso de acreditación** en las metodologías Common Criteria y LINCE:

The evaluation activity is carried out by public or private laboratories that have been accredited and authorized to operate within the framework of the National Evaluation and Certification Scheme. These are the laboratories that are **currently accredited or in the process of being accredited** in the Common Criteria and LINCE methodologies:

12

Evaluación y certificación

Evaluation and certification

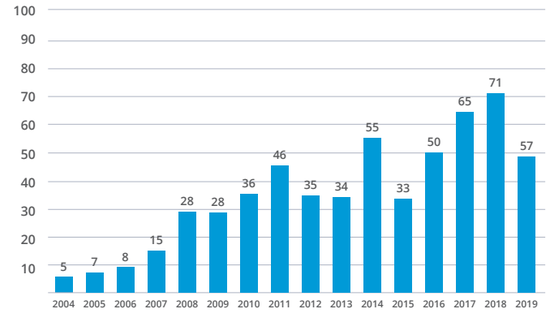
El CCN realiza los siguientes tipos de evaluación y certificación, en función de los criterios empleados en dicho proceso:

The CCN carries out the following types of evaluation and certification, according to the criteria used in this process:

- Evaluación y certificación funcional
  Functional evaluation and certification
- Evaluación y certificación criptológica
  Cryptologic evaluation and certification
- Evaluación y certificación TEMPEST
  TEMPEST evaluation and certification

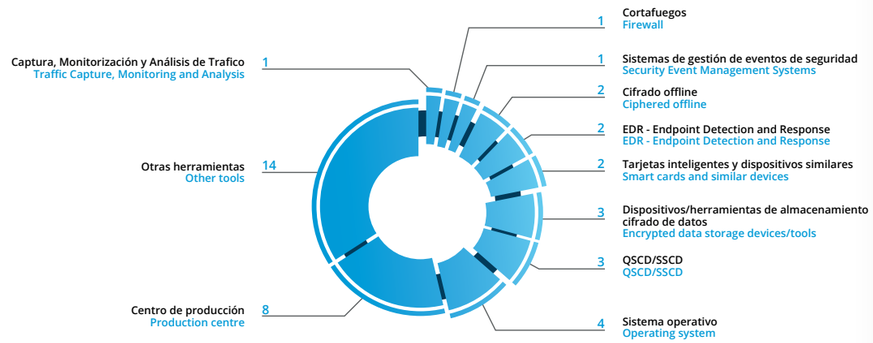
12.1 Evaluación y certificación funcional
Functional evaluation and certification

El Organismo de Certificación del CCN (OC/CCN) inició en **2019** un total de **60 expedientes** (cinco expedientes de acreditación de laboratorios y 55 de certificación de productos), de los cuales 47 han sido solicitudes de certificación de nuevos productos; uno de mantenimiento; dos de revisiones de vigencia abiertas de oficio; tres de recertificaciones y dos renovaciones de certificado.

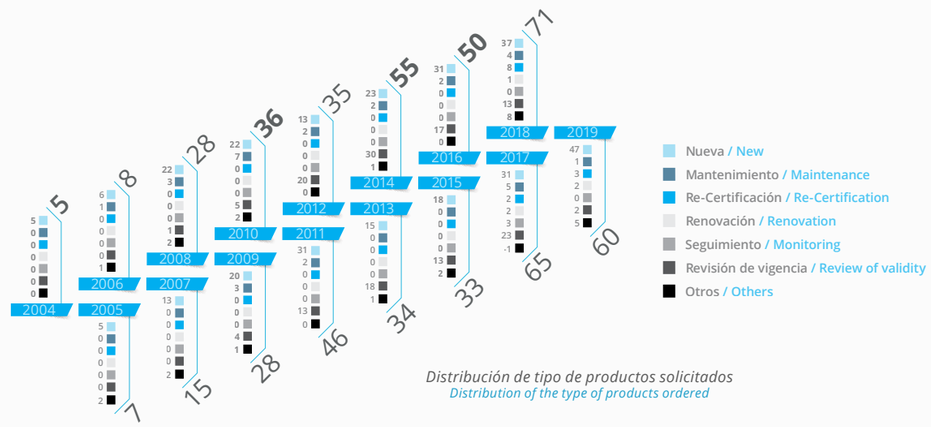


Expedientes abiertos por año
Open files per year

In **2019,** the CCN Certification Body (OC/CCN) initiated a total of **60 dossiers** (five laboratory accreditation dossiers and 55 product certification dossiers), of which 47 were applications for new product certification; one for maintenance; two for ex officio validity reviews; three for recertification and two for certificate renewals.



Expedientes por categoría
Files by category



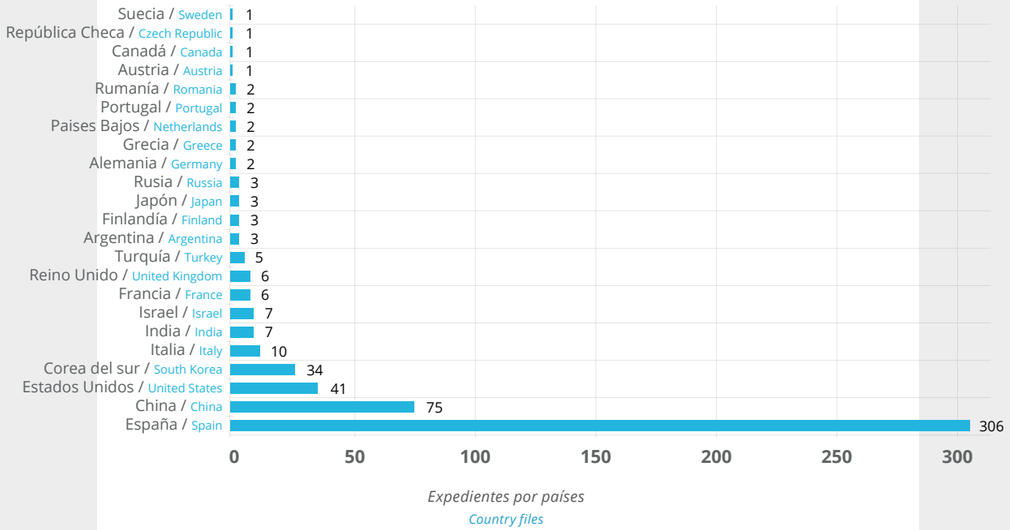
Distribución de tipo de productos solicitados
Distribution of the type of products ordered

Asimismo, durante 2019, se publicaron en el BOE **32 resoluciones**, de las cuales 22 fueron de productos STIC, seis de centros de desarrollo y cuatro de acreditación de laboratorios.

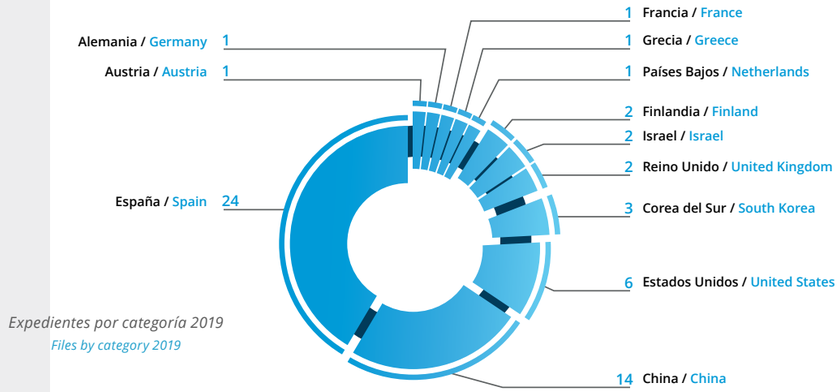
El OC continúa teniendo una gran proyección internacional como puede verse por el elevado número de expedientes de certificación de países extranjeros (cerca del 50%), lo que muestra el reconocimiento y el prestigio internacional del esquema español. Destacan las solicitudes de **China** (13%), **Estados Unidos** (7%) y **Corea del Sur** (6%).
Likewise, during 2019, **32 resolutions** were published in the BOE, of which 22 were for STIC products, six for development centres and four for laboratory accreditation.

The OC continues to have a great international projection as can be seen by the high number of certification dossiers from foreign countries (nearly 50%), which shows the recognition and international prestige of the Spanish framework. The applications from **China** (13%), the **United States** (7%) and **South Korea** (6%) stand out.

Expedientes de certificación por año españoles vs extranjeros
Certification files per year Spanish vs foreigners



Expedientes por países
Country files



Expedientes por categoría 2019
Files by category 2019

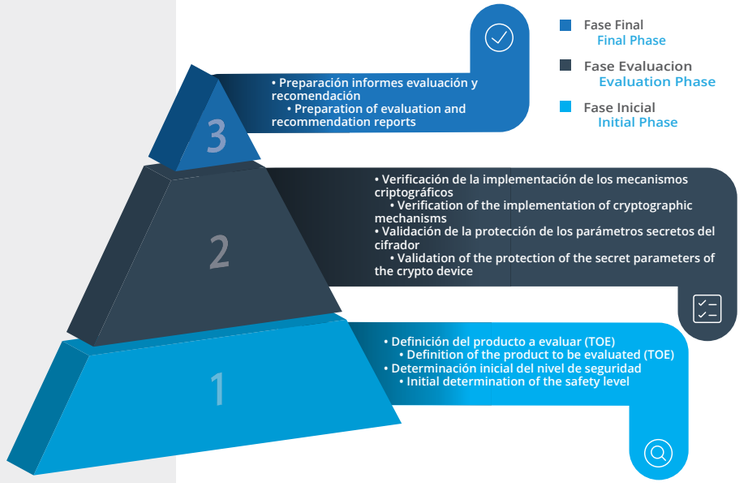
12.2 Evaluación y certificación criptológica
Cryptologic evaluation and certification

Esta evaluación permite valorar y acreditar la capacidad de un producto de cifra para manejar información clasificada de forma segura. Su objetivo fundamental es garantizar que dicho producto realiza su función adecuadamente.
Para ello, se ha de comprobar la correcta implementación de los algoritmos y protocolos criptográficos y su capacidad para proteger adecuadamente la información que va a procesar, así como la eficacia de los mecanismos de seguridad que incorpora.

This evaluation allows to assess and accredit the capacity of an encryption product to handle classified information in a secure way. Its main objective is to ensure that the product performs its function properly. To this end, the correct implementation of cryptographic algorithms and protocols and their ability to adequately protect the information to be processed must be verified, as well as the effectiveness of the security mechanisms it incorporates.

12.2.1 Proceso de evaluación criptológica
Cryptologic evaluation process

Los procesos de evaluación consumen una cantidad importante de recursos y requieren de unos plazos de tiempo que dependen del nivel de clasificación de la información a proteger, pero que suelen prolongarse entre unos 6 y 18 meses.



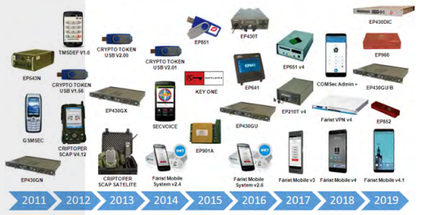
Evaluation processes are resource-intensive and require time frames that depend on the level of classification of the information to be protected, but usually last between 6 and 18 months.

Estructura de la evaluación criptológica.
Structure of the cryptological evaluation.

12.2.2 Certificación de productos de cifra
Certification of encryption products

La certificación de un producto de cifra es la constatación de su capacidad para proteger información clasificada tras haber superado el correspondiente proceso de evaluación criptológica, y constata que la evaluación ha sido realizada de acuerdo a la metodología y que sus resultados son coherentes. Una vez finalizado el proceso de evaluación criptológica, la **Autoridad de Certificación Criptológica** (el director del CCN) emite el correspondiente certificado, donde se autoriza el uso del producto de cifra para proteger información clasificada.

Cifradores certificados 2011-2019



Cifradores cerificados 2011-2019
Certified Headers 2011-2019

The certification of an encryption device is the confirmation of its capacity to protect classified information after having passed the corresponding cryptologic evaluation process, and it confirms that the evaluation has been carried out according to the methodology and that its results are consistent. Once the cryptologic evaluation process has been completed, the **Cryptologic Certification Authority** (the director of the CCN) issues the corresponding certificate authorising the use of the encryption product to protect classified information.

Hay que resaltar que existen productos de cifra certificados, a nivel nacional, por el CCN que han sido aprobados por OTAN (para proteger información clasificada hasta NATO SECRET) y por parte de la UE (para proteger información clasificada EU-RESTRICTED).

It should be noted that there are encryption products certified, at national level, by the CCN which have been approved by NATO (to protect classified information up to NATO SECRET) and by the EU (to protect EU-RESTRICTED information).

12.2.3 Actividades realizadas en 2019
Activities carried out in 2019

Durante el año 2019, se ha finalizado la evaluación criptológica de los cifradores **EP430GU/B**, **EP430DIC** y **EP960IC**, que fueron modificados a finales de 2018 para su adaptación a las necesidades de la Operación ATALANTA. Todos ellos superaron satisfactoriamente el proceso de evaluación, consiguiendo la aprobación para el manejo de información nacional clasificada hasta el grado de CONFIDENCIAL.

During 2019, the cryptologic evaluation of the **EP430GU/B**, **EP430DIC** and **EP960IC** coders was completed and they were modified at the end of 2018 to adapt them to the needs of Operation ATALANTA. All of them successfully passed the evaluation process, obtaining approval for the handling of classified national information up to the level of CONFIDENTIAL.


EP430GU/B


EP430DIC


EP960

También se ha evaluado el sistema para la protección de las comunicaciones móviles **Färist Mobile en su versión 4.1**, con una nueva versión del Sistema Operativo, Android 9, y una nueva plataforma, BQ Aquaris X2. Este sistema ha superado la evaluación siendo aprobado para manejar información clasificada hasta el grado DIFUSIÓN LIMITADA. Esta aprobación ha sido refrendada por la UE de manera que esta versión del sistema también ha sido aprobada por la UE hasta el grado RESTREINT EU / UE RESTRICTED.

The system for the protection of mobile communications **Färist Mobile** has also been evaluated in **its version 4.1,** with a new version of the Operating System, Android 9, and a new platform, BQ Aquaris X2. This system has passed the evaluation being approved to handle classified information up to the degree of LIMITED DIFFUSION. This approval has been endorsed by the EU so that this version of the system has also been approved by the EU up to RESTREINT EU / UE RESTRICTED.

Asimismo, se evaluó y certificó la nueva versión (ver.4.1) de la aplicación para protección de las comunicaciones móviles **COMSecAdmin+**, que permite cifrar voz, mensajería instantánea y VTC adecuadamente cuando se utiliza en un terminal móvil aprobado o cualificado.

Por otra parte, se ha continuado la evaluación de diferentes cifradores IP de la familia **EP430T**, y se iniciaron los procesos de evaluación de las nuevas versiones del cifrador “off-line” **EP852** y del cifrador software **EP880**.

The new version (ver.4.1) of the mobile communication protection application **COMSecAdmin+** was also evaluated and certified, which allows voice, instant messaging and VTC encryption properly when used in an approved or qualified mobile terminal.

On the other hand, the evaluation of different IP coders of the **EP430T** family has continued, and the evaluation processes of the new versions of the “off-line” coder **EP852** and the software coder **EP880** were started.

12.3 Evaluación y certificación TEMPEST
TEMPEST evaluation and certification

Todo dispositivo electrónico genera un campo electromagnético que puede contener o estar relacionado con la información que procesa. Estas emanaciones pueden comprometer la seguridad de esta información, una vulnerabilidad conocida como TEMPEST.

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.

Every electronic device generates an electromagnetic field that may contain or be related to the information it processes. These emanations can compromise the security of this information, a vulnerability known as TEMPEST.

The CCN, as the ICT security certification authority in the EMSEC (Emission Security) field, is responsible for the development of national regulations in this field, the evaluation and certification of equipment, systems, platforms and installations, as well as the participation in and advice 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.

12.3.1.Certificación ZONING de Instalaciones
Zoning Certification of Facilities

El CCN aplica el modelo ZONING para la certificación de instalaciones y equipos, tanto de administraciones como de empresas públicas y privadas, que procesan información clasificada. En 2019 han sido **27** y las renovaciones **113**.

The CCN applies the ZONING model for the certification of facilities and equipment, both for administrations and public and private companies, that process classified information. In 2019 there have been **27** certifications and 113 **renewals**.

12.3.2. Certificación ZONING de equipos y sistemas
ZONING certification of equipment and systems

Del mismo modo que se evalúan los locales en los que se procesa información clasificada, también es necesario tener control sobre el nivel de las emanaciones generadas en los equipos y sistemas con los que se trabaja. En 2019 se evaluaron 200 equipos y sistemas, los cuales aparecen en la guía CCN-STIC-104, actualizada dos veces al año por el CCN.

In the same way that premises where classified information is processed are evaluated, it is also necessary to have control over the level of emanations generated in the equipment and systems with which one works. In 2019, 200 pieces of equipment and systems were evaluated, which appear in the CCN-STIC-104 guide, updated twice a year by the CCN.

12.3.3. Certificación TEMPEST de equipos
TEMPEST certification of equipment

Siguiendo los procedimientos especificados en las normas SDIP-27 o IASG-7-03, el CCN evalúa y certifica TEMPEST todo tipo de equipos y sistemas, verificando que no es posible la obtención de la información procesada. Durante 2019 se han certificado **nueve equipos y sistemas informáticos** y se han realizado pruebas TEMPEST a diferentes dispositivos móviles a fin de detectar vulnerabilidades y fugas de información.

Following the procedures specified in the standards SDIP-27 or IASG-7-03, the CCN evaluates and certifies TEMPEST all types of equipment and systems, verifying that it is not possible to obtain the information processed. During 2019, **nine pieces of equipment and computer systems have been** certified and TEMPEST tests have been carried out on different mobile devices in order to detect vulnerabilities and information leaks.

12.3.4. Certificación TEMPEST de Armarios Apantallados
TEMPEST Certification of Shielded Cabinets

El CCN ha llevado a cabo el estudio, evaluación y certificación de armarios apantallados para determinar la atenuación que aportan tanto ante señales radiadas como en las líneas que entren o salgan del mismo, con el fin de determinar la protección que ofrecerían ante la instalación en su interior de cualquier tipo de equipamiento.

The CCN has carried out the study, evaluation and certification of shielded cabinets to determine the attenuation they provide to both radiated signals and the lines entering or leaving them, with a view to determining the protection they would offer in the event of the installation of any type of equipment inside them.

12.3.5. Certificación TEMPEST de Plataformas
TEMPEST Platform Certification

El CCN ha seguido participando en 2019 en diversos programas internacionales 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 de su Grupo de Transmisiones. Además, ha llevado a cabo la certificación de una nueva versión del avión tanquero MRTT para Australia, así como la certificación de la fragata F-102 "Almirante Juan de Borbón" de la Armada en las instalaciones del Arsenal Militar de Ferrol o nuevos PODs LDP para el caza Eurofighter.

In 2019, the CCN has continued to participate 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 its Transmission Group. In addition, it has carried out the certification of a new version of the MRTT tanker aircraft for Australia, as well as the certification of the Navy's F-102 frigate "Almirante Juan de Borbón" at the Ferrol Military Arsenal facilities or new LDP PODs for the Eurofighter.

13

Catálogo de productos de seguridad TIC (CPSTIC)

ICT Security Product Catalogue (CPSTIC)

El Catálogo de productos de seguridad TIC (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.

El CPSTIC 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.

The purpose of the Information and Communication Technologies Security Product Catalogue (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.

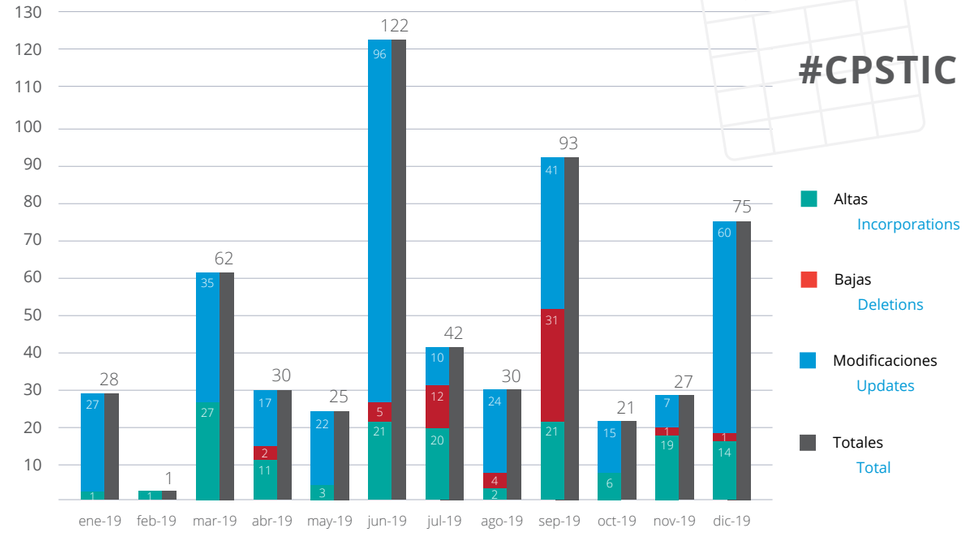
El CPSTIC consta de dos partes: **Productos Aprobados** y **Productos Cualificados**.

Tras su puesta en marcha en diciembre de 2017, el CPSTIC es actualizado **con carácter mensual**, para poder ofrecer a la Administración un listado actualizado de productos y servicios. Durante el año 2019 se han contabilizado **556 actualizaciones** (altas, bajas, modificaciones) del CPSTIC:

The CPSTIC consists of two parts: **Approved Products** and **Qualified Products**.

After its launch in December 2017, the CPSTIC is updated on a **monthly basis**, in order to provide the Administration with an updated list of products and services. During 2019, **556 updates** (additions, deletions, modifications) of the CPSTIC have been accounted for:

Sello Stamp	Tipo de producto Type of product	Información que maneja Information managed
PRODUCTO STIC APROBADO · CCN · INFORMACIÓN CLASIFICADA	Aprobado Approved	Clasificado Classified
PRODUCTO SEGURIDAD TIC · CCN · CUALIFICADO	Cualificado Qualified	Sensible (ENS) Sensitive (ENS)



Actualizaciones CPSTIC 2019
CPSTIC 2019 Updates

Esquema Nacional de Seguridad

Durante el año 2019, CCN-PYTEC amplió el alcance del CPSTIC para incluir productos para sistemas de categoría MEDIA y BÁSICA en el ENS.

During 2019, CCN-PYTEC expanded the scope of CPSTIC to include products for MEDIUM and BASIC category systems in the ENS.

Para ello, se definieron nuevos RFS, en base a las necesidades transmitidas por la Administración y los fabricantes de seguridad. En total, se han publicado cinco nuevos conjuntos de RFS para categoría MEDIA del ENS:

For this purpose, new RFS were defined, based on the needs transmitted by the Administration and the security manufacturers. In total, five new RFS sets have been published for the MEDIUM category of the ENS:

1. Anti-virus/EPP (Endpoint Protection Platform)
   Anti-virus/EPP (Endpoint Protection Platform)
2. Herramientas de gestión de red
   Networks management tools
3. Sistemas de gestión de eventos de seguridad (SIEM)
   Security event management systems
4. Enrutadores
   Routers
5. Switches
   Switches

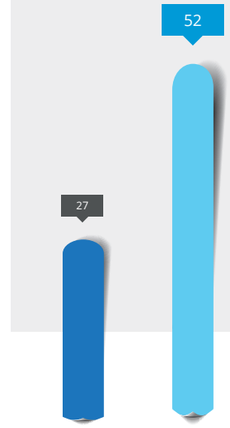
13.1 Aprobación productos STIC
STIC product approval

Los **Productos Aprobados** son aquellos que se consideran adecuados para el manejo de información clasificada (*véase apartado de Evaluación y Certificación Criptográfica*).

En el año 2019, el número de productos aprobados se ha incrementado un **92%** respecto al año anterior.

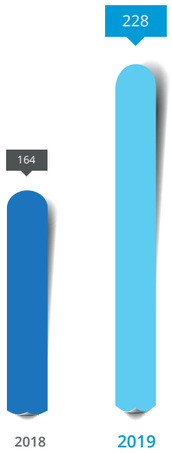
Approved Products are those considered suitable for handling classified information (*see section on Cryptographic Evaluation and Certification*).

In 2019, the number of approved products has increased by **92%** over the previous year.



Nº de productos aprobados en el CPSTIC
Number of products approved in the CPSTIC

13.2 Cualificación productos STIC
STIC product qualification



Nº de productos cualificados en el CPSTIC
Number of qualified products in the CPSTIC

Los **Productos Cualificados** son aquellos que cumplen los requisitos de seguridad exigidos para el manejo de información en sistemas bajo el alcance del ENS, en cualquiera de sus categorías de seguridad.

A lo largo de 2019, el número de productos cualificados se ha incrementado un **39%** respecto al año anterior.

The **Qualified Products** are those that meet the security requirements demanded for the handling of information in systems under the scope of the ENS, in any of its security categories.

In 2019, the number of qualified products increased by **39%** over the previous year.

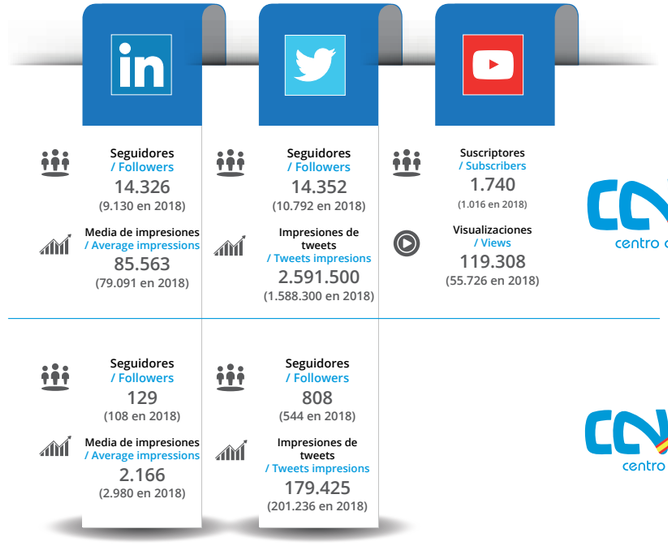
14

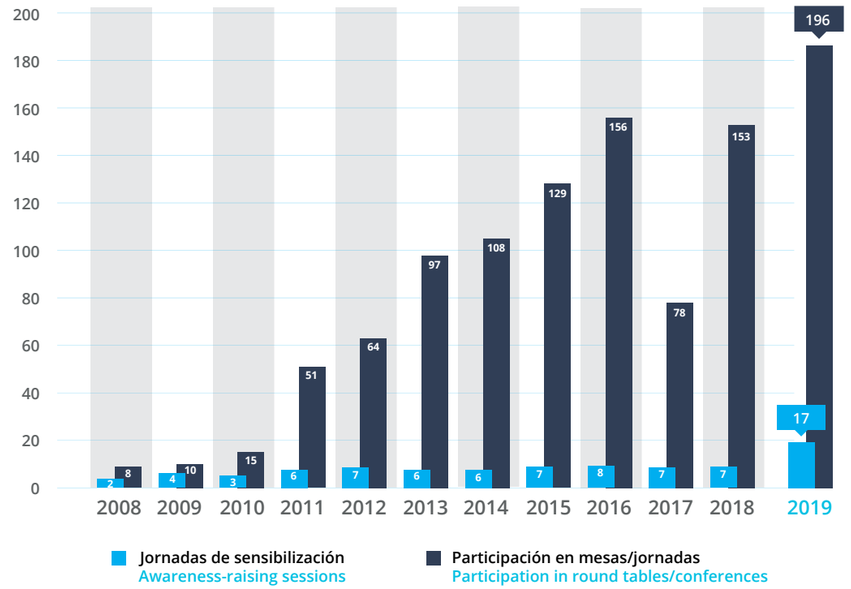
Cultura de ciberseguridad

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 a 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,** while promoting and participating in different cybersecurity events. It also maintains a strong media presence with significant **activity on social media**:
LinkedIn, YouTube and Twitter.





Participación del CCN en jornadas y mesas redondas
Participation of the CCN in conferences and round tables

14.1 Ciberconsejos
CyberTips

El Centro Criptológico Nacional (CCN) incorporó en 2019 a su portal web una nueva sección dedicada a consejos de ciberseguridad, con el objetivo de ofrecer recomendaciones para prevenir y detectar contratiempos en la utilización diaria de las nuevas tecnologías.

En 2019 se encontraban disponibles para su consulta un total de ocho consejos de ciberseguridad, enmarcados en cuatro categorías: **Redes Sociales**, **Desinformación**, **Amenazas** y **Empleo de la Tecnología**.

In 2019, the National Cryptologic Centre (CCN) incorporated a new section to its website dedicated to cybersecurity advice, 'Ciberconsejos', offering recommendations in order to prevent and detect setbacks in the daily use of new technologies.

In this year, a total of eight cybersecurity councils were available for consultation in four categories: **Social Networks**, **Disinformation**, **Threats,** and **Use of Technology**.

Amenazas
Threat

En esta categoría se incluyen informes, infografías y píldoras multimedia con información sobre prevención de incidentes, cryptojacking, phishing y el modelo de seguridad Zero Trust para proteger redes corporativas.

This category includes reports, infographics and videos with information on incident prevention, cryptojacking, phishing and the Zero Trust security model to protect corporate networks.

Desinformación
Disinformation

En este apartado se ofrecen diferentes recursos para que los ciudadanos puedan desarrollar las habilidades necesarias que les permitan identificar productos y plataformas de comunicación propias de las herramientas de desinformación.

This section offers different resources for citizens to develop the necessary skills that will allow them to identify products and communication platforms typical of disinformation tools.

Redes Sociales
Social Networks

Aquí los usuarios pueden conocer cuáles son los principales riesgos derivados del mal uso de las redes sociales, como el robo o suplantación de identidad, el ciberacoso, el perjuicio reputacional, la publicidad dañina o la distribución de malware, así como una serie de recomendaciones para facilitar el uso de las redes sociales en los entornos empresariales.

Here users can learn about the main risks derived from the misuse of social networks, such as identity theft or impersonation, cyberbullying, reputational harm, harmful advertising or the distribution of malware, as well as a series of recommendations to facilitate the use of social networks in business environments.

Empleo Tecnología
Use of technology

Configuración segura de dispositivos iOS y Android, recomendaciones en ciberseguridad y buenas prácticas en el empleo de la tecnología son los principales contenidos elaborados por el CCN para esta categoría.

Secure configuration of iOS and Android devices, cybersecurity recommendations and best practices in the use of technology are the main contents developed by the CCN for this category.

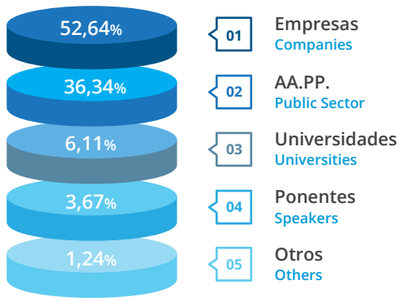
14.2 XIII Jornadas STIC CCN-CERT
XIII STIC CCN-CERT Conference

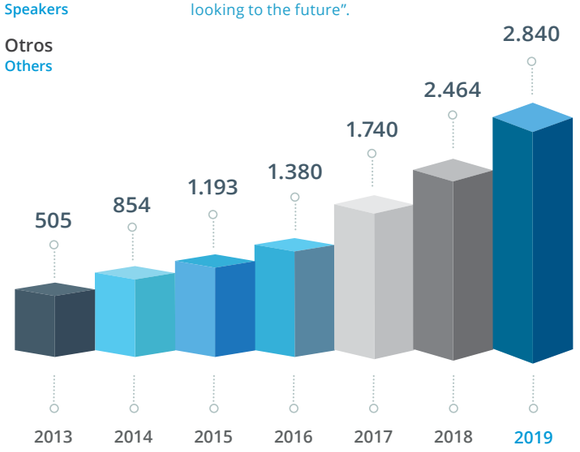
El CCN organiza el principal encuentro de ciberseguridad que se celebra en España, no solo por la calidad y prestigio de sus ponentes, sino por el número de asistentes, el apoyo institucional recibido y el número de empresas patrocinadoras. Inauguradas por la ministra de Defensa, Margarita Robles, las XIII Jornadas STIC CCN-CERT, celebradas en Madrid durante los días 11 y 12 de diciembre, contaron con más de 3.300 asistentes, 130 ponentes de reconocido prestigio, 7 módulos con temática diferente y 60 empresas patrocinadoras.

De especial relevancia fue también la entrega del **premio a la trayectoria profesional en favor de la ciberseguridad del CCN**, otorgado al General del Ejército de Tierra, Félix Sanz Roldán, por "impulsar una España más cibersegura, con voluntad y esfuerzo, y siempre mirando al futuro".

The CCN organizes the main cybersecurity meeting held in Spain, not only because of the quality and prestige of its speakers, but also because of the number of attendees, the institutional support received and the number of sponsoring companies. Inaugurated by the Minister of Defence, Margarita Robles, the XIII STIC CCN-CERT Conference, held in Madrid on 11 and 12 December, had more than 3,300 attendees, 130 renowned speakers, 7 modules with different themes and 60 sponsoring companies.

Of special relevance was also the presentation of the **award for the CCN's professional career in favour of cybersecurity**, given to the General of the Spanish Army, Félix Sanz Roldán, for "promoting a more cybersecure Spain, with will and effort, and always looking to the future".





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

14.2.1. CCN-CERT LABS
CCN-CERT LABS

En el marco de las **XIII Jornadas STIC CCN-CERT**, se organizó la primera edición de los CCN-CERT LABS, donde se impartieron un total de **16 talleres** prácticos sobre los siguientes ámbitos: Seguridad TIC, Respuesta a Incidentes, Ciberinteligencia, y Seguridad Operacional. Esta jornada de talleres reunió a **más de 200 profesionales de la ciberseguridad**.

The first edition of the CCN-CERT LABS was organised within the framework of the XIII STIC CCN-CERT Conference, where a total of **16** practical **workshops** were given on the following areas: ICT Security, Incident Response, Cyberintelligence, and Operational Security. This event of workshops brought together **more than 200 cybersecurity professionals**.

14.3 I Encuentro ENS
I Meeting of the ENS

Tras más de nueve años de recorrido del Esquema Nacional de Seguridad, el CCN, en colaboración con el Ministerio de Política Territorial y Función Pública (Secretaría General de Administración Digital) y la Fundación Círculo de Tecnologías para la Defensa y la Seguridad, organizó, el 18 de junio de 2019, el "I Encuentro del Esquema Nacional de Seguridad, ENS" que llevaba por título *Tendencias y Políticas de Seguridad*.

En él se hizo balance de las mejoras que la implantación y adecuación del ENS han supuesto a la seguridad del Sector Público; se analizó el nivel de madurez alcanzado y se evaluó cuáles deben ser las siguientes medidas a adoptar para conseguir una implementación de seguridad real y no solo en la demostración del cumplimiento (seguridad legal). El I Encuentro del ENS tuvo lugar en la sede del **Museo Casa de la Moneda** con la asistencia de más de 350 responsables de seguridad, tanto del sector público como privado.

After more than nine years of the National Security Framework, the CCN, in collaboration with the Ministry of Territorial Policy and Public Function (General Secretary of Digital Administration) and the Foundation Círculo de Tecnologías para la Defensa y la Seguridad, organized, on 18 June 2019, the "I Meeting of the National Security Framework, ENS" which was entitled *Security Trends and Policies*.

It took stock of the improvements that the implementation and adaptation of the ENS have meant for the security of the Public Sector; it analysed the level of maturity achieved and evaluated which should be the next steps to be taken to achieve a real security implementation and not only in the demonstration of compliance (legal security). The I Meeting of the ENS took place at the headquarters of the **Mint Museum** with the attendance of more than 350 security managers from both the public and private sectors.

14.4 Jornadas SAT
SAT Conference

El 3 de abril de 2019 se celebró la **IX Jornada del Sistema de Alerta Temprana (SAT)** del CCN-CERT. Al evento, que tuvo lugar en el Auditorio de la Fábrica Nacional de la Moneda y Timbre (FNMT) en Madrid, acudieron un total de **255 personas**, provenientes de todas las administraciones públicas españolas, así como de empresas de interés estratégico para el país y de las Universidades.

On 3 April 2019, the **IX Early Warning System Conference (CCN-CERT SAT)** was held. The event, which took place in the Auditorium of the Fábrica Nacional de la Moneda y Timbre (FNMT) in Madrid, was attended by a total of **255 people** from all the Spanish public administrations, as well as from companies of strategic interest to the country and from universities.

14.5 Desayunos tecnológicos
Technological breakfasts

En noviembre de 2019, en el Salón de Actos del Consejo Superior de Investigaciones Científicas (CSIC), se celebró una nueva edición de los desayunos tecnológicos, organizado por el **Departamento de Productos y Tecnologías del CCN (CCN-PYTEC)**, bajo el título "Dispositivos móviles en el ENS: la base para la Transformación Digital en la Administración". El evento contó con la participación de **casi 100 organismos de la Administración**.

In November 2019, a new edition of the technological breakfasts, organised by the **Department of Products and Technologies of the CCN (CCN-PYTEC),** was held in the Assembly Hall of the Spanish National Research Council (CSIC), under the title "Mobile devices in the ENS: the basis for the Digital Transformation in the Administration". The event was attended by **almost 100 government agencies.**

14.6 Otros eventos
Other events

El CCN, en su firme compromiso de **fomentar el intercambio y la divulgación de conocimientos** entre expertos de la ciberseguridad y el público general, ha mostrado su apoyo y colaborado con **numerosos eventos del sector a lo largo de 2019**. Los más destacados han sido: RootedCon, Hack&Beers, #CONPILAR19, Mundo Hacker Day 2019, x1RedMásSegura, Working Hackers Labs, Security High School, la Feria Internacional de Defensa y Seguridad (FEINDEF), la XXI Conferencia Internacional de ISMS Forum, SEDIAN Day, Cibertod@s de ISACA Madrid, Mundo Hacker Academy 2019 y C1b3rWall.

Asimismo, conviene destacar el XVI Premio de la Revista SIC a la labor del Consejo Nacional de Ciberseguridad, cuyo presidente, el entonces secretario de Estado director del Centro Nacional de Inteligencia y del Centro Criptológico Nacional, Félix Sanz Roldán, fue el encargado de recogerlo.

Además de estos encuentros nacionales, el Centro Criptológico Nacional ha participado en diferentes actividades llevadas a cabo en otros países de **América Latina**, como México, Chile y Perú, donde ha colaborado en el impulso a la cultura de ciberseguridad.

The CCN, in its commitment to **promote the exchange and dissemination of knowledge** among cybersecurity experts and the general public, has shown its support and collaboration with **numerous industry events throughout 2019**. The most prominent of these have been RootedCon, Hack&Beers, #CONPILAR19, World Hacker Day 2019, x1RedMásSegura, Working Hackers Labs, Security High School, the Feria Internacional de Defensa y Seguridad (FEINDEF), the XXI Conferencia Internacional de ISMS Forum, SEDIAN Day, Cybertod@s of ISACA Madrid, World Hacker Academy 2019 and C1b3rWall.

It should also be noted that the XVI Award of the SIC Magazine to the work of the National Council on Cybersecurity, whose President, the then Secretary of State and Director of the National Intelligence Centre and the National Cryptologic Centre, Felix Sanz Roldan, was responsible for collecting it.

In addition to these national meetings, the National Cryptologic Centre has participated in different activities carried out in other **Latin American** countries, such as Mexico, Chile and Peru, where it has collaborated in promoting a culture of cybersecurity.

Por otro lado, ATENEA recibió en 2019 el **Premio ISACA Madrid 2019** en el marco del congreso anual High Level Conference que organiza esta asociación. Este galardón, entregado dentro de la categoría de conocimiento, premia a aquellas personas u organizaciones que realizan grandes contribuciones al desarrollo y mejora del cuerpo de conocimiento común utilizado por los constituyentes de la asociación en los campos de la auditoría TI, seguridad y/o control y gobierno de las TIC.

On the other hand, **ATENEA** received in 2019 the **ISACA Madrid 2019 Award** in the framework of the annual *High-Level Conference* organized by this association.

This award, given within the knowledge category, rewards those individuals or organisations that make great contributions to the development and improvement of the body of common knowledge used by the association's constituents in the fields of IT audit, security and/or control and governance of ICT.

15

Programas, grupos de trabajo y acuerdos de colaboración

Programmes, working groups and collaboration agreements

El Centro Criptológico Nacional tiene la firme convicción de que la colaboración entre diferentes organismos y países es esencial para compartir y ampliar conocimientos y proteger a los ciudadanos de la mejor manera posible. En este sentido, el CCN participa y colabora con numerosos organismos y grupos de trabajo, tanto a nivel nacional como internacional. Asimismo, desde su creación ha firmado cuantiosos acuerdos de colaboración y convenios para prestar su apoyo y experiencia en materia de ciberseguridad, una cifra que se ha ampliado notablemente durante 2019.

The purpose of the Information and Communication Technologies Security Product Catalogue (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.

15.1 Ciberseguridad
Cybersecurity

Durante el año 2019, fueron numerosos los acuerdos de colaboración firmados por el CCN, así como los apoyos brindados a otros organismos, tanto españoles como internacionales. Entre los apoyos, cabe citar:

During 2019, the CCN signed numerous collaboration agreements, and provided support to other Spanish and international organisations. Among the supports, it is worth mentioning:

- Resolución de incidentes en Iberoamérica
  Resolution of incidents in Latin America
- Difusión de cultura de la ciberseguridad en Iberoamérica y Norte de África
  Dissemination of cybersecurity culture in Latin America and North Africa
- CSIRT de Chile para vigilancia digital
  Chile's CSIRT for digital surveillance
- Elecciones en El Salvador
  Elections in El Salvador
- Ministerio del Interior:
  Ministry of the Interior:
  - Elecciones Generales (abril y noviembre de 2019) / General Elections (April and November 2019)
  - Elecciones Europeas, Autonómicas y locales (mayo 2019) / European, regional and local elections (May 2019)
  - Cumbre del Clima (noviembre 2019) / Climate Summit (November 2019)
- Comunidades Autónomas y Administración General del Estado
  Autonomous Communities and General State Administration
- Empresas estratégicas para el país
  Strategic companies for the country

Acuerdos y convenios / Agreements and conventions

- **Generalitat Valenciana**: convenio firmado y apoyo al CSIRT-CV. Prorrogado el 6 de septiembre de 2017.
  Generalitat Valenciana: Agreement signed and support for CSIRT-CV. Extended on 6 September 2017.

- **Región de Murcia**: convenio de colaboración en materia de ciberseguridad, firmado el 20 de abril de 2017.
  Region of Murcia: Collaboration agreement on Cybersecurity, signed on 20 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, 3 October 2017.

- **Gobierno de Aragón**: convenio de colaboración en materia de ciberseguridad, el 3 de julio de 2018
  Gobierno de Aragon: Collaboration agreement on Cybersecurity, signed on 3 July 2018.

- **Microsoft**: Acuerdo de colaboración en seguridad, renovado el 27 de junio de 2018.
  Microsoft: Security Collaboration Agreement, renewed on 27 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 15 June 2018.

- **Ministerio de Justicia**: convenio de colaboración en materia de ciberseguridad, firmado el 31 de julio de 2018.
  Ministry of Justice: collaboration agreement on cybersecurity, signed on 31 July 2018.

- **Ministerio de Política Territorial y Función Pública (MPTFP)**: gracias a él se crea el Centro de Operaciones de Ciberseguridad para el Ministerio de Política Territorial y Función Pública (en adelante SOC del MPTFP), que operará como una extensión del futuro Centro de Operaciones de Ciberseguridad de la Administración General del Estado (SOC de la AGE).
  Ministry of **Territorial Policy and Public Function (MPTFP)**: this agreement creates the Cybersecurity Operations Centre for the Ministry of Territorial Policy and the Civil Service (hereinafter the SOC of the MPTFP), which will operate as an extension to the future Cybersecurity Operations Centre of the General State Administration (SOC of the AGE).

- **Junta de Andalucía**: el 10 de junio de 2019 se firma el Protocolo General de Actuación en materia de ciberseguridad entre ambas instituciones (renovación de un acuerdo anterior).
  Junta de Andalucía: On 10 June 2019, the General Protocol of Action on cybersecurity was signed between both institutions (renewal of a previous agreement).

Grupos de trabajo / Working groups

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 organisations 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; and Working Group on Critical Infrastructures with the Secretary of State for Security.

- **Federación Española de Municipios y Provincias**.
  Spanish Federation of Towns and Provinces

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 cybersecurity division of the National Cryptologic Centre participates in the following working groups or forums:

- **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.

  NCIRC of the OTAN (NATO Computer Incident Response Capability), in which the different CERTs of the member countries of this Organisation analyse and share information.

- **Agencia Europea de la Seguridad de las Redes y la Información** (ENISA -European Network & Information Security Agency-) de la Unión Europea.

  European Network & Information Security Agency (ENISA) 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 del phishing, pharming o correos fantasmas.

  APWG (Anti-Phishing Working Group), European Council Programme aiming 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 organisations, 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 CERTs on the continent work together, innovate and share information. It 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. Organisation that brings together the main governmental CERTs in Europe.

- **Grupo de Cooperación de la Unión Europea**. **European Union Cooperation Group**.
- **CSIRT-Networks**. **CSIRT-Networks**.
- **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.

These forums share objectives, ideas and information about vulnerabilities and attacks globally.

15.1.1. Programa GALILEO
GALILEO Programme

Programa internacional
International programme

Desde el CCN se ejerce la representación nacional en los siguientes grupos de trabajo internacionales:
The CCN is the national representative in the following international working groups:

"Security Accreditation Board" (SAB), autoridad conjunta de acreditación de todos los segmentos del sistema GALILEO. Security Accreditation Board (SAB), the joint accreditation authority for all the segments of the GALILEO system.

"GNSS Security Accreditation Panel" (GSAP), órgano de trabajo del anterior encargado de revisar la documentación técnica de los sistemas y de elevar sus recomendaciones al SAB. GNSS Security Accreditation Panel (GSAP), the working body of the previous one responsible for reviewing the technical documentation of the systems and submitting its recommendations to the SAB.

"Tec Working Group", grupo de expertos nacionales al que la Comisión Europea encarga la elaboración de distintos documentos de aplicación en el programa (guía de clasificación, requisitos de seguridad, especificaciones técnicas). Tec Working Group, a group of national experts entrusted by the European Commission with the preparation of various application documents in the programme (classification guide, security requirements, technical specifications).

"OPS Working Group", grupo encargado de la política y coordinación en la gestión de incidentes de seguridad, así como de la implementación de la decisión CD/496 sobre escenarios de amenaza al sistema. OPS Working Group, group responsible for the policy and coordination in the management of security incidents, as well as the implementation of the decision CD/496 on system threat scenarios.

Programa nacional
National programme

Grupo Interministerial. Grupo creado por la Comisión Delegada del Gobierno para Asuntos Económicos con el fin de coordinar la actuación del Estado en los programas europeos de navegación por satélite. Interministerial Group. Group created by the Delegate Commission of the Government for Economic Affairs to coordinate the State's action in European satellite navigation programmes.

Grupo Horizontal. Grupo de trabajo técnico que prepara los temas que deberán ser discutidos en el Grupo Interministerial. Horizontal Group. Technical working group that prepares the topics to be discussed in the Interministerial Group.

Grupo Técnico de Seguridad. Grupo de trabajo técnico que entiende específicamente de los aspectos de seguridad relacionados con los temas del Grupo Interministerial. Technical Security Group. Technical working group that deals specifically with the security aspects related to the topics of the Interministerial Group.

15.1.2. Otros programas
Other programmes

Sistema Conjunto de Radio Táctica (SCRT)
Joint Tactical Radio System (JTRS)

El CCN apoya a la Dirección General de Armamento y Material (DGAM) en el establecimiento de este programa.

The CCN supports the Directorate General of Armament and Material (DGAM) in the establishment of this programme.

Plan MC3
Plan MC3

Durante el año 2019 el CCN ha apoyado a la DGAM en las reuniones y actividades propias de la fase de determinación de viabilidad del programa Plan MC3, que tiene como objetivo la renovación de los medios CIS de los puestos de mando de Cuerpo de Ejército, División y Brigada del Ejército de Tierra y del Cuerpo de Infantería de Marina.

During 2019, the CCN has supported the DGAM in the meetings and activities of the viability determination phase of the MC3 Plan programme, which aims to renew the CIS resources of the Army Corps, Division and Brigade Land Army and the Marine Corps.

A400M
A400M

Desde los inicios del programa A400M, el CCN ha estado participando en todos los grupos de trabajo relacionados con la seguridad de las TI:
Since the beginning of the A400M programme, the CCN has been participating in all the working groups related to IT security:

Comité Conjunto de Acreditación. / Joint Accreditation Board (JAB).
Panel Conjunto de Certificación. / Joint Certification Panel (JCP).
Panel de Control TEMPEST. / TEMPEST Control Panel (TCP).
Panel COMSEC. / COMSEC Panel (CP)
Panel Conjunto de Acreditación de la red corporativa del Grupo AIRBUS para los programas en los que está involucrado (A400M, TIGER). / Joint Accreditation Panel of the AIRBUS Group corporate network for the programmes in which it is involved (A400M, TIGER).

EF2000
EF2000

El CCN participa en el programa EF2000 asistiendo a los siguientes grupos de trabajo:
The CCN participates in the EF2000 programme by attending the following working groups:

Grupo de Trabajo TEMPEST COMSEC Group (TCG). / TEMPEST COMSEC Group (TCG).
Grupo de Trabajo INFOSEC Working Group (IWG). / INFOSEC Working Group (IWG).

Edita /Edit: Centro Criptológico Nacional

Arte Portada /Cover Art: leandro.elzaurdia.com

Imprime /print: AINERGESA Services S.L. (Langayo)

D.L. M-22102-2020

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
2020.09.22 09:21:37 +02'00'

AÑOS

Centro Criptológico Nacional
Argentona, 30 - 28023 Madrid

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