CCN
Centro Criptológico Nacional

Informe de Actividades
Activity Report

2013 - 2014

CCN
CENTRO CRIPTOLÓGICO NACIONAL

Informe de Actividades
Activity Report

2013 - 2014

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA

1 Carta del secretario de Estado director del Centro Nacional de Inteligencia (CNI)
Letter from the Secretary of State-Director of the CNI

Querido/a lector/a,

Cuando en el año 2002 y en el seno del Centro Nacional de Inteligencia (CNI), se creó el Centro Criptológico Nacional (CCN), ampliada su regulación por el **Real Decreto 421/2004**, de 12 de marzo, ya se preveía una insaciable demanda de información por parte de la sociedad española y un uso masivo de las tecnologías de la información y las telecomunicaciones (TIC). En este nuevo escenario, se incrementaban, sin lugar a dudas, las posibilidades de progreso de la población pero también las amenazas existentes.

Hoy, más de doce años después, y cuando el volumen de las aplicaciones TIC es tan elevado y los dispositivos de todo tipo (ordenadores, teléfonos inteligentes, tabletas, etc.) son masivamente utilizados, la dependencia de las TIC es un hecho innegable, al igual que los riesgos asociados a ella.

De ahí que, la labor del CCN, cuya actividad en los dos últimos años presentamos en estas páginas, haya ido encaminada a reducir los riesgos y amenazas provenientes del **ciberespacio**, adecuándose a los nuevos desafíos y buscando, a través de las funciones que tiene encomendadas, prevenir su propagación y atajar su impacto de la forma más rápida y eficaz posible.

La creación en el año 2006 del **CERT Gubernamental Nacional español (CCN-CERT)** como gestor de ciberincidentes en sistemas clasificados, Administraciones Públicas y empresas y organizaciones de interés estratégico; la constitución en 2007 del **Organismo de Certificación (OC)** de la seguridad de los productos y sistemas; su papel desde el año 2010 en el desarrollo e implantación del **Esquema Nacional de Seguridad (ENS)**; la mejora de la capacidad nacional de **evaluación y certificación** de productos de cifra; así como su cometido en la **formación** del personal experto en la materia y en la difusión de normas, instrucciones y guías (**Series CCN-STIC**), ha sido la respuesta del CCN a esta situación.

Una respuesta enmarcada en la actividad del Centro Nacional de Inteligencia en donde la ciberseguridad, en la que se llevaba trabajando décadas, ha pasado a ser un objetivo prioritario y en donde se está realizando un gran esfuerzo de integración de todas sus capacidades de defensa de redes, de inteligencia y de contrainteligencia. La visión amplia de la que dispone el CNI permite una respuesta ágil y nos puede ayudar, no sólo a resolver los ciberincidentes, sino también, a conocer su origen y prevenir futuros ataques.

Precisamente su papel medular dentro de la ciberseguridad en España, nos ha hecho presidir el **Consejo Nacional de Ciberseguridad**, constituido el 25 de abril de 2014, tal y como se preveía en la **Estrategia de Ciberseguridad Nacional** hecha pública unos meses antes (el 5 de diciembre de 2013).

Una presidencia que nos obliga aún más, si cabe, a impulsar el **Plan Nacional de Ciberseguridad** aprobado por el Consejo, como herramienta clave para afrontar el grave desafío ante el que nos encontramos. Un marco en el que deberemos propiciar la coordinación y comunicación entre todos los agentes implicados (instituciones y organismos del Estado, empresas y ciudadanos) y en el que actuaremos como estandarte de la defensa de un ciberespacio más seguro y confiable, preservando la información clasificada y la información sensible, evitando la interrupción de servicios, y defendiendo el Patrimonio Tecnológico español.

Félix Sanz Roldán
Secretario de Estado director del CNI,
Director del CCN
Secretary of State-Director of CNI, Director of CCN

Dear Reader,
When the National Cryptologic Centre (CCN) was set up within the National Intelligence Centre (CNI) in 2002, extending its regulation with Royal Decree 421/2004, dated 12th March, an insatiable demand was forecast for information from Spanish society plus massive use of information and telecommunication and information technologies (ICT). This scenario doubtlessly improved the population's chances of making progress but also increased existing threats.

Today, over 12 years later, and with such a high volume of applications and devices of all types (computers, smartphones, tablets, etc.) used massively, ICT-dependence is undeniable, just like the risks associated with it.
Within this context the CCN's work over the last two years, as presented here, has revolved around reducing risks and threats from cyberspace, adapting to new challenges and searching, through the functions that it has been entrusted with, to prevent propagation and stem its impact as quickly and effectively as possible.

The CCN's response to this situation involved setting up the Spanish Government CERT (CCN-CERT) in 2006 to manage cyber-incidents in classified systems, Public Administrations and companies and organisations with strategic interest; setting up the Certification Body (OC) for product and system security in 2007; its role since 2010 in developing and implanting the National Security Scheme (ENS); improving national evaluation and certification skills for encryption products; as well as work on training expert personnel on the content and dissemination of standards, instructions and guides (CCN-STIC series).

This response is framed within the National Intelligence Centre where cybersecurity, a field it has been working on for decades, has become a priority objective, making a great effort to integrate all its skills to defend networks, intelligence and counter-intelligence. The CNI's wide-ranging vision gives a streamlined response and can help us not only to resolve cyber-attacks but also to find out about the attacker to prevent future attacks. This backbone role within cybersecurity in Spain has led to us permanently presiding over the National Cybersecurity Council, set up on 25 April 2014, as mentioned in the National Cybersecurity Strategy published a few months previously (05 December 2013).

This presidency has required us to boost the National Cybersecurity Plan further still if possible, approved by the Council as a key tool to tackle the serious challenge we are facing. A framework in which we should provide coordination and communication among all agents involved (State institutions and organisation, companies and citizens) and where we act as standards defending safer and more reliable cyberspace, preserving classified information and sensitive information, preventing services from breaking down and defending Spanish Technological Patrimony.

2 Índice
Table of contents

3 Panorama de la ciberseguridad
Cybersecurity Landscape

El cibersespionaje ha centrado su atención en el robo de la propiedad intelectual/industrial de organizaciones con un importante patrimonio tecnológico esencial para la seguridad nacional o para el conjunto de la economía de un país

Si algo ha caracterizado a los años 2013 y 2014 ha sido la especial virulencia en los ataques contra la seguridad de los sistemas de las Tecnologías de la Información y las Comunicaciones (TIC) de gobiernos, administraciones públicas y empresas con alto valor estratégico. Los incidentes de gran envergadura se han venido sucediendo, mes a mes, en un intento continúo, por parte de los atacantes, de apropiarse de información valiosa o sensible desde los puntos de vista político, estratégico, de seguridad o económico. Son las denominadas acciones de ciberespionaje que tiene su origen, tanto en los propios Estados como en terceras empresas, y que han alcanzado su máxima intensidad conocida, incrementándose considerablemente la detección de **Amenazas Persistentes Avanzadas (APT)**[1] contra objetivos **gubernamentales y empresas estratégicas.**

Así, estos dos últimos años (y muy particularmente 2014) ha sido testigo del incremento del número de campañas, de su complejidad y del impacto de dichas acciones de ciberespionaje. Entre ellas, merece destacarse, por su preparación, sofisticación y metodología utilizada, los ciberataques con origen en Estados que han evidenciado el uso de herramientas específicamente diseñadas para infiltrarse en los objetivos, especialmente de los sectores de la industria de **defensa, aeroespacial, energético, gubernamental, farmacéutico, químico, sanitario, tecnológico, financiero**, de **transporte** y de **explotación de recursos naturales.**

En este tipo de ataques se busca, principalmente, información de altísimo valor para el atacante o para un tercero que la vende al mejor postor en el mercado. Información esencial para la seguridad nacional o para el conjunto de la economía de un país, como puede ser la propiedad intelectual/industrial de organizaciones con un importante patrimonio tecnológico; claves del sistema financiero o de la propia Administración.

La **ciberdelincuencia**, con nuevos modelos de negocio como el Crimen como Servicio; el **hacktivismo**[2], con intenciones más modestas, pero que también pueden poner en peligro la prestación de servicios y el normal funcionamiento de las organizaciones; o el **ciberterrorismo** y la **ciberguerra**, como potencial amenaza, también han hecho acto de presencia en los dos últimos años. Un período en el que **España** no ha sido ajena a este tipo de ciberataques. Por el contrario, nuestro país ha sido uno de los más castigados, especialmente en materia de ciberespionaje y ciberdelincuencia organizada.

DEBILIDADES DE NUESTROS SISTEMAS DE PROTECCIÓN Weaknesses in our protection systems
Fata de concienciación y desconocimiento del riesgo Lack of awareness and knowledge of the risk
Sistemas con vulnerabilidades, escasas configuraciones de seguridad y seguridad reactiva (objetivos blandos) Systems with vulnerabilities, limited security configurations and reactive security (soft targets)
Escasez de personal de seguridad y poca vigilancia, con ausencia de herramientas que faciliten la investigación Limited security personnel and little surveillance, lack of tools to help investigation
Mayor superficie de exposición (redes sociales, telefonía móvil, uso de dispositivos propietarios (BYOD), servicios en nube) Greater exposed surface area (social networks, mobile phone, BYOD, cloud services)
Afectados NO comparten información y NO comunicacn incidentes People who are affected do NOT share information and do NOT report incidents

[1] Advanced Persistent Threat. Amenaza Persistente Avanzada.
[2] Activismo digital antisocial. Anti-social digital activism.

If anything can sum up 2013 and 2014, it would be the particular virulence of attacks against Information Communication Technology (ICT) system security among governments, local authorities and companies with high strategic value. Wide-reaching incidents have been occurring, month by month, in a continuous attempt by attackers to get hold of valuable or sensitive information from a political, strategic, security or economic point of view. These are known as **ciber-espionage** actions that originate both in their own countries and in third party companies and that have achieved their maximum known intensity, considerably improving detection of **Advanced Persistent Threats (APT)**[1] against **government and strategic company targets**.

So, over the last two years (and very specifically 2014), there has been an increase in the number of campaigns, their complexity and the impact of these cyber-espionage actions. Among them, due to their preparation, sophistication and methodology, it is worth highlighting cyber-attacks originating in states that have demonstrated the use of tools specifically designed to infiltrate the chosen targets, particularly sectors including the **Defence Industry, aerospace, energy, government, pharmaceutical, chemical, health, technology, finance, transport and exploitation of natural resources.**

This type of attack mainly aims to search for information with very high value for the attacker or for a third party who will sell it to the highest bidder in the market. Essential information for national security or for the country's economy such as intellectual/industrial property from organisations with significant technological patrimony, essential for the financial system or the actual Administration.

Cyber-espionage has focused on stealing intellectual/industrial property from organisations with significant technological patrimony, essential for national security or for the country's economy as a whole.

Como muestra de todo lo expuesto, en el año 2014, el CCN-CERT (véase el capítulo correspondiente de este Informe), gestionó un total de **12.916 incidentes** en las Administraciones Públicas y en empresas de interés estratégico para el país; una cifra que representa un incremento del 78% con respecto al año 2013 que ya se aumentó a su vez más del 150% con relación al 2012. Además, el número de incidentes con una peligrosidad **Crítica** ascendió casi un 250%

Atacantes y métodos utilizados

Entre los atacantes siguen destacando, por orden de importancia, las **agencias de inteligencia** y las unidades de ciberdefensa de las **Fuerzas Armadas** de diferentes países; la **ciberdelincuencia**, el **hacktivismo** y en menor medida los **grupos terroristas** y otros actores.

En cuanto a las herramientas y los métodos utilizados, son ataques a todo tipo de dispositivos (con especial incremento en los móviles) y utilizando en numerosas ocasiones técnicas de ingeniería social a través de las Redes Sociales; así como ataques contra servicios web o los denominados Ransomware (en los que se cifran datos o se bloquea el acceso a un sistema exigiendo dinero a cambio de recuperar la información y/o el sistema), abonadas todas ellas por la falta de concienciación del usuario, la escasa vigilancia del tráfico de red y la protección inadecuada.

Estas amenazas, originariamente dirigidas a empresas e instituciones públicas, actúan también sobre personas individuales, incluyendo altos directivos de compañías y de organismos públicos, personajes notorios y responsables políticos. Se observa, además, una tendencia a atacar a los elementos más débiles que formen parte de la "cadena de intercambio de datos" (por ejemplo, contratistas, proveedores, etc.) antes que hacerlo directamente contra los objetivos finales que han mejorado significativamente sus estrategias y capacidades defensivas.

Las organizaciones, por tanto, se enfrentan a un nuevo paradigma en el tratamiento de las amenazas contra los sistemas de información, que pasa por poner más énfasis en la detección de los ataques que en su prevención, en depender más de la cualificación de las personas complementado con la tecnología y en invertir suficientemente en estos campos de forma continuada. La confianza y el intercambio de información, tanto en el ámbito público como privado, se convierten así, en pieza clave de este nuevo paradigma.

However, in addition to this cyber-espionage there is also **cyber-crime**, with new business models such as Crime as a Service; **hacktivism**[2], with more modest intentions, but that can also endanger service provision and normal operation of organisations; **cyber-terrorism** and **cyber-war**, as a potential threat, have made their presence felt over the last two years. During this period, **Spain** has not escaped this type of cyber-attack. On the contrary, our country has been one of the most severely punished, particularly concerning cyber-espionage and organised cyber-crime.

As an example of the above, in 2014, the CCN-CERT (see corresponding chapter of this Report), managed a total of **12,916 incidents** in the Pubic Administrations in companies of strategic interest for the country; this figure represents an increase of 78% on 2013 that in turn had already increased 150% on 2012. In addition, the number of incidents with **Critical** danger levels increased by almost 250%.

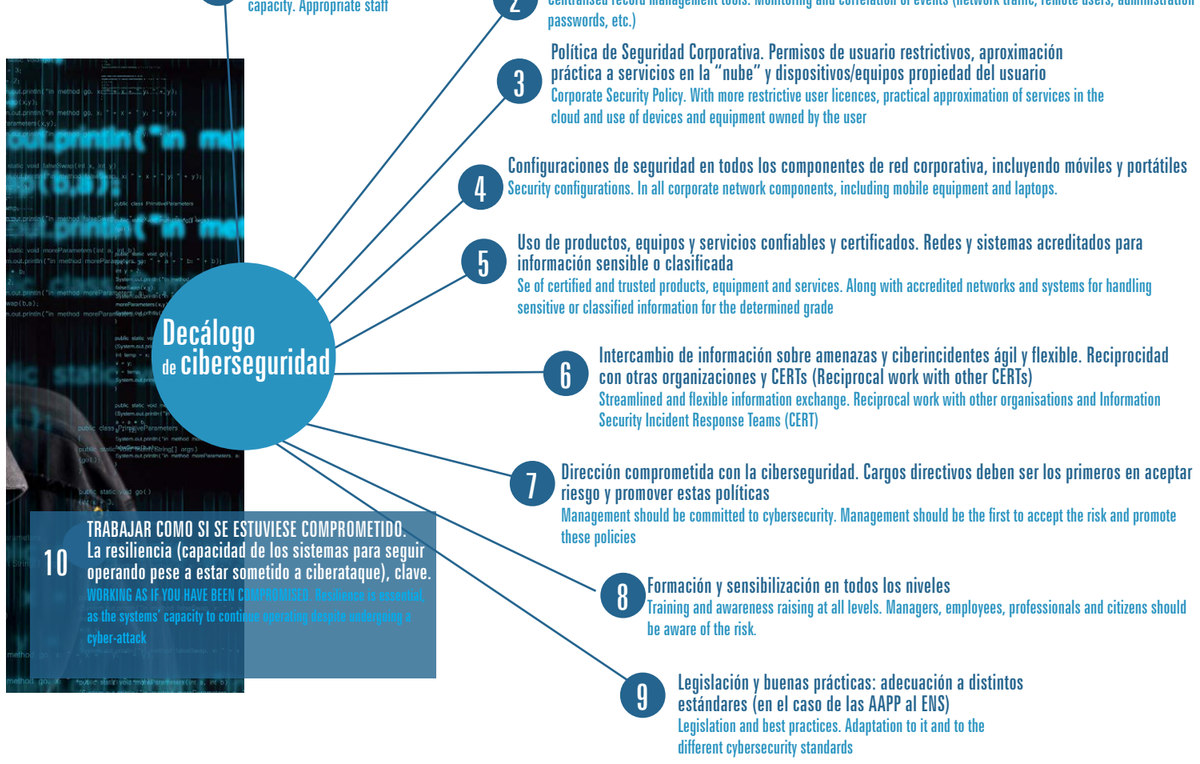
Attackers and methods

Among the attackers, we can continue to highlight, in order of importance, **intelligence agencies** and cyber-defence units for the **Armed Forces** in different countries, **cyber-crime**, **hacktivism** and to a lesser extent, **terrorist groups** and other players.

As far as tools and attack methods are concerned, these are attacks on all types of devices (with a particular increase in mobile devices), often using social engineering techniques through the Social Networks; in addition, attacks against web services or what is known as Ransomware (where data is encoded or access is blocked to a system, demanding money to recover information and/or the system) are some of the threats most present nowadays, not helped by users' lack of awareness, poor surveillance of network traffic and inappropriate protection.

These threats, originally targeting companies and public institutions, also act on individual persons including top executives in companies and public organisations, famous people and political leaders. We can also see a tendency to attack the weakest elements that form part of the "data exchange chain" (e.g. contractors, suppliers, etc.) before directly working against end targets that might have significantly improved their defensive strategies and skills.

The organisations are therefore facing a new paradigm in treating threats against information systems that involves putting a greater emphasis on detecting the attacks than preventing them, on depending more on the qualification of the people given the technology and continuously making sufficient investments in these fields. Trust and information exchange both in the public and private field thereby become key in this new paradigm.



Agentes de la amenaza
Threat agents

Objetivos
Aims

	Origen / Origin	Motivación / Motivation	Conocimiento / Knowledge	Sector Público / Public sector	Sector Privado / Private sector	Ciudadanos / Citizens
1	ESTADOS STATE	• Contraterrorismo o protección de la seguridad nacional • Mejora de su posición geopolítica o estratégica • Terrorismo, como segunda opción • COUNTER-TERRORISM OR PROTECTING NATIONAL SECURITY • IMPROVING THEIR GEOPOLITICAL OR STRATEGIC POSITION • TERRORISM, AS A SECONDARY OPTION	Alto HIGH	Ciberespionaje CYBER-ESPIONAGE Cibercapacidad ofensiva OFFENSIVE CYBER-SKILLS	Ciberespionaje CYBER-ESPIONAGE Cibercapacidad ofensiva OFFENSIVE CYBER-SKILLS	Ciberespionaje CYBER-ESPIONAGE
2	PROFESIONALES DEL CIBERDELITO CYBER-CRIME PROFESSIONAL	• Beneficio económico (directo o indirecto) • ECONOMIC BENEFIT (DIRECT OR INDIRECT)	Medio - Alto MEDIUM - HIGH	Sustracción, publicación o venta de información THEFT, PUBLICATION OR SALE OF INFORMATION Manipulación de información MANIPULATING INFORMATION Interrupción de sistemas INTERRUPTING SYSTEMS Toma de control de sistemas TAKING CONTROL OF SYSTEMS	Sustracción, publicación o venta de información THEFT, PUBLICATION OR SALE OF INFORMATION Manipulación de información MANIPULATING INFORMATION Interrupción de sistemas INTERRUPTING SYSTEMS Toma de control de sistemas TAKING CONTROL OF SYSTEMS	Sustracción, publicación o venta de información THEFT, PUBLICATION OR SALE OF INFORMATION Manipulación de información MANIPULATING INFORMATION Interrupción de sistemas INTERRUPTING SYSTEMS Toma de control de sistemas TAKING CONTROL OF SYSTEMS
3	HACKTIVISTAS HACKTIVISTS	• Acercarse a sus objetivos ideológicos • APPROACH THEIR IDEOLOGICAL TARGETS	Medio MEDIUM	Sustracción y publicación de la información sustraída THEFT AND PUBLICATION OF STOLEN INFORMATION Desfiguración en páginas web DEFACING WEBSITES Interrupción de sistemas INTERRUPTING SYSTEMS Toma de control de sistemas TAKING CONTROL OF SYSTEMS	Sustracción y publicación de la información sustraída THEFT AND PUBLICATION OF STOLEN INFORMATION Desfiguración en páginas web DEFACING WEBSITES Interrupción de sistemas INTERRUPTING SYSTEMS Toma de control de sistemas TAKING CONTROL OF SYSTEMS	Sustracción y publicación de infomación sustraída THEFT AND PUBLICATION OF STOLEN INFORMATION
4	GRUPOS TERRORISTAS TERRORIST GROUPS	• Lograr cambios en la sociedad, mediante el uso del terror, o influir en la toma de decisiones políticas • ACHIEVE CHANGES IN SOCIETY BY USING TERROR, OR INFLUENCE IN POLITICAL DECISION-MAKING	Medio - Bajo Medium - Low	Interrupción de Sistemas/ Toma de control INTERRUPTING SYSTEMS / TAKING CONTROL	Interrupción de Sistemas/ Toma de control INTERRUPTING SYSTEMS / TAKING CONTROL	
5	CIBERVÁNDALOS Y SCRIPT KIDDIES CYBER-VANDALS AND SCRIPT KIDDIES	• Picardía y búsqueda de desafíos • MISCHIEVOUSNESS. LOOKING FOR A CHALLENGE	Bajo LOW	Sustracción de información THEFT OF INFORMATION Interrupción de Sistemas INTERRUPTING SYSTEMS	Sustracción de información THEFT OF INFORMATION Interrupción de Sistemas INTERRUPTING SYSTEMS	Sustracción de información THIEF OF INFORMATION
6	ACTORES INTERNOS INSIDERS	• Venganza o beneficios económicos o ideológicos (en ocasiones dirigido desde el exterior) • REVENGE OR ECONOMIC OR IDEOLOGICAL BENEFIT (OCCASIONALLY RUN FROM THE OUTSIDE)	Alto - Bajo HIGH - LOW	Sustracción, publicación o venta de información THEFT, PUBLICATION OR SALE OF INFORMATION Interrupción de Sistemas INTERRUPTING SYSTEMS	Sustracción, publicación o venta de información / Interrupción de Sistemas THEFT, PUBLICATION OR SALE OF INFORMATION/ INTERRUPTING SYSTEMS Interrupción de Sistemas INTERRUPTING SYSTEMS	
7	CIBERINVESTIGADORES CYBER-DETECTIVES	• Revelación de debilidades (y su propio perfil) • REVEALING WEAKNESSES (AND OWN PROFILE)	Alto HIGH	Recibir y publicar información RECEIVING AND PUBLISHING INFORMATION	Recibir y publicar información RECEIVING AND PUBLISHING INFORMATION	
8	ORGANIZACIONES PRIVADAS PRIVATE ORGANISATIONS	• Obtener o vender información valiosa • OBTAIN OR SELL VALUABLE INFORMATION	Alto - Bajo HIGH - LOW		Sustracción de información (espionaje industrial) THEFT OF INFORMATION (INDUSTRIAL ESPIONAGE)	Uso/ abuso o reventa de información de clientes THEFT OF INFORMATION (INDUSTRIAL ESPIONAGE)

Nivel de peligrosidad DANGER LEVEL

BAJO LOW
- No se han observado nuevas amenazas tendencias.
- Se dispone de medidas suficientes para neutralizar la amenaza.
- No ha habido incidentes escialmente significativos en el periodo analizado.
- NO NEW THREATS TRENDS HAVE BEEN OBSERVED.
- THERE ARE SUFFICIENT MEASURES TO NEUTRALISE THE THREAT.
- THERE HAVE BEEN NO PARTICULARLY SIGNIFICANT INCIDENTS IN THE PERIOD BEING ANALYSED.

MEDIO MEDIUM
- No se han observado nuevas amenazas o tendencias.
- Se dispone de medidas (parciales) para neutralizar la amenaza.
- Los incidentes detectados no han sido especialmente significativos.
- NO NEW THREATS OR TRENDS HAVE BEEN OBSERVED.
- THERE ARE (PARTIAL) MEASURES TO NEUTRALISE THE THREAT.
- THE INCIDENTS DETECTED HAVE NOT BEEN PARTICULARY SIGNIFICANT.

ALTO HIGH
- Las amenazas o su tendencia se ha incrementado significativamente.
- Las medidas adoptadas tienen un efesto muy limitado, por lo que la amenaza permanece.
- Los incidentes detectados han sido especialmente significativos.
- THE THREATS OR THEIR TRENDS HAVE INCREASED SIGNIFICANTLY.
- THE MEASURES ADOPTED HAVE A VERY LIMITED EFFECT, SO THE THREAT REMAINS
- THE INCIDENTS DETECTED HAVE BEEN PARTICULARLY SIGNIFICANT.

4 Centro Criptológico Nacional (CCN)
National Cryptologic Centre (CCN)

Centro Nacional de Inteligencia

El Centro Criptológico Nacional (CCN) está adscrito al Centro Nacional de Inteligencia (CNI), el Organismo público responsable de facilitar al Presidente del Gobierno y al Gobierno de la Nación las informaciones, análisis, estudios o propuestas que permitan prevenir y evitar cualquier peligro, amenaza o agresión contra la independencia o integridad territorial de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones. Así, entre sus funciones se encuentra la contrainteligenica ante la actuación de cualquier Estado o grupo organizado que intente atentar contra el Gobierno o contra las organizaciones, públicas o privadas, que sean de interés estratégico para España.

La información obtenida por el CNI y los correspondientes análisis que a partir de ella se realizan tienen como destinatarios al Presidente del Gobierno y a los Ministros.
Los ministerios que más habitualmente reciben los trabajos elaborados por el Centro son los de Asuntos Exteriores y Cooperación, Defensa e Interior. Asimismo, el CNI proporciona información a otros departamentos de la Administración.

El CNI, adscrito al **Ministerio de la Presidencia**, se rige por el principio de sometimiento al ordenamiento jurídico y lleva a cabo sus actividades específicas en el marco de las facultades expresamente establecidas en la Ley 11/2002 de 6 de mayo reguladora del CNI y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.

Desde febrero de 2014, el secretario de Estado director del CNI preside el **Consejo Nacional de Ciberseguridad (CNCS)** órgano creado al amparo de la Estrategia de Ciberseguridad Nacional (aprobada en diciembre de 2013) y cuyo principal objetivo se encuentra el coordinar las actuaciones de los distintos ámbitos del Estado para hacer frente a las amenazas del ciberespacio.

El 19 de marzo de 2004, se publicaba en el Boletín Oficial del Estado, **el Real Decreto 421/2004, de 12 de marzo**, por el que se regula el Centro Criptológico Nacional (CCN), adscrito al Centro Nacional de Inteligencia (CNI) y compartiendo con él, medios, procedimientos, normativa y recursos. De igual forma, se confiere al secretario de Estado director del CNI la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Este RD define el ámbito y funciones de este Organismo, cuya actividad había sido recogida previamente en la **Ley 11/2002, de 6 de mayo**, reguladora del CNI. Se daba cuerpo a un departamento surgido a principios de los años 80, en el seno del propio Centro, que ya había alcanzado un profundo conocimiento en amenazas, vulnerabilidades y riesgos de los sistemas de información y comunicaciones.

En función del citado RD, el CCN es el Organismo responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las Tecnologías de la Información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo.

On 19 March 2004, the Official State Gazette published Royal Decree 421/2004, dated 12th March, regulating the National Cryptologic Centre (CCN), depending on the National Intelligence Centre (CNI) and sharing equipment, procedures, standard and resources with it. In the same way, the Secretary of State-Director of the CNI was given the responsibility of running the National Cryptologic Centre (CCN).

This RD was intended to regulate and define the field and functions of this Organisation, whose activity had been recognised previously in Law 11/2002, dated 6th May, regulating the CNI. This shaped a department that emerged in the early 80s, within the actual Centre, that had already attained in-depth knowledge of threats, vulnerabilities and risks for information and communication systems.

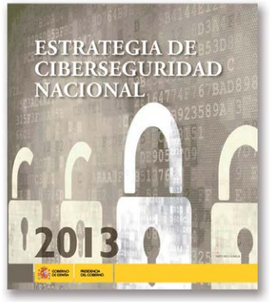
According to the aforementioned RD, the CCN is the Organisation in charge of coordinating actions among different Administration organisations that used encryption resources or procedures, guaranteeing security for Information Technologies in that field, providing information on coordinated purchases of cryptologic equipment and training specialist Administration staff in this field.

National Intelligence Centre

The National Cryptologic Centre (CCN) depends on the National Intelligence Centre (CNI), the public organisation responsible for providing the President of the Government and the Government of the Nation with the information, analysis, studies or proposals that help prevent or avoid any danger, threat or attack on the independence or territorial integrity and stability of the Rule of Law and its institutions. So, its functions include counter-intelligence on actions by any State or organised group that attempts to attack the Government or against public or private organisations that are of strategic interest for Spain.
The information obtained by the CNI and its corresponding analysis is intended for the President of the Government and the Ministers.
The ministries that most often receive the work drawn up by the Centre are Foreign Affairs and Cooperation, Defence and the Home Office. In addition, the CNI provides information to other Administration departments.
Depending on the **President's Office**, the CNI is governed by the principle of submitting to legal ordinance and carries out its specific activities within the framework of the authorities expressly set in Law 11/2002 dated 6th May regulating the CNI and Organic Law 2/2002, dated 6th May, regulating prior legal control of the National Intelligence Centre.
Since February 2014, the Secretary of State-Director of the CNI has presided over the **National Cybersecurity Council (CNCS)**, a body created within the National Cybersecurity Strategy (approved in 2013) whose main goal is to coordinate actions among different State fields to tackle cyberspace threats.

5 Estrategia de Ciberseguridad Nacional y Esquema Nacional de Seguridad
National Cybersecurity Strategy and the National Security Scheme

5.1 Estrategia de Ciberseguridad Nacional (ECSN)



En diciembre de 2013, el Consejo de Seguridad Nacional, presidido por el Presidente del Gobierno, Mariano Rajoy, aprobó la Estrategia de Ciberseguridad Nacional "con el fin de dar respuesta al enorme desafío que supone la preservación del ciberespacio de los riesgos y amenazas que se ciernen sobre él".

La aprobación de dicho documento de carácter estratégico, tal y como se recoge en el preámbulo, ponía de manifiesto las capacidades colectivas y el compromiso de una nación que apuesta en firme por garantizar su seguridad en el ciberespacio. Para España, los avances en el ámbito de la ciberseguridad contribuyen además a incrementar nuestro potencial económico, ya que promueven un entorno más seguro para la inversión, la generación de empleo y la competitividad.

La Estrategia delimita el entorno del ciberespacio, fija unos propósitos y principios rectores, seis objetivos y ocho líneas de acción para el logro de la ciberseguridad nacional, y define el marco de coordinación de la política de ciberseguridad, creando una estructura orgánica que se integra en el marco del Sistema de Seguridad Nacional.

Así, y dependiente del Consejo de Seguridad Nacional, el 25 de febrero de 2014, se constituyó el Consejo Nacional de Ciberseguridad (CNCS) con el objetivo de coordinar las actuaciones de los distintos ámbitos del Estado para hacer frente a las amenazas del ciberespacio. Este Consejo está presidido por el secretario de Estado director del Centro Nacional de Inteligencia (CNI) y en su reunión del 25 de febrero de 2014, acordó proceder a marcar las directrices de desarrollo de la Estrategia para los dos próximos años, mediante un Plan Nacional de Ciberseguridad (PNCS), que desarrolle a través de actuaciones concretas las líneas de acción previstas en la ECSN utilizando los mecanismos necesarios para ello.

El secretario de Estado director del Centro Nacional de Inteligencia (CNI) preside el Consejo Nacional de Ciberseguridad (CNCS)

5.1 National Security Strategy

In December 2013, the National Security Council, presided over by the President of the Government, Mariano Rajoy, approved the **National Cybersecurity Strategy** (https://www.ccn-cert.cni.es/publico/dmpublidocuments/EstrategiaNacionalCiberseguridad.pdf) "in order to meet the enormous challenge represented by keeping cyberspace safe from the risks and threats targeting it".

Approval of this strategic document, as compiled in the introduction, demonstrated that collective capabilities and the commitment of a nation that is firmly guaranteeing its security in cyberspace. For Spain, progress in the field of cybersecurity also helps increase our economic potential as it promotes a more secure environment for investment, generating employment and competition.

The Strategy marks out the cyberspace environment, sets **proposals and governing principles, six goals** and **eight lines of action** to achieve national cybersecurity and define the coordination framework for the cybersecurity policy, creating an organic structure that fits within the framework of the National Security System.

In this way, and depending on the National Security Council, on 25th February 2014, the **National Cybersecurity Council (CNCS)** was set up in order to coordinate the actions of the different State fields to tackle cyberspace threats. This Council is permanently presided over by the SSecretary of State-Director of the National Intelligence Centre (CNI) and in its meeting on 25th February 2014, it agreed to draw up guidelines to develop the Strategy for the next two years, by means of a National Cybersecurity Plan (PNCS) that uses specific actions to develop the lines of action given in the ECSN using the necessary mechanisms.

This Council is permanently presided over by the Secretary of State Director of the National Intelligence Centre (CNI)

Estrategia de Ciberseguridad Nacional
National Cyber Securyty Strategy

Estrategia de Ciberseguridad Nacional
National Cyber security Strategy

Ciberespacio y su seguridad
Cyberspace and its security

+

Propósitos y principios rectores de la ciberseguridad en España
Purpose and guiding principles of cyber security in Spain

+

6 objetivos de ciberseguridad
6 Objectives of cyber security

=

8 líneas de acción de la Ciberseguridad Nacional
8 Lines of action of National cyber security

Líneas de acción para la Ciberseguridad Nacional
Lines of action for National cyber security

1. Capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas.
   Increase prevention, defence, detection, analysis, response, recovery and coordination capabilities vis-à-vis cyber threats.
2. Seguridad de los Sistema de Información y Telecomunicaciones que soportan las Administraciones Públicas.
   Security of the Information Systems of Public Administrations.
3. Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Infraestructuras Críticas.
   Foster the implementation of the regulations on the Protection of Critical Infrastructures and of the necessary capabilities for protecting essential services.
4. Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia.
   Strengthen capabilities to detect, investigate and prosecute terrorist and criminal activities in cyberspace on the basis of an effective legal and operational framework.
5. Seguridad y resiliencia de las TIC en el sector privado.
   Security and resilience of ICT in the private sector.
6. Conocimientos,Competencias e I+D+i.
   Knowledge, skills and R&D&I.
7. Cultura de ciberseguridad.
   Cyber security culture.
8. Compromiso internacional.
   International cooperation.

Objetivos de Ciberseguridad Nacional
Objectives for National cyber security

Objetivo Global
Overall Objective

Lograr que España haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección, y respuesta a los ciberataques.

To ensure that Spain uses Information and Telecommunications Systems securely by strengthening prevention, defense, detection and response capabilities vis-à-vis cyber attacks.

Objetivos específicos 6
Specific Objectives 6

- Administraciones Públicas
  Public Administration
- Empresas e Infraestructuras Críticas
  Companies and Critical Infrastructure
- Ciberterrorismo y cibercrimen
  Cyberterrorism and Cybercrime
- Colaboración internacional
  International Collaboration
- I+D+i en ciberseguridad
  R&D&I in Cyber Security
- Sensibilización
  Awareness

Consejo Nacional de Ciberseguridad
National Cyber Security Council

- Presidencia: Mº de la Presidencia. Centro Nacional de Inteligencia
  Ministry of the Presidency. National Intelligence Centre (Presidency)
- Vicepresidencia: Departamento de Seguridad Nacional. Oficina del Presidente del Gobierno
  National Security Department Prime Minister´s Office (Vice)
- Vicepresidencia: Ministerio de Hacienda y Administraciones Públicas
  Ministry of Finance and Public Administrations (Vice)
- Secretaría: Departamento de Seguridad Nacional. Oficina del Presidente del Gobierno
  National Security Department Prime Minister´s Office (Secretariat)
- Ministerio de Asuntos Exteriores y Cooperación
  Ministry of Foreing Affairs
- Ministerio de Defensa
  Ministry of Defence
- Ministerio del Interior
  Ministry of Interior
- Ministerio de Industria, Energía y Turismo
  Ministry of Industry, Energy and Tourism
- Ministerio de Educación, Cultura y Deporte
  Ministry of Education
- Centro Nacional de Inteligencia
  National Intelligence Centre
- Ministerio de Economía y Competitividad
  Ministry of Economy
- Ministerio de Empleo y Seguridad Social
  Ministry of Employment and Social Security
- Ministerio de Fomento
  Ministry of Development
- Ministerio de Justicia
  Ministry of Justice
- Departamento de Seguridad Nacional. Oficina del Presidente del Gobierno
  National Security Department Prime Minister´s Office

Consejo Nacional de Ciberseguridad
National Cyber Security Council

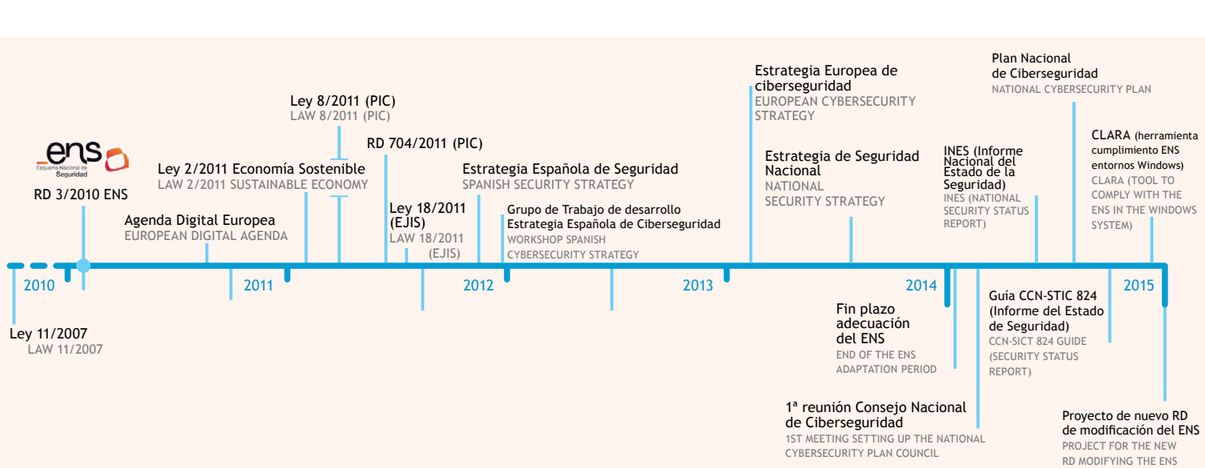
5.2 Esquema Nacional de Seguridad (ENS)

El Centro Cripotológico Nacional, en colaboración con el Ministerio de Hacienda y Administraciones Públicas (MINHAP), participó activamente en el desarrollo e implantación del Esquema Nacional de Seguridad (ENS) regulado por el Real Decreto 3/2010, de 8 de enero (BOE de 29 de enero).

Desde su entrada en vigor, han sido numerosas las acciones emprendidas por el CCN para la adecuación de los sistemas de las Administraciones Públicas a dicho Esquema. Entre otras medidas se encuentra la publicación de **30 Guías CCN-STIC** (dentro de la serie 800) que sirven de marco de referencia en esta materia, así como el desarrollo de diferentes herramientas de seguridad que facilitan la adecuación al ENS (*véase **CLARA**, **INES** y **PILAR** en el apartado de Herramientas del CCN-CERT*).

En estos momentos, y una vez que el plazo de adecuación concluyera el 30 de enero de 2014, se encuentra en trámite parlamentario un Real Decreto que modifique el anterior en el que se mejora todo lo relativo a la ciberseguridad, incluyendo, por supuesto, la Administración Electrónica.

El cambio de la naturaleza jurídica del conjunto de guías CCN-STIC serie 800, pasando de meras recomendaciones a **Instrucciones Técnicas de Seguridad** de obligado cumplimiento, así como la obligatoriedad de notificar los ciberincidentes que tengan un impacto significativo en los organismos, son algunas de las cuestiones que recogerá el nuevo RD.



5.2 National Security Scheme (ENS)

The National Cryptologic Centre participated actively in developing and implanting the National Security Scheme (ENS) and Royal Decree 3/2010, dated 8th January (BOE dated 29th January) regulating it.

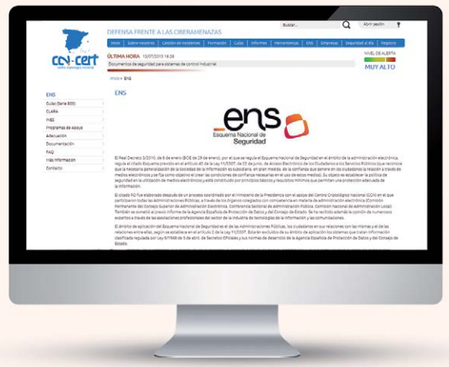
Since it came into force, numerous actions have been undertaken by the CCN to adapt the Public Administration's systems to this Framework. Other measures include publishing **30 CCN-SICT guides** (within the 800 series) that are used as a reference framework for this matter, as well as developing different security tools that make it easier to adapt to the ENS (*see **CLARA**, **INES** and **PILAR** in the CCN-CERT Tools section*).

Right now, and once the adaptation period finishes on 30th January 2014, there will be a Royal Decree being processed through parliament that modifies the previous decree, improving everything related to cybersecurity, including Electronic Administration of course.

The change in the legal nature of the set of CCN-SICT 800 series guides passing from mere recommendations to **Technical Security Instructions** that must be met, such as the obligation to report cyber-incidents that have a significant impact on the organisations, are some of the matters compiled in the new RD.

Marco normativo que regula la actuación del CCN
STANDARD FRAMEWORK REGULATING CCN ACTIONS

Normativa STANDARDS	Función FUNCTION
Ley 11/2002 reguladora del Centro Nacional de Inteligencia LAW 11/2002 REGULATING THE NATIONAL INTELLIGENCE CENTRE	- Inteligencia y contrainteligencia. Defensa del Patrimonio Tecnológico español. - Autoridad Nacional de Seguridad Delegada(protección de sistemas información clasificada, tanto nacional como internacional). - INTELLIGENCE AND COUNTER-INTELLIGENCE. DEFENCE OF SPANISH TECHNOLOGICAL PATRIMONY - NATIONAL DELEGATED SECURITY AUTHORITY (PROTECTION OF CLASSIFIED INFORMATION SYSTEMS, BOTH NATIONAL AND INTERNATIONAL)
R.D. 421/2004 Centro Criptológico Nacional R.D. 421/2004 NATIONAL CRYPTOLOGIC CENTRE	- Garantizar la seguridad TIC en Administración - GUARANTEE ICT SECURITY IN ADMINISTRATION
R.D. 3/2010 Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica R.D. 3/2010 NATIONAL SECURITY SCHEME IN THE ELECTRONIC ADMINISTRATION FIELD	- CERT Gubernamental Nacional español - Gestión de ciberincidentes que afecten a sistemas clasificados, de las Administraciones Públicas y de empresas y organizaciones de interés estratégico para el país. - SPANISH GOVERNMENT CERT - MANAGEMENT OF CYBER-INCIDENTS THAT AFFECT CLASSIFIED SYSTEMS, FOR PUBLIC ADMINISTRATIONS AND BUSINESSES AND ORGANISATIONS OF STRATEGIC INTEREST FOR THE COUNTRY.
Orden PRE/2740/2007 del Reglamento de Evaluación y Certificación de las Tecnologías de la Información ORDER PRE/2740/2007 OF THE REGULATION FOR EVALUATION AND CERTIFICATION OF INFORMATION TECHNOLOGIES	- Organismo de Certificación del Esquema Nacional de Evaluación y Certificación TIC - CERTIFICATION BODY FOR THE NATIONAL EVALUATION SCHEME AND ICT CERTIFICATION
Estrategia de Ciberseguridad Nacional 2013 NATIONAL CYBERSECURITY STRATEGY 2013	- Presidencia del Consejo Nacional de Ciberseguridad por parte del secretario de Estado director del CNI-CCN - PRESIDENCY OF THE NATIONAL CYBERSECURITY COUNCIL BY THE SECRETARY OF STATE-DIRECTOR OF THE CNI



6 Funciones del CCN
CCN functions

Las funciones desarrolladas por el Centro Criptológico Nacional están reguladas en la distinta normativa citada anteriormente. Entre otras, comprende:

- Elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los Sistemas de las Tecnologías de la Información y las Comunicaciones (STIC) de la Administración.
- Formar al personal de la Administración especialista en el campo de la seguridad de los Sistemas de las Tecnologías de la Información y las Comunicaciones.
- Constituir el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de Información, de aplicación a productos y sistemas en su ámbito
- Valorar y acreditar la capacidad de los productos de cifra y de los sistemas de las Tecnologías de la Información, que incluyan medios de cifra, para procesar, almacenar o transmitir información de forma segura.
- Coordinar la promoción, el desarrollo, la obtención, la adquisición y puesta en explotación y la utilización de la tecnología de seguridad de los sistemas mencionados.
- Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en su ámbito de competencia, para evitar el acceso a ésta de individuos, grupos y Estados no autorizados.
- Establecer las relaciones necesarias y firmar los acuerdos pertinentes con organizaciones similares de otros países y nacionales.
- Contribuir a la mejora de la ciberseguridad en España articulando la respuesta y gestión de incidentes, en torno al CCN-CERT.

The functions assigned to the CCN, regulated by different rules cited above, are:

• Drawing up and disseminating standards, instructions, guides and recommendations to guarantee security for the Administration's information and communication technology systems.

• Training Administration staff specialising in the sphere of security for information and communication technology systems.

• Setting up the Certification Body for the National Evaluation and Certification Scheme and certification of information technology security, to be applied to products and systems in its field.

• Assessing and accrediting the capacity of encryption products and information technology systems that include encryption devices to process, store or send out information securely.

• Coordinating promotion, development, obtaining, purchasing and operating plus the use of security technology for the aforementioned systems.

• Making sure that standards are met relating to protecting classified information in its field of competence.

• Establishing the necessary relationships and signing relevant agreements with similar organisations from other countries to develop the aforementioned functions.

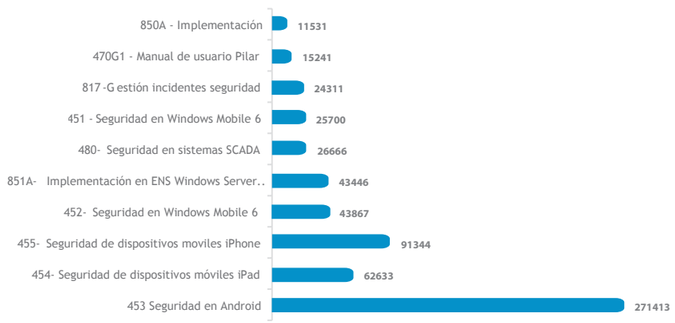
• Helping to improve cybersecurity in Spain, organising how to tackle and manage cyberincidents around the CCN-CERT.

6.1 Guías CCN-STIC

A finales de 2014 existían un total de **250 documentos** enmarcados en alguna de las nueve series CCN-STIC (la **serie 800**, de acceso público, se elaborada en colaboración con el **Ministerio de Hacienda y Administraciones Públicas)**, de las cuales 79 fueron nuevas o actualizadas entre 2013 y 2014 (35 el primer año y 44 el segundo).

El éxito de estos documentos, como material de consulta y ayuda en materia de ciberseguridad, queda reflejada en el número de descargas tanto de las Guías reservadas a los usuarios registrados del portal del CCN-CERT, como las que son de acceso público. En total, se **descargaron 649.250 veces** alguna de las 250 Guías CCN-STIC. De ellas, 640.454 correspondieron a las guías de acceso público.

A finales de 2014 existían un total de 250 documentos enmarcados en alguna de las nueve series CCN-STIC, de las cuales 79 fueron nuevas o actualizadas entre los años 2013 y 2014



Guías de acceso público más descargadas del portal del CCN-CERT en 2014
MOST DOWNLOADED GUIDES PUBLIC ACCESS CCN-CERT PORTAL IN 2014

6.1 CCN-STIC Guides

By the end of 2014 there were **250 documents** within the CCN-STIC series (the CCN-STIC **800 series**, drawn up in collaboration with the Ministry of the Finance and Public Administrations). Of these, 79 have been drawn up or updated over the last two (35 the first year and 44 the second).

The success of these documents as reference material and help on cybersecurity, is reflected in the number of downloads. In total, they downloaded **649 250 times**. Of these, 640 454 were for public access guidelines.

By the end of 2014 there were 250 documents within the CCN-STIC series, of these, 79 have been drawn up or updated over the last two

Listado de Guías CCN-STIC 2015
List of CCN-STIC guides 2015

* Difusión limitada / LIMITED DIFUSSION
** Confidencial / CONFIDENTIAL

Cumple con el ENS / COMPLIES WITH ENS
Adaptables al ENS / ADAPTED TO ENS
Pendientes de publicar / PENDING PUBLICATION

Serie 000: Políticas / SERIE 000: POLICIES

0 01	Seguridad de las TIC en la Administración ICT SECURITY IN THE PUBLIC ADMINISTRATION	AGO-13
002	Coordinación Criptológica CRYPTOLOGIC COORDINATION	MAR 11
003**	Uso de Cifradores Certificados USE OF CERTIFIED CIPHER EQUIPMENT	MAY 13

Serie 100: Procedimientos / SERIE 100: PROCEDURE

101	Procedimiento de Acreditación Nacional NATIONAL ACCREDITATION PROCEDURE	NOV 12
102*	Procedimiento de evaluación de productos criptológicos CRYPTOLOGIC PRODUCTS EVALUATION PROCEDURE	
103*	Catálogo de Productos Certificados CERTIFIED PRODUCTS CATALOGUE	MAY 13
104	Catálogo de Productos con clasificación Zoning ZONING PRODUCTS CLASIFICATION CATALOGUE	ENE 13
150**	Evaluación y Clasificación TEMPEST de Cifradores con Certificación Criptológica TEMPEST EVALUATION AND CLASSIFICATION OF EQUIPMENT WITH CRYPTOLOGIC CERTIFICATION	DIC 06
151*	Evaluación y Clasificación TEMPEST de Equipos TEMPEST EVALUATION AND CLASSIFICATION OF EQUIPMENT	DIC 06
152*	Evaluación y Clasificación ZONING de Locales FACILITY ZONING, EVALUATION AND CLASSIFICATION	DIC 06
153	Evaluación y Clasificación de Armarios Apantallados EVALUATION AND CLASSIFICATION OF SHIELDED CABINETS	FEB 10
154*	Medidas de protección TEMPEST para instalaciones PROTECTION TEMPEST MEASURES FOR FACILITIES	NOV 11

Serie 200: Norma / SERIE 200: STANDARDS

201	Estructura de Seguridad SECURITY ORGANIZATION	ENE 09
202	Estructura y Contenido DRS SSRS. STRUCTURE AND CONTENT	MAR 05
203	Estructura y Contenido POS SECOPS. STRUCTURE AND CONTENT	MAR 05
204	CO-DRES-POS Pequeñas Redes CONCEPT OF OPERATION, SSRS AND SECOPS FOR LITTLE NETWORKS	ENE 09
205	Actividades Seguridad Ciclo Vida CIS SECURITY LIFE CYCLE ACTIVITIES (CIS)	DIC 07
207	Estructura y Contenido del Concepto de Operación CONCEPT OF OPERATION. STRUCTURE AND CONTENT	NOV 05
210*	Norma de Seguridad en las Emanaciones TEMPEST/ Safety Estándar SAFETY STANDARD TEMPEST EMANATIONS	JUL 12

Serie 300: Instrucciones Técnicas / SERIE 300: TECHNICAL INSTRUCTIONS

301*	Requisitos STIC IT SECURITY REQUIREMENTS	DIC 07
302*	Interconexión de CIS CIS SYSTEMS INTERCONNECTION	JUL 12
303*	Inspección STIC IT SECURITY INSPECTION	ENE 09
304	Baja y Destrucción de Material Criptológico DESTRUCTING AND TAKING CRYPTOLOGIC MATERIAL OUT OF CIRCULATION	MAR 11
305*	Destrucción y Sanitización de Soportes MEDIA SANITIZATION AND DESTRUCTION	JUL 13
307*	Seguridad en Sistemas Multifunción SECURITY IN MULTIFUNCTION SYSTEMS	ENE 09

Serie 400: Guías Generales / SERIE 400: GENERAL GUIDES

400	Manual STIC ICT SECURITY MANUAL	MAY 13
401	Glosario / Abreviaturas GLOSSARY / ABBREVIATIONS	AGO 13
402	Organización y Gestión STIC ICT SECURITY ORGANIZATION AND MANAGEMENT	DIC 06
403	Gestión de Incidentes de Seguridad SECURITY INCIDENTS MANAGEMENT	DIC 07
404	Control de Soportes Informáticos COMPUTING DEVICES CONTROL	DIC 06
405	Algoritmos y Parámetros de Firma Electrónica ELECTRONIC SIGNATURE: ALGORITHMS AND PARAMETERS	FEB 12
406	Seguridad en Redes Inalámbricas WIRELESS SECURITY	JUL 13
407	Seguridad en Telefonía Móvil MOBILE PHONE SECURITY	DIC 06
408	Seguridad Perimetral - Cortafuegos PERIMETER SECURITY - FIREWALLS	MAR 10
409A**	Colocación de Etiquetas de Seguridad SECURITY LABELS	MAY 13
409B**	Colocación de Etiquetas de Seguridad en Equipos de Cifra SECURITY LABELS	MAY 13
410	Análisis de Riesgos en Sistemas de la Administración RISK ANALYSIS IN THE ADMINISTRATION	DIC 06
411*	Modelo de Plan de Verificación STIC PLAN MODEL OF ICT SECURITY VERIFICATION	ENE 09
412	Requisitos de Seguridad en Entornos y Aplicaciones Web SECURITY REQUIREMENTS FOR ENVIRONMENTS AND WEB APPLICATIONS	ENE 09
413	Auditoría de Entornos y Aplicaciones Web AUDIT ENVIRONMENTS AND WEB APPLICATIONS	
414	Seguridad en Voz sobre IP VOIP SECURITY	ENE 09
415	Identificación y Autenticación Electrónica ELECTRONIC IDENTIFICATION AND AUTHENTICATION	DIC 07
416	Seguridad en VPN,s VPN SECURITY	DIC 07
417	Seguridad en PABX PABX SECURITY	MAY 10
418	Seguridad en Bluetooth BLUETOOTH SECURITY	ENE 09
419	Configuración Segura con IPtables SECURE CONFIGURATION WITH IPTABLES	DIC 07
420	Test de penetración PENTEST	
421	Copias de seguridad y recuperación ante desastres BACKUP AND DISASTER RECOVERY	
422	Desarrollo seguro de aplicaciones web SECURE DEVELOPMENT OF WEB APPLICATIONS	JUL 13
423	Indicadores de Compromiso (IOC) INDICATORS OF COMMITMENT (IOC)	JUL 13
425	Seguridad en IP versión 6 IP 6 SECURITY	
430	Herramientas de Seguridad SECURITY TOOLS	ENE 09
431	Herramientas de Análisis de Vulnerabilidades TOOLS FOR VULNERABILITIES EVALUATION	DIC 06
432	Seguridad Perimetral - IDS PERIMETER SECURITY - INTRUSION DETECTION SYSTEMS	ENE 09
434	Herramientas para el Análisis de Ficheros de Logs TOOLS FOR LOG FILES ANALYSIS	JUN 09

* Difusión limitada
LIMITED DIFUSSION

** Confidencial
CONFIDENTIAL

Cumple con el ENS
COMPLIES WITH ENS

Adaptables al ENS
ADAPTED TO ENS

Pendientes de publicar
PENDING PUBLICATION

435	Herramientas de Monitorización de Tráfico TOOLS FOR DATA FLOW MONITORING	DIC-12
436	Herramientas de Análisis de Contraseñas PASSWORD ANALYSIS TOOLS	DIC 07
437	Herramientas de Cifrado Software ENCRYPTED SOFTWARE TOOLS	DIC 07
438	Esteganografía STEGANOGRAPHIA	SEP 11
440	Mensajería Instantánea INSTANT MESSAGING	DIC 07
441	Configuración Segura de VMWare SECURE CONFIGURATION OF VMWARE	ENE 10
442	Seguridad en VMWare ESXi VMWARE ESXI SECURITY	
443	RFID RFID	ENE 09
444	Seguridad en WiMAX WIMAX SECURITY	MAR 11
445A	Curso de Especialidades Criptológicas (correspondencia) - Probabilidad CRYPTOLOGIC SPECIALISED COURSE (CEC) - PROBABILITY	JUL 10
445B	Curso de Especialidades Criptológicas (correspondencia) - Principios digitales CSC- DIGITAL PRINCIPLES	JUL 10
445C	Curso de Especialidades Criptológicas (correspondencia) - Teoría de números CEC - NUMBERS THEORY	JUL 10
450	Seguridad en Dispositivos Móviles SECURITY ON MOBILE DEVICES	MAY 13
451	Seguridad en Windows Mobile 6.1 SECURITY ON WINDOWS MOBILE 6.1	MAY 13
452	Seguridad en Windows Mobile 6.5 SECURITY ON WINDOWS MOBILE 6.5	MAY 13
453	Seguridad en Android 2.1 SECURITY IN ANDROID	MAY 13
454	Seguridad en iPad SECURITY IN IPAD	JUL 14
455	Seguridad en iPhone SECURITY IN IPHONE	JUL 14
456	Seguridad en entornos BES BES SECURITY ENVIROMENTS	
457	Herramientas de gestión de dispositivos móviles: MDM MOBILE DEVICE MANAGEMENT TOOL	NOV 13
460	Seguridad en WordPress WORDPRESS SECURITY	
470A	Manual de la Herramienta de Análisis de Riesgos PILAR 4.1 RISK ANALYSIS TOOL MANUAL PILAR 4.1	DIC 07
470B	Manual de la Herramienta de Análisis de Riesgos PILAR 4.3 RISK ANALYSIS TOOL MANUAL PILAR 4.3	DIC 08
470C	Manual de la Herramienta de Análisis de Riesgos PILAR 4.4 RISK ANALYSIS TOOL MANUAL PILAR 4.4	FEB 10
470D	Manual de la Herramienta de Análisis de Riesgos PILAR 5.1 RISK ANALYSIS TOOL MANUAL PILAR 5.1	MAY 11
470E1	Manual de la Herramienta de Análisis de Riesgos PILAR 5.2 RISK ANALYSIS TOOL MANUAL PILAR 5.2	JUL 12
470E2	Manual de la Herramienta de Análisis de Riesgos PILAR 5.2. Análisis del Impacto y Continuidad del Negocio. RISK ANALYSIS TOOL MANUAL PILAR 5.2 IMPACT ANALYSIS AND BUSINESS CONTINUITY	JUL 12
470F1	Manual de la Herramienta de Análisis de Riesgos PILAR 5.3 RISK ANALYSIS TOOL MANUAL PILAR 5.3	NOV 13
470F2	Manual de la Herramienta de Análisis de Riesgos PILAR 5.3. Análisis del Impacto y Continuidad del Negocio. RISK ANALYSIS TOOL MANUAL PILAR 5.3 IMPACT ANALYSIS AND BUSINESS CONTINUITY	NOV 13
470G1	Manual de la Herramienta de Análisis de Riesgos PILAR 5.4 RISK ANALYSIS TOOL MANUAL PILAR 5.3	AGO 14
470G2	Manual de la Herramienta de Análisis de Riesgos PILAR 5.4. Análisis del Impacto y Continuidad del Negocio. RISK ANALYSIS TOOL MANUAL PILAR 5.3 IMPACT ANALYSIS AND BUSINESS CONTINUITY	AGO 14
471B	Manual de Usuario de RMAT 4.3 HANDBOOK FOR RMAT 4.3	DIC 08
471C	Manual de Usuario de RMAT 5.1 HANDBOOK FOR RMAT 5.1	AGO 11
471D	Manual de Usuario de RMAT 5.4 HANDBOOK FOR RMAT 5.1	AGO 14
472A	Manual de la Herramienta de Análisis de Riesgos PILAR BASIC 4.3 RISK ANALYSIS TOOL MANUAL PILAR BASIC V.4.3	DIC 08
472B	Manual de la Herramienta de Análisis de Riesgos PILAR BASIC 4.4 RISK ANALYSIS TOOL MANUAL PILAR BASIC V.4.4	FEB 10
472C	Manual de la Herramienta de Análisis de Riesgos PILAR BASIC 5.2 RISK ANALYSIS TOOL MANUAL PILAR BASIC 5.2	JUL 12
472D	Manual de la Herramienta de Análisis de Riesgos PILAR BASIC 5.3 RISK ANALYSIS TOOL MANUAL PILAR BASIC 5.3	NOV 13
472E	Manual de la Herramienta de Análisis de Riesgos PILAR BASIC 5.4 RISK ANALYSIS TOOL MANUAL PILAR BASIC 5.4	AGO 14
473A	Manual de la Herramienta de Análisis de Riesgos µPILAR RISK ANALYSIS TOOL MANUAL (MPILAR)	MAR 11
473B	Manual de la Herramienta de Análisis de Riesgos µPILAR 5.2 RISK ANALYSIS TOOL MANUAL MPILAR 5.2	JUL 12
473C	Manual de la Herramienta de Análisis de Riesgos µPILAR 5.3 RISK ANALYSIS TOOL MANUAL MPILAR 5.3	NOV 13
473D	Manual de la Herramienta de Análisis de Riesgos µPILAR 5.4 RISK ANALYSIS TOOL MANUAL MPILAR 5.4	AGO 14
480	Seguridad en Sistemas SCADA SECURITY ON SCADA SYSTEMS	MAR 10
480A	Seguridad en Sistemas SCADA - Guía de Buenas Prácticas SCADA- BEST PRACTICES	FEB 10
480B	Seguridad en Sistemas SCADA - Comprender el Riesgo del Negocio SCADA- UNDERSTANDING BUSINESS RISKS	MAR 10
480C	Seguridad en Sistemas SCADA - Implementar una Arquitectura Segura SCADA- IMPLEMENTING SECURE ARCHITECTURE	MAR 10
480D	Seguridad en Sistemas SCADA - Establecer Capacidades de Respuesta SCADA- ESTABLISHING RESPONSE CAPABILITIES	MAR 10
480E	Seguridad en Sistemas SCADA - Mejorar la Concienciación y las Habilidades SCADA IMPROVING AWARENESS AND CAPABILITIES	ENE 10
480F	Seguridad en Sistemas SCADA - Gestionar el Riesgo de Terceros SCADA- DEALING WITH RISKS DERIVED FROM THIRD PARTIES	MAR 09
480G	Seguridad en Sistemas SCADA - Afrontar Proyectos SCADA- CONFRONT PROJECTS	MAR 09
480H	Seguridad en Sistemas SCADA - Establecer una Dirección Permanente SCADA - ESTABLISHING A PERMANENT ADDRESS	MAR 10
490	Dispositivos Biométricos de Huella Dactilar BIOMETRIC FINGERPRINTS DEVICES	DIC 07
491	Dispositivos Biométricos de Iris IRIS BIOMETRIC DEVICES	DIC 08
492	Evaluación de Parámetros de Rendimiento en Dispositivos Biométricos EVALUATION OF PERFORMANCE PARAMETERS IN BIOMETRIC DEVICES	MAR 11

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

501A	Seguridad en Windows XP SP2 (cliente en dominio) WINDOWS XP SP2 SECURITY (CLIENT WITHIN A DOMAIN)	DIC 07
501B	Seguridad en Windows XP SP2 (cliente independiente) WINDOWS XP SP2 SECURITY (INDEPENDENT CLIENT)	DIC 07
502	Seguridad en Aplicaciones Cliente. Navegador y Correo Electrónico CLIENT WINDOWS SECURITY: BROWSER AND E-MAIL	DIC 08
502B	Seguridad en Aplicaciones Cliente Windows Vista. Navegador y Correo Electrónico CLIENT WINDOWS VISTA SECURITY. BROWSER AND E-MAIL	ENE 10
503A	Seguridad en Windows 2003 Server (controlador de dominio) WINDOWS 2003 SERVER SECURITY (DOMAIN CONTROLLER)	NOV 05
503B	Seguridad en Windows 2003 Server (servidor independiente WINDOWS 2003 SERVER SECURITY (INDEPENDENT SERVER)	DIC 07
504	Seguridad en Internet Information Server INTERNET INFORMATION SERVER SECURITY	OCT 05
505	Seguridad en Bases de Datos SQL 2000 BD SQL SECURITY	DIC 06
506	Seguridad en Microsoft Exchange Server 2003 MS EXCHANGE SERVER 2003 SECURITY	JUN 07
507	Seguridad en ISA Server ISA SERVER SECURITY	DIC 06
508	Seguridad en Clientes Windows 2000 WINDOWS 2000 CLIENTS SECURITY	DIC 07
509	Seguridad en Windows 2003 Server. Servidor de Ficheros SECURITY ON WINDOWS 2003 SERVER. FILE SERVER	DIC 07
510	Seguridad en Windows 2003 Server. Servidor de Impresión SECURITY ON WINDOWS 2003 SERVER. PRINTING SERVER	ENE 09
512	Gestión de Actualizaciones de Seguridad en Sistemas Windows SECURITY UPDATES MANAGEMENT	DIC 05
515	Seguridad Servidor de Impresión en Windows 2008 Server R2 PRINT SERVER IN WINDOWS 2008 SERVER R2 SECURITY	
517A	Seguridad en Windows Vista (cliente en dominio) WINDOWS VISTA SECURITY (CLIENT WITHIN A DOMAIN)	ENE 10
517B	Seguridad en Windows Vista (cliente independiente) WINDOWS VISTA SECURITY (INDEPENDENT CLIENT)	ENE 09
519A	Configuración Segura del Internet Explorer 7 y Outlook en Windows XP SECURE CONFIGURATION OF INTERNETEXPLORER 7 AND OUTLOOK IN WINDOWS XP	ENE 10
520	Configuración Segura de Internet Explorer 11 SECURE CONFIGURATION OF INTERNET EXPLORER 11	FEB 15
521A	Seguridad en Windows 2008 Server (controlador de dominio) WINDOWS 2008 SERVER SECURITY (DOMAIN CONTROLLER)	MAY 14
521B	Seguridad en Windows 2008 Server (servidor independiente) WINDOWS 2008 SERVER SECURITY (INDEPENDENT SERVER)	AGO 10
521C	Seguridad en Windows 2008 Server Core (controlador de dominio) WINDOWS 2008 SERVER CORE SECURITY (DOMAIN CONTROLLER)	MAY 14
521D	Seguridad en Windows 2008 Server Core (servidor independiente) WINDOWS 2008 SERVER CORE SECURITY (INDEPENDENT SERVER)	JUN 13
522A	Seguridad en Windows 7 (cliente en dominio) WINDOWS 7 SECURITY (DOMAIN CLIENT)	JUN 11
522B	Seguridad en Windows 7 (cliente independiente) WINDOWS 7 SECURITY (INDEPENDENT CLIENT)	NOV 10
523	Seguridad en Windows 2008 Server. Servidor de Ficheros. WINDOWS 2008 SERVER SECURITY. FILE SERVER	FEB 12
524	Seguridad en Internet Information Server (IIS) 7.5 INTERNET INFORMATION SERVER 7.5 SECURITY	FEB 14
525	Seguridad en Microsoft Exchange Server 2007 sobre Windows 2003 Server MICROSOFT EXCHANGE SERVER 2007 ON WINDOWS 2003 SECURITY	JUN 13
526	Seguridad en Microsoft Exchange Server 2007 sobre Windows 2008 Server MICROSOFT EXCHANGE SERVER 2007 ON WINDOWS 2008 SECURITY	AGO 13
527	Failover Clustering para Windows 2008 Server R2 FAILOVER CLUSTERING PARA WINDOWS 2008 SERVER R2	AGO 13
528	Seguridad en Hyper-V sobre Windows 2008 Server R2 Core HYPER-V WINDOWS 2008 SEVER R2 CORE SECURITY	DIC 13
526	Seguridad en Microsoft Office 2013 SEGURIDAD EN MICROSOFT OFFICE 2013	FEB 15
530	Seguridad en Microsoft Office 2010 SEGURIDAD EN MICROSOFT OFFICE 2010	JUL 13
531	Seguridad en Sharepoint Server 2007 SHAREPOINT SERVER SECURITY 2007	DIC 12
532	Seguridad en Microsoft Sharepoint Server 2007 sobre Windows Server 2008 R2 MICROSOFT SHAREPOINT SERVER 2007 ON WINDOWS SERVER 2008 R2 SECURITY	
533	Seguridad en Microsoft Sharepoint Server 2010 sobre Windows Server 2008 R2 MICROSOFT SHAREPOINT SERVER 2010 ON WINDOWS SERVER 2008 R2 SECURITY	
540	Seguridad en Bases de Datos SQL Server 200 DATABASE SQL SERVER 2000 SECURITY	ABR 14
550	Seguridad en Microsoft Exchange Server 2010 sobre Windows Server 2008 R2 MICROSOFT EXCHANGE SERVER 2010 ON WINDOWS SERVER 2008 R2 SECURITY	SEP 14
560A	Seguridad en Windows 2012 Server R2 (controlador de dominio) WINDOWS 2012 SERVER R2 (DOMAIN CONTROLLER) SECURITY	MAR 15
560B	Seguridad en Windows 2012 Server R2 (servidor independiente) WINDOWS 2012 SERVER R2 (INDEPENDENT SERVER) SECURITY	MAY 15
590	Recolección y consolidación de eventos con Windows Server 2008 R2 COLLECTIONS AND CONSOLIDATION OF EVENTS IN WINDOWS SERVER 2008 R2	ABR 14
596	AppLocker APPLOCKER	

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

601	Seguridad en HP-UX v 10.20 HP-UX V 10.20 SECURITY	DIC 06
602	Seguridad en HP-UX 11i HP-UX 11I SECURITY	OCT 04
603	Seguridad en AIX-5L AIX-5L SECURITY	MAR 11
610	Seguridad en Red Hat Linux 7 RED HAT LINUX 7 SECURITY	DIC 06
611	Seguridad en Suse Linux SUSE LINUX SECURITY	DIC 06

* Difusión limitada
LIMITED DIFUSSION

** Confidencial
CONFIDENTIAL

Cumple con el ENS
COMPLIES WITH ENS

Adaptables al ENS
ADAPTED TO ENS

Pendientes de publicar
PENDING PUBLICATION

612	Seguridad en sistemas basados en Debian DEBIAN SECURITY	AGO 14
614	Seguridad en Red Hat Linux (Fedora) RED HAT LINUX (FEDORA) SECURITY	DIC 06
615	Seguridad en Entornos basados en Redhat SECURITY ON REDHAT-BASED ENVIRONMENTS	
621	Seguridad en Sun Solaris 8.0 SUN-SOLARIS 8.0 SECURITY	JUL 04
622	Seguridad en Sun Solaris 9.0 para Oracle 8.1.7 SUN-SOLARIS 9.0 SECURITY FOR ORACLE 8.1.7	DIC 06
623	Seguridad en Sun Solaris 9.0 para Oracle 9.1 SUN-SOLARIS 9.0 SECURITY FOR ORACLE 9.I	DIC 06
624	Seguridad en Sun Solaris 9.0 para Oracle 9.2 SUN-SOLARIS 10 SECURITY FOR ORACLE 9.2	DIC 06
625	Seguridad en Sun Solaris 10g ORACLE 10G | SUN-SOLARIS 10 SECURITY FOR ORACLE 10G	MAR 10
626	Guía de Securización de Sun Solaris 10 con NFS SECURITY GUIDE FOR SUN SOLARIS 10 WITH NFS	DIC 07
627	Guía de Securización de Sun Solaris 9 con Workstation SECURITY GUIDE FOR SUN SOLARIS 9 WITH WORKSTATION	DIC 07
628	Guía de Securización de Sun Solaris 9 con NFS SECURITY GUIDE FOR SUN SOLARIS 9 WITH NFS	DIC 07
629	Guía de Securización de Sun Solaris 10 con Workstation SECURITY GUIDE FOR SUN SOLARIS 10 WITH WORKSTATION	DIC 07
631	Seguridad en Base de Datos Oracle 8.1.7 sobre Solaris SECURITY FOR DB ORACLE 8.1.7 ON SOLARIS	SEP 05
632	Seguridad en Base de Datos Oracle 11g sobre Suse Linux Enterprise Server 11 SECURITY FOR DB ORACLE 11G ON SUSE LINUX ENTERPRISE SERVER	
633	Seguridad en Base de Datos Oracle 9i sobre Red Hat 3 y 4 SECURITY FOR DB ORACLE 9I ON RED HAT 3 Y 4	DIC 07
634	Seguridad en Base de Datos Oracle 9i sobre Solaris 9 y 10 SECURITY FOR DB ORACLE 9I ON SOLARIS 9 Y 10	DIC 07
635	Seguridad en Base de Datos Oracle 9i sobre HP-UX 11i SECURITY FOR DB ORACLE 9I ON HP-UX 11I	DIC 07
636	Seguridad en Base de Datos Oracle 10gR2 sobre Red Hat 3 y 4 SECURITY FOR DB ORACLE 10GR2 ON RED HAT 3 Y 4	DIC 07
637	Seguridad en Base de Datos Oracle 10gR2 sobre Solaris 9 y 10 SECURITY FOR DB ORACLE 10GR2 ON SOLARIS 9 Y 10	DIC 07
638	Seguridad en Base de Datos Oracle 10gR2 sobre HP-UX 11i SECURITY FOR DB ORACLE 10GR2 ON HP-UX 11I	DIC 07
639	Seguridad en Base de Datos Oracle 10g sobre Windows 2003 Server SECURITY FOR DB ORACLE 10G ON WINDOWS 2003 SERVER	AGO 10
641	Seguridad en Equipos de Comunicaciones. Router Cisco ROUTERS CISCO | SECURITY FOR COMMUNICATION EQUIPMENT. ROUTERS CISCO	NOV 13
642	Seguridad en Equipos de Comunicaciones. Switches Enterasys SECURITY FOR COMMUNICATION EQUIPMENT. SWITCHES ENTERASYS	DIC 06
643	Seguridad en Equipos de Comunicaciones. Allied Telesis. SECURITY FOR COMMUNICATION EQUIPMENT. ALLIED TELESIS	SEP 13
644	Seguridad en Equipos de Comunicaciones. Switches Cisco SECURITY FOR COMMUNICATION EQUIPMENT. SWITCHES CISCO	DIC 07
645	Sistemas de Gestión de Red (Cisco Works LMS) NETWORK MANAGEMENT SYSTEMS (CISCO WORKS LMS)	MAR-11
646	Seguridad en Equipos de Comunicaciones. Switches HP SECURITY FOR COMMUNICATION EQUIPMENT. SWITCHES HP	
650	Seguridad en cortafuegos Firewall security Fortigate FIREWALL SECURITY FORTIGATE	ABRIL 15
651	Seguridad en cortafuegos Firewall security Cisco ASA Cisco ASA FIREWALL SECURITY CISCO ASA	
655	Guía de Securización para Sun Solaris 9 con Oracle 10 SECURITY GUIDE FOR SUN SOLARIS 9 WITH ORACLE 10	DIC 07
656	Guía de Securización para Sun Solaris 9 con Oracle 10 y VCS 4.1 GUIDE FOR SUN SOLARIS 9 WITH ORACLE 10 AND VCS 4.1	DIC 07
660	Seguridad en Proxies PROXIES SECURITY	MAY 14
661	Seguridad en Firewalls de Aplicación APPLICATION FIREWALLS SECURITY	MAR 11
662	Seguridad en Apache Traffic Server SECURITY OF APACHE TRAFFIC SERVER	NOV 12
663	Seguridad en DNS (BIND) SECURITY OF DNS (BIND)	ABR 14
664*	Passive DNS PASSIVE DNS	MAR 14
665	Configuración segura de SSH SSH secure configuration SSH SECURE CONFIGURATION	OCT 14
671	Seguridad en Servidores Web Apache SECURITY OF WEB APACHE SERVER	DIC 06
672	Seguridad en Servidores Web Tomcat SECURITY OF WEB TOMCAT SERVER	ENE 09
673	Seguridad en Servidores Web Tomcat7 SECURITY OF TOMCAT 7 SERVER	
674	Seguridad en GlassFish 3.1 SECURITY IN GLASSFISH 3.1	ENE 13
681	Seguridad en Servidores de Correo Postfix SECURITY OF POSTFIX EMAIL SERVER	DIC 06
682	Configuración Segura de Sendmail SECURE CONFIGURATION FOR SENDMAIL	ENE 10
691	Guía de Securización de Oracle Application Server 10gR2 para Red Hat 3 y 4 SECURITY IN ORACLE APPLICATION SERVER 10GR2 FOR RED HAT 3 Y 4	DIC 07
692	Guía de Securización de Oracle Application Server 10gR2 para Solaris 9 y 10 SECURITY IN ORACLE APPLICATION SERVER 10GR2 FOR SOLARIS 9 Y 10	DIC 07
693	Guía de Securización de Oracle Application Server 10gR2 para HP-UX 11i SECURITY IN ORACLE APPLICATION SERVER 10GR2 FOR HP-UX 11I	DIC 07

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

800	Glosario de Términos y Abreviaturas GLOSSARY OF TERMS AND ABBREVIATIONS	MAR 11
801	Responsabilidades en el ENS RESPONSIBILITIES IN THE NATIONAL SECURITY SCHEME	FEB 11
802	Auditoría del Esquema Nacional de Seguridad AUDIT FOR THE NATIONAL SECURITY SCHEME	JUN 10
803	Valoración de Sistemas en el ENS SYSTEMS EVALUATION IN THE NATIONAL SECURITY SCHEME	ENE 11
804	Medias DE Implementación en el ENS IMPLEMENTATION MEASURES IN THE NATIONAL SECURITY SCHEME	MAR 13
805	Política de Seguridad de la Información INFORMATION SECURITY POLICY	SEP 11
806	Plan de Adecuación del ENS ADAPTATION PLAN IN THE NATIONAL SECURITY SCHEME	ENE 11
807	Criptología de Empleo en el ENS ENCRYPTION IN THE NATIONAL SECURITY SCHEME	NOV 12
808	Verificación del Cumplimiento de las Medidas en el ENS (BORRADOR) VERIFICATION OF COMPLIANCE WITH MEASURES ESTABLISHED BY THE NATIONAL SECURITY SCHEME	SEP 11
809	Declaración de conformidad del ENS ENS DECLARATION OF CONFORMITY	JUL 10
810	Guía de Creación de CERT,s CERTS CONSTRUCTION GUIDE	SEP 11
811	Interconexión en el ENS ENS INTERCONNECTION	NOV 12
812	Seguridad en Servicios Web en el ENS SECURITY IN ENS WEB SERVICES	OCT 11
813	Componentes Certificados en el ENS ENS COMPONENTS CERTIFICATES	FEB 12
814	Seguridad en Servicio de Correo en el ENS (BORRADOR) SECURITY IN ENS MAIL	AGO 11
815	Indicadores y Métricas en el ENS INDICATORS AND METRICS ENS	ABR 12
816	Seguridad en Redes Inalámbricas en el ENS WIRELESS NETWORK SECURITY ENS	
817	Gestión de Ciberincidentes en el ENS CYBERINCIDENT MANAGEMENT	MAR 15
818	Herramientas de seguridad en el ENS (BORRADOR) SAFETY TOOLS NATIONAL SECURITY SCHEME	OCT 12
819	Guía de contratos en el marco del ENS ENS FRAMEWORK CONTRACTS GUIDE	
820	Guía de protección contra Denegación de Servicio DDOS PROTECTION GUIDE	JUN 13
821	Ejemplos de Normas de Seguridad EXAMPLES OF SAFETY STANDARDS	ABR 13
822	Ejemplos de Procedimientos de Seguridad EXAMPLES OF SECURITY PROCEDURES	OCT 12
823	Requisitos de seguridad en entornos CLOUD (BORRADOR) SAFETY REQUIREMENTS CLOUD ENVIRONMENTS	ABR 14
824	Informe del estado de seguridad SECURITY STATUS REPORT	NOV 14
825	Certificaciones 27001 27001 CERTIFICATES	NOV 13
826	Esquema de certificación de personas PERSON CERTIFICATION SCHEMES	
827	Gestión y uso de dispositivos móviles MANAGEMENT AND USE OF MOBILE DEVICES	MAY 14
828	Borrado de metadatos en el marco del ENS DELETING METADATA IN ENS	
829	Seguridad en VPN en el marco del ENS VPN SECURITY IN ENS	
830	Seguridad en Bluetooth en el marco del ENS BLUETOOTH SECURITY IN ENS	
850A	Seguridad en Windows 7 en el ENS (cliente en dominio) WINDOWS 7 SECURITY IN ENS (CLIENT WITHIN A DOMAIN)	AGO 14
850B	Seguridad en Windows 7 en el ENS (cliente independiente) WINDOWS 7 SECURITY IN ENS (INDEPENDENT CLIENT)	OCT 14
851A	Seguridad en Windows 2008 Server R2 en el ENS (controlador de dominio) WINDOWS 2008 SERVER R2 SECURITY IN ENS (DOMAIN CONTROLLER)	AGO 14
851B	Seguridad en Windows 2008 Server R2 en el ENS (servidor independiente) WINDOWS 2008 SERVER R2 SECURITY IN ENS (INDEPENDENT SERVER)	AGO 14
859	Recolección y consolidación de eventos con Windows Server 2008 R2 en el ENS COLLECTIONS AND CONSOLIDATION OF EVENTS IN WINDOWS SERVER 2008 R2 IN ENS	ENE 15
860	Seguridad en el servicio de Outlook Web App del Microsoft Exchange Server 2010 OUTLOOK WEB APP OF MICROSOFT EXCHANGE SERVER 2010 SECURITY	JUL 15
869	AppLocker en el ENS ENS APPLOCKER	
870A	Seguridad en Windows 2012 Server R2 en el ENS (controlador de dominio) WINDOWS 2012 SERVER R2 SECURITY IN ENS (DOMAIN CONTROLLER)	
870B	Seguridad en Windows 2012 Server R2 en el ENS (servidor independiente) WINDOWS 2012 SERVER R2 SECURITY IN ENS (INDEPENDENT SERVER)	

Serie 900: Informes técnicos
SERIE 900: TECHNICAL REPORTS

903	Configuración Segura de HP-IPAQ HP-IPAQ SECURE CONFIGURATION	DIC 05
911A	Ciclo de una APT APT GEBERAL RECOMENDATIONS	
911B*	Recomendaciones generales ante un APT (BORRADOR) APT GENERAL RECOMENDATIONS	JUL 13
912	Procedimiento de investigación de código dañino MALWARE INVESTIGATION PROCEDURE	JUN 13
920	Análisis de malware con Cuckoo Sandbox ANÁLISIS DE MALWARE CON CUCKOO SANDBOX	
951	Recomendaciones de Empleo de la Herramienta Ethereal/Wireshark RECOMMENDATIONS FOR USING ETHEREAL/ WIRESHARK TOOL	DIC 06
952	Recomendaciones de Empleo de la Herramienta Nessus USAGE RECOMMENDATIONS FOR NESSUS TOOL	AGO 11
953	Recomendaciones de Empleo de la Herramienta Snort USAGE RECOMMENDATIONS FOR SNORT TOOL	JUN 09
954	Recomendaciones de Empleo de la Herramienta Nmap USAGE RECOMMENDATIONS FOR NMAP TOOL	AGO 12
955	Recomendaciones de Empleo de GnuPG USAGE RECOMMENDATIONS FOR GNUPG TOOL	DIC 07
956	Entornos Virtuales VIRTUAL ENVIRONMENTS	DIC 07
957	Recomendaciones de empleo de TrueCrypt TRUECRYPT RECOMENDATIONS	ENE 13
958*	Procedimiento de empleo Crypto Token USB CRYPTO TOKEN USB EMPLOYMENT PROCEDURE	ENE 13
970**	Uso de Cifradores IP en Redes Públicas USE OF IP CYPHERS IN PUBLIC NETWORKS	SEP 13

6.2 Formación

Disponer del personal cualificado en todos los niveles de una organización (dirección, gestión e implantación) es fundamental para proteger todos los sistemas de las ciberamenazas. De ahí que una de las funciones principales del CCN sea la formación y concienciación de usuarios, a través de cursos presenciales y online.

	2008	2009	2010	2011	2012	2013	2014
Alumnos STUDENTS	380	450	510	500	500	500	525
Solicitud de Cursos presenciales REQUEST FOR CLASSROOM COURSES	-	-	2.119	2.493	3.090	4.300	4.850
Cursos presenciales CLASSROOM COURSES	17	18	17	14	14	14	16
Horas lectivas CLASS HOURS	1.200	1.400	1.200	900	900	1.000	1.100
Cursos online ONLINE COURSES	-	1	3	5	6	6	7

6.2.1 Cursos STIC

Cursos 2013-2014

- Cursos informativos y de concienciación en seguridad
  - X-XI Curso específico para el Mando Conjunto de Ciberdefensa de Seguridad de las tecnologías de la Información y las Comunicaciones (STIC) con fase online. Online: 30 horas/ Presencial: 50 h. TOTAL: 80h.
- Cursos básicos de seguridad
  - VIII y IX Curso Básico STIC- Infraestructura de Red .25 h.
  - VIII y IX Curso Básico STIC- Base de Datos.25 h.
- Cursos Específicos de Gestión de Seguridad
  - X y XI Curso de Gestión STIC- implantación del ENS. Online: 30 horas / Presencial 50 h. TOTAL: 80 h.
  - XXIV y XXV Curso de Especialidades Criptológicas Fase a distancia: 125 horas / Presencial: 75. TOTAL: 200 h.
- Cursos de Especialización en Seguridad
  - VIII y IX Curso STIC - Seguridad en Redes Inalámbricas. 25 h.
  - II y III Curso STIC- Seguridad en Dispositivos móviles. 25 h.
  - V y VI Curso STIC- Seguridad en Aplicaciones Web. 25 h
  - IX y X Curso STIC- Cortafuegos. 25 h.
  - IX y X Curso STIC- Detección de Intrusos. 25 h.
  - X y XI Curso Acreditación STIC- Entornos Wndows. 25 h.
  - VI y VII Curso STIC- Búsqueda de Evidencias. 25 h.
  - VIII y IX Curso STIC- Inspecciones de Seguridad. 25 h.
  - IV y V Curso STIC- Herramienta PILAR. Online: 10 h. / Presencial 25h. TOTAL: 35 h.

6.2.2 Formación on-line

Durante 2013 y 2014, el Centro Criptológico Nacional ha ido ampliando su oferta formativa, adaptándose a las demandas de muchos usuarios y facilitando, a través de métodos de enseñanza a distancia y e-learning, algunos de sus cursos más demandados. Los cursos disponibles en el portal del CCN-CERT son los siguientes:

- Curso de Seguridad de las Tecnologías de la Información y las Comunicaciones STIC.
- Curso PILAR (Manejo de la herramienta / Funciones más usadas)
- Curso Básico de Seguridad. Entorno Windows
- Curso Básico de Seguridad. Entorno Linux.
- Curso del Esquena Nacional de Seguridad (acceso público).
- Curso de Análisis y Gestión de Riesgos de los Sistemas de Información (acceso público).

En apenas cinco años desde la puesta en funcionamiento del primero de los cursos se ha conseguido un total de 4.688 alumnos y más de 46.700 accesos.

Evolución del número de alumnos (acumulado)
EVOLUTION OF THE NUMBER OF STUDENTS

	2010	2011	2012	2013	2014
Nº accesos cursos online NUMBER OF HITS ON ONLINE COURSES	5.430	13.876	11.735	16.261	**46.763**
Nº alumnos inscritos NUMBER OF STUDENTS SIGNED UP	891	1.511	1.887	2.224	**4.688**

6.2 Training

Having qualified personnel at all Organization levels (executives, management and implementation) is fundamental to protect systems from cyber threats. This means that one of the National Cryptologic Centre's main functions is training and awareness, through classroom courses and online.

6.2.1 STIC Courses

2013-2014 Courses

• Security Information and Awareness Courses
- X-XI Specific course for Ciberdefence Joint Command about Security Information and Communication Technologies (STIC) with blende learning.

• Basic Security Courses
- VIII-IX Basic STIC Course - Network Infrastructure
- VIII-IX Basic STIC Course - Databases

• Specific Courses on Security Management
- X-XI STIC Management Course. Application to ENS
- XXIV-XXV Cryptologic Specialized Course

• Courses Specializing on Security
- VIII-IX STIC Course - Wireless Network
- II-III STIC Course - Security in Mobile Devices
- V-VI STIC Course - Security in Web Applications
- IX-X STIC Course - Firewall
- IX-X STIC Course - Intrusion Detection
- X- XI Accreditation STIC Course - Windows Environment
- VI-VII STIC Course - Search for Evidence and Integrity Control
- VIII-IX STIC Course - Security Inspections
- IV-V III STIC Course - PILAR Tool (online)

6.2.2 Online training

During 2013 and 2014, the National Cryptologic Centre has been extending its training offer, incorporating many users' needs and providing access to some of its most sought-after courses through an e-learning method. The following courses were available on the CCN-CERT website:

• STIC Information and Communication Technology Security Course
• PILAR Course (Using the tool / Most used functions)
• Basic Security Course. Windows environment
• Basic Security Course. Linux environment
• National Security Scheme Course (public access)
Information System Risk Analysis and Management Course (public access)

In barely five years since the first courses were up and running, there have been a total of 4.688 students and over 46.700 hits on the website section.

6.3 Acreditación de sistemas clasificados. Inspecciones STIC

La protección de los sistemas de las Tecnologías de la Información y Comunicaciones (TIC) es una actividad crítica en una Organización dada la importancia que tiene la información que manejan dichos sistemas. De ahí, la necesidad de estar al día respecto a las **amenazas y vulnerabilidades** relacionadas con los sistemas, ya que éstos deben garantizar el acceso a la información en cualquier momento (**disponibilidad**), que sea sólo accesible a personas autorizadas (**confidencialidad**) y que no sea modificada o destruida sin autorización (**integridad**).

Por ello, es preciso implantar un conjunto de medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro para la información, las aplicaciones y los sistemas que sustentan a todos ellos.

Las inspecciones de seguridad permiten verificar la seguridad implementada en un sistema y que los servicios y recursos utilizados cumplen con lo mínimo especificado y requerido.

Los sistemas que manejen **información clasificada** deben trabajar en unos modos seguros de operación y una de las condiciones para la acreditación de un sistema es el cumplimiento de los requisitos STIC que, por otra parte, constituyen el nivel mínimo de protección exigible que deberá ser completado con los requisitos obtenidos de un análisis de riesgos.

La Autoridad Nacional de Acreditación de los sistemas que manejan información clasificada corresponde al secretario de Estado director del CCN

AOSTIC:Autoridad Operativa del Sistema TIC
CO:Concepto de Operación

Dentro de las responsabilidades del CCN en este aspecto y, en concreto, de su grupo de **Acreditación e Inspecciones de Seguridad**, se han desarrollado, entre 2013 y 2014, las siguientes acciones:

- **60 inspecciones STIC**, previas a la acreditación de un sistema, cuyo resultado fue:
  - **Acreditación completa** de 15 ordenadores aislados y siete sistemas completos. Entre otros:
    - Dentro del entorno BICES (*Battlefield Intelligence Collection and Explotation System*) se ha colaborado con la acreditación de varios CSD (*Coalition Shared Database*), procedente del programa MAJIIC (*Multi-Sensor Aerospace-Ground Joint Interoperability ISR -Intelligence, Surveillance and Reconnaisssance-Coalition*), tanto para el nodo español como para ejercicios y pruebas de interoperabilidad con otros CSD y para la evaluación de estos como CSD de referencia de la BGX (*BICES Group Executive*).
    - TVF (*Timing and Geodetic Validation Facility*) de Galileo.
    - Centro de Satélites de la UE acreditado por primera vez para manejar información clasificada hasta EU SECRET.
    - Reacreditación de AMN ESP (*Afghan Mission Network ESP*) tras su migración a los sistemas operativos Windows 2008 / Windows 7.
  - **29 autorizaciones temporales** para manejar información NATO SECRET con motivo de ejercicios a diferentes buques de la Armada y al NRDC ESP (*Nato Rapid Deployment Corp en Bétera*) con la nueva versión de SIMACET (Sistema de Mando y Control del Ejército de Tierra) y a la NS WAN (Wide Area Network Nato Secret) del EMAD (*Estado Mayor de la Defensa*).
- Colaboración con el Ejército del Aire e ISDEFE **en el diseño de la seguridad del Sistema de Mando y Control Aéreo ACCS (Air Command & Control System).**

6.3 Accreditation of classified systems. SICT inspections

The protection of the Information and Communication Technologies systems (ICT) is a critical activity in an Organisation given the importance of the information handled by these Systems. From there we have the need to be up to date regarding the **threats and vulnerabilities** related to the Systems as they should guarantee access to the information at any time (**availability**), that it should only be accessible to authorised persons (**confidentiality**) and not modified or destroyed without authorisation (**integrity**).

To do this, it is necessary to implant a set of measures, both procedural and technical/organisational, giving a secure environment for the information, the applications and the Systems sustaining them.

Security inspections can verify the security implemented in a System and that the services and resources used meet the specified and required minimum.

Systems that handle **classified information** should work in secure operation modes and one of the conditions for a System's accreditation is meeting the SICT requirements that, on the other hand, constitute the minimum level of protection required that should be completed with the requirements obtained from a risk analysis.

The National Accreditation Authority for the systems that handle classified information corresponds to the Secretary of State-Director of the CNI

Within the CCN responsibilities in this aspect and specifically for its **Security Accreditation and Inspections** group, the following actions were run between 2013 and 2014:

- **60 SICT inspections**, prior to accrediting a system, whose result was:
  - **Complete accreditation** of 15 isolated computers and seven complete systems. Among others:
    - Within the BICES environment (Battlefield Intelligence Collection and Exploitation System), it has worked on the accreditation for several CSD (Coalition Shared Database), from the MAJIIC program (Multi-Sensor Aerospace-Ground Joint Interoperability ISR -Intelligence, Surveillance and Reconnaissance- Coalition), both for the Spanish node and for exercises and tests for interoperability with other CSD and to assess them as reference CSD for the BGX (BICES Group Executive).
    - TVF (Timing and Geodetic Validation Facility) by Galileo.
    - EU Satellites Centre accredited for the first time to handle classified information up to EU SECRET.
    - Reacreditation of AMN ESP (Afghan Mission Network ESP) after its migration to the Windows 2008 / Windows 7.
  - **29 temporary authorisations** to handle NATO SECRET information for the purposes of exercises for different ships in the Navy and the NRDC ESP (Nato Rapid Deployment Corp in Betera) with the new version of SIMACET (Sistema de Mando y Control del Ejército de Tierra/Land Army Command and Control System) and the NS WAN (Nato Secret Wide Area Network) for the EMAD (Estado Mayor de la Defensa/Chief of the Defence Staff) ..
- Collaboration with ISDEFE (*Ingeniería de Sistemas para la Defensa de España/Spanish Defence Engineering Systems*) and the Air Force in **designing security** for the ACCS (*Air Command & Control System*).

6.4 Investigación y desarrollo de productos

Una de las funciones del Centro Criptológico Nacional es la de coordinar la promoción, desarrollo, obtención, adquisición, puesta en explotación y utilización de la tecnología de la seguridad de los sistemas TIC que incluyan cifra, para procesar, almacenar o transmitir información de forma segura. Este capítulo de I+D es fundamental para garantizar la seguridad de los sistemas TIC y representa un apoyo al desarrollo de empresas españolas que apuestan por la innovación.

Durante los años 2013 y 2014, el CCN ha participado y/o llevado la dirección técnica en los siguientes proyectos:

- Cifrador IP[3] EP430GN
  - Continuación del proyecto que, en 2013, superó la **evaluación de SECAN** (agencia OTAN para la evaluación seguridad criptológica) y consiguió la **aprobación del Comité Militar de la OTAN** para procesar información OTAN clasificada (el primer cifrador nacional aprobado para procesar información con esta clasificación).

- Cifrador IP EP430GU
  - Financiado en parte con fondos I+D del Programa Galileo entre los años 2014-2015, bajo la dirección técnica del CCN y desarrollado por Epicom.
  - Versión europea del cifrador IP EP430G con el que se espera conseguir la certificación de España como nación AQUA (Appropriated Qualified Authority) lo que permitirá ingresar a nuestro país en el selecto grupo de naciones europeas con esta capacidad.
- Criptoper SCAP[4] Procif for Satellite
  - Continuación del desarrollo de nuevas funcionalidades de este cifrador (voz y datos) con protocolo de interoperabilidad SCIP (Secure Communications Interoperability Protocol)
  - Nueva versión que admite los sistemas de satélite IRIDIUM (Constelación mundial de satélites de comunicaciones móviles) e INMARSAT (International Maritime Satellite Organization).

Se está trabajando para conseguir la certificación de España como nación AQUA (Appropriated Qualified Authority) lo que permitirá ingresar en el selecto grupo de naciones europeas con esta capacidad

[3] Internet Protocol
[4] Secure Communications Aplication

6.4 Product research and development

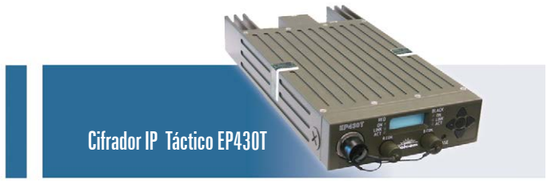
One of the National Cryptologic Centre's functions is coordinating promotion, development, obtaining, purchasing, operating and using ICT systems' security technology including encryption to process, store or send out information securely. This R&D chapter is fundamental to guarantee security for ICT systems used by public administrations and it represents support for developing Spanish companies that are backing innovation.

Over 2013 and 2014, the CCN has participated and/or taken over technical management in the following projects:

- **IP[3] EP430GN cryptographic equipment**
  - Continuation of the project that passed the **SECAN evaluation** (The Military Committee Communications and Information Security and Evaluation Agency) in 2013 and achieved **approval from the NATO Military Committee** to process classified NATO information (the first national cryptographic equipment approved to process information with this classification)
- **IP EP430GU cryptographic equipment**
  - Partly financed with R&D funding from the Galileo Programme for 2014-2015, under the technical management of the CCN and developed by Epicom.
  - European version of the IP EP430G cryptographic equipment that is expected to achieve certification for Spain as an AQUA (Appropriately Qualified Authority) nation, putting our country into the select group of European nations with this capability.

Work is being performed to achieve certification for Spain as an AQUA (Appropriately Qualified Authority) nation, putting our country into the select group of European nations with this capability

- Pasarelas seguras
  - Continuación del desarrollo de una familia de pasarelas para intercambio seguro de información con la empresa AUTEK con fondos de DGAM y CCN:
    - **PSTMail**: intercambio seguro de correo electrónico.
    - **PSTfile**: intercambio de ficheros automáticamente.
    - **PSTDoc**: acceso seguro a documentos externos bajo demanda, desde una red aislada, con el fin de intercambiar ficheros situados en otra red.
- Cifrador IP Táctico, EP430T
  - Con módulo criptológico reprogramable permitiendo disponer sobre la misma plataforma de diferentes aplicaciones de cifra para manejar información clasificada de diferentes dominios de seguridad (nacional/OTAN/UE).
  - Será compatible con las respectivas versiones nacionales /OTAN/UE del cifrador IP EP430G.



- **PKI SCIP-NINE**
  - Proyecto financiado con fondos del Centro Nacional de Inteligencia (años 2014 y 2015). La finalidad de esta infraestructura de clave pública (PKI[5]) es la gestión de claves y certificados de equipos basados en protocolos de interoperabilidad criptológica SCIP[6] y NINE[7]. De esta manera, se dotará al CCN de una Autoridad de Certificación (CA) Raíz, que le permita generar y gestionar Certificados Digitales en una estructura centralizada. A partir de dicha CA Raíz se podrán establecer las distintas autoridades de certificación secundarias (o subCAs) para su empleo en los diferentes sistemas de cifra desplegados.
- EP641M
  - Financiado con fondos de I+D de la Dirección General de Armamento y Material DGAM (2014-2015) del Ministerio de Defensa. Desarrollo del prototipo de un terminal militar telefónico de voz segura sobre IP Interoperable, basado en el cifrador de comunicaciones EP641 con protocolo SCIP para su adecuación a entornos tácticos y mejora de la seguridad.
- COMSec Admin+
  - Mejora de la seguridad de la aplicación e inicio del desarrollo y certificación de la nueva versión basada en certificados digitales.

[5] Public key Infraestructure (PKI)
[6] Secure Communications Interoperability Protocol
[7] Networking and Information Infrastructure (NII) Internet Protocol (IP) Network Encryption

- **Criptoper SCAP[4] Procif for Satellite**
  - Continued development of new features for this cryptographic equipment (voice and data) with SCIP (Secure Communications Interoperability Protocol)
  - New version that accepts IRIDIUM satellite systems (Worldwide constellation of mobile communications satellites) and INMARSAT (International Maritime Satellite Organization).
- **Secure gateways**
  - Continuation of the project started in 2011 along with the company Autek to develop secure gateways:
    - **PSTMail:** secure exchange of electronic mail.
    - **PSTfile:** automatic secure file exchange.
    - **PSTDoc:** secure access to external documents on request, from an isolated network, in order to exchange files located in another network.
- **Tactical IP cryptographic equipment , EP430T**
  - With a reprogrammable cryptological module giving different encryptions on the same platform to handle classified information from different security fields (national/NATO/EU).
  - It will be compatible with the respective national/NATO/EU versions of the IP EP430G cryptographic equipment .
- **PKI SCIP-NINE**
  - Funded by the National Intelligence Centre (2014-2015). The purpose of the system for managing keys and certificates for equipment based on encrypted SCIP[6] and NINE[7] (PKISCIP)interoperability protocols is to equip the CCN with a Root Certification Authority (CA) allowing it to generate and manage Digital Certificates in a centralised structure. Working from this Root CA, it will be possible to establish the different secondary certification authorities (or subCAs) and use them in the different encryption systems that are deployed.
- **EP641M**
  - Financed by R&D funds from DGAM (2014-2015). Development of a prototype for a secure voice telephone military terminal on Interoperable IP, based on the EP641 communications cryptographic equipment and on the SCIP protocol for adaptation to tactical environments and improvement in security.
- **COMSec Admin+**
  - Improvement of the application security and start of development and certification of the new version based on digital certificates.

6.4.1 Apoyos técnicos más significativos

En esta labor de valorar y acreditar la capacidad de los productos de cifra y de los sistemas, el CCN realizó durante los años 2013 y 2014 una intensa actividad de apoyo técnico a distintos desarrollos, entre los que destacan:

- Asesoramiento a diferentes Organismos de la Administración, sobre productos de cifra, sistemas de intercambio seguro de información y de protección TEMPEST.
- Gestión y programación de los algoritmos de cifrado en todos los equipos producidos por Epicom para la Administración del Estado.
  - Asesoramiento en el empleo de la criptología en el ENS y en el DNIe y evaluación y certificación de la seguridad funcional de los productos STIC.
- Apoyo a la Comisión Permanente del Consejo Superior de la Administración Electrónica (**CP CSAE**), en la correcta definición de los **Codigos Seguros de Verificación** de los distintos organismos de la Administración.

6.5 Programas internacionales

El CCN ha participado en los paneles de seguridad de los proyectos internacionales clasificados, desarrollados por la industria española y patrocinados por los ministerios de Defensa, Fomento e Industria. Entre otros:

- **Programa GALILEO**
  - Representante de España en panel de seguridad (Galileo Security Accreditation Panel GSAP) del programa y en el Consejo de seguridad (Security Accreditation Board SAB) del mismo.
  - Ha ejercido como autoridad nacional responsable del servicio público regulado (PRS) de forma interina.
  - Presencia en proyectos que permitan cumplir con los requisitos funcionales y de seguridad para el Servicio Público Regulado (PRS) y su utilización en el Punto de Contacto a nivel nacional (POC-P y POC-IS).
  - Acreditación a las empresas GMV, Tecnobit, Isdefe, Deimos y Epoche para acceso a la información clasificada del programa.
  - Inauguración del Centro de Servicios Loyola de Palacio, en el Instituto Nacional de Técnica Aeroespacial (INTA), sede del programa que albergará la distribución comercial del servicio abierto. Una actividad que se prevé importante y dinamizadora de la industria española de navegación.
  - Dirección del grupo de trabajo de seguridad creado por la comisión interministerial de coordinación del programa.
  - Establecimiento de relaciones con Portugal dentro del programa Galileo y hermanamiento con la República de Macedonia para fomentar el uso de los sistemas de navegación en ese Estado.

El CCN dirige el grupo de trabajo de seguridad creado en el seno de la comisión interminiserial de coordinación del programa Galileo

- **Programa A-400M (avión militar de transporte)**
  - Continúa la dirección de la actividad COMSEC del programa coordinando las actividades de certificación funcional y TEMPEST:
    - » Gestión de claves de los sistemas de comunicación HF, VHF y Radares y de los sistemas GPS con la Agencia estratégica de comunicaciones de EEUU.
    - » Coordinación de la contribución de la empresa Tecnobit en el sistema de Audio del avión.
    - » Laboratorio TEMPEST acreditado para la realización de las medidas de evaluación del avión que se está montando en la factoría de EADS-CASA en Sevilla en las distintas versiones disponibles para cada uno de los países participantes en el Programa.
- **Programa PAZ (Sistema espacial de observación de la Tierra en el espectro Radar).**
  Asesoramiento en la topología de la red del sistema.
- **Programa ACCS (Air Command and Control System)**
  Apoyo y asesoramiento en normativa y productos de seguridad para el intercambio seguro de información.
- **Programa EF2000 (avión militar de combate)**
  Asesoramiento en proyecto CV Bulk Preparation Facility (P-8615) de generación de claves en formato bulk (masivo), así como en las fases de revisión del diseño preliminar (PDR Previous Design Review) y del diseño crítico (CDR Critical Design Review).

6.4.1 Most significant technical supports

In this work of assessing and accrediting the capacity of the encryption products and the systems, the CCN worked intensely during 2013 and 2014 on technical support for different developments including:

• Consultancy for different Administration Organisations on encryption products and TEMPEST protection systems.
• Management and programming of the encryption algorithms in all equipment produced by Epicom for the State Administration.
• Consultancy on the use of Cryptologic in the ENS and in the electronic ID (DNIe) and evaluation and certification of functional security for SICT products.
• Support for the Senior Electronic Administration Council Permanent Commission (**CP CSAE**) when correctly defining **Secure Verification Codes** for the different Administration organisations.

6.5 Supports in International Programmes

The CCN has taken part in security panels for classified international projects, developed by Spanish industry and sponsored by the Ministries of the Defence, Development and Industry. Among others:

• **GALILEO Programme**
- Spanish representative on the Galileo Security Accreditation Panel GSAP for itsSecurity Accreditation Board SAB.
- Working as Interim CPA (Competent PRS Authority).
- Regulated Service (PRS) and its use in the national Point of Contact (POC-P and POC-IS).
- Security accreditation for GMV, Tecnobit, Isdefe, Deimos and Epoche for access to the programme's classified information.
- Inauguration of the Loyola de Palacio Service Centre in the National Aerospace Technical Institute (INTA), headquarters for the programme that will host the commercial distribution of the open service. An activity that is forecast to be important and enabling for the Spanish navigation industry.
- Management of the security work group set up by the inter-ministry programme coordination commission.
- Forming ties with Portugal within the programme and twinning with the Republic of Macedonia to encourage the use of navigation systems in this State.

The CCN runs the security work group set up by the inter-ministry programme coordination commission for the Galileo programme.

• **A-400M programme (military transport aircraft)**
- Continuing management of the COMSEC activity (Communications security) for the programme coordinating functional certification and TEMPEST activities:
  - Managing keys for the HF, VHF and Radar communication systems and the GPS systems with the USA strategic communications agency.
- Coordination of the contribution from Tecnobit in the aircraft's Audio system.
- TEMPEST lab accredited to take evaluation measurements on the aircraft being assembled in the EADS-CASA factory in Seville in the different versions available for each of the countries participating in the Programme.

• **PAZ programme**
Consultancy on the system network topology.

• **ACCS programme (Air Command and Control System)**
Support and consultancy on the standards and security products for secure exchange of information.

• **EF2000 programme (military fighter aircraft)**
Consultancy on the project to generate keys in bulk format and in the Preliminary Design Review (PDR) and the Critical Design Review (CDR) for the CV Bulk Preparation Facility project (P-8615).

7 Organismo de Certificación, OC
Certification Body, OC

El CCN constituye el Organismo de Certificación (OC) del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, de aplicación a productos y sistemas en su ámbito.

EL OC realiza tres tipos de Certificación en función de los aspectos de seguridad que se evalúen, pero siempre referidos a productos y sistemas STIC:

- Certificación Funcional
- Certificación Criptológica
- Certificación TEMPEST

Anualmente se realiza una **auditoría interna** y una **auditoría externa** al OC. La auditoría primera la realiza personal del CNI (no perteneciente al CCN), para comprobar que la actividad de certificación se efectúa de acuerdo a las normas y procedimientos establecidos en cada caso.

La auditoría externa la realiza la **Entidad Nacional de Acreditación (ENAC)**, según la correspondiente norma ISO, y es necesaria para que el OC mantenga la acreditación como entidad de certificación de producto. En 2014 se realizó la primera auditoría siguiendo la nueva normativa **ISO 17065**.

En el marco del reconocimiento internacional, el OC, sigue participando activamente en dos importantes grupos de trabajo (técnicos y de gestión):

- **CCRA** (*Common Criteria Recognition Arrangement*)
  - Ratificado en septiembre de 2014 por los 26 países integrantes. En el caso de España la firma fue compartida entre el secretario de Estado de Administraciones Públicas y el secretario de Estado director del Centro Criptológico Nacional.
- **SOGIS-MRA** (*Senior Officers Group on Information Security - Mutual Recognition Agreement*).
  - Se ha creado un nuevo dominio técnico para dispositivos hardware seguros “Hardware Devices with Security Boxes” en el que el OC español ha conseguido la autorización para emitir certificados al más alto nivel de garantía.

The CCN constitutes the Certification Body (OC) for the National Evaluation and Certification Scheme for Information Technology Security to be applied to products and systems in its field. In this respect, the OC carries out three types of certification depending on the security aspects being assessed, but always referring to SICT products and systems: **Functional Certification, Cryptological Certification** and **TEMPEST Certification**.

The OC is given an **internal audit** and an **external audit** every year. The audit is firstly carried out by CNI personnel (not belonging to the CCN) to check that the certification activity is following the rules and procedures set in each case.

The external audit is run by the **National Accreditation Entity (ENAC)**, according to the corresponding ISO standard, and it is necessary so that the OC maintains the accreditation as a product certification entity. In 2014, the first audit was performed according to the new **ISO 17065** standard.

Within the framework of international recognition, the OC continues to participate actively in two important work groups (technical and management):

- CCRA (Common Criteria Recognition Arrangement)
  - Ratified in September 2014 by the 26 member countries. In Spain’s case, the signature was shared between the Secretary of State for Public Administrations and the Secretary of State-Director of the National Cryptography Centre.
- SOGIS-MRA (Senior Officers Group on Information Security – Mutual Recognition Agreement).
  - A new technical domain has been set up for “Hardware Devices with Security Boxes” in which the Spanish OC has achieved the authorisation to issue certificates to the highest level of guarantee.

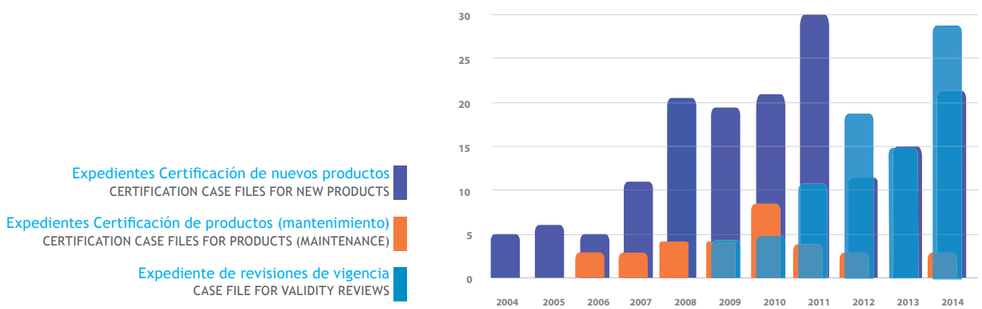
7.1 Certificación Funcional

Este tipo de certificación se articula mediante el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, aprobado por **Orden PRE/2740/2007**, de 19 de septiembre, completado con sus procedimientos internos y haciendo uso de los documentos de soporte que se generan en los grupos internacionales CCRA y SOGIS-MRA.

Actuaciones destacadas en 2013 y 2014:

- Inicio de **83 expedientes de certificación**, entre nuevas solicitudes y mantenimiento o revisión de vigencia de los certificados ya existentes.
  - El 50% de las solicitudes llegaron de compañías extranjeras, un hecho explicado, en parte por la situación económica, por la falta de una normativa nacional clara que fomente y valore la utilización de productos de seguridad confiables y, también, por la proyección internacional del propio Organismo.
- **20 resoluciones de certificación de productos o sistemas**
  - Publicado en el BOE, tras pasar el proceso de evaluación.
- Resolución de la ampliación de alcance de la acreditación del laboratorio APPLUS (EAL 5).

Evolución del número de expedientes de certificación funcional
EVOLUTION OF THE NUMBER OF CASE FILES FOR FUNCTIONAL CERTIFICATION



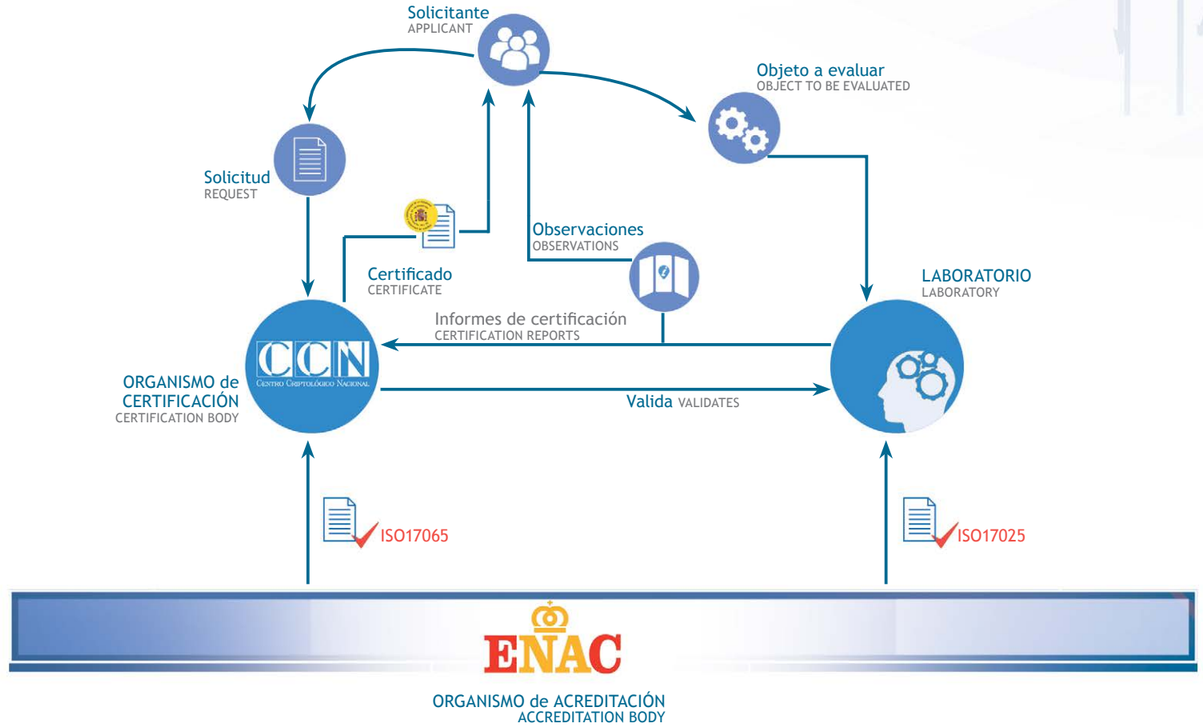
7.1 Functional certification

This type of certification is articulated by means of the Information Technology Security Evaluation and Certification Ruling, approved by **Order PRE/2740/2007**, dated 19th September, completed by its own internal standard adapted to the necessary requirements to be recognised both nationally, according to standard EN45011, and internationally, in accordance with the CCRA and SOGIS-MRA.

Outstanding actions in 2013 and 2014:

- Start of **83 certification files** among new applicants and maintenance or review of existing certificates.
- 50% of applications came from foreign companies, partly down to the economic situation, the lack of a clear national standard that encourages and values the use of reliable security products and, also, due to the actual Organisation's international projection.
- **20 certification resolutions for products or systems**
- Published in the BOE, after passing the evaluation process,
- Resolution of extending the scope of the accreditation for the APPLUS laboratory (EAL 5).

PROCEDIMIENTO DE CERTIFICACIÓN
CERTIFICATION PROCEDURE



Resoluciones BOE año 2013

OFFICIAL STATE GAZETTE RESOLUTIONS 2013

OBJETO A EVALUAR	SOLICITANTE DE LA CERTIFICACIÓN	TIPO RESOLUCIÓN	NÚMERO DE RESOLUCIÓN EN EL BOE
POLYMNIE LDS EAC APPLET 2.2 BAC	OBERTHUR	CERTIFICADO	1544, de 9 de enero
POLYMNIE LDS EAC APPLET 2.2 BAP	OBERTHUR	CERTIFICADO	1545, de 9 de enero
POLYMNIE LDS EAC APPLET 2.2 EAC	OBERTHUR	CERTIFICADO	1546, de 9 de enero
POLYMNIE LDS EAC APPLET 2.2 EAP	OBERTHUR	CERTIFICADO	1547, de 9 de enero
SITE HUAWEI SHANGHAI	HUAWEI	CERTIFICADO	9452, de 30 de julio de 2013
SITE HUAWEI SHENZEN	HUAWEI	CERTIFICADO	9453, de 30 de julio de 2013
TIMECOS JAVACARD	WATCHDATA	CERTIFICADO	11580 de 20 de septiembre
KONA102 BAC	KONA@I Co., Ltd.	CERTIFICADO	6125, de 14 de mayo
KONA102 EAC	KONA@I Co., Ltd.	CERTIFICADO	6126, de 14 de mayo
CYBEROAM FIRMWARE	ELITECORE TECHNOLOGIES	CERTIFICADO	11581 de 30 de septiembre
WISE WASTE RFID	SOMA	CERTIFICADO	9454, de 30 de julio de 2013
AMPLIACIÓN DE ALCANCE APPLUS	---------	ACREDITADO	6124, de 14 de mayo

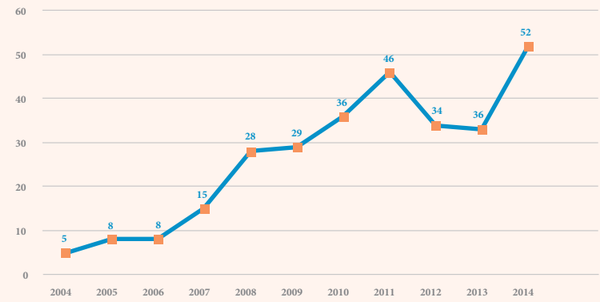
Resoluciones BOE año 2014

OFFICIAL STATE GAZETTE RESOLUTIONS 2014

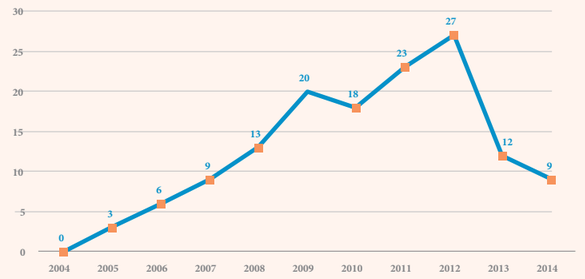
OBJETO A EVALUAR	SOLICITANTE DE LA C ERTIFICACIÓN	TIPO RESOLUCIÓN	NÚMERO DE RESOLUCIÓN EN EL BOE
EXACARD SMART CARD v1.0	IDONEUM	CERTIFICADO	12802, de 17 de noviembre
MFED	RCI Banque S.A.	CERTIFICADO	4931, de 1 de abril
CRM H1202 CC	HV SISTEMAS	CERTIFICADO	5989 de 28 abril de 2014
CRM H1202 19790	HV SISTEMAS	CERTIFICADO	5990 de 28 de abril de 2014
PSTfile	AUTEK	CERTIFICADO	3360, de 5 de febrero de 2014
Boreal IT Security Platform	Boreal IT	CERTIFICADO	4375, de 24 de marzo de 2014
KEYONE CA 4.0.13S2R1	SAFELAYER	CERTIFICADO	12801, de 11 de noviembre de 2014
Huawei LTE eNodeB	HUAWEI	CERTIFICADO	11343, de 25 de septiembre de 2014
MFED	RCI Banque S.A.	CERTIFICADO	12803, de 17 de noviembre

Actividad del Organismo de Certificación
ACTIVITY OC

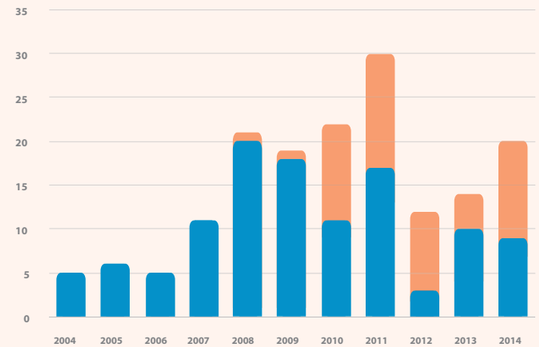
Expedientes Certificados Funcional
FUNCIONAL CERTIFICATION CASES



Resoluciones publicadas en el BOE
RESOLUTIONS PUBLISHED IN THE BOE

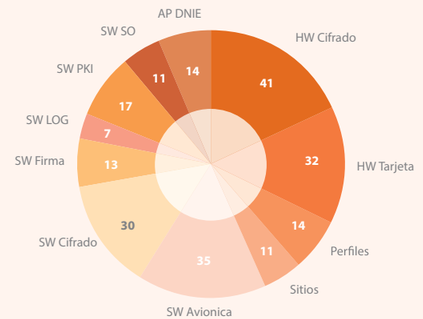


Expedientes Certificados de nuevos productos
NEW PRODUCT CERTIFICATION CASES



Españoles/ SPANISH
Extranjeros/ FOREIGN

Tipos de productos certificados
TYPES OF CERTIFIED PRODUCTS



7.2 Certificación Criptológica

El CCN es el Organismo responsable de la elaboración del Catálogo de Productos con Certificación Criptológica que incluye los productos capaces de proteger la **información nacional clasificada**. Tiene la consideración de cifrador nacional, con certificación criptológica, aquel equipo de cifra que ha sido evaluado y ha obtenido dicha certificación del CCN. Se dispone de distintos tipos de cifradores: IP, de datos, voz, fax, PKI, generadores de números aleatorios, centros de gestión, etc.

Los productos aprobados para el cifrado de información nacional clasificada o que legalmente requiera protección, se incluyen en el catálogo de productos con certificación criptológica **CCN-STIC 103**, y el procedimiento de evaluación de productos criptológicos está recogido en la guía **CCN-STIC 102.**

En cuanto a la evaluación y certificación criptológica durante los años 2013 y 2014 se realizaron las siguientes actividades:

- Cifrador IP EP430GN

Evaluado y certificado hasta nivel RESERVADO, ha superado, tal y como ya se ha mencionado, la aprobación del Comité Militar de la OTAN para procesar información OTAN clasificada (*véase apartado de Investigación y desarrollo de productos*).

- Cifrador IP EP430GX

Evaluación y certificación de la versión nacional para procesar información nacional clasificada.

- Cifrador Criptoer SCAP Procif para Iridium e Inmarsat

Reevaluación y certificación de dos nuevas versiones del cifrador (para ambos satélites) aprobado para procesar información nacional y OTAN clasificada.

- Centro de gestión CRIPTOPER CMAP PROCIF

Se ha llevado a cabo la reevaluación de una nueva versión del Centro de Gestión de los cifradores CRIPTOPER SCAP PROCIF para Iridium y también se ha reevaluado su adaptación para el cifrador CRIPTOPER SCAP PROCIF for SATELLITE (Iridium + Inmarsat).

- Cifrador Crypto Token USB

Reevaluación y recertificación de la versión 2 del cifrador de datos sin conexión a redes Crypto Token USB. Esta nueva versión es compatible con los sistemas operativos Windows Vista y Windows 7.

- Sistema Färist Mobile

Proporciona comunicaciones móviles seguras (voz y datos) mediante una red privada virtual (VPN) desde los terminales móviles seguros (Terminal Móvil Nexus 5) hasta un concentrador VPN (dispositivo de cifrado Färist VPN).

Evaluado y certificado por el CCN en 2014, este cifrador está aprobado para procesar **información nacional clasificada**.

Este sistema será presentado a una nación AQUA en el año 2015 para someterse a una segunda evaluación criptológica para su aprobación para la protección de información clasificada de la Unión Europea. En caso de ser aprobado, será el primer dispositivo con certificación nacional con aprobación de la Unión Europea para proteger información clasificada.

Sistema Färist Mobile

- Cifrador Secvoice

Permite en los dispositivos móviles, con sistema operativo Android o compatible, el establecimiento de comunicaciones de voz seguras utilizando el protocolo interoperable SCIP.

El cifrador Secvoice ha sido evaluado y certificado en el 2014 para la protección de **información nacional clasificada**.

El sistema creado por la unión del sistema Färist Mobile y el cifrador Secvoice permite proteger las comunicaciones móviles de los organismos.

- COMSEC Admin

El COMSEC Admin es un sistema comercial para su uso en la Administración, creado por INDRA SCS, que asegura la confidencialidad de las comunicaciones de voz y mensajería.

Durante el año 2014 el CCN ha realizado la revisión de los mecanismos de seguridad del sistema y verificado su correcta implementación.

- Cifradores IP

Durante el año 2014 debido a la necesidad de actualización de diversos componentes que se habían quedado obsoletos en la familia de cifradores IP de la empresa EPICOM se ha procedido a la reevaluación y recertificación de los siguientes cifradores: EP430, EP430B, EP430C EP430D Y EP430S.

7.2 Cryptological Certification

The CCN is the Organisation in charge of drawing up the Catalogue of Products with Cryptological Certification that includes products capable of protecting **national classified information**. Encryption equipment is considered as a national cryptographic equipment , with Cryptological certification, if it has been assessed and has obtained this certification from the CCN. There are different types of cryptographic equipments: IP, data, voice, fax, PKI, random number generators, management centres, etc.

Products that have been approved for encryption national classified information or that legally require protection are included in the catalogue of products with **CCN-SICT 103** cryptological certification and the cryptological product evaluation procedure is compiled in the **CCN-SICT 102** guide.
Regarding the evaluation and cryptological certification during 2013 and 2014, the following activities were run:

• IP EP430GN cryptographic equipment

Assessed and certified nationally, as mentioned previously, it has passed the NATO Military Commission's approval to process classified NATO information (see section on Product Research and Development).

• IP EP430GX cryptographic equipment

Evaluation and certification of the national version to process classified national information.

• Criptoer SCAP Procif cryptographic equipment for Iridium and Inmarsat

Reevaluation and certification of the two new versions of the cryptographic equipment (for both satellites) approved to process national information and classified NATO information.

• CRIPTOPER CMAP PROCIF management centre

Reevaluation was carried out on a new version of the Management Centre for CRIPTOPER SCAP PROCIF cryptographic equipment s for Iridium and its adaptation was also reassessed for the CRIPTOPER SCAP PROCIF cryptographic equipment for SATELLITE (Iridium + Inmarsat).

• Crypto Token USB cryptographic equipment

Reevaluation and recertification of version 2 of the data cryptographic equipment without connection to Crypto Token USB networks. This new version is compatible with the Windows Vista and Windows 7 operating systems.

• System Färist Mobile

This provides secure mobile communications (voice and data) by means of a virtual private network (VPN) from secure mobile terminals (Nexus 5 Mobile Terminal) to a VPN concentrator (Färist VPN encryption device).

Assessed and certified by the CCN in 2014, this cryptographic equipment is approved to process **national classified information.**

This system will be presented to an AQUA nation in 2015 to undergo a second Cryptologic evaluation for approval to protect European Union classified information. If it is approved, this will be the first encryption device assessed nationally with approval from the European Union to protect classified information.

• Secvoice cryptographic equipment

In mobile devices, using the Android system or compatible, this allows secure voice communications using the SCIP interoperable protocol.
The Secvoice cryptographic equipment was assessed and certified in 2014 to protect **national classified information**.
The system created to bring together the Färist Mobile system and the Secvoice cryptographic equipment helps to protect organisations' mobile communications.

• COMSEC Admin

COMSEC Admin is a commercial system for use in the Administration, created by INDRA SCS, ensuring confidentiality for voice communications and message services.

During 2014, the CCN reviewed the system's security mechanisms and verified that it was being implemented correctly.

• IP cryptographic equipment s

During 2014, due to the need to update different components that had become obsolete in the EPICOM family of IP cryptographic equipment s, the following cryptographic equipment s were reassessed and recertified: EP430, EP430B, EP430C EP430D and EP430S.

7.3 Certificación STIC

El CCN recibe recibe múltiples consultas de Organismos de la Administración sobre qué productos emplear para proteger sus sistemas.

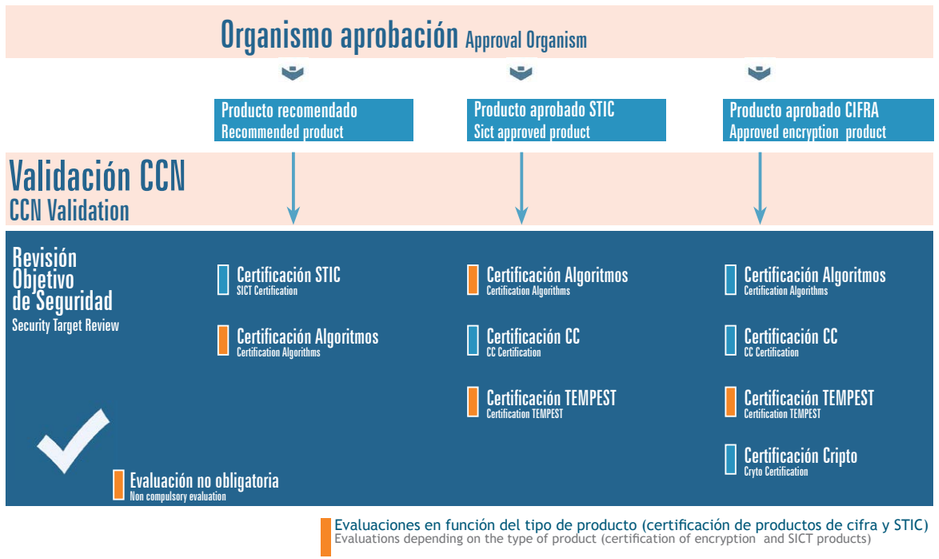
Por este motivo, está en proceso de creación el **Catálogo de Productos Aprobados y Recomendados** para la Seguridad TIC (STIC), que serán recogidos en la **Guía CCN-STIC 105** (pendiente de publicación). En ella se incluirán productos cuya finalidad **no** sea el cifrado de información nacional clasificada o que legalmente requiera protección y que hayan pasado previamente una evaluación STIC.

En la guía CCN-STIC 106 (pendiente de publicación) se explica el procedimiento del CCN para recomendar o aprobar un producto para la seguridad de las TIC y el formato para solicitar la inclusión en dicho catálogo.

En 2014 se comenzó la evaluación STIC de la pasarela PSTfile (de la empresa Autek), teniendo prevista la finalización de la misma en 2015. Será el primer producto con certificación STIC.

Pasarela PSTfile

Se ha creado el Catálogo de Productos Aprobados y Recomendados para la Seguridad TIC (STIC), que serán recogidos en la Guía CCN-STIC 105 que incluirá productos cuya finalidad no sea el cifrado de información nacional clasificada



7.3 SICT certification

The CCN receives many enquiries from Administration Organisations on which products to use to protect their systems.

For this reason, the **Catalogue of Approved and Recommended Products** has been drawn up for ICT Security (SICT), compiled in the **CCN-SICT 105 Guide**. This includes projects whose purpose does not include encryption national classified information or that legally require protection and that have previously passed an SICT evaluation.

The CCN-SICT 106 guide explains the procedure followed by the CCN to recommend or approve a product for ICT security and the procedure to follow to request inclusion in this catalogue.

7.4 Certificación TEMPEST

El término TEMPEST hace referencia a las investigaciones y estudios de emanaciones comprometedoras relacionadas con la información clasificada que está siendo transmitida, recibida, manejada o de alguna manera procesada por equipos o sistemas electrónicos. Estas emanaciones no intencionadas, una vez detectadas y analizadas, pueden llevar a la obtención de la información. Asimismo, el término TEMPEST se refiere también a las medidas aplicadas para la protección contra dichas emanaciones comprometedoras.

El CCN, como autoridad de certificación de seguridad TIC en el ámbito EMSEC (Seguridad de las emanaciones), tiene entre otras misiones, el desarrollo de normativa nacional en este campo, la evaluación y certificación de equipos, sistemas e instalaciones, así como la participación y asesoramiento en diferentes foros, actuando en todos ellos como Autoridad TEMPEST Nacional (NTA National TEMPEST Authority).

Respecto a evaluación de la seguridad de las emanaciones y las instalaciones donde están ubicados, en los dos últimos años se realizaron las siguientes actividades:

- Certificación ZONING de locales

Se han realizado 20 expedientes de certificación (tanto a empresas como a organismos de la Administración Pública). Esta cifra se ha incrementado notablemente, debido a la la renovación de los certificados que deben hacerse cada 5 años.

- Certificación ZONING/TEMPEST de equipos y sistemas:

La actividad se ha centrado principalmente en la evaluación TEMPEST de equipos de cifra y de productos STIC, así como del sistema de gestión de audio AMS de Tecnobit para el Airbus A400M.

Es importante resaltar la importancia de solicitar a las empresas proveedoras de equipamiento informático los certificados ZONING de los equipos, previamente a su adquisición. En la **Guía CCN-STIC 104 de Catálogo Productos ZONING** se puede consultar los resultados de los equipos comerciales ya evaluados.

- Evaluación y certificación TEMPEST de plataformas

El CCN sigue participando en los procesos de certificación de las plataformas del Eurofighter (EF2000) y del Airbus A400M.

Es importante resaltar la importancia de solicitar a las empresas proveedoras de equipamiento informático los certificados ZONING de los equipos, previamente a su adquisición

2014 saw the start of the SICT evaluation for the PSTfile gateway (for Autek) which is due to finish in 2015. It will be the first product with SICT certification.

The Catalogue of Approved and Recommended Products has been drawn up for ICT Security (SICT), compiled in the CCN-SICT 105 Guide. It includes products whose purpose is not encryption national classified information

7.4 TEMPEST Certification

The term TEMPEST refers to research and studies on compromising emanations related to classified information that is being sent out, received, handled or in any way processed by electronic equipment or systems. These unintentional emanations, once detected and analysed, can lead to information being obtained. In addition, the term TEMPEST also refers to measures applied to guard against these compromising emanations.

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

Regarding the security evaluation of the emanations and facilities where they are located, over the last two years the following activities have been carried out:

• **ZONING certification for premises**

They have conducted 20 certification cases (businesses and public administration organisations). This figure has increased significantly, due to the renewal of licenses to be made every five years.

• ZONING/TEMPEST certification for equipment and systems

The activity has mainly focussed on the TEMPEST evaluation for encryption equipment and SICT products, as well as the Tecnobit AMS audio management system for the Airbus A400M.

It is important to highlight the importance of asking the companies providing computer equipment for the ZONING certificates for this equipment, prior to purchase. The **ZONING Products Catalogue CCN-SICT 104 Guide** can be used to consult results for commercial equipment that have already been assessed.

• TEMPEST evaluation and certification for platforms

The CCN continues participating in the certification processed for Eurofighter (EF2000) and Airbus A400M platforms.

It is important to highlight the importance of asking the companies providing computer equipment for the ZONING certificates for this equipment, prior to purchase

8 CCN-CERT, defensa frente a las ciberamenazas
CCN-CERT, defence against cyberthreats

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

Del mismo modo, la **Estrategia de Ciberseguridad Nacional** confiere al CCN-CERT un papel central en el desarrollo de su línea de acción 1: Capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas; así como, en colaboración con el MINHAP, de su línea de acción 2: Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas.

Así, y de acuerdo a toda esta normativa y legislación, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a **sistemas clasificados**, de las **Administraciones Públicas** y de **empresas y organizaciones de interés estratégico** para el país; es decir aquellos que son esenciales para la seguridad nacional y para el conjunto de la economía española. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

Es competencia del CCN-CERT la gestión de ciberincidentes que afecten a sistemas clasificados, de las Administraciones Públicas y de empresas y organizaciones de interés estratégico para el país

The CCN-CERT is the Capability to Respond to Information Security Incidents by the National Cryptologic Centre (CCN). This service was set up in 2006 as the Spanish Government CERT and its functions are compiled in Law 11/2002 regulating the National Intelligence Centre (CNI), RD 421/2004 regulating the CCN and RD 3/2010, dated 8th January, regulating the National Security Scheme (ENS).

In the same way, the **National Cybersecurity Strategy** gives the CCN-CERT a central role in developing its line of action 1: Capabilities to prevent, detect and defeat cyber threats, and, in collaboration with the MINHAP , his line of action 2: Information and Communication Technology Security for Public Administrations.

Consequently and according to all these standards and legislation, it is the CCN-CERT's responsibility to manage cyber-incidents that affect **classified systems** from **Public Administration** and **companies and organisations with strategic interest** for the country; in other words, any that are essential for national security and for the Spanish economy as a whole. Its assignment is therefore to help improve cybersecurity as the alarm and national response centre that cooperates and helps provide a fast and effective response to cyber-attacks and actively tackles cyber-threats.

it is the CCN-CERT's responsibility to manage cyber-incidents that affect classified systems, for Public Administrations and businesses and organisations of strategic interest for the country

8.1 Servicios del CCN-CERT

Los servicios que ofrece el CCN-CERT son todos aquellos recogidos en la distinta normativa y los que el estado de la ciberseguridad requiere en cada momento, con una constante actualización en función de las nuevas amenazas y los riesgos emergentes. Entre los principales se encuentran:

- Gestión de Incidentes.
- Sistema de Alerta Temprana (SAT)
- Formación y sensibilización
- Guías de Seguridad
- Herramientas
- Informes, avisos y vulnerabilidades
- Cumplimiento del ENS
- Auditorias de seguridad y de páginas web
- Capacidad forense y de ingeniería inversa

8.1 CCN-CERT Services

The services offered by the CCN-CERT are those envisaged by applicable regulations and any service required by the cybersecurity situation at a given time, with a continuous updating on emerging threats and risks.

- Incident Management
- Early Warning System (SAT)
- Training and Awareness-raising
- Security Guides
- Cybersecurity Reports
- Tools
- ENS Compliance
- Web Audits
- Forensic and Reverse Engineering Capability

aplicación.

8.2 Gestión de Incidentes

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 este intercambio.

Su presencia como CERT Gubernamental Nacional en todos los foros internacionales con organizaciones similares de otros países le proporciona una información muy valiosa para una gestión rápida y eficaz de cualquier incidente.

Así, durante el año 2014 gestionó **12.916** incidentes. Esta cifra representa un incremento del 78% con respecto al año 2013 en el que se gestionaron 7.259 incidentes. De ellos, el **10,8% (1.404)** fueron catalogados por el equipo de expertos del CERT Gubernamental Nacional con un nivel de peligrosidad de entre **muy alto y crítico**; es decir, se tuvo constancia de que el ataque afectó a los sistemas de la organización y a su información sensible (estos tipos de ataque, incluido la categoria de Alto, en virtud del cumplimiento del Esquema Nacional de Seguridad, debe ser notificado al CCN-CERT, tal y como queda registrado en la Guía CCN-STIC 817 de Gestión de Ciberincidentes).

Se constató, además, un incremento en la intensidad y sofisticación de dichos ataques, tanto a las Administraciones Públicas como a las empresas y organizaciones de interés estratégico para el país, fundamentalmente de los sectores energético, de defensa, aeroespacial, farmacéutico y químico.

Las Administraciones Públicas y en virtud del cumplimiento del ENS, deben notificar al CCN-CERT todos aquellos incidentes que sean catalogados con un nivel de peligrosidad de Alto, Muy Alto y Crítico

Propuesta de Intercambio de Información de ciberincidentes en España.
CCN-CERT as a node for Coordination and Exchange on information regarding cyber-incidents in Spain.

Throughout this process —which always ensures strict confidentiality between the parties—, the CCN-CERT provides technical and operational support to detect, react, contain and defeat incidents. A preventive approach is also implemented, and a team of experts investigates the techniques, trends, solutions and the most appropriate procedures to counter incidents, including methodologies to gather and analyze data and events, and procedures to assess the risk level and to determine priority.

The CCN-CERT also operates as a Cyber Incident Information Exchange Node in the Information Systems of the Public Administrations, and as the main coordinator of information exchange among the relevant entities.

As the National Government CERT, it participates in international forums attended by counterparts from a number of countries, which provides it with very valuable information to manage any incident efficiently and swiftly.

It consequently managed **12,916** incidents during 2014. This figure represents a 78% increase on 2013 when 7,259 incidents were managed. Of these incidents, **10.8% (1,404)** were catalogued by the team of experts from the National Governmental CERT with a danger level between **very high** and **critical**; in other words, there was evidence that the attack affected the organisation's systems and its sensitive information (CCN-CERT should be notified about this type of attack and by virtue of meeting the National Security Scheme, as recorded in the CCN-SICT 817 Cyber-incident Management Guide).

An increase was also seen in the intensity and sophistication of these attacks, both on Public Administrations and on companies and organisations with strategic interest for the country, fundamentally from the energy, defence, aerospace, pharmaceutical and chemical sectors.

Public Administrations, in compliance with the National Security Scheme, are compelled to report to the CCN-CERT on any incident whose threat level is assessed as high, very high or critical

INCIDENTES PRIORITARIOS PARA EL CCN-CERT
Priority incident for the CCN-CERT

- Incidentes que afecten a información clasificada
  Incidents affecting classified information
- Ciberespionaje: APTs, campañas de malware, incidentes especiales Cyber espionage: APTs, malware campaigns, special incidents
- Interrupción de los Servicios IT
  Disruption of IT Services
- Exfiltración de datos
  Data Exfiltration
- Existencia de algún servicio comprometido
  Potentially compromised services
- Toma de control de algún sistema
  Takeover of system control
- Robo y publicación o venta de información sustraído
  Theft, disclosure or sale of stolen information
- Hacktivismo
  Hacktivism
- Suplantación de identidad
  Identity theft

Los incidentes son detectados a través de distintas vías, entre ellas el **Sistema de Alerta Temprana, SAT**, implantado en la red SARA (Intranet de la Administración) como en Internet (SAT-SARA y SAT-INET). De este modo, al ser detectados, se notifican a los distintos organismos adscritos a este servicio (AGE, Comunidades Autónomas, Ayuntamientos y empresas de interés estratégico).

En este sentido conviene reseñar que el SAT-INET, y tras la incorporación, durante los dos últimos años de nuevos organizaciones, estaba desplegado al finalizar 2014 en un total de **64 organizaciones públicas y privadas (76 sondas)**, frente a los 37 que había a principios de 2013.

Organismos de la Administración General del Estado (entre ellos todos los Ministerios), diferentes Comunidades Autónomas, Ayuntamientos, Diputaciones y empresas de interés estratégico para el país están adheridos a este servicio que espera cerrar el año 2015 con un total de 85 organizaciones recibiendo este servicio.

Por su parte, el SAT-SARA cuenta con **49 áreas de conexión.**

Al término de 2014 había 64 organizaciones adscritas al SAT-INET y 49 áreas de conexión al SAT-SARA

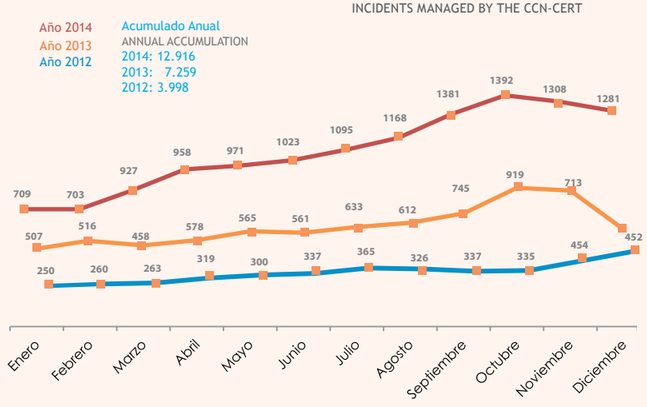
Incidents are detected in different ways, including the **Early Warning System, SAT**, implanted both in the **SARA (Administration Intranet)** network and on the **Internet (SAT-SARA and SAT-INET)**. In this way, when they are detected, notification is sent to the different organisations that are members of this service (General State Administration (AGE), Regions, Town Councils and companies with strategic interest).

In this respect, it is advisable to highlight that after incorporatiing new organisations over the last two years, the SAT-INET was deployed at the end of 2014 in a total of **64 public and private organisations (71 probes)**, compared to 38 that existed in early 2013.

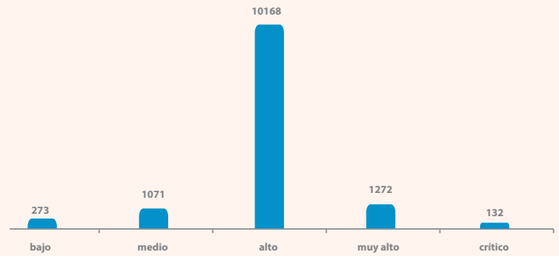
General State Administration Organisations (including all Ministries), different Regions, Town Councils, Local Governments and companies with strategic interest for the country are members of this service that expects to close in 2015 with a total of 85 organisations.

In turn, the SAT-SARA has **49 connection areas**.

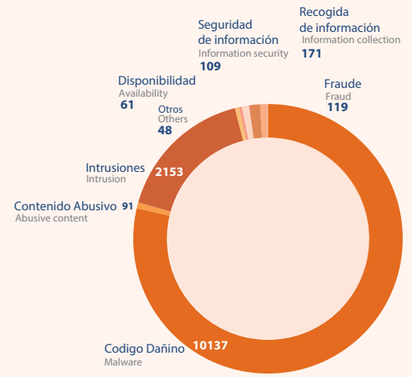
Incidentes gestionados por el CCN-CERT
INCIDENTS MANAGED BY THE CCN-CERT



Nivel de peligrosidad de los incidentes gestionados por el CCN-CERT en 2014
DANGER LEVEL FOR INCIDENTS MANAGED BY THE CCN-CERT IN 2014

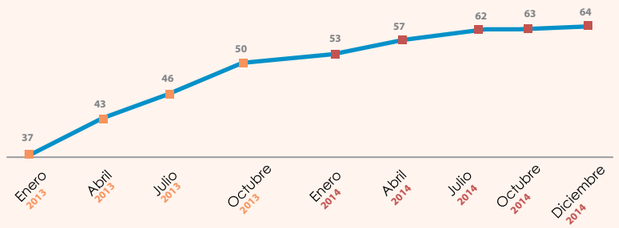


Clasificación por tipología de incidentes gestionados en 2014
INCIDENT TYPES MANAGED BY THE CCN-CERT (2014)

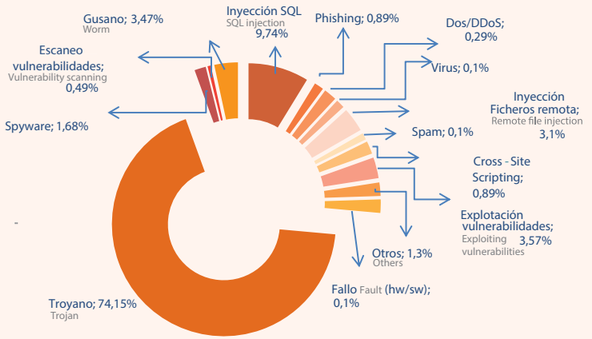


1) Código Dañino: troyanos, sypware, etc.
MALWARE: TROJANS, SPYWARE, ETC.
2) Intrusiones: ataques dirigidos a explotar vulnerabilidades e introducirse
INTRUSION: ATTACKS AIMING TO EXPLOIT VULNERABILITIES AND GAIN ENTRY
3) Recogida de información: primeros pasos para una campaña mayor (vulnerabilidades, ingeniería social)
COLLECTING INFORMATION: FIRST STEPS FOR A MAJOR CAMPAIGN (VULNERABILITIES, SOCIAL ENGINEERING)
4) Seguridad de la información: violaciones de políticas de seguridad
INFORMATION SECURITY: SECURITY POLICY VIOLATIONS
5) Contenido abusivo: contra la imagen
ABUSIVE CONTENT: AGAINST IMAGE
6) Disponibilidad: daños de imagen y productividad (rendimiento)
AVAILABILITY: DAMAGING TO IMAGE AND PRODUCTIVITY (PERFORMANCE)
7) Fraude: propiedad intelectual, protección de datos o suplantación de identidad (phishing)
FRAUD: INTELLECTUAL PROPERTY, DATA PROTECTION OR IDENTITY THEFT (PHISHING)

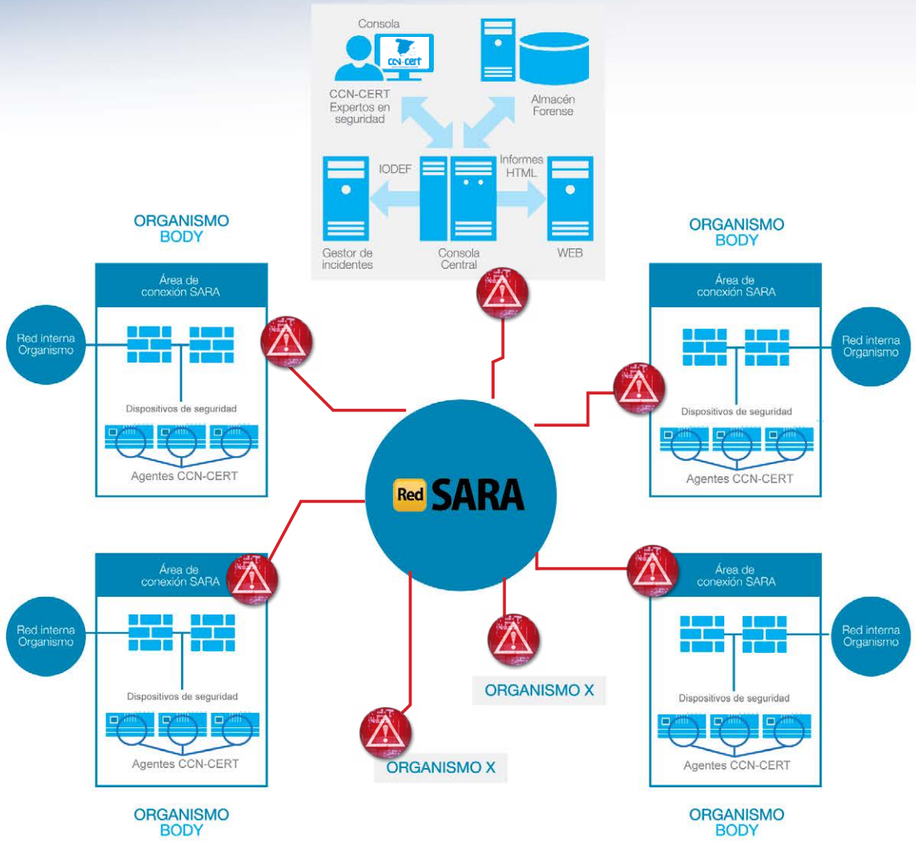
Nº de organizaciones adscritas al Sistema de Alerta Temprana, SAT, de Internet
NO. OF ORGANISATIONS THAT ARE MEMBERS OF THE EARLY WARNING SYSTEM, SAT, ON THE INTERNET



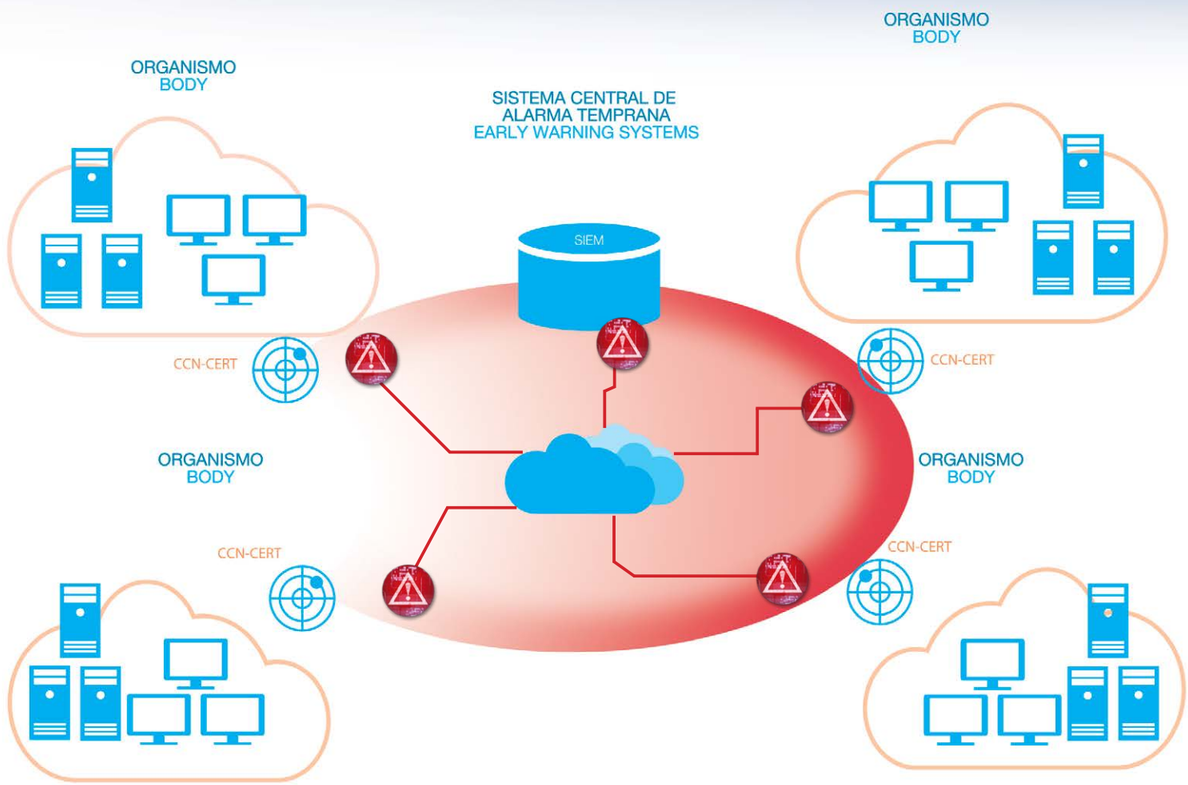
Categorías de los ciberincidentes gestionados por el CCN-CERT
CATEGORIES OF CYBER-INCIDENTS MANAGED BY CCN-CERT



Servicio de Alerta Temprana (SAT)
EARLY WARNING SYSTEM



Arquitectura red SARA
SARA NETWORK ARCHITECTURE



Arquitectura SAT-INET
INTERNET EARLY WARNING SYSTEM ARCHITECTURE

8.3 Herrramientas de ciberseguridad
Cybersecurity tools

Dentro de las funciones del Centro Criptológico Nacional se encuentra la coordinación, promoción y desarrollo de herramientas que garanticen la seguridad de los sistemas y contribuyan a una mejor gestión de la ciberseguridad en cualquier organización y permitan una mejor defensa frente a los ciberataques.

Among other tasks, the National Cryptologic Centre is responsible for coordinating, promoting and developing tools that ensure the security of the system and that contribute to a more efficient management of cybersecurity in any given organization and to a better defense against cyber attacks.

Finalidad de herramientas desarrolladas por el CCN-CERT:

- Evitar dependencia tecnológica en materia de ciberseguridad (herramientas propiedad de la Administración española)
- Permanencia del Conocimiento en la organización
- Promover la Universidad española
- Fomentar la colaboración público-privada

Purpose of tools developed by the CCN-CERT:

- Avoid technological dependence in terms of cybersecurity (tools owned by Spanish Administration)
- Knowledge remains in the organisation
- Promoting Spanish universities
- Encouraging public-private collaboration

8.3.1 CARMEN, detección de APTs

CARMEN (**C**entro de **A**nálisis de **R**egistros y **M**inería de **E**ventos) es un desarrollo del Centro Criptológico Nacional y la empresa S2Grupo para la identificación de los posibles compromisos por parte de amenazas persistentes avanzadas (APT), constituyendo la primera capacidad española en este sentido, basada en conocimiento y tecnología nacionales.

CARMEN es una herramienta de adquisición, procesamiento y análisis de información para la generación de inteligencia principalmente a partir de los tráficos de una red. Además, aporta capacidades para la detección de la amenaza en su etapa de intrusión.

Su primera versión fue puesta en marcha en **el año 2013**. A finales de 2014 estaba desplegada en 21 organismos públicos y 13 empresas.

En la actualidad se trabaja en la versión 3.2 con nuevas funcionalidades.

Contacto: carmen@ccn-cert.cni.es

8.3.2 CLARA, auditoría de cumplimiento ENS/STIC en sistemas Windows

Herramienta desarrollada por el Centro Criptológico Nacional y la empresa Sidertia para analizar las características de seguridad técnicas definidas a través del Real Decreto 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 de seguridad que han sido proporcionadas a través de la aplicación de plantillas de seguridad, según las guías CCN-STIC de la serie 800: 850A, 850B, 851A y 851B.

La herramienta funciona exclusivamente en sistemas Windows, tanto en sus versiones cliente como servidor, miembros de un dominio o independientes al mismo.

Su primera versión fue puesta en marcha en **diciembre de 2014**.

Contacto: clara@ccn-cert.cni.es
Enlace: https://www.ccn-cert.cni.es/ens/clara.html

8.3.1 CARMEN, APT Detection Tool

CARMEN, Centre of Log Analysis and Mining of Events, is a tool developed by the National Cryptologic Centre and the company S2Grupo to identify compromises by advanced persistent threats (APTs), and is the first tool based on Spanish technology and know-how.

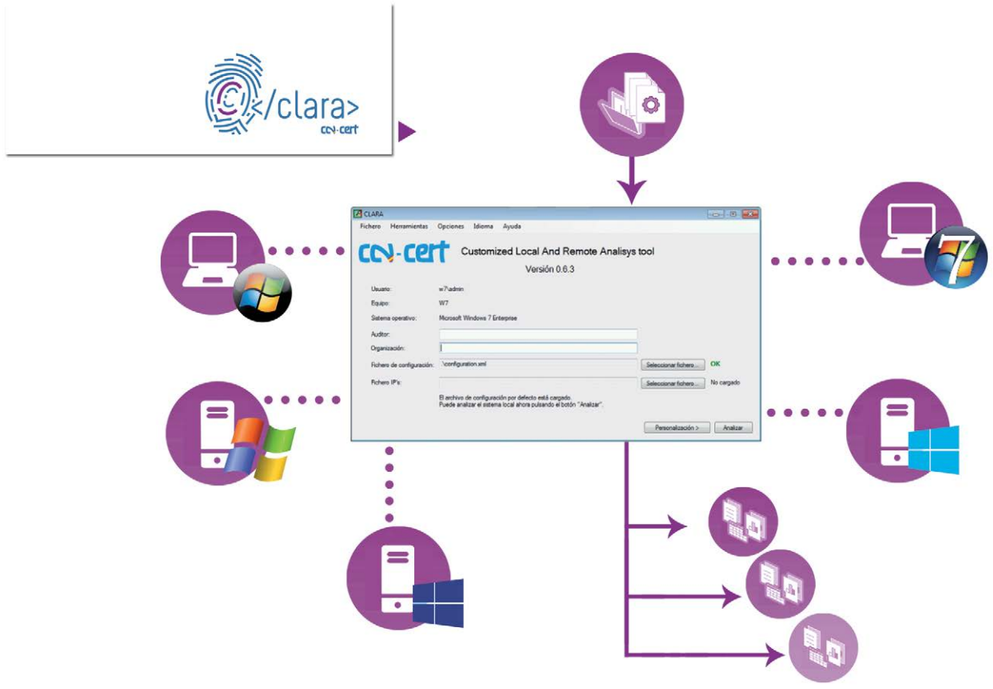
CARMEN is a tool that collects, processes and analyzes information to generate intelligence mainly from the network traffic. It provides capabilities to detect the threat at the intrusion stage.

Its first version was launched in 2013. In late 2014 he was deployed in 21 government agencies and 13 companies.
Contact: carmen@ccn-cert.cni.es

8.3.1 CLARA, audit to comply with the ENS/SICT in Windows systems

Tool designed by the National Cryptologic Centre and Sidertia to analyse the technical security features defined via Royal Decree 3/2010 regulating the ENS in the field of Electronic Administration. Compliance analysis is based on security rules that have been provided through applying security templates according to the CCN-SICT 800 series guides: 850A, 850B, 851A and 851B.

The tool works exclusively in Windows systems, both in client and server versions, members of a domain or independently from it.
Its first version was set up in **December 2014**.
Contact: clara@ccn-cert.cni.es



8.3.3 INES, informe nacional del estado de seguridad en el ENS

INES (**I**nforme **N**acional del **E**stado de **S**eguridad) ha sido desarrollado por el CCN-CERT y la empresa Nethaphora con el fin de facilitar la labor de todos los organismos a la hora de evaluar regularmente el estado de la seguridad de sus sistemas, tal y como recoge el ENS. Este proyecto proporciona a las distintas Administraciones Públicas un conocimiento más rápido e intuitivo de su nivel de adecuación al ENS y del estado de seguridad de sus sistemas.

Su primera versión fue puesta en marcha en **octubre de 2014** y a finales de 2014 había 156 organismos de la Administración General del Estado, Comunidades Autónomas, Administraciones locales y Universidades cargando datos.

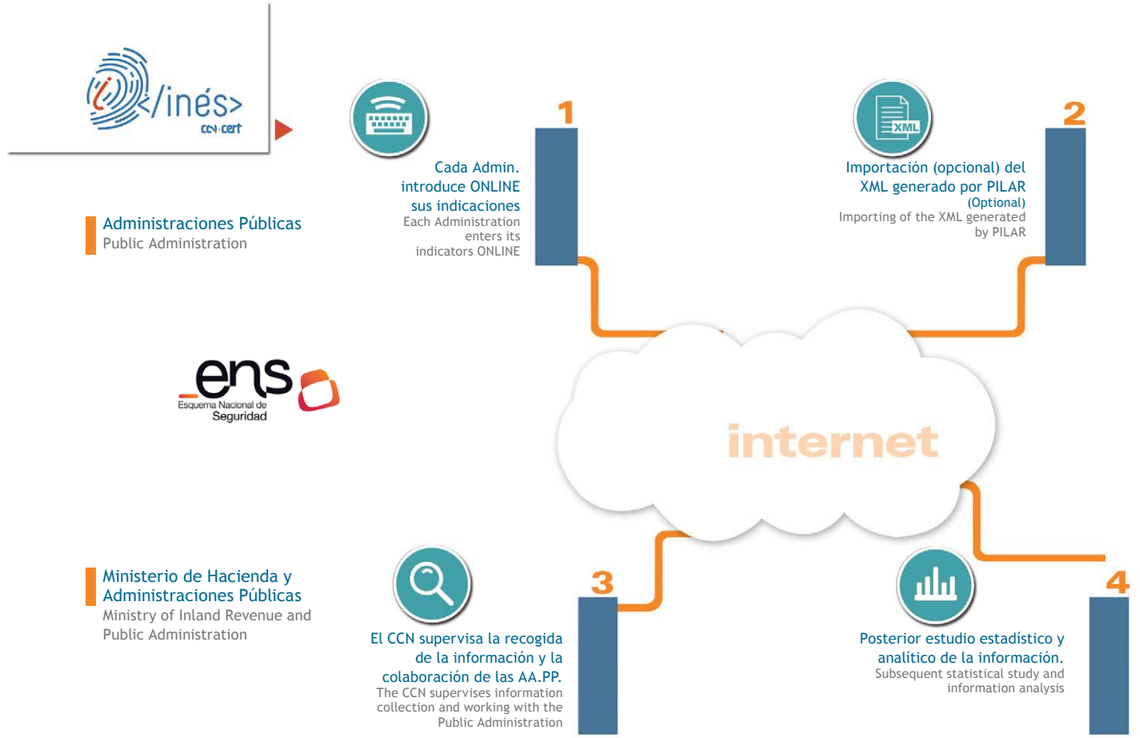
Contacto: ines@ccn-cert.cni.es
Enlace: https://www.ccn-cert.cni.es/herramientas-de-seguridad/ines.html

8.3.3 INES, Status report on security in the ENS

INES (Informe **N**acional del **E**stado de **S**eguridad/National Security Status Report) was developed by the CCN-CERT and Nethaphora in order to make life easier for all organisations when regularly assessing the security status for their systems, as complied in the ENS. This project provides different Public Administrations with faster and more intuitive knowledge of its level of adaptation to the ENS and the security status of its systems.

Its first version was set up in **October 2014** and by the end of 2014 it had achieved 856 hits.

Contact: ines@ccn-cert.cni.es



8.3.4 LUCIA, sistema federado de gestión de incidentes

LUCIA (**L**istado **U**nificado de **C**oordinación de **I**ncidentes y **A**menazas) es una herramienta desarrollada por el CCN-CERT y la empresa CSA para la Gestión de Ciberincidentes en las entidades del ámbito de aplicación del Esquema Nacional de Seguridad. Con ella se pretende mejorar la coordinación entre el CERT Gubernamental Nacional y los distintos organismos y organizaciones con las que colabora.

LUCIA está basada en el sistema de ticketing de código abierto RT (Request Tracker) en el que se incluye el módulo específico de respuesta a incidentes RTIR(Incident Response IR), ambos mantenidos por la empresa Best Practical Solutions.

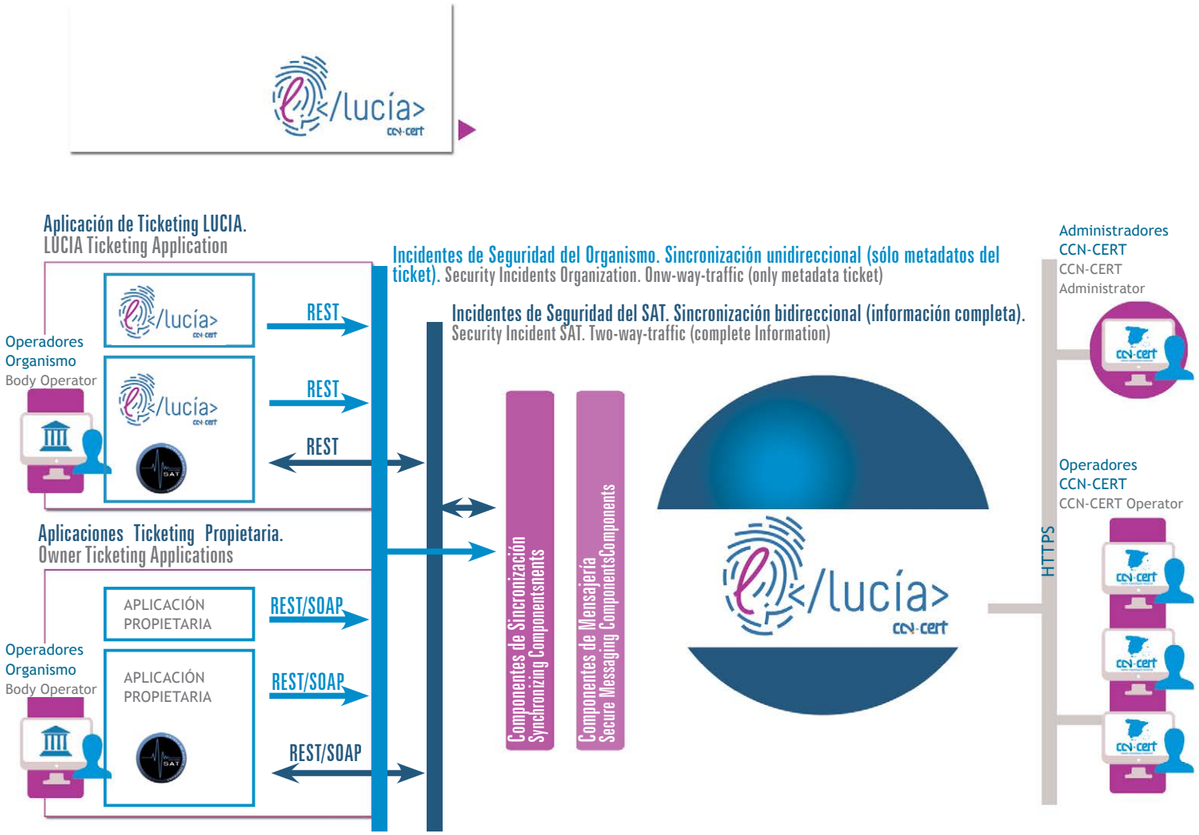
LUCIA ofrece un lenguaje común de peligrosidad y clasificación del incidente y mantiene la trazabilidad y el seguimiento del mismo, de acuerdo a la guía CCN-STIC **817 de Gestión de Incidentes**. El sistema permite, además, automatizar las tareas e integrarse con otros sistemas ya implantados.

Contacto: lucia@ccn-cert.cni.es
Enlace: https:\\www.ccn-cert.cni.es/herramientas-de-ciberseguridad/lucia.html

8.3.4 LUCIA, federated system management of incidents

LUCIA (**L**istado **U**nificado de **C**oordinación de **I**ncidentes y **A**menazas/ Unified Coordination List for Incidents and Threats) is a tool developed by the CCN-CERT and CSA to manage cyber-incidents in entities in the field of applying the National Security Scheme. It aims to improve coordination between the Spanish Government CERT and the different organisms and organisations that it works with.

LUCIA offers a common language for danger levels and classification of incidents and maintains its traceability and monitoring in accordance with the **CCN-SICT 817 Incident Management** guide. The system also allows you to automate the tasks and integrate with other systems that are already implanted.
Its first version was implemented in **March 2015.**
Contact: lucia@ccn-cert.cni.es



REST/SOAP: Protocolos Intercambio Mensajes
Interchange Messages Protocol

8.3.5 MARÍA, análisis estático de malware

MARIA (**M**ultiAnalizadoR Integrado de **A**menazas) es una herramienta de detección desarrollada por el CCN-CERT para el análisis estático de código dañino.

Permite analizar todo tipo de malware, utilizando las versiones de líneas de comando de múltiples motores antivirus y antimalware (están en proceso de incorporación más de 30), actualizados en tiempo real. Es, de hecho, una evolución de la plataforma MultiAntiVirus con la que ya contaba el CCN-CERT.

Cuenta con la posibilidad de integrarse con otros servicios del CCN-CERT, como MARTA o REYES.
Herramienta en proceso de implantación.

Esta herramienta iniciará su implantación en el último trimestre de 2015

8.3.6 MARTA, análisis dinámico de malware

MARTA (**M**otor de **A**nálisis **R**emoto de **T**royanos **A**vanzados) es una herramienta de análisis desarrollada por el CCN-CERT y la empresa InnoTec System para la detección, análisis y notificación de malware de forma automática.

Entre sus principales características se encuentran la detección temprana del código dañino, el análisis y clasificación de las amenazas de forma automática (a través de su motor inteligente) y la generación de Informes personalizados y detallados de cada una de las muestras.

Herramienta en proceso de desarrollo.

8.3.5 MARÍA, static malware analysis

MARIA (**M**ulti**A**nalizado**R** **I**ntegrado de **A**menazas/Built-in Threat Multi-Analyser) is a detection tool developed by the CCN-CERT to statistically analyse malware.

It helps to analyse all types of malware, using the command line versions of multiple antivirus and antimalware engines (they are in the process of incorporating over 30), updated in real time. It is, in fact, an evolution of the Multi-Antivirus platform already used by CCN-CERT.

It has an application to be integrated with other services from the CCN-CERT such as MARTA or REYES.

Tool currently being implanted.

8.3.6 MARTA, dynamic malware analysis

MARTA (**M**otor de **A**nálisis **R**emoto de **T**royanos **A**vanzados/Remote Analysis Engine for Advanced Trojans) is an analysis tool developed by the CCN-CERT and InnoTec System to detect, analyse and warn about malware automatically.

Its main features include early detection of malware, analysis and classification of threats automatically (through its intelligent engine) and generating personalised and detailed reports for each of the samples.

Tool currently being implanted.

8.3.7 PILAR, análisis y gestión de riesgos

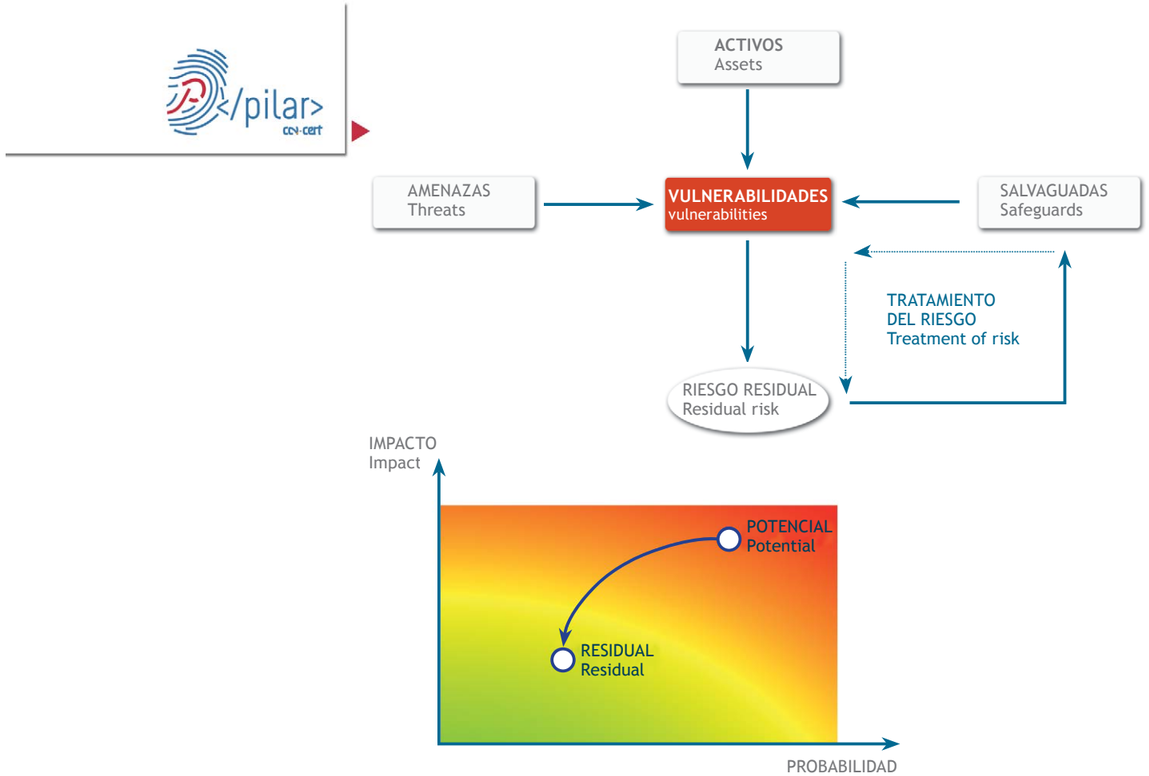
Las herramientas PILAR (Procedimiento Informatico y lógico de Análisis de Riesgos) soportan el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) y está desarrollada y financiada parcialmente por el CCN y la empresa A.L.H.J.Mañas.

PILAR se actualiza periódicamente y existen diversas variedades, todas ellas con su correspondiente guía CCN-STIC (470G/1, 470G/2, 471/D, 472E y 473D):

PILAR: versión íntegra de la herramienta en donde se analizan los riesgos en varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad
PILAR Basic: versión sencilla para Pymes y Administración Local
µPILAR: versión de PILAR reducida, destinada a la realización de análisis de riesgos muy rápidos
RMAT (Risk Management Additional Tools) Personalización de herramientas

Su primera versión fue puesta en marcha en **el año 2006** (desde marzo de 2015 está disponible la versión 5.4.3).

Contacto: ccn@cni.es
Enlace: https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar/pilar.html



8.3.8 REYES, intercambio de información de ciberamenazas

REYES (**RE**positorio común **Y ES**tructurado de amenazas y código dañino) es una herramienta desarrollada por el CCN-CERT para automatizar el intercambio de información y conocimiento sobre ciberamenazas. Está basada en la Plataforma de Intercambio de Información de Código dañino (MISP[8]), desarrollada por Bélgica en el seno de la OTAN y nace ante la necesidad imperiosa **automatizar** y **estandarizar** el intercambio de información para resultar eficientes en la lucha contra los ciberataques. Es decir, dar un paso más allá de la utilización del correo electrónico para este tipo de difusiones y migrar a modelos más proactivos en el intercambio de información.

Herramienta en proceso de implantación.

8.3.5 EAR/PILAR, risk analysis and management

EAR (Risk Analysis Environment) tools support the risk analysis and management for an information system following the Magerit methodology(Information System Risk Analysis and Management Methodology) and it is developed and partially funded by the CCN and A.L.H.J.Mañas.

PILAR (**P**rocedimiento **I**nformático y **L**ógico de **A**nálisis de **R**iesgos/Computer-based and Logical Risk Analysis Procedure) is updated periodically and there are several varieties, all with their corresponding CCN-SICT guide (470G/1, 470G/2, 471/D, 472E and 473D):

PILAR: full version of the tool
PILAR Basic: simple version for SMEs and Local Administration
µPILAR: reduced PILAR version, intended to perform very fast risk analyses
RMAT (Risk Management Additional Tools) Tool personalisation

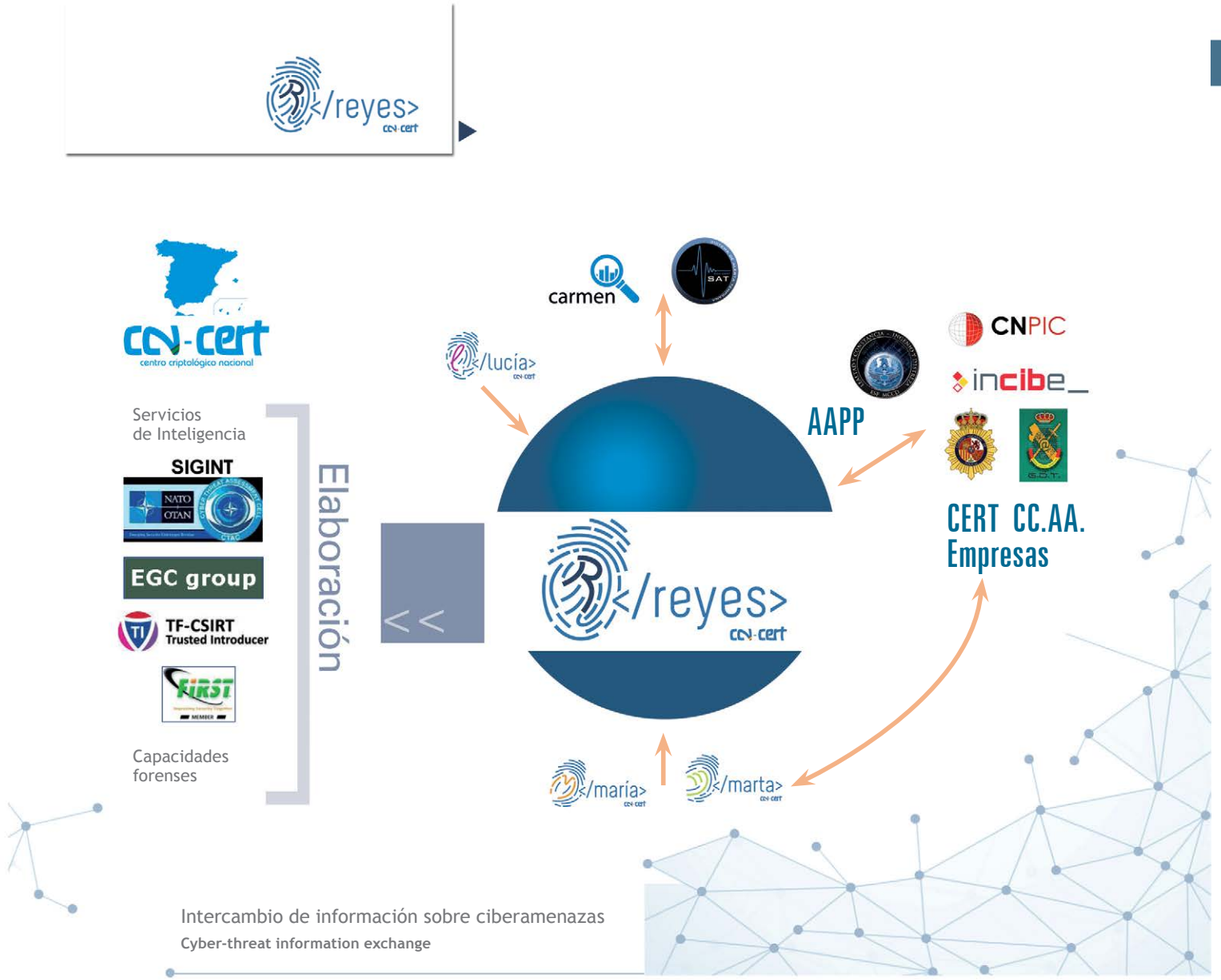
Its first version was implemented in **2006** (version 5.4 is currently available).

8.3.8 REYES, cyber-threat information exchange

REYES (**RE**positorio común **Y ES**tructurado de amenazas y código dañino/Common directory and Threat and Malware structuring) is a tool developed by the CCN-CERT to automate the exchange of information and knowledge on cyber-threats. It is based on the Malware Information Sharing Platform (MISP), developed by Belgium within NATO and it came about due to the pressing need to **automate** and **standardise** effective exchange of information in the fight against cyber-attacks. In other words, this means a further step in using email for this type of dissemination and migrating to more proactive models in information sharing.

Tool currently being implanted

[8] Malware Information Sharing Platform



8.4 Reports, warnings and vulnerabilities

The CCN-CERT offers information on the Cybersecurity status, in order to reduce both technical vulnerabilities (hardware and software) and human and organisational vulnerabilities. Its main target audience are users registered on the site (5,320 on 30th December 2014, among Public Administrations and companies of strategic interest), and anyone who informs periodically on warnings, alarms, vulnerabilities and publication of reports on different issues.

In total, over the last two years **64 reports** have been published that have been downloaded more than **5,562 times** from the CCN-CERT website (however, these reports are also sent out to over 6,000 registered users by email so distribution is actually much wider).

8.4 Informes, avisos y vulnerabilidades

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** del portal (5.320 a 30 de diciembre de 2014, entre Administraciones Públicas y empresas de interés estratégico), a los que notifica periódicamente avisos, alertas, vulnerabilidades y la publicación de informes de diferentes materias.

En total, a lo largo de los dos últimos años se han publicado **64 informes**, que fueron descargados en más de **5.562 ocasiones** desde el portal del CCN-CERT (no obstante, dichos informes también son enviados a los usuarios registrados por correo electrónico, por lo que su difusión es mucho mayor).

Principales informes publicados en 2013 y 2014
MAIN REPORTS PUBLISHED IN 2013 AND 2014

INFORMES PUBLICADOS POR EL CCN-CERT EN SU PORTAL Reports published by the CCN-CERT on its website	FECHA Date
CCN-CERT IA-02/14 Riesgos de uso de Windows XP tras el fin del soporte	ene-14
CCN-CERT IA-03/14 Ciberamenazas 2013 Tendencias 2014 (versión privada)	abr-14
CCN-CERT IA-03/14 Ciberamenazas 2013 Tendencias 2014 Anexos	abr-14
CCN-CERT IA-06/14 Recomendaciones generales ante ataques a servicios web	abr-14
CCN-CERT IA-21/14 Ransomware	dic-14
CCN-CERT ID-01/14 Informe de Código Dañino e IOC de Win32/Palevo	feb-14
CCN-CERT ID-02/14 Informe de Código Dañino e IOC de Win32/Skintrim	feb-14
CCN-CERT ID-03/14 Informe de Código Dañino Win32.Conficker	mar-14
CCN-CERT ID-04/14 Informe de Código Dañino Zero Access	abr-14
CCN-CERT ID-07/14 Informe de Código Dañino Win32/Vobfus	jun-14
CCN-CERT ID-08/14 Informe de Código dañino e IoC eBury	jun-14
CCN-CERT ID-09/14 Informe de Código Dañino e IoC Cycbot	jul-14
CCN-CERT ID-10/14 Informe de Código Dañino e IoC Antivirus XP	jul-14
CCN-CERT ID-11/14 Informe de Código Dañino e IoC Win32.Cridex	jul-14
CCN-CERT ID-14/14 Informe de Código Dañino e IOC de Magania	jul-14
CCN-CERT ID-15/14 Informe de Código Dañino e IOC de Daonol	nov-14
CCN-CERT ID-17/14 Informe de Código Dañino e IOC de Critoni	ago-14
CCN-CERT ID-20/14 Informe de Código Dañino e IOC de GeckaSeka	nov-14
CCN-CERT IA-17/13 Código Dañino. Técnicas de Persistencia	Dic-13
CCN-CERT IA-21/13 Riesgos y amenazas del BYOD	Nov-13
CCN-CERT IA-09/13 Ciberamenazas 2012 y Tendencias 2013	Jun-13
CCN-CERT IA-08/13 Análisis de Facebook (Android). Vulnerabilidades	Abr-13
CCN-CERT IA-06/13 Análisis de Facebook (iPhone). Vulnerabilidades	Abr-13
CCN-CERT IA 03/13 Riesgos derivados del uso de Redes Sociales	Feb-13
CCN-CERT IA-01/13 Análisis de WhatsApp (iPhone). Vulnerabilidades	Ene-13

Vulnerabilidades
Diariamente el CCN-CERT publica (con hilo RSS) las vulnerabilidades de los siguientes fabricantes: Microsoft, Red Hat, Cisco, Oracle, Adobe, Suse, Debian, IBM, Apple y Symantec.

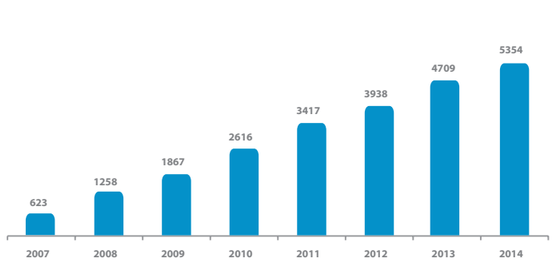
Entre 2013 y 2014 se publicaron un total de 6.540 vulnerabilidades

Avisos y alertas
Todos los usuarios registrados del portal del CCN-CERT reciben directamente los avisos y alertas de ciberseguridad en los que se informa de las nuevas amenazas detectadas por el CERT Gubernamental.

En concreto, en los dos últimos años se han notificado: 36 Avisos y 14 Alertas.

Del mismo modo, el equipo CCN-CERT lleva a cabo **auditorías a páginas web** de distintos organismos de las administraciones públicas en busca de posibles vulnerabilidades críticas, con el fin de establecer las pautas adecuadas para reducirlas o eliminarlas.Durante 2013 y 2014 se han realizado 16 auditorías web.

Evolución del número de usuarios registrados en el portal del CCN-CERT
EVOLUTION OF THE NUMBER OF USERS REGISTERED ON THE CCN-CERT WEBSITE



El CCN-CERT cuenta desde marzo de 2015 con un nuevo portal web
CCN-CERT HAS A NEW WEBSITE SINCE MARCH 2015

CCN Vulnerabilities
Every day the CCN-CERT uses the RSS news feed to publish vulnerabilities for the following manufacturers: Microsoft, Red Hat, Cisco, Oracle, Adobe, Suse, Debian, IBM, Apple and Symantec.

A total of 6,540 vulnerabilities were published between 2013 and 2014

Warnings and alarms
The CCN has carried out the audit of webs from different Organizations of the Public Administration in search of possible risks and vulnerabilities, in order to establish the appropriate guidelines to reduce or eliminate them.

8.5 Cultura de ciberseguridad

La ya citada Estrategia de Ciberseguridad Nacional fija como Objetivo IV el "*sensibilizar a los ciudadanos, profesionales, empresas y Administraciones Públicas españolas de los riesgos derivados del ciberespacio*". En esta tarea, el CCN acomete un gran número de acciones de información y sensibilización, promoviendo una sólida cultura de ciberseguridad, en la que se proporciona a todos los actores implicados la conciencia y confianza necesarias para el uso del ciberespacio, los riesgos que conlleva, así como las herramientas y conocimientos necesarios para la protección de su información, sistemas y servicios.

De entre sus más de doscientas acciones y participaciones en mesas redondas y jornadas, destacan las Jornadas STIC CCN-CERT y la Jornada SAT.

Nº de asistencias del CCN
NUMBER OF ASSISTANCES OF CCN

	2008	2009	2010	2011	2012	2013	2014
Jornadas de sensibilización AWARENESS-RAISING SESSIONS	2	4	3	6	7	6	6
Participación en mesas / jornadas PARTICIPATION IN ROUND TABLES/SESIONS	8	10	15	51	64	97	108

Jornadas STIC CCN-CERT

En sus ocho ediciones (la última celebrada los días 10 y 11 de diciembre de 2014), este evento, organizado anualmente por el CCN, se ha convertido en el principal encuentro de expertos en ciberseguridad en España, no sólo por el gran éxito de convocatoria (con más de mil asistentes), sino también por la calidad de los temas abordados y por la experiencia y conocimiento de los ponentes.

Abiertas a la participación de expertos de la Administración Pública y de empresas de interés estratégico para el país, estas Jornadas son además, una apuesta por la necesario cooperación público-privada y por el intercambio de información entre las distintas organizaciones.

8.5 Cybersecurity culture
The aforementioned National cybersecurity strategy sets as Target IV "*raising awareness on the risks derived from cyberspace among citizens, professionals, companies and Spanish Pubic Administrations.*" In this task, the CCN performs a large number of information and awareness raising actions, promoting a solid cybersecurity culture where all the players involved are given the necessary awareness and confidence for using cyberspace, the risks this involves as well as the tools and knowledge required to protection their information, systems and services.

The following stand out among over two hundred actions and participation in round table discussions:

• SICT CCN-CERT sessions
In its eight editions (the latest was held on 10th and 11th December 2014), this event, organised every year by the CCN, has become the main meeting of Cybersecurity experts in Spain, not only due to the number of people it brings in (over a thousand people attending) but also due to the quality of the topics covered and the speakers' experience and knowledge.

Open to participation from experts in the Public Administration and companies with strategic interest for the country, these Sessions also back the necessary public-private cooperation and information sharing between the different organisations.

Evolución de las Jornadas STIC CCN-CERT
EVOLUTION OF THE SICT CCN-CERT SESSIONS

Año YEAR	2013	2014
Nº de personas inscritas NO. OF PEOPLE REGISTERED	650	1.095
Nº asistentes NO. OF PEOPLE ATTENDING	510	956
Nº de organizaciones representadas NO. OF ORGANISATIONS REPRESENTED	140	265
Personal Administración Pública PUBLIC ADMINISTRATION STAFF	394	544
Personal de empresas interés estratégico STAFF FROM COMPANIES OF STRATEGIC INTEREST	81	306
Ponentes SPEAKERS	35	65
Prensa PRESS	-	41

Satisfacción global de las VIII Jornadas STIC CCN-CERT (%)
OVERALL SATISFACTION FOR THE 8TH CCN-CERT SICT SESSIONS (%)

	Excelente EXCELLENT	Muy bien VERY GOOD	Bien GOOD	Regular REGULAR	Insuficiente POOR
Aplicación de contenidos en su puesto de trabajo APPLICATION OF CONTENTS IN YOUR WORKPLACE	26,89	56,60	13,68	2,83	-
Duración de las Jornadas DURATION OF THE SESSIONS	22,86	51,43	20,48	2,86	2,38
Presentación y contenido de las Jornadas PRESENTATION AND CONTENT OF THE SESSIONS	31,60	52,36	13,68	1,89	0,47
Conocimientos adquiridos KNOWLEDGE ACQUIRED	20,38	53,08	22,27	3,79	0,47
Desarrollo y comprensión de lo expuesto DEVELOPMENT AND UNDERSTANDING OF PRESENTATIONS	24,64	55,92	18,96	0,47	-
Contenidos Contents	24,88	53,59	18,66	1,91	0,96
Ponentes Speakers	30,48	48,57	19,52	1,43	-

Más de mil personas se dieron cita en las VIII Jornadas STIC CCN-CERT, celebradas en el Colegio de Médicos de Madrid
Over a thousand people met up at the 8th CCN-CERT SICT Sessions held in the College of Doctors in Madrid

El secretario de Estado director del CNI, Félix Sanz Roldán, y el Jefe del Estado Mayor de la Defensa, Fernando García Sánchez, fueron los encargados de inaugurar las VIII jornadas, el 10 y 11 de diciembre de 2014
Secretary of State-Director of the CNI, Félix Sanz Roldán, and the Chief of the Defence Staff, Fernando García Sánchez, were in charge of inaugurating the 8th sessions, on 10th and 11th December 2014

Jornada SAT CCN-CERT[9]

En el año 2010, y con el fin de realizar una puesta en común con todos los organismos adscritos al **Sistema de Alerta Temprana (SAT)**, compartir conocimientos y necesidades y facilitar las novedades del servicio, el CCN-CERT organizó la primera edición de su Jornada SAT. Cinco años después, en 2014, se celebró su quinta edición, con más de 260 asistentes, representantes de las 66 organizaciones públicas y privadas (incluidos todos los Ministerios, ocho Comunidades Autónomas, tres ayuntamientos y seis empresas de interés estratégico para el país) adscritas al Sistema de Alerta Temprana de Internet, SAT-INET, del CCN-CERT. También, los responsables de seguridad de los 54 Organismos de las Administraciones Públicas conectadas a la red SARA y adheridos al Sistema de Alerta Temprana de la citada intranet, SAT-SARA.

[9] Todas las ponencias ofrecidas en estas Jornadas, como en las del SAT, se encuentran disponibles en el portal: https://www.ccn-cert.cni.es/
All the papers given at these Sessions, as for the SAT, are available on the website: https://www.ccn-cert.cni.es/

La sede de la Fábrica Nacional de la Moneda y Timbre acogió la V Jornada SAT del CCN-CERT
The National Mint headquarters hosted the 5th SAT Session by CCN-CERT

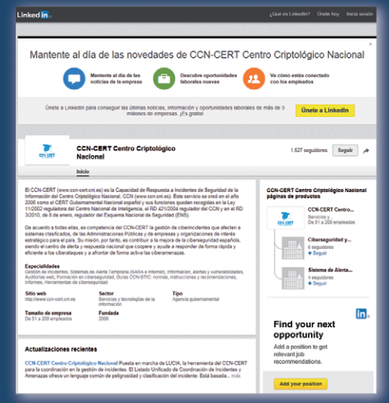
• **CCN-CERT SAT sessions**

In 2010, in order to pool all the organisms that are members of the **Early Warning System (SAT)**, share knowledge and needs and facilitate the new aspects of the service, the CCN-CERT organised the first edition of their SAT Sessions. Five years later, in 2014, it held its fifth edition with over 260 participants, representing the 66 public and private organisations (including all the Ministries, eight Regions, three town councils and six companies of strategic interest for the country) members of the Internet Early Warning System, SAT-INET, from the CCN-CERT. In addition, the people in charge of security for 54 Public Administration Organisations connected to the SARA network and members of the Early Warning Systems for the aforementioned Intranet, SAT-SARA.

A estas dos Jornadas se une la participación del CCN en jornadas especiales de sensibilización y concienciación sobre ciberseguridad y del Esquema Nacional de Seguridad en muy diversos organismos: CESEDEN, Agregados de Defensa, Funcionarios en prácticas de la Carrera Diplomática, futuros Oficiales Academia de Artillería de Segovia, Mando Conjunto de Ciberdefensa, Escuela de Técnicas de Mando Control y Telecomunicaciones. Así mismo, durante 2013 y 2014 se ha participado en más de 205 mesas redondas o jornadas como las desarrolladas por el Ministerio de Defensa, Fundación Circulo, Securmática, Cursos de verano del Mando de Doctrina (MADOC), etc.

En este mismo intento por promover una cultura de la ciberseguridad en nuestro país, el CCN-CERT colabora habitualmente con distintos medios de comunicación a los que facilita información detallada de los aspectos más destacados del sector y mantiene una actividad importante en diferentes redes sociales, como **Linkedin, Twitter y Youtube**, sumando más de cinco mil seguidores entre todas ellas.

En el intento por promover una cultura de la ciberseguridad en nuestro país, el CCN-CERT colabora habitualmente con distintos medios de comunicación y mantiene una actividad importante en diferentes redes sociales, como Linkedin, Twitter y Youtube, con más de cinco mil seguidores entre todas ellas



Alongside these two Sessions, the CCN also participated in special awareness raising sessions on cybersecurity and the National Security Scheme in very different organisations: CESEDEN, Military attachés, civil servants on work placements for the Diplomatic Service, future Officials from the Artillery Academy in Segovia, Cyver-defence Joint Command, School of Control and Telecommunication Command Techniques. In addition, during 2013 and 2014, it has taken part in over 205 round table discussions or sessions such as developed by the Ministry of Defence, Fundación Circulo, Securmática, Summer Courses on Doctrine Command (MADOC), etc.

In this same attempt to promote a cybersecurity culture in our country, the CCN-CERT works on a regular basis with different media by providing detailed information on the most outstanding aspects of the sector and maintains significant activity on different social networks such as **Linkedin, Twitter and Youtube**, bringing in over five thousand followers between them.

In an attempt to promote a cybersecurity culture in our country, the CCN-CERT works on a regular basis with different media and maintains significant activity on different social networks such as Linkedin, Twitter and Youtube with over five thousand followers between them

8.6 Relaciones y acuerdos institucionales

En el plano nacional

el CCN-CERT es miembro o colabora con:

- **Coordinador del grupo que elaboró la Estrategia Nacional de Ciberseguridad**
- **Ministerio de Hacienda y Administraciones Públicas**
  - Subdirección General del Comité Ejecutivo de la Comisión de Estrategia TIC, encargada de impulsar la transformación digital de la Administración de acuerdo a una Estrategia común en el ámbito de las TIC.
  - Acuerdo y colaboración con el Instituto Nacional de Administración Pública (INAP) y Secretaría de Estado para la Función Pública para impulsar la seguridad en el ámbito de la Administración Electrónica. En dicho acuerdo se contempla el desarrollo del Esquema Nacional de Seguridad.
  - Grupos de trabajo sobre comunicaciones electrónicas seguras; transposición de la directiva europea de medios de pago (SEPA), identificación y autenticación y servicios WEB de la Administración.
  - Grupo de Trabajo del Esquema Nacional Seguridad.
  - Grupo de Trabajo de Seguridad del Comité Sectorial de la Administración Electrónica (CCAA)
- **Ministerio de Defensa**

Grupo de Trabajo de cifra con el Estado Mayor Conjunto

Colaboración con el Mando Conjunto de Ciberdefensa..

- **Ministerio de Industria, Turismo y Comercio**
  - Grupos de trabajo de los proyecto Rescata, Seguridad y Confianza, usabilidad del DNIe (e-ID)
- **Ministerio del Interior**
  - Grupo de Trabajo sobre DNI electrónico con la Dirección General de la Policía
  - Grupo de Trabajo de Infraestructuras Críticas con la Secretaría de Estado de Seguridad
- **Federación Española de Municipios y Provincias**
  - Acuerdo de colaboración en materia de seguridad de la Información en los entidades locales
- **Junta de Castilla y León: apoyo a su Centro de Operaciones de Seguridad.**
- **Generalitat Valenciana. Convenio firmado y apoyo al CSIRT-CV.**
- **Generalitat de Catalunya: Firma de convenio de colaboración y apoyo al Centro de Seguridad: CESICAT.**
- **Junta de Andalucía: Convenio de colaboración para el Impulso de la Sociedad de la Información y apoyo al AndalucíaCERT.**

8.6 Agreements and partnerships

At the domestic level, the CCN-CERT is a member of and/or cooperates with:

- Coordinator of the group responsible for drafting the Spanish Cybersecurity Strategy
- Ministry of Finance and Public Administrations

• Deputy Directorate of the Executive Committee of the Commission of CIS Strategy, in charge of fostering the digital transformation of the Administration in compliance with a common CIS strategy.

• Agreement and partnership with the National Institute of Public Administration (INAP) and the State Secretariat for the Civil Service to promote security in the field of the Electronic Administration. This agreement envisages the drafting of the National Security Scheme.

• Working groups on secure electronic communications; implementation of the Single Euro Payments Area (SEPA), identification and authentication of Administration WEB services.

• Working group on the National Security Scheme.

• Working Group on Security of the Sectorial Committee of the Electronic Administration (Autonomous Regions)

- Ministry of Defense
- Ministry of Industry, Energy and Tourism

• Working groups on projects Rescata, Seguridad y Cofianza, DNIe (e-ID).

- Ministry of the Interior

• Working Group on e-ID in partnership with the General Directorate of the National Police.

• Working Group on Critical Infrastructure in partnership with the State Secretariat for Security.

- **Otras Comunidades Autónomas y Ayuntamientos (Adhesión al Servicio de Alerta Temprana, SAT, del CCN-CERT).**
- **Miembro de CSIRTes: grupo de trabajo CERT nacionales**
- **AENOR: Subcomités de seguridad TIC e identificación biométrica**
- **Foro ABUSES Grupo de Trabajo con Proveedores de Servicio de Internet (ISP)**

En el ámbito internacional

el CCN-CERT participa en las siguientes reuniones y grupos de trabajo:

- **NCIRC de la OTAN** (NATO Computer Incident Response Capability), en las que los distintos CERTs de los países miembros de esta Organización analizan y comparten información sobre seguridad de la información.
- Agencia Europea de la Seguridad de las Redes y la Información (**ENISA** -European Network & Information Security Agency-) de la Unión Europea.
- **APWG** (Anti-Phishing Working Group), un programa del Consejo de Europa enfocado a eliminar todo tipo fraude y robo de identidad a través del phishing[10], pharming[11] o correos fantasmas.
- 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.
- **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.
- **EGC** (European Government CERTs) group. Organización que reúne a los principales CERTs gubernamentales en Europa.

[10] Suplantación de identidad a través del envío de correos electrónicos que aparentan ser fiables y que suelen derivar a páginas web falsas/ Identity theft. This consists of sending emails that seem to be reliable and that usually lead to false websites

[11] Redirecciona malintencionadamente al usuario a un sitio web falso y fraudulento, mediante la explotación del sistema DNS/A. Users session is redirected to a masquerading website by corrupting a DNS server

- Spanish Federation of Municipalities and Provinces

• Agreement on cooperation on information security in local entities.

- Regional Government of Castilla and Leon: support to the Security Operation Centre.
- Regional Government of Valencia. Agreement and support to CSIRT-CV.
- Regional Government of Catalonia: Agreement and support to the Security Center: CESICAT.
- Regional Government of Andalusia: Cooperation agreement to foster Information Society and support to AndalucíaCERT.
- Other Autonomous Regions and City Councils (Adhesion to CCN-CERT's Early Alert System, SAT).
- Member of CSIRTes: Working group on national CERTs.
- AENOR (Spanish Association for Standardization and Certification): Subcommittees on CIS security and biometric identification.
- ABUSES Forum: Working group on Internet Service Providers (ISP).

Institutional connections and agreements

Internationally, the CCN-CERT takes part in the following meetings and work groups:

• **NCIRC** (NATO Computer Incident Response Capability), where the different CERTs from this Organisation's member countries analyse and share information on information security.

• **ENISA** - European Network & Information Security Agency.

• **APWG** (Anti-Phishing Working Group), a European Council Programme aiming to wipe out all types of fraud and identity theft through phishing[10], pharming[11] or ghost mails.

• **FIRST** (Forum of Incident Response and Security Teams), 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**, main European forum for CERTs where the most outstanding CERTS on the continent work together, innovate and share information; they also form part of TERENA, the Pan-European Association of Network Research and Education.

• **EGC** (European Government CERTs) group. Organisation that brings together the main governmental CERTS in Europe.

Edita: Centro Criptológico Nacional
Edit: National Cryptologic Centre

Diseño, maquetación e infografías: V.O. infográfica
Design: V.O. infográfica

Fotografía: Centro Criptológico Nacional
Photography: National Cryptologic Centre

D.L. 27859-2015

Centro Criptológico Nacional
Argentona, 20 - 28023 Madrid
www.ccn-cni.es - www.ccn-cert.es - www.oc.ccn.cni.es