MEMORIA
ACTIVIDAD
CCN

INFORME DE ACTIVIDADES _2020

ACTIVITY REPORT

CCN
centro criptológico nacional

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

MEMORIA ACTIVIDAD CCN

INFORME DE ACTIVIDADES _2020

ACTIVITY REPORT

Carta de la SED

Letter from the Secretary of State Director of the CNI

Querido/a lector/a

Es indudable que vivimos un tiempo nuevo, un tiempo que nos exige a todos un gran esfuerzo para estar en condiciones de aprovechar las enormes oportunidades que la tecnología nos ofrece. Pero también, a su vez, para hacer frente a los considerables desafíos que la revolución digital está generando.

En este sentido, la pandemia de COVID-19 que nos ha obligado a utilizar la tecnología hasta niveles impensables hace poco más de un año, ha propiciado un aumento significativo en las ciberamenazas a las que nos enfrentamos. Su agresividad y su criticidad queda patente en el número de ciberincidentes que gestionó en 2020 la Capacidad de Respuesta a Incidentes del Centro Criptológico Nacional, CCN-CERT. En total, fueron 82.530 (un 91% más que el año anterior) de los cuales, 62 fueron considerados críticos por nuestros expertos.

Como secretaria de Estado directora del Centro Nacional de Inteligencia, he podido comprobar la evolución e incremento de estas amenazas en los últimos años y cómo la actual pandemia está acelerando esta tendencia. Nos encontramos en una situación excepcional, en la que organizaciones, instituciones y profesionales han tenido que desarrollar el grueso de su actividad de forma remota. Nos ha puesto a prueba a todos: a nosotros como Servicio de Inteligencia, al sector de la ciberseguridad en general y a la sociedad en su conjunto.

Prueba de ello es el enorme despliegue de entornos tecnológicos de teletrabajo que se han implementado para salvaguardar la continuidad de actividades y negocios y que han supuesto nuevos escenarios de riesgo para las propias organizaciones: el aumento de la superficie de exposición y nuevos vectores de ataque, el incremento del uso de equipos personales para acceder a recursos corporativos o las vulnerabilidades detectadas en herramientas, plataformas y aplicaciones que tanto han facilitado el trabajo a distancia.

Dear reader

There is no doubt that we are living in a new time, a time that demands a great effort from all of us to be in a position to take advantage of the enormous opportunities that technology can offer to us. But also, at the same time, to face the considerable challenges that the digital revolution is generating.

In this regard, the COVID-19 pandemic, which has forced us to use technology to levels that were unthinkable just over a year ago, has led to a significant increase in the cyber threats we face. Their aggressiveness and criticality are evident in the number of cyber incidents managed in 2020 by the Computer Emergency Response Team of the National Cryptologic Centre, CCN-CERT. In total, there were 82,530 (91% more than the previous year) of which 62 were considered critical by our experts.

As Secretary of State and Director of the National Intelligence Centre, I have been able to see the evolution and increase of these threats in recent years and how the current pandemic is accelerating this trend. We are in an exceptional situation, in which organisations, institutions and professionals have had to carry out the bulk of their activities remotely. It has tested all of us: as an Intelligence Service, as the cyber security industry in general and society as a whole.

A proof of this is the enormous deployment of teleworking technological environments that have been implemented to safeguard the continuity of activities and businesses and that have led to new risk scenarios for the organisations themselves: the increase in the surface of exposure and new attack vectors, the increase in the use of personal computers to access corporate resources or the vulnerabilities detected in tools, platforms and applications that have made remote work so much easier.

Esta situación extraordinaria e imprevista nos ha exigido a todos reaccionar y adaptarnos con rapidez. Por ello, desde el inicio de la pandemia, tal y como podrá verse en estas páginas que presentamos, reforzamos todas nuestras capacidades para la defensa del ciberespacio español y, en especial, de su sector público y de los sectores estratégicos, con prioridad absoluta en el de la salud y la educación. Desde entonces, hemos estado a pleno rendimiento, brindando apoyo y colaboración a todas las organizaciones ante cualquier emergencia que pudieran sufrir.

Del mismo modo, seguimos colaborando en cuantas iniciativas doten a España de un marco de actuación óptimo para la defensa de su ciberespacio y donde la actualización del Esquema Nacional de Seguridad, cuya publicación está prevista para finales de este año 2021, es buena prueba de ello.

Nos sentimos especialmente orgullosos de haber contribuido a situar a nuestro país en el cuarto puesto a nivel mundial en el Índice Global de Ciberseguridad 2020 elaborado por la Unión Internacional de Telecomunicaciones de Naciones Unidas.

Y todo ello con el compromiso firme y constante de todos los hombres y mujeres que trabajan en el CCN. Un compromiso que ha caracterizado a este Centro durante sus casi 17 años de historia en los cuales ha trabajado sin descanso por fortalecer la ciberseguridad nacional, velar por la información segura y confiable, promocionar el uso de productos y tecnologías seguras y proteger, en definitiva, el ciberespacio español.

This extraordinary and unforeseen situation has required us all to react and adapt quickly. For this reason, since the beginning of the pandemic, as can be seen in these pages, we have reinforced all our capabilities to defend Spanish cyberspace and, in particular, its public sector and strategic sectors, with absolute priority given to the health and education sectors. Since then, we have been at full capacity, providing support and collaboration to all organisations in the event of any emergency they might suffer.

In the same way, we continue to collaborate in all initiatives that provide Spain with an optimal framework for the defence of its cyberspace, and the updating of the National Security Framework, whose publication is planned for the end of 2021, is good proof of this.

We are especially proud to have contributed to placing our country in fourth place worldwide in the Global Cybersecurity Index 2020 prepared by the United Nations International Telecommunications Union.

And all this with the firm and constant commitment of all the men and women who work at the CCN. A commitment that has characterised this Centre during its almost 17 years of history, during which it has worked tirelessly to strengthen national cybersecurity, ensure secure and reliable information, promote the use of secure products and technologies and protect, in short, Spanish cyberspace.

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

ÍNDICE
INDEX

04 Carta de la SED
Letter from the Secretary of State Director of the CNI

08 1. El año de la pandemia
1. The year of the pandemic

12 2. Nueva normativa
2. New regulations

13 3. ENS
3. ENS

13 3.1 EVENS
3.1 EVENS

14 3.2 CoCENS
3.2 CoCENS

15 3.3 Entidades de certificación
3.3 Certification Bodies

16 Servicios de Ciberseguridad
Cybersecurity Services

17 4. Prevención
4. Prevention

17 4.1 Prevención proactiva
4.1 Proactive prevention

17 4.1.1 Gestión continua de la seguridad
4.1.1 Continuous Security Management

20 4.1.2 Formación y concienciación
4.1.2 Training and awareness

26 4.1.3 Informes, avisos, alertas y vulnerabilidades
4.1.3 Reports, warnings, alerts and vulnerabilities

30 4.1.4 Guías CCN-STIC
4.1.4 CCN-STIC Guides

33 4.2 Seguridad TIC. Desarrollo, evaluación y certificación de productos
4.2 ICT security. Product development, evaluation and certification

33 4.2.1 Productos para la seguridad de las TIC
4.2.1 ICT Security Products

36 4.2.2 Evaluación de productos de cifra
4.2.2 Crypto products evaluation

37 4.2.3 Evaluación y certificación TEMPEST / ZONING
4.2.3 TEMPEST / ZONING evaluation and certification

38 4.2.4 Cualificación y aprobación de productos STIC
4.2.4 STIC products qualification and approval

40 4.2.5 Certificación de productos STIC
4.2.5 STIC Product Certification

43 4.2.6 Grupos de trabajo nacionales e internacionales
4.2.6 National and international working groups

45 4.2.7 Programas nacionales e internacionales
4.2.7 National and international programs

46 4.2.8 Arquitecturas de seguridad y otros documentos
4.2.8 Security architectures and other documents

47 5. Detección
5. Detection

47 5.1 Gestión y respuesta a incidentes
5.1 Incident Management and Response

49 5.2 Sistema de Alerta Temprana (SAT)
5.2 Sistema de Alerta Temprana (SAT)

51 5.3 Análisis
5.3 Analysis

52 5.4 Vigilancia
5.4 Surveillance

53 5.5 Intercambio de información
5.5 Information exchange

54 6. Respuesta
6. Response

54 6.1 Centro de Operaciones de Ciberseguridad
6.1 Cybersecurity Operations Centre

56 7. Cultura de ciberseguridad
7. Cybersecurity Culture

66 8. Programas, grupos de trabajo y acuerdos de colaboración
8. Programmes, working groups and collaboration agreements

1. El año de la pandemia
1. The year of the pandemic

El 2020 pasará a la historia universal como el año de la pandemia provocada por la COVID-19 con todas sus dramáticas consecuencias. En el caso de España provocó la activación del estado de alarma desde el 14 de marzo hasta el 20 de junio y desde el 25 de octubre hasta mayo de 2021.

The year 2020 will be referred to in universal History as the year of the pandemic caused by the COVID-19 with all its dramatic consequences. In the case of Spain, it provoked the activation of the state of alarm from March 14 to June 20 and from October 25 to May 2021.

Desde los primeros días de esta situación, el Centro Criptológico Nacional (CCN), y especialmente su Capacidad de Respuesta a Incidentes de Seguridad (CCN-CERT), registraba un incremento importante en el número de ciberataques en todos los sectores.

Los ciberatacantes, conocedores de la necesidad de los ciudadanos por querer estar al día sobre las novedades relativas a la pandemia, adaptaron sus ataques empleando esta temática para atraer interés y aprovecharon la excepcional y apresurada situación de teletrabajo para incrementar sus acciones. De esta forma, surgía otra crisis, pero en este caso en el ciberespacio.

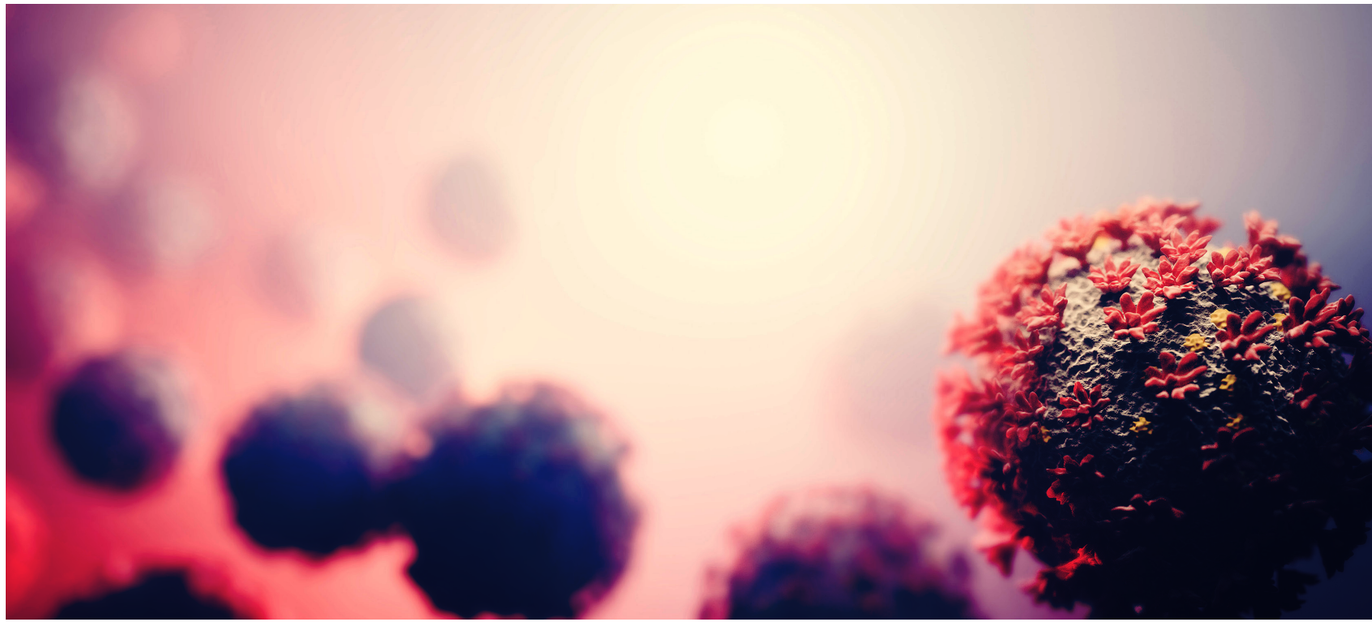
El CCN fue detectando campañas de código dañino que empleaban temáticas relacionadas con la pandemia, como NetWalker, que simulaba aportar información sobre el estado actual de la COVID-19 a través de correos electrónicos, Guloader, que usaba de gancho una falsa vacuna, y AZORult que se distribuía a través de una app que fingía ser un "mapa del coronavirus" para conocer su evolución. En menos de diez días, se registraron más de 24.000 dominios en Internet que contenían los términos: "coronavirus" y "covid-19". De ellos, más de la mitad, 16.000, fueron creados en el mes de marzo (10.000 en una semana). Algunos de ellos tenían fines legítimos, pero otros estaban dedicados a realizar campañas de spam, spear-phishing o como servidores de mando y control, C2.

From the first days of this situation, the National Cryptologic Centre (CCN), and especially its Computer Emergency Response Team (CCN-CERT), recorded a significant increase in the number of cyberattacks in all sectors.

The cyberattackers, aware of the need for citizens to keep up to date with news about the pandemic, adapted their attacks using this theme to attract interest and took advantage of the exceptional and hurried situation of teleworking to increase their actions. In this way, another crisis arose, but in this case in cyberspace.

The CCN was detecting malware campaigns that used themes related to the pandemic, such as NetWalker, which pretended to provide information on the current status of COVID-19 through emails, Guloader, which used a fake vaccine as a hook, and AZORult, which was distributed through an app that pretended to be a "coronavirus map" to know its evolution. In less than ten days, more than 24,000 domains were registered on the Internet containing the terms: "coronavirus", "covid19" and "covid-19". More than half of them, about 16,000, were created in March (10,000 in one week). Some of them had legitimate purposes, but others were dedicated to spam campaigns, spear-phishing or as command and control servers, C2.

INFORME DE ACTIVIDADES _2020 - ACTIVITY REPORT _2020



También se detectó que algunos troyanos como Trickbot y Emotet habían evolucionado sus tácticas, técnicas y procedimientos (TTP) para evadir los procesos de detección.

Dada esta situación, el CCN desde el primer momento reforzó todas sus capacidades para la defensa del ciberespacio español y, en especial, de su sector público y de los sectores estratégicos, con prioridad absoluta en el de la salud. Desde entonces, el CCN-CERT redobló sus esfuerzos, brindando apoyo y colaboración a todas las organizaciones ante cualquier emergencia que pudieran sufrir.

Se pusieron en marcha numerosas iniciativas encaminadas a gestionar esta crisis, para lo cual fue clave la coordinación a nivel público estatal de los distintos CERT/CSIRT, la información permanente sobre la seguridad en el teletrabajo y la colaboración público-privada. En este sentido, surgió una iniciativa insólita hasta la fecha: coordinados por el CCN-CERT, diferentes empresas que operan en nuestro país en el sector de la ciberseguridad decidieron ofrecer de manera altruista algunos servicios y soluciones para diferentes organizaciones, principalmente del sector público.

Some Trojans such as Trickbot and Emotet were also found to have evolved their tactics, techniques and procedures (TTP) to evade detection processes.

Given this situation, the CCN immediately reinforced all its capabilities to defend Spanish cyberspace and, in particular, its public sector and strategic sectors, with absolute priority given to the health sector. Since then, the CCN-CERT has redoubled its efforts, providing support and collaboration to all organisations in the event of any emergency they might suffer.

Numerous initiatives were launched to manage this crisis, for which the coordination of the different CERTs/CSIRTs at state public level, the permanent information on security in telework and the public-private collaboration were key. In this sense, an unusual initiative arose: coordinated by the CCN-CERT, different companies operating in our country in the cybersecurity sector, decided to altruistically offer some services and solutions for different organisations, mainly in the public sector.

Del mismo modo, el CCN proporcionó numerosos recursos de interés, tales como listas negras con indicadores de compromiso, Informes de Buenas Prácticas, ciberconsejos, etc[1].

Similarly, the CCN provided numerous resources of interest, such as blacklists with indicators of compromise, Good Practice Reports, cyber-advice, etc[1].

Iniciativa *Initiative*	#CiberCOVID19	Creación del hashtag para informar de campaña de ransomware. *Creation of the hashtag to report the ransomware campaign.*
Concienciación *Awareness*	35	Infografías elaboradas con recomendaciones de ciberseguridad. *Infographics with cybersecurity recommendations.*
Formación *Training*	30	Actividades de formación a distancia impulsadas por el CCN. *Distance learning activities promoted by the CCN.*
Dominios *Domains*	#185	Dominios de hospitales, agencias y empresas públicas, auditados. *Audited hospital, agency and public company domains.*
Subdominios *Subdomains*	+2,1K	Subdominios relacionados con el sector salud, analizados. *Subdomains related to the health sector, analysed.*
Soluciones *Solutions*	2	Soluciones de seguridad para incrementar la vigilancia: ANA y EMMA. *Security solutions for increased vigilance: ANA and EMMA.*

Detección / *Detection*

Dominios *Domains*	103k	Nombres de sitios web detectados que hacen referencia al COVID-19. *Website names detected that refer to COVID-19.*
Informes *Reports*	20	Informes de análisis de código dañino con temática COVID-19. *Malware reports with COVID-19 thematic.*
Vulnerabilidades *Vulnerabilities*	18	Alertas publicadas sobre riesgos y vulnerabilidades en servicios externos. *Alerts published on risks and vulnerabilities in external services.*

Respuesta / Response

Seguridad ampliada *Extended security*	125	Representantes de CC.AA. y servicios de salud, en un mismo grupo de trabajo. *Representatives of CC.AA. and health services, in the same working group.*
Soluciones *Solutions*	2	Soluciones CCN: **EMMA-VAR** y **microCLAUDIA** *CCN Solutions:* ***EMMA-VAR*** *y* ***microCLAUDIA***
Coordinación nacional *National Coordination*	44	CERT nacionales, en contacto para fomentar el intercambio. *National CERTs in contact to promote exchange.*

Principales acciones del CCN durante la pandemia de COVID-19

Key CCN Actions During the COVID-19 Pandemic

1. Dado el gran número de iniciativas llevadas a cabo por el CCN para hacer frente a los riesgos cibernéticos asociados a la pandemia, el Organismo creó la sección 'CiberCOVID19', para recoger todas estas acciones.

1. Given the large number of initiatives carried out by the CCN to address the cyber risks associated with the pandemic, the Centre created the section **'CiberCOVID19'** to collect all these actions.

Dichas iniciativas se agruparon en seis categorías:

- Alertas y avisos: el CCN-CERT fue alertando a su Comunidad de la detección de nuevas campañas de malware que empleaban temáticas relacionadas con la pandemia del coronavirus.
- Indicadores de compromiso: se recopilaron en tres listas negras los IOC que permitían la detección y bloqueo de muchas de las campañas que se aprovechaban de la situación provocada por la crisis de la COVID-19: listas de IP, dominios y hashes de las muestras empleadas.
- Formación: rápidamente, el Centro Criptológico Nacional hizo un importante esfuerzo por adaptar la oferta formativa presencial a enseñanzas en modalidad online. Además de impartir las acciones formativas previstas, se organizaron 30 webinars en Vanesa especialmente enfocados a la protección del teletrabajo. Asimismo, se desarrolló un nuevo curso online sobre principios y recomendaciones básicas en ciberseguridad, al objeto de fomentar la formación en ciberseguridad.
- Informes: documentación desarrollada por el CCN para abordar, desde el punto de vista de la ciberseguridad, algunos de los aspectos más destacados generados en esta crisis. Entre los informes elaborados, caben destacar el Informe de Buenas Prácticas CCN-CERT BP/18 *Recomendaciones de Seguridad para situaciones de teletrabajo y refuerzo en vigilancia,* así como un documento sobre Acceso Remoto Seguro o los diversos informes de código dañino que se publicaron en el portal del CCN-CERT.
- Asimismo, se creó un espacio de colaboración con las distintas Administraciones Públicas. En el portal del CCN-CERT se compartió la labor llevada a cabo desde estos organismos, tanto de la Administración General del Estado como de las Comunidades Autónomas y Entidades Locales, frente a la crisis generada por la COVID-19.
- Concienciación: desde el Centro Criptológico Nacional se desarrollaron diversas campañas de concienciación, en las que se compartieron diferentes recomendaciones de ciberseguridad elaboradas por el CCN-CERT para evitar los riesgos asociados al incremento de las campañas de malware. Asimismo, se creó un hilo en redes sociales bajo los hashtags #NoTeinfectesConElMail y #CiberCOVID19, con información actualizada frecuentemente sobre la detección de nuevas amenazas.

These initiatives were grouped into six categories:

- Alerts and warnings: the CCN-CERT alerted its Community of the detection of new malware campaigns employing topics related to the coronavirus pandemic.
- Indicators of compromise: IOC that allowed the detection and blocking of many of the campaigns that took advantage of the situation caused by the COVID-19 crisis were collected in three blacklists: lists of IPs, domains and hashes of the samples used.
- Training: the National Cryptologic Centre quickly made a major effort to adapt its face-to-face training offer to online courses. In addition to the training courses, 30 webinars were organized in Vanessa, especially focused on the protection of telework. A new online course on basic principles and recommendations in cybersecurity was also developed in order to promote training in cybersecurity.
- Reports: documentation developed by the CCN to address, from the cybersecurity point of view, some of the most important aspects generated in this crisis. Among the reports produced, it is worth highlighting the CCN-CERT Best Practices Report BP/18 *Security Recommendations for teleworking and surveillance reinforcement situations*, as well as a document on Secure Remote Access or the various malware reports that were published on the CCN-CERT website.
- A space for collaboration with the different Public Administrations was also created. The CCN-CERT website shared the work carried out by these bodies, both from the General State Administration and the Autonomous Communities and Local Entities, in the face of the crisis generated by COVID-19.
- Awareness: the National Cryptologic Centre developed various awareness campaigns, in which different cybersecurity recommendations developed by the CCN-CERT were shared to avoid the risks associated with the increase in malware campaigns. Likewise, a thread was created on social networks under the hashtags #NoTeinfectesConElMail and #CiberCOVID19, with frequently updated information on the detection of new threats.

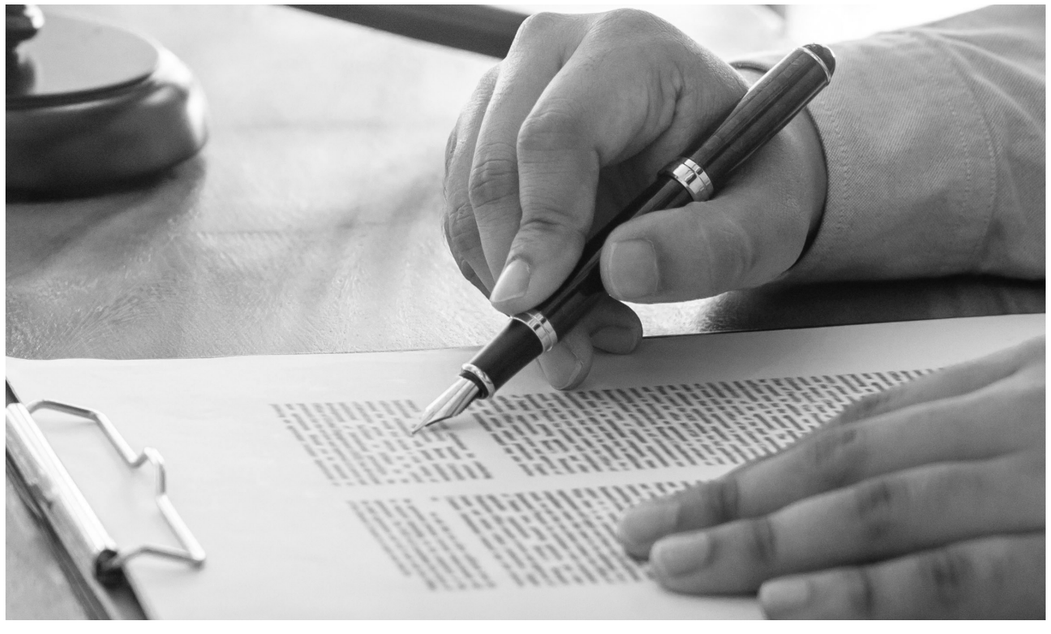
2. Nueva normativa
2. New regulations

A la espera del desarrollo definitivo de un nuevo Esquema Nacional de Seguridad, cuya publicación está prevista para el año 2021, el 28 de enero de 2021 se publicó en el Boletín Oficial del Estado el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

Pending the definitive development of a new National Security Framework, whose publication is scheduled for 2021, on 28 January 2021 Royal Decree 43/2021, of 26 January, was published in the Official State Bulletin, developing Royal Decree-Law 12/2018, of 7 September, on the security of networks and information systems.

Este RD en el que se trabajó a lo largo de todo el año 2020 tiene como objeto desarrollar la trasposición de la Directiva NIS al ordenamiento jurídico español en lo relativo al marco estratégico e institucional de seguridad de las redes y sistemas de información, la supervisión del cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales, y la gestión de incidentes de seguridad.

This RD, which was worked on throughout 2020, aims to develop the transposition of the NIS Directive to the Spanish legal system regarding the strategic and institutional framework for the security of networks and information systems, the supervision of compliance with the security obligations of operators of essential services and digital service providers, and the management of security incidents.



3. ENS
3. ENS

El Esquema Nacional de Seguridad (ENS) proporciona al sector público en España un planteamiento común de seguridad para la protección de la información que maneja y los servicios que presta.

The National Security Framework (ENS) provides the public sector in Spain with a common security approach for the protection of the information it handles and the services it provides.

Impulsa la gestión continuada de la seguridad, imprescindible para la transformación digital en un contexto de ciberamenazas; a la vez que facilita la cooperación y proporciona un conjunto de requisitos uniforme a la Industria, constituyendo también un referente de buenas prácticas.

It promotes continuous security management, essential for digital transformation in a context of cyber threats; at the same time, it facilitates cooperation and provides a uniform set of requirements to the industry, also constituting a benchmark of good practices.

3.1 EVENS
3.1 EVENS

Durante el año 2020, el CCN desarrolló el Entorno de validación del ENS (EVENS), con el objetivo de integrar en un único espacio colaborativo todos los recursos relacionados con el Esquema Nacional de Seguridad disponibles hasta la fecha (Información, Herramientas, Desarrollos, Guías, Noticias, Normativa, Entidades, Cultura de Ciberseguridad, etc.).

During 2020, the CCN developed the ENS Validation Environment (EVENS), with the aim of integrating in a single collaborative space all the resources related to the National Security Framework available to date (Information, Tools, Developments, Guides, News, Regulations, Entities, Cybersecurity Culture, etc.).

ENTORNO DE VALIDACIÓN ENS

El EVENS permite medir el estado de seguridad a través de un cuadro de mandos para la gobernanza de la ciberseguridad del sector público al permitir obtener información, analizar datos, extraer conclusiones y tomar decisiones estratégicas mediante el Módulo de Inteligencia de INÉS.

EVENS makes it possible to measure the state of security through a scorecard for the governance of public sector cybersecurity by making it possible to obtain information, analyse data, draw conclusions and make strategic decisions through the INÉS Intelligence Module.

3.2 CoCENS

3.2 CoCENS

El Consejo de Certificación del Esquema Nacional de Seguridad (CoCENS) es un órgano colegiado, regulado por lo dispuesto en la Sección 3ª del Capítulo II del Título Preliminar, de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y lo establecido en la Guía CCN-STIC 809 de Declaración y Certificación de Conformidad con el ENS.

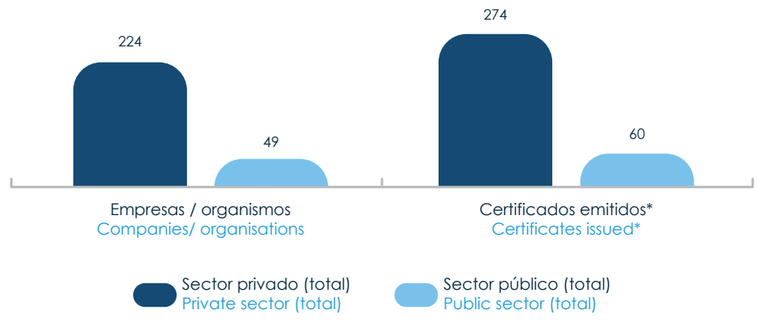
The Certification Council of the National Security Framework (CoCENS) is a collegiate body, regulated by the provisions of Section 3 of Chapter II of the Preliminary Title of Law 40/2015, of 1 October, on the Legal Regime of the Public Sector and the provisions of the CCN-STIC Guide 809 of Declaration and Certification of Conformity with the ENS.

CoC ens
Consejo de Certificación del Esquema Nacional de Seguridad

Entre sus funciones tiene la de alentar los procesos de Certificación de la Conformidad con el ENS en las entidades de los sectores público y privado. Y en 2020 fueron certificadas un total de 114 empresas y 24 organismos públicos.

One of its functions is to encourage the processes of Certification of Conformity with the ENS in public and private sector entities. In 2020, a total amount of 114 companies and 24 public bodies were certified.

Total de empresas y organismos certificados
Total number of certified companies and organizations



* Una empresa u organismo puede tener más de una certificación

*A company or body may have more than one certification.

Entre las funciones del CoCENS, también destaca la redacción y publicación de Normas, Criterios o Buenas Prácticas en materia de Certificación de la Conformidad con el ENS. En este sentido, en 2020 elaboró un nuevo informe y tres nuevos abstracts.

Among the functions of CoCENS, the drafting and publication of Standards, Criteria or Good Practices in the field of ENS Conformity Certification also stands out. In this regard, in 2020 it produced a new report and three new abstracts.

3.3 Entidades de certificación

3.3 Certification Bodies

La Entidad Nacional de Acreditación (ENAC) pone a disposición de los interesados el esquema de acreditación de entidades que quieran certificar el cumplimiento con el Esquema Nacional de Seguridad (ENS). Este esquema fue desarrollado por ENAC en colaboración con la Secretaría General de Administración Digital (Ministerio de Asuntos Económicos y Transformación Digital) y el CCN. En 2020, las organizaciones, tanto del sector privado como público, que fueron certificadas fueron IVAC - Instituto de Certificación, OCA Global y SGS Española de Control. Unidad técnica: CyberLab Madrid.

The National Accreditation Entity (ENAC) makes available to interested parties the accreditation framework for entities that want to certify compliance with the National Security Framework (ENS). This framework was developed by ENAC in collaboration with the General Secretariat for Digital Administration (Ministry of Economic Affairs and Digital Transformation) and the CCN. In 2020, the organisations, both private and public sector, that were certified were IVAC - Certification Institute, OCA Global and SGS Española de Control. Technical Unit: CyberLab Madrid.

SERVICIOS DE CIBERSEGURIDAD

CYBERSECURITY SERVICES

INFORME DE ACTIVIDADES _2020 - ACTIVITY REPORT _2020

4. Prevención
4. Prevention

La prevención es una de las principales medidas de ciberseguridad para evitar posibles incidentes. Conocer la organización, sus vulnerabilidades, deficiencias, malas praxis, carencias, así como sus potenciales amenazas, suponen una información de gran valor a la hora de evitar ciberincidentes. Por este motivo, el Centro Criptológico Nacional lleva años desarrollando y mejorando herramientas y soluciones que contribuyan a prevenir estos riesgos.

Prevention is one of the main cybersecurity measures to avoid possible incidents. Knowing the organisation, its vulnerabilities, deficiencies, malpractices, shortcomings and potential threats is extremely valuable information when it comes to avoiding cyberincidents. For this reason, the National Cryptologic Centre has been since its creation developing and improving tools and solutions to prevent these risks.

4.1 Prevención proactiva
4.1 Proactive prevention

4.1.1 Gestión continua de la seguridad
4.1.1 Continuous Security Management

La gestión continua de la seguridad es un aspecto clave de la prevención proactiva, en la que el Centro Criptológico Nacional ha trabajado durante 2020 mediante soluciones que facilitan la mejora continua y la gobernanza de la seguridad.

Continuous security management is a key aspect of proactive prevention, which the National Cryptologic Centre has been working on during 2020 through solutions that facilitate continuous improvement and security governance.

Mejora continua de la seguridad
Continuous security improvement

En 2020 se hizo más evidente la necesidad de analizar las deficiencias de configuración y vulnerabilidades de equipos, y medir la superficie de exposición de los sistemas; tareas que el Centro Criptológico Nacional lleva a cabo con su solución ANA, al objeto de reducir el tiempo de respuesta ante posibles incidentes.

In 2020 it became more evident the need to analyse configuration deficiencies and equipment vulnerabilities, and to measure the exposure surface of the systems; tasks that the National Cryptologic Centre carries out with its ANA solution, in order to reduce the response time to possible incidents.

Precisamente, en 2020 y mediante el empleo de ANA, el CCN realizó un importante esfuerzo extra con motivo de la pandemia de COVID-19. Concretamente, en la protección de sectores muy críticos como el de la salud y la educación. Por ello, el CCN llevó a cabo auditorías de seguridad en 23 organismos y 185 hospitales y agencias, con el objetivo de reducir su superficie de exposición. Del mismo modo, dado el incremento de exámenes online, el CCN protegió a las instituciones de enseñanza, asegurando las plataformas de 25 universidades para que estas fueran resilientes a ataques de denegación de servicio.

Precisely, in 2020 and through the use of ANA, the CCN made an important extra effort on the occasion of the COVID-19 pandemic. Specifically, in the protection of very critical sectors such as health and education. Therefore, the CCN carried out security audits in 23 organisations and 185 hospitals and agencies, with the aim of reducing their exposure surface. Similarly, given the increase in online exams, the CCN protected educational institutions, securing the platforms of 25 universities to make them resilient to denial-of-service attacks.

Gobernanza de la seguridad
Security governance

El Centro Criptológico Nacional ha desarrollado los asistentes del Plan de Adecuación y el de Implantación y Gestión de la Conformidad como elementos de apoyo para la Obtención y Gestión de la Declaración / Certificación de Conformidad con el ENS, que junto con el resto de soluciones del ecosistema CCN-CERT contribuyen a la Gestión Continua de la seguridad.

Los diferentes desarrollos llevados a cabo en 2020 en las soluciones INES y AMPARO para la gobernanza de la seguridad han facilitado los procesos de implantación y gestión de la seguridad en entidades y organismos.

The National Cryptologic Centre has developed the assistants of the Adaptation Plan and the Implementation and Compliance Management Plan as support elements for obtaining and managing the Declaration / Certification of Conformity with the ENS, which contribute to the Continuous Management of security with the rest of the solutions of the CCN-CERT ecosystem.

The different developments carried out in 2020 in the INES and AMPARO solutions for security governance have facilitated the processes of implementation and management of security in entities and organisations.

INÉS

Para conocer y evaluar el estado de seguridad de los sistemas TIC de las entidades y su adecuación al ENS, más de 1.200 organismos hacen uso de la solución INÉS. De esta forma, en 2020 aumentó un 11% la participación de los organismos en la elaboración del Informe Nacional del Estado de Seguridad (INÉS).

Para facilitar la conformidad con el Esquema Nacional de Seguridad de los sistemas de los organismos del sector público, el CCN-CERT automatizó en INÉS las fases del proceso de adecuación al ENS y desarrolló el nuevo Asistente que permite elaborar y obtener de manera guiada el Plan de Adecuación de un sistema.

También como novedad la solución INÉS permaneció abierta durante todo el año para que los organismos pudieran actualizar sus datos y conocer sus índices de seguridad TIC en todo momento. El objetivo de este cambio es fomentar la mejora continua y la gestión de la seguridad.

In order to know and evaluate the security status of the ICT systems of the entities and their compliance with the ENS, more than 1,200 organisations use the INES solution. Thus, in 2020, the participation of organisations in the preparation of the National Security Status Report (INÉS) increased by 11%.

In order to facilitate the compliance with the National Security Framework of the systems of public sector organisations, the CCN-CERT automated the phases of the ENS compliance process in INÉS and developed the new Assistant that allows to elaborate and obtain in a guided way the Compliance Plan of a system.

Also, as a novelty, the INÉS solution remained open throughout the year so that organisations could update their data and know their ICT security indexes at all times. The aim of this change is to promote continuous improvement and security management.

INFORME DE ACTIVIDADES _2020 - ACTIVITY REPORT _2020

AMPARO

Para facilitar el proceso de implantación de seguridad y adecuación al Esquema Nacional de Seguridad (ENS) de entidades y organismos, el Centro Criptológico Nacional mejoró e incrementó en 2020 las capacidades de la solución AMPARO. A través de su asistente de implantación de Seguridad y Conformidad, se incorporaron en AMPARO diversas funcionalidades para facilitar este proceso, así como las posteriores fases de certificación y gestión continua de la seguridad.

De este modo, la solución guía a los usuarios en todo el proceso, aportando ayudas, guías, herramientas e información útil para la implementación de cada una de las medidas de seguridad. Asimismo, una vez completada la implantación, AMPARO permite evaluar la seguridad del sistema y obtener de forma automática la Declaración de Aplicabilidad para ENS categoría BÁSICA.

Además, a través de AMPARO, los usuarios pueden solicitar auditorías de conformidad del ENS a Entidades de Certificación acreditadas, puesto que también actúa como punto de encuentro entre los diferentes actores que participan en el proceso: Organismos, Entidades de Certificación, Organismos de Auditoría y Entidades supervisoras de seguridad.

In order to facilitate the process of security implementation and adaptation to the National Security Framework (ENS) of entities and organisations, the National Cryptologic Centre improved and increased the capabilities of the AMPARO solution in 2020. Through its Security and Compliance implementation assistant, various functionalities were incorporated into AMPARO to facilitate this process, as well as the subsequent phases of certification and continuous security management.

In this way, the solution guides users throughout the process, providing help, guides, tools and useful information for the implementation of each of the security measures. Likewise, once the implementation is completed, AMPARO allows to evaluate the security of the system and automatically obtain the Declaration of Applicability for ENS BASIC category.

In addition, through AMPARO, users can request ENS compliance audits from accredited Certification Bodies, since it also acts as a meeting point between the different actors involved in the process: Bodies, Certification Bodies, Audit Bodies and Security Supervisory Bodies.

EMMA

Durante 2020 se potenció especialmente la función de EMMA que permite la vigilancia de accesos remotos. Además, esta solución para el control de acceso a las infraestructuras de red fue incluida durante este año como producto cualificado en el Catálogo de Productos y Servicios STIC (CCN-STIC-105), por lo que desde entonces se considera adecuada para ser utilizada en sistemas de Categoría Alta en el Esquema Nacional de Seguridad (ENS).

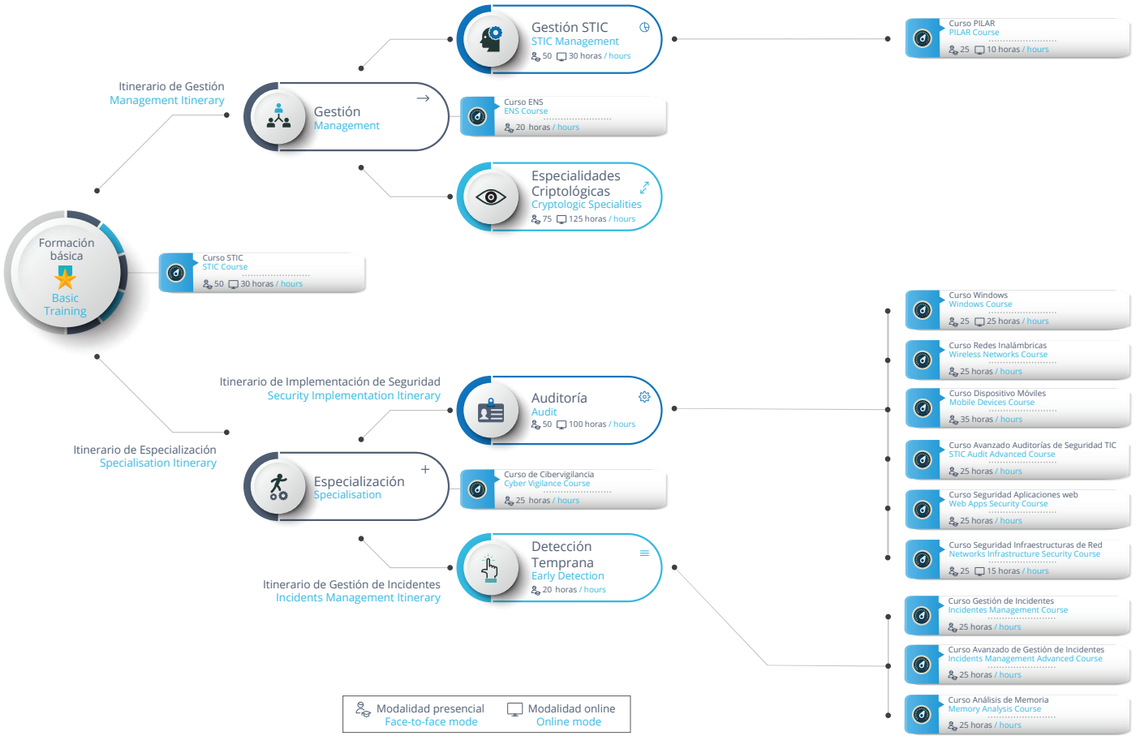
During 2020, the EMMA function that enables remote access monitoring was particularly enhanced. In addition, this solution for access control to network infrastructures was included during this year as a qualified product in the Catalogue of Products and Services STIC (CCN-STIC-105), so since then it is considered suitable for use in High Category systems in the National Security Framework (ENS).

4.1.2 Formación y concienciación
4.1.2 Training and awareness

Plan de Formación
Training Plan

Una de las principales misiones del CCN es llevar a cabo iniciativas de concienciación y formación en ciberseguridad, plasmadas en su Plan de Formación 2020, un documento en el que se contempla un amplio programa de cursos, siempre adaptado a las necesidades planteadas por su Comunidad de referencia.

One of the main missions of the CCN is to carry out awareness and training initiatives in cybersecurity, embodied in its Training Plan 2020, a document in which a wide program of courses is contemplated, always adapted to the needs raised by its Community of reference.



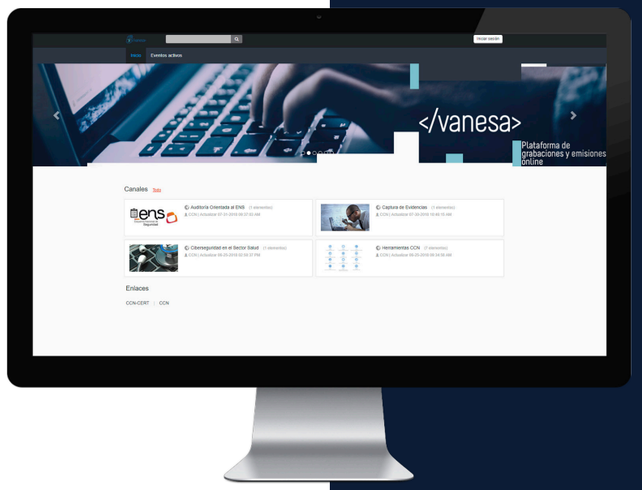
Itinerario de Formación 2020
Training Itinerary 2020

Sin embargo, dadas las circunstancias excepcionales provocadas por la crisis de la COVID-19, se realizó un importante esfuerzo para continuar con el Plan de Formación del Centro Criptológico Nacional. Entre las iniciativas llevadas a cabo destacan las siguientes:

- Desarrollo de un nuevo curso online sobre principios y recomendaciones básicas en ciberseguridad, con una duración de 10 horas, para todo aquel interesado en adquirir conocimientos básicos sobre el sector.
- Sesiones semanales de formación a través de su plataforma de streaming VANESA, con el objetivo de permitir, de manera práctica y visual, que los usuarios pudieran llevar a cabo las recomendaciones de seguridad publicadas por este organismo.
- Cursos presenciales adaptados a la modalidad en remoto. Ante la dificultad de poder llevar a cabo formaciones *in situ*, el CCN realizó un gran esfuerzo por continuar con estos cursos a distancia, los cuales estaban especialmente centrados en buenas prácticas y/o herramientas para la implantación segura del teletrabajo.

However, given the exceptional circumstances caused by the COVID-19 crisis, a major effort was made to continue with the National Cryptologic Centre's Training Plan. Among the initiatives carried out, the following stand out:

- Development of a new online course on basic principles and recommendations in cybersecurity, with a duration of 10 hours, for anyone interested in acquiring basic knowledge about the sector.
- Weekly training sessions through its streaming platform VANESA, with the aim of allowing, in a practical and visual way, that users could carry out the security recommendations published by this organism.
- On-site courses adapted to the remote modality. Given the difficulty of being able to carry out on-site training, the CCN made a great effort to continue with these distance courses, which were especially focused on good practices and/or tools for the safe implementation of teleworking.



ángeles

ÁNGELES

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

A través de este portal, el CCN facilita tanto a los profesionales como a aquellas personas interesadas en este ámbito el acceso a un buen número de recursos destinados a incrementar sus conocimientos, independientemente de su nivel de formación. Para ello, ÁNGELES está integrada por tres grandes áreas:

- Formación: incluye los diferentes cursos ofrecidos por el CCN, tanto de forma presencial como online y con todos los niveles; desde la formación básica, hasta los cursos de gestión o de especialización en diferentes materias. En esta sección, se detallan los diferentes Cursos STIC desarrollados en colaboración con el Instituto Nacional de Administración Pública (INAP), así como VANESA (sesiones formativas en directo).
- Talento: incluye las plataformas de desafíos del CCN, ATENEA y ATENEA Escuela, a través de las cuales los profesionales se enfrentan a diferentes retos, en función de su destreza.
- Concienciación y sensibilización: en el que se recopilan diferentes recursos para un uso seguro de las TIC, como ciberconsejos, recomendaciones y guías de buenas prácticas.

With the desire to promote the culture of cybersecurity, the National Cryptologic Centre launched, in October 2020, the new ÁNGELES website, its solution entirely dedicated to the education, awareness, training and talent of professionals in this field.

Through this website, the CCN provides both professionals and those interested in this field with access to many resources aimed at increasing their knowledge, regardless of their level of training. To this end, ANGELES is made up of three main areas:

- Training: it includes the different courses offered by the CCN, both face-to-face and online and at all levels; from basic training to management or specialisation courses in different subjects. This section details the different STIC Courses developed in collaboration with the National Institute of Public Administration (INAP), as well as VANESA (live training sessions).
- Talent: it includes the challenge platforms of the CCN, ATENEA and ATENEA School, through which professionals face different challenges, depending on their skills.
- Awareness and sensitisation: in which different resources are compiled for a safe use of ICT, such as cyber-tips, recommendations and good practice guides.

Cursos STIC 2020

STIC 2020 courses

23

Cursos presenciales en colaboración con INAP

On-site courses in collaboration with INAP

600

Alumnos formados en colaboración con INAP

Students trained in collaboration with INAP

30

Sesiones Vanesa

Vanesa sessions

6.712

Asistentes sesiones Vanesa

Vanesa sessions attendees

20

Cursos online (www.ccn-cert.cni.es)

Online courses (www.ccn-cert.cni.es)

15.977

Número de alumnos inscritos online

Number of students enrolled online

121.171

Número de accesos a cursos

Number of course accesses

1.988

Certificados emitidos

Certificates issued

ATENEA

Atenea es la plataforma de desafíos desarrollada por el CCN-CERT para que cualquier persona con inquietudes en el campo de la ciberseguridad pueda poner a prueba sus conocimientos. Por tanto, los retos que aquí se pueden encontrar son de distinta dificultad y muy diversas temáticas, como criptografía y esteganografía, exploiting, forense, análisis de tráfico o reversing, de forma que cualquier usuario pueda evaluar sus destrezas, independientemente de su nivel de partida.

En 2020 esta plataforma tuvo 2.880 nuevas inscripciones, ascendiendo la cifra total de usuarios a 12.680 al finalizar el año. En cuanto al número de retos publicados, estos eran 170 en diciembre de 2020.

Atenea is the challenge platform developed by the CCN-CERT so that anyone interested in the field of cybersecurity can test their knowledge. Therefore, the challenges that can be found here are of varying difficulty and very diverse topics, such as cryptography and steganography, exploiting, forensics, traffic analysis or reversing, so that any user can evaluate their skills, regardless of their starting level.

In 2020 this platform had 2,880 new registrations, bringing the total number of users to 12,680 by the end of the year. In terms of the number of challenges published, there were 170 in December 2020.

Ciberconsejos
Cybertips

Desde sus orígenes, el Centro Criptológico Nacional ha tenido entre sus principales objetivos fomentar el conocimiento y el uso seguro de las Tecnologías de la Información y la Comunicación. En esta apuesta por la cultura de la ciberseguridad entre todos los usuarios, el CCN ha continuado en 2020 publicando diversas recomendaciones de ciberseguridad para prevenir y detectar contratiempos en la utilización diaria de las nuevas tecnologías.

A lo largo de 2020, esta sección se ha ampliado con nuevos apartados y material de concienciación, incluyéndose nuevos informes, abstracts, infografías y vídeos.

Since its origins, the National Cryptologic Centre has had among its main objectives to promote the knowledge and secure use of Information and Communication Technologies. In this commitment to the culture of cybersecurity among all users, the CCN has continued in 2020 publishing various cybersecurity recommendations to prevent and detect mishaps in the daily use of new technologies.

Throughout 2020, this section has been expanded with new sections and awareness material, including new reports, abstracts, infographics and videos.

Entre ellas, cabe destacar la campaña de concienciación #CiberCOVID19, que sirvió para concienciar a los usuarios de las amenazas y vectores de infección que los atacantes estaban empleando para lograr infectar los equipos de los usuarios.

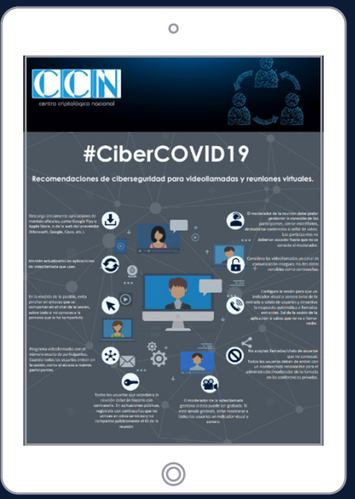
These included the #CiberCOVID19 awareness campaign, which served to make users aware of the threats and infection vectors that attackers were using to infect users' computers.

Ciberconsejos
Cybertips

41.027

Descargas 2020

2020 Downloads



4.1.3 Informes, avisos, alertas y vulnerabilidades
4.1.3 Reports, warnings, alerts and vulnerabilities

El grupo de expertos del CCN-CERT ha elaborado y actualizado durante 2020 numerosos informes de seguridad de muy diversa temática y con diferente nivel de complejidad. Estos documentos incluyen características de la amenaza o código dañino, procedimientos de infección, formas de detección, recomendaciones, así como medidas preventivas y correctivas para hacerles frente.

Asimismo, todos los usuarios registrados en el portal del CCN-CERT (14.045 en 2020) han recibido múltiples avisos y alertas en los que informaba de nuevas amenazas detectadas, convocatorias de cursos, cambios en el portal y en diversos servicios y soluciones, etc.

During 2020, the CCN-CERT's group of experts has prepared and updated numerous security reports on a wide range of topics and with different levels of complexity. These documents include characteristics of the threat or malware, infection procedures, detection methods, recommendations, as well as preventive and corrective measures to deal with them.

Likewise, all registered users of the CCN-CERT website (14,045 in 2020) have received multiple warnings and alerts informing them of new threats detected, course announcements, changes on the website and in different services and solutions, etc.

INFORME DE ACTIVIDADES _2020 - ACTIVITY REPORT _2020

Informes
Reports

Durante 2020 se publicaron numerosos informes en el portal del CCN. Las cifras son, por categorías, las siguientes:

Numerous reports were published on the CCN website during 2020. The figures by category are as follows:

20

Informes de Amenazas

Threat Reports

33

Informes de Código Dañino

Malware Reports

57

Informes Técnicos

Technical Reports

5

Informes de Buenas Prácticas

Best Practice Reports

Entre todos estos documentos, algunos de los más destacados en función del número de descargas que han tenido a lo largo del año son:

Among all these documents, some of the most outstanding in terms of the number of downloads they have had throughout the year are:

CCN-CERT BP/20 Buenas Prácticas en la Gestión de Cibercrisis

CCN-CERT BP/20 Good Practices in Cybercrisis Management

27.885

descargas en total

downloads in total

CCN-CERT IA-14/20 Marco Normativo y Salvaguardas. Edición 2020

CCN-CERT IA-14/20 Regulatory Framework and Safeguards. 2020 Edition

183.162

descargas en total

downloads in total

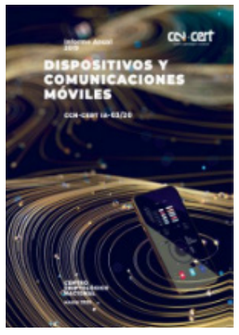
CCN-CERT IA-04/20 Informe Anual 2019. Hacktivismo y Ciberyihadismo

CCN-CERT IA-04/20 Annual Report 2019. Hacktivism and Cyberjihadism

19.674

descargas en total

downloads in total



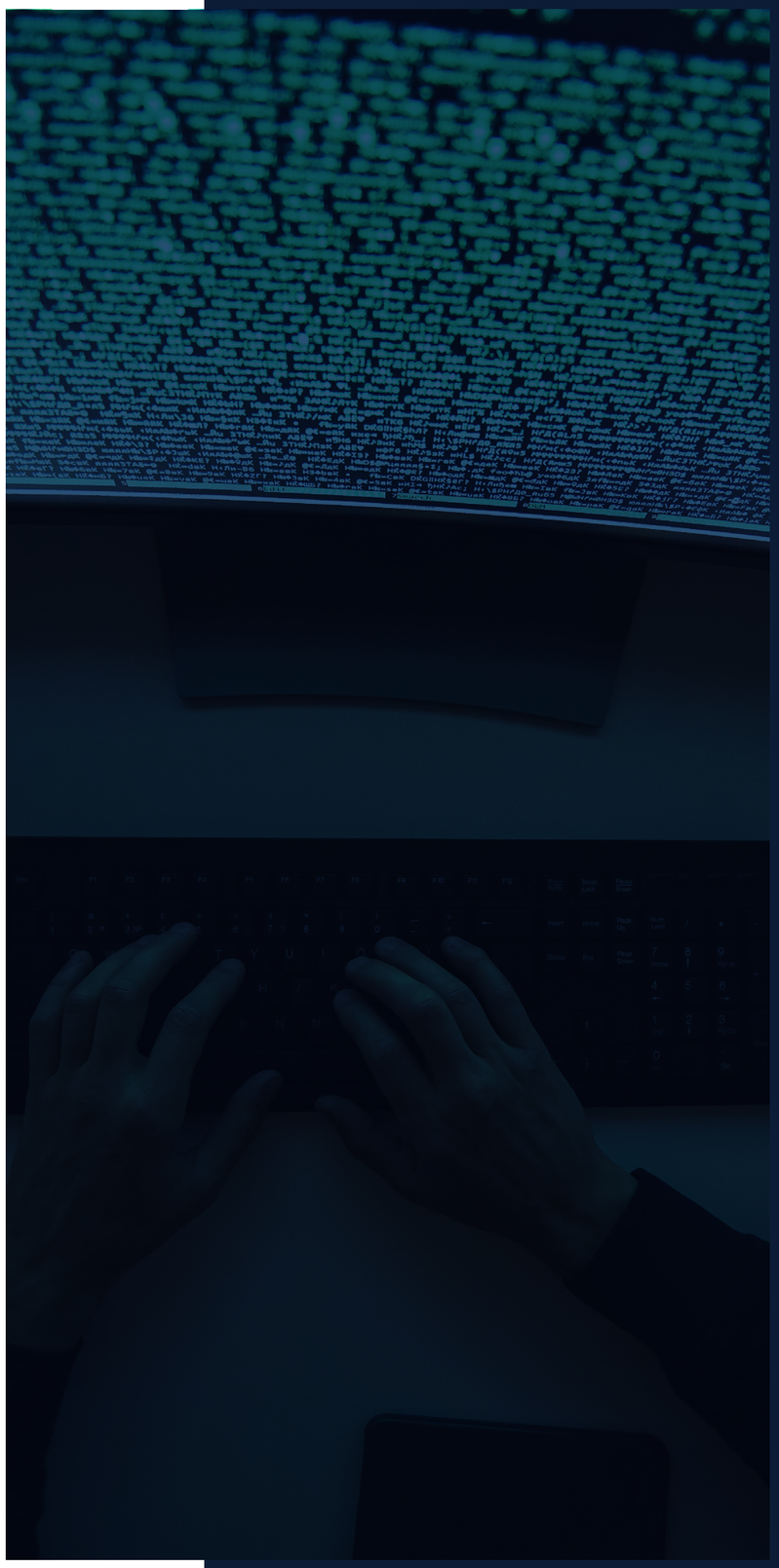
CCN-CERT IA-03/20 Informe Anual 2019. Dispositivos y Comunicaciones Móviles

CCN-CERT IA-03/20 Annual Report 2019. Mobile Devices and Communications

129.490

descargas en total

downloads in total



Avisos, alertas y vulnerabilidades

Warnings, alerts and vulnerabilities

Avisos / Warnings

2020	2019
81	48

Alertas / Alerts

2020	2019
11	10

Vulnerabilidades / Vulnerabilities

2020	2019
1.899	4.563

4.1.4 Guías CCN-STIC
4.1.4 CCN-STIC Guides

Las Series CCN-STIC son normas, instrucciones, guías y recomendaciones desarrolladas por el CCN, con el fin de mejorar el grado de ciberseguridad de las organizaciones. Periódicamente son actualizadas y completadas con otras nuevas, en función de las amenazas y vulnerabilidades detectadas por el CCN-CERT. A lo largo de 2020 se llegaron a publicar 49 nuevas guías. Asimismo, un total de 6 guías fueron actualizadas. Estas cifras hacen que el total de guías disponibles a finales de 2020 fuera de 415. El éxito de estas guías se muestra en el número de descargas realizadas: un total de 360.353 veces.

The CCN-STIC Series are standards, instructions, guides and recommendations developed by the CCN, in order to improve the degree of cybersecurity of organisations. They are periodically updated and completed with new ones, depending on the threats and vulnerabilities detected by the CCN-CERT. Throughout 2020, 49 new guides were published. Likewise, a total of 6 guides were updated. These figures bring the total number of guides available at the end of 2020 to 415. The success of these guides is shown by the number of downloads: a total of 360,353 times.

415

Total Guías / Total Guides

49

Nuevas en 2020 /

New New in 2020

6

Actualizadas en 2020 /

Updated in 2020

360.353

Número de descargas /

Number of downloads

347.588 Públicas / Public

12.765 Restringidas / Restricted

INFORME DE ACTIVIDADES _2020 - ACTIVITY REPORT _2020

Top 5 guías de acceso público descargadas en 2020
Top 5 public access guides downloaded in 2020

Guías / Guides
CCN-STIC-105 Catálogo de Productos y Servicios de las Tecnologías de la información y la Comunicación CCN-STIC-105 Catalogue of Information and Communication Technologies Products and Services
CCN-STIC-817 Gestión de Ciberincidentes CCN-STIC-817 Cyberincident Management
CCN-STIC-459 Guía práctica de seguridad de servicios de Apple CCN-STIC-459 Practical Guide to Securing Apple Services
CCN-STIC-885D Guía de configuración segura para Microsoft Teams CCN-STIC-885D Secure Configuration Guide for Microsoft Teams
CCN-STIC-1406 Procedimiento de empleo seguro Cortafuegos FortiGate CCN-STIC-1406 Secure Use Procedure FortiGate Firewall

Top 5 guías de acceso privado descargadas en 2020
Top 5 private access guides downloaded in 2020

Guías / Guides
CCN-STIC-301 Requisitos STIC CCN-STIC-301 STIC Requirements
CCN-STIC-210 Norma de Seguridad en las Emanaciones (DL) CCN-STIC-210 Emission Security Standard (DL)
CCN-STIC-202 Estructura y Contenidos DRS CCN-STIC-202 Structure and Contents DRS
CCN-STIC-203 Estructura y Contenido POS CCN-STIC-203 Structure and Content POS
CCN-STIC-302 Interconexión de CIS CCN-STIC-302 CIS Interconnection

4.2 Seguridad TIC. Desarrollo, evaluación y certificación de productos

4.2 ICT security. Product development, evaluation and certification

4.2.1 Productos para la seguridad de las TIC

4.2.1 ICT Security Products

Líneas de actividad del Departamento en relación con el desarrollo de productos de cifra y para seguridad de las Tecnologías de la Información:

- Nueva generación de equipos de cifra IP con capacidad dual (nacional - OTAN/UE) y con nuevas características (mayor capacidad de transmisión; distintos niveles de seguridad ...).
- Interoperabilidad de productos de cifra (implementación de protocolos para interoperabilidad cripto OTAN: SCIP, NINE, STaC-IS, NKMIS ...).
- Seguridad de dispositivos móviles y protección de la información de usuarios desplazados (cifradores personales).
- Comunicaciones tácticas y navegación satélite seguras.
- Intercambio seguro de información entre diferentes dominios de seguridad.

Lines of activity of the Department in relation to the development of encryption and IT security products:

- New generation of IP encryption equipment with dual capacity (national - NATO/EU) and with new features (higher transmission capacity; different security levels ...).
- Interoperability of encryption products (implementation of protocols for crypto NATO interoperability: SCIP, NINE, STaC-IS, NKMIS ...).
- Mobile device security and protection of mobile user information (personal encryptors).
- Secure tactical communications and satellite navigation.
- Secure information exchange between different security domains.

Productos de cifra

- Librería cripto con algoritmos aceptados para su uso.
- Cifradores personales para transmisión de información clasificada a través de redes públicas (software y hardware; versión VPN ...).
- Cifrado de Disco Duro (versión inicial) con capacidad de autenticación fuerte.
- Prototipo de cargador de claves OTAN/UE y nacional.

Desarrollos de productos de cifra en curso

- Nueva generación de equipos de cifra IP y no IP.
- Modernización de equipos de cifra nacionales (capacidad resistencia computación cuántica).
- Versión nacional cifrado disco duro (CryhodÑ).
- Integración de cifra táctica en gestores de comunicaciones del ET.
- Desarrollo de la versión operativa del cargador de claves OTAN/UE y nacional (ÈRMES).
- Nuevo cifrador multipropósito multidominio embarcable (CMME) con posibilidad de proteger información nacional y OTAN.
- Módulo de seguridad para el canal secundario de los receptores PRS del sistema Galileo.
- HSM (módulo seguridad) para infraestructura de claves públicas de nivel alto de seguridad (HA PKI).
- Versión rugerizada cifrador personal combatiente.
- ...

Products by number

- Crypto library with accepted algorithms for your use.
- Personal encryptors for transmission of classified information over public networks (software and hardware; VPN version ...).
- Hard Disk Encryption (initial version) with strong authentication capability.
- NATO/EU and National Key Loader Prototype.

Ongoing encryption product developments

- New generation of IP and non-IP encryption equipment.
- Upgrading of national encryption equipment (quantum computational resilience).
- National version encrypted hard disk (CryhodÑ).
- Tactical code integration in ET communication managers.
- Development of operational version of NATO/EU and national key loader (ÈRMES).
- New multi-purpose multi-domain shippable multi-domain encryptor (CMME) with the ability to protect national and NATO data.
- Security module for the secondary channel of Galileo PRS receivers.
- HSM (Security Module) for High Assurance Public Key Infrastructure (HA PKI).
- Ruggedized version of the personal combatant cipher.
- ...

Productos Seguridad TIC

- Soluciones para el intercambio seguro de información (pasarelas / CDS).
- Modernización de hardware y software, así como actualización criptológica de pasarelas.
- Desarrollo de nuevas pasarelas para sistemas específicos militares (Data Links, Asterix, BICES, etc.).
- Desarrollo de nuevas pasarelas para servicios genéricos (Web Services, PKI ...).
- Herramienta de borrado seguro para sistemas Windows y Android (Olvido).

Tecnologías Seguridad TIC

Durante el año 2020 se han realizado diferentes estudios relacionados con la seguridad de las TIC, como es el caso de la amenaza de la computación cuántica, y se ha publicado información básica sobre aspectos de seguridad de diferentes tecnologías.

- Estudio sobre la amenaza de la computación cuántica a la criptología actual y nueva generación de algoritmos de cifra (PQSC).
- Participación en grupo de trabajo para análisis de los aspectos de seguridad de 5G.
- Análisis de requisitos de seguridad para TLS.
- Estudio de la seguridad de los servicios en la nube.
- Autenticación multifactor.
- Acceso remoto seguro.
- ...

Otras actividades relacionadas con productos y tecnologías STIC

- Asesoramiento técnico a las Fuerzas Armadas (FAS) y a diferentes Oficinas de Programa del Ministerio de Defensa.
- Apoyo a la Administración en el desarrollo de arquitecturas de seguridad para sistemas clasificados.
- Participación en diferentes ejercicios (como es el Plan de Experimentación BRIEX2035 del ET) y en demostraciones de productos y tecnologías de seguridad para las FAS.

ICT Security Products

- Solutions for secure information exchange (gateways / CDS).
- Hardware and software modernisation, as well as cryptologic update of gateways.
- Development of new gateways for military specific systems (Data Links, Asterix, BICES, etc.).
- Development of new gateways for generic services (Web Services, PKI ...).
- Secure deletion tool for Windows and Android systems (Oblivion).

ICT Security Technologies

During 2020, different studies related to ICT security have been carried out, such as the case of the threat of quantum computing, and basic information on security aspects of different technologies has been published.

- Study on the threat of quantum computing to current cryptology and new generation of encryption algorithms (PQSC).
- Participation in working group for analysis of the security aspects of 5G.
- Security Requirements Analysis for TLS.
- Cloud services security study.
- Multi-factor authentication.
- Secure remote access.
- ...

Other activities related to STIC products and technologies

- Technical advice to the Armed Forces (FAS) and to different Programme Offices of the Ministry of Defence.
- Support to the Administration in the development of security architectures for classified systems.
- Participation in different exercises (such as the ET's BRIEX2035 Experimentation Plan) and in demonstrations of security products and technologies for the Armed Forces.

4.2.2 Evaluación de productos de cifra

4.2.2 Crypto products evaluation

Evaluaciones cripto finalizadas en 2020

- Cifrador IP EP430GU (actualmente en proceso de evaluación por la UE para protección de información clasificada EU-SECRET).
- Cifrador IP EP430GU/B (versión CONFIDENCIAL).
- Cifrador táctico TZ-1001 (versiones CONFIDENCIAL y DIF. LIMITADA).

Evaluaciones cripto en curso

- Nueva generación de equipos de cifra para redes IP.
- Evaluación de diferentes radios definidas por software (SDR) de varios fabricantes.
- Evaluación de los productos de cifra TZ-501R y TZ-2001MC (DL) para la Red Radio de Combate.
- Evaluación del módulo de seguridad receptor PRS nacional (PRESENCE2).
- POC-SM (elemento de cifra en el Canal Secundario de Galileo PRS).
- Nueva versión del sistema de comunicaciones móviles seguro Färist Mobile sobre terminal actual (nuevo sistema operativo, Android 10).

Evaluaciones futuras

- Nueva generación de equipos de cifra nacionales para redes IP y no IP.
- Nueva versión del sistema de comunicaciones móviles seguras Färist Mobile (nuevo terminal y versión del sistema operativo, Android 11).
- ...

Crypto evaluations completed in 2020

- EP430GU IP Encryptor (currently undergoing EU evaluation for protection of classified information EU-SECRET).
- IP Encryptor EP430GU/B (CONFIDENTIAL version).
- Tactical Encryptor TZ-1001 (CONFIDENTIAL and DIF. LIMITED versions).

Ongoing crypto evaluations

- New generation of encryption equipment for IP networks.
- Evaluation of different software defined radios (SDR) from various manufacturers.
- Evaluation of TZ-501R and TZ-2001MC (DL) cipher products for the Combat Radio Network.
- PRS National PRS Receiving Security Module Evaluation (PRESENCE2).
- POC-SM (Galileo PRS Secondary Channel Figure Element).
- New version of secure mobile communications system Färist Mobile on current terminal (new operating system, Android 10).

Future evaluations

- New generation of national encryption equipment for IP and non-IP networks.
- New version of the secure mobile communications system Färist Mobile (new terminal and operating system version, Android 11).
- ...

INFORME DE ACTIVIDADES _2020 - ACTIVITY REPORT _2020

4.2.3 Evaluación y certificación TEMPEST / ZONING

4.2.3 TEMPEST / ZONING evaluation and certification

Zoning instalaciones y equipos

- Se han realizado 213 certificaciones ZONING de Instalaciones (de evaluaciones realizadas por LABINGE, GRUTRA y CCN/EMSEC).
- Abiertos 110 nuevos expedientes de evaluaciones ZONING relativos a nuevos equipos y realizada la evaluación de 183 equipos para distintos organismos y empresas.

Evaluación TEMPEST

- Evaluados 7 equipos TEMPEST y 1 cifrador.
- Evaluación preliminar módulo seguridad.
- Evaluación de 3 armarios TEMPEST.

Certificación TEMPEST

- Certificación de 2 plataformas aéreas evaluadas por el GRUTRA (EA).
- Certificación radio empleada en THYPOON para NETMA a petición OP.

Otras actividades TEMPEST

- Apoyo y asesoramiento técnico en temas TEMPEST a diferentes Oficinas de Programa del Ministerio de Defensa.

Zoning facilities and equipment

- 213 ZONING certifications of installations have been carried out (from evaluations carried out by LABINGE, GRUTRA and CCN/EMSEC).
- 110 new ZONING evaluation dossiers opened for new equipment and 183 equipment evaluations carried out for various organisations and companies.

TEMPEST Evaluation

- Evaluated 7 TEMPEST devices and 1 coder.
- Preliminary assessment security module.
- Evaluation of 3 TEMPEST cabinets.

TEMPEST Certification

- Certification of 2 aerial platforms evaluated by GRUTRA (EA).
- Radio certification used at THYPOON for NETMA upon request OP.

Other TEMPEST activities

- Support and technical advice on TEMPEST issues to different Programme Offices of the Ministry of Defence.

4.2.4 Cualificación y aprobación de productos STIC

4.2.4 STIC products qualification and approval

Cualificación de productos STIC

STIC Products Qualification

70

Expedientes de cualificación iniciados en 2020

Qualification dossiers started in 2020

255

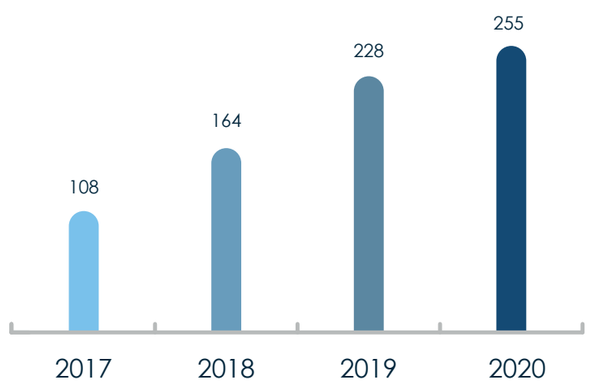
Número total de productos cualificados incluidos en el CPSTIC a finales de 2020

Total number of qualified products included in CPSTIC by the end of 2020

11,84%

Incremento número de productos cualificados incluidos en CPSTIC respecto al año 2019

Increase in the number of qualified products included in CPSTIC with respect to 2019



Número de productos cualificados

Number of qualified products

Aprobación de productos STIC

STIC Products Approval

15

Expedientes de aprobación iniciados en 2020

Approval files started in 2020

64

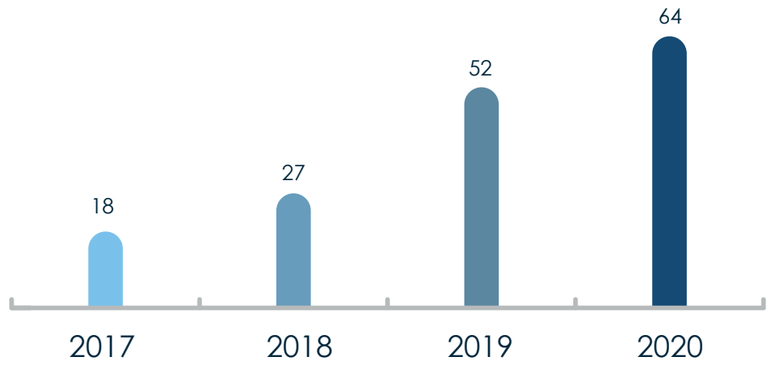
Total de productos aprobados incluidos en el CPSTIC a finales de 2020

Total approved products included in CPSTIC by the end of 2020

23,08%

Incremento número de productos aprobados incluidos en CPSTIC respecto al año 2019

Increase in the number of approved products included in CPSTIC compared to 2019



Número de productos aprobados

Number of approved products

4.2.5 Certificación de productos STIC

4.2.5 STIC Product Certification

Expedientes certificación abiertos

Open certification files

72

Total de expedientes abiertos

Total open files

58

De certificación de productos TIC y sitios de producción

Certification of ICT products and production sites

9

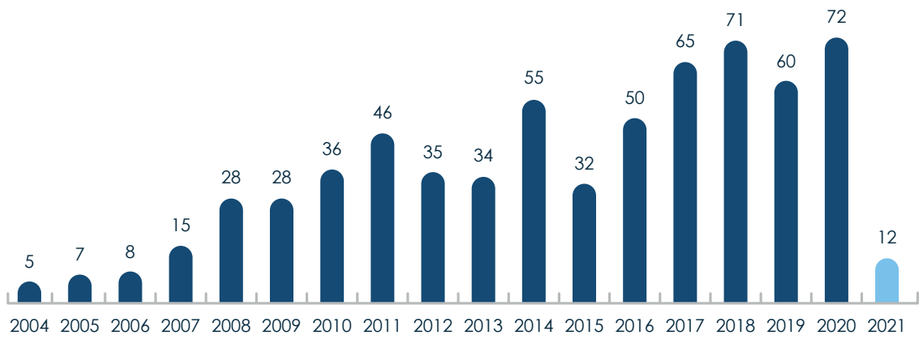
Para revisar la vigencia de certificados

To check the validity of certificates

5

Para acreditar nuevos laboratorios de evaluación o ampliar su acreditación

To accredit new assessment laboratories or extend their accreditation



Expedientes abiertos

Open files

Certificaciones realizadas

Certifications carried out

41

Total de certificaciones

Total number of certifications

34

Productos certificados

Certified products

2

Productos re-certificados

Re-certified products

5

Centros de producción certificados

Certified production sites

Acreditaciones de laboratorios realizadas

Laboratory accreditations carried out

5

Acreditación laboratorios

Laboratory accreditation

2

Nuevos laboratorios acreditados

New accredited laboratories

3

Laboratorios ampliaron el alcance de su acreditación

Laboratories extended the scope of their accreditation

Metodologías para la evaluación funcional de seguridad de productos

Methodologies for functional security assessment of products

- Common Criteria (ISO/IEC 15408).
- LINCE (UNE 320001).
- Common Criteria (ISO/IEC 15408).
- LYNX (UNE 320001).

Laboratorios acreditados en el ENECSTI

ENECSTI Accredited Laboratories

- Incorporación de nuevos laboratorios de evaluación al esquema nacional en los últimos años (2019-2020).
- Addition of new assessment laboratories to the national framework in recent years (2019-2020).

Laboratorios acreditados en el periodo 2019-2020 en el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI).

Laboratories accredited in the period 2019-2020 in the National Scheme for the Evaluation and Certification of Information Technology Security (ENECSTI).

INFORME DE ACTIVIDADES _2020 - ACTIVITY REPORT _2020

Reconocimiento internacional del OC

El OC representa a España en los acuerdos internacionales para reconocimiento mutuo de certificaciones SOGIS MRA y CCRA.

- España es emisor de certificados con reconocimiento en los correspondientes acuerdos internacionales.
- Reconocimiento internacional se mantiene tras superar las correspondientes auditorias que se realizan cada 5 años.
- Últimas auditorias superadas por el OC: CCRA en 2017 y SOGIS MRA en 2018.

International recognition of the OC

The OC represents Spain in the international agreements for mutual recognition of SOGIS MRA and CCRA certifications.

- Spain is an issuer of certificates with recognition in the corresponding international agreements.
- International recognition is maintained after passing the corresponding audits that are carried out every 5 years.
- Latest audits passed by the OC: CCRA in 2017 and SOGIS MRA in 2018.

4.2.6 Grupos de trabajo nacionales e internacionales

4.2.6 National and international working groups

Personal del Departamento de Productos y Tecnologías STIC participa habitualmente en diferentes grupos de trabajo sobre seguridad de los sistemas TIC tanto a nivel nacional como de la OTAN y la Unión Europea, así como en otros grupos de distintas iniciativas internacionales, aunque durante el año 2020 esta participación se ha visto condicionada por la pandemia mundial.

Staff from the STIC Products and Technologies Department regularly participates in different working groups on ICT systems security both at national, NATO and European Union level, as well as in other groups of different international initiatives, although during 2020 this participation has been conditioned by the global pandemic.

OTAN (Cifra y Seguridad Sistemas TIC)

- Panel para Aseguramiento de la Información y Ciberdefensa (CP/4).
- Grupos de trabajo sobre Cifra del C3B y del MC (Crypto CaT y ACTF).
- Grupos para la definición de requisitos técnicos en equipos de cifra OTAN.
- ...

NATO: (Cypher and ICT Systems Security)

- Panel on Information Assurance and Cyber Defence (CP/4).
- C3B and MC Cipher Working Groups (Crypto CaT and ACTF).
- Groups for the definition of technical requirements NATO figure equipment.
- ...

Grupos de trabajo internacionales sobre interoperabilidad cripto

International crypto interoperability working groups

- CIS3 C&IP
- SCIP WG
- NINE WG
- ...

- CIS3 C&IP
- SCIP WG
- NINE WG
- ...

Algunos grupos de trabajo nacionales

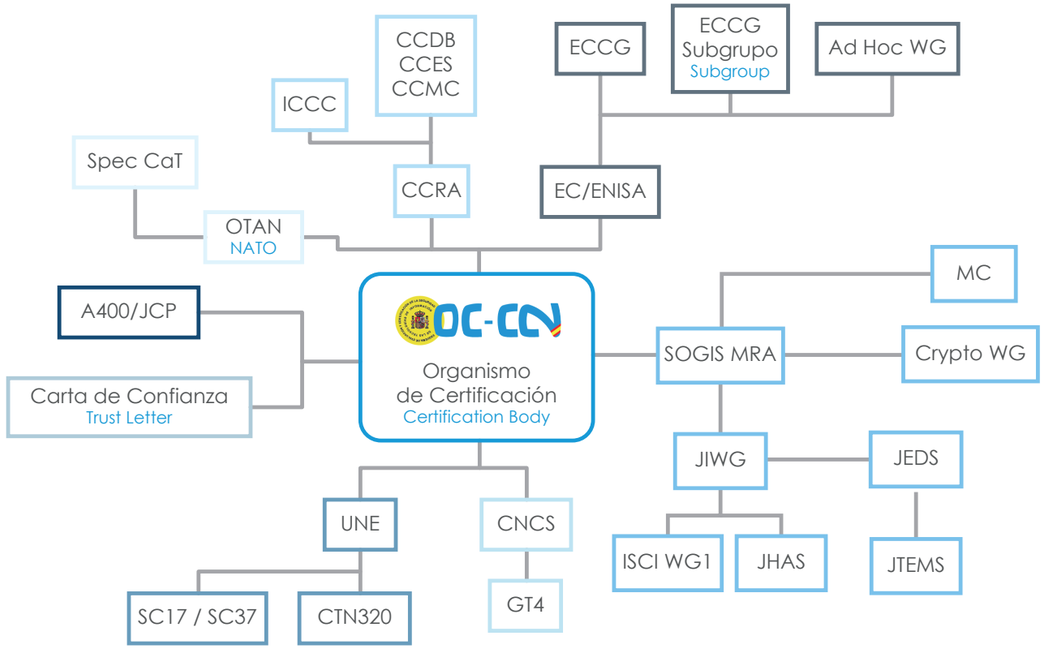
Some national working groups

- GTC3 del EMAD (liderado por MCCE).
- GT Comunicaciones Tácticas de la JUPROAM.
- GT para el desarrollo DDV del Programa del Sistema Conjunto de Radiocomunicaciones Tácticas (SCRT).
- ...

- GTC3 of EMAD (led by MCCE).
- JUPROAM Tactical Communications WG.
- WG for the DDV development of the Joint Tactical Radiocommunication System (JTRS) Programme.
- ...

Otros grupos de trabajo (OC)

Other working groups (OC)



Grupos de Trabajo con participación del OC

Working Groups with CO participation

4.2.7 Programas nacionales e internacionales

4.2.7 National and international programs

Apoyo a programas y Oficinas de Programa nacionales

- Programas MC3 y SCRT (Sistema Conjunto de Radio Táctica).
- Programa SECOMSAT.
- Programa MALE RPAS (EuroDron) y SIRTAP.
- Programa helicóptero TIGRE MKIIII.
- Programa C295.
- Programa ESPRES para el despliegue del Canal Secundario nacional para gestión de receptores PRS.
- Programa GEODE (nueva generación de equipos Galileo PRS).

Support to national programmes and programme offices

- MC3 and SCRT (Joint Tactical Radio System) Programs.
- SECOMSAT Program.
- MALE RPAS (EuroDron) and SIRTAP Programme.
- TIGRE MKIIII helicopter program.
- C295 Program.
- ESPRES Programme for the deployment of the national Secondary Channel for PRS receiver management.
- GEODE Programme (new generation of Galileo PRS equipment).

Participación en grupos de seguridad de programas internacionales

- Grupo INFOSEC y JAB del Programa MALE RPAS (EuroDron).
- Grupo Certificación (JCP) del Programa A400M.
- Panel COMSEC del programa A400M.
- Panel COMSEC del programa MIDS.
- Grupo TEMPEST-COMSEC del programa EUROFIGHTER.
- Grupo de Trabajo TEC del programa Galileo (Comisión Europea).

Participation in security groups of international programs

- INFOSEC and JAB Group of the MALE RPAS Programme (EuroDron).
- A400M Programme Certification Group (JCP).
- COMSEC panel of the A400M program.
- COMSEC panel of the MIDS program.
- TEMPEST-COMSEC group of the EUROFIGHTER programme.
- Galileo Programme TEC Working Group (European Commission).

4.2.8 Arquitecturas de seguridad y otros documentos

4.2.8 Security architectures and other documents

Desarrollo de arquitecturas de seguridad

Development of security architectures

- Preparación de arquitecturas de seguridad que permitan disponer de soluciones verificadas y con garantías.
- Arquitectura multidominio de puesto de trabajo ("End Point") seguro (CCN-STIC-498).
- Arquitectura multidominio de Puesto de Trabajo (End Point) seguro Caso de Uso: Difusión Limitada – Sin Clasificar (CCN-STIC-498A).

- Preparation of security architectures that allow for verified and guaranteed solutions.
- Secure Multidomain End Point Architecture (CCN-STIC-498).
- Multidomain End Point Architecture Secure Use Case: Limited Broadcast - Unclassified (CCN-STIC-498A) .

Interconexión
Interconnection

Cloud
Cloud

End Point
End Point

5. Detección

5. Detection

5.1 Gestión y respuesta a incidentes

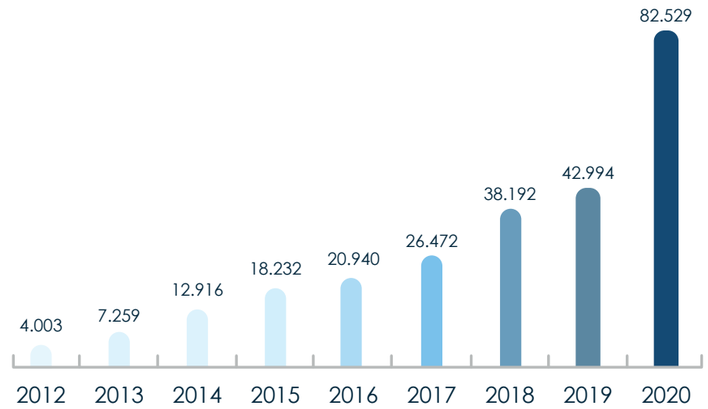
5.1 Incident Management and Response

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

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

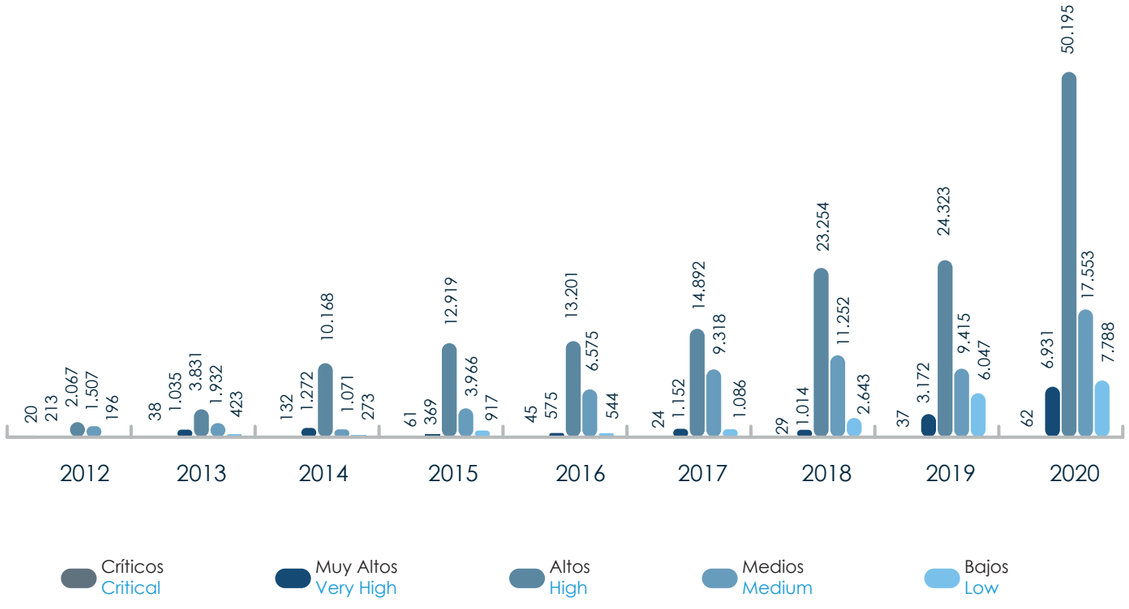
En 2020 el CCN-CERT detectó un total de 82.529 incidentes, 39.535 más que en 2019.

In 2020 the CCN-CERT detected a total of 82,529 incidents, 39,535 more than in 2019.



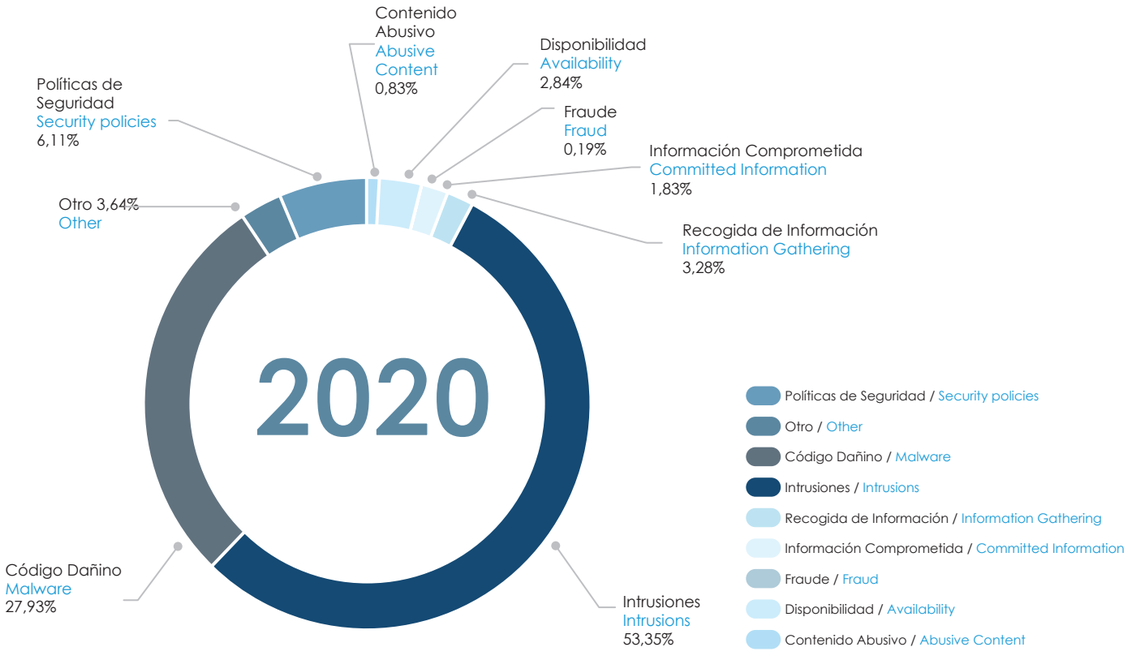
Incidentes gestionados por el CCN-CERT

Incidents managed by the CCN-CERT



Criticidad de los incidentes gestionados

Criticality of managed incidents



Tipología de los incidentes gestionados

Types of incidents managed

5.2 Sistema de Alerta Temprana (SAT)

5.2 Early Warning System (SAT)

El Sistema de Alerta Temprana (SAT) fue desarrollado por el CCN-CERT en 2008 con el objetivo de actuar antes de que se produzca un incidente en la Administración y empresas de interés estratégico, o bien reducir su impacto y alcance. Y a lo largo del pasado año, el CCN-CERT desplegó multitud de sondas para la puesta en marcha de este Sistema en diversos organismos, en alguna de sus tres modalidades de servicio: SAT-INET, SAT-SARA y SAT-ICS:

The Early Warning System (SAT) was developed by the CCN-CERT in 2008 with the aim of acting before an incident occurs in the Administration and companies of strategic interest, or to reduce its impact and scope. Throughout last year, the CCN-CERT deployed a multitude of probes for the implementation of this System in different organisations, in one of its three service modalities: SAT-INET, SAT-SARA and SAT-ICS:

SAT-INET / SAT-INET

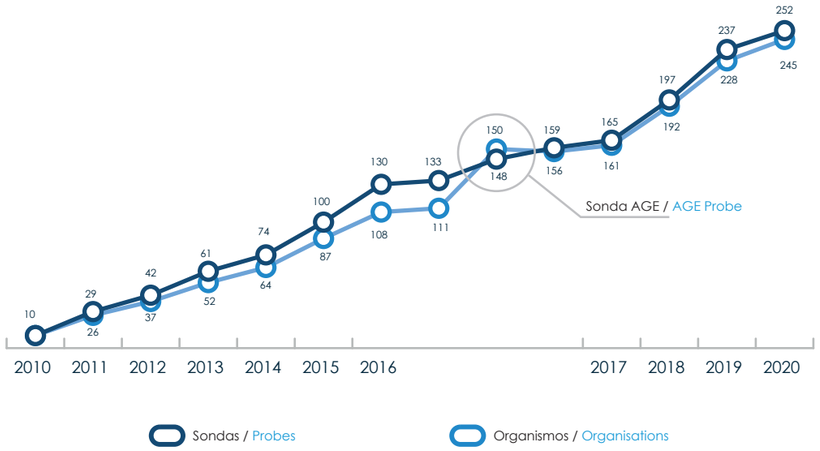
Sondas desplegadas / *Probes deployed*

252

Organismos / *Organisations*

245

- Ministerios y organismos AGE / *Ministries and agencies AGE*
- Comunidades Autónomas / *Autonomous Communities*
- Diputaciones provinciales / *Provincial councils*
- Ayuntamientos / *City Councils*
- Confederaciones Hidrográficas / *Hydrographic Confederations*
- Puertos / *Ports*
- Universidades / *Universities*
- Empresas de interés estratégico / *Companies of strategic interest*



SAT-SARA / SAT-SARA

Sondas desplegadas / *Probes deployed*

50

Organismos / *Organisations*

50

SAT-ICS / SAT-ICS

Sondas desplegadas / *Probes deployed*

21

Organismos / *Organisations*

33

Sonda distribuida
Distributed probe

Lanzada en septiembre de 2020, permite proporcionar al organismo que se beneficia del SAT-INET de todo un SIEM que pueda hacer toda la ingesta de fuentes.

Launched in September 2020, it allows to provide the organisation benefiting from the SAT-INET with a whole SIEM that can make all the source ingestion.

5.3 Análisis
5.3 Analysis

GLORIA

Plataforma para la gestión de incidentes y amenazas de ciberseguridad a través de técnicas de correlación compleja de eventos. Basado en los sistemas SIEM (Security Information and Event Management), permite una orientación muy flexible hacia la vigilancia del mundo IP.

Platform for the management of cybersecurity incidents and threats through complex event correlation techniques. Based on SIEM (Security Information and Event Management) systems, it allows a very flexible orientation towards the surveillance of the IP world.

MÓNICA

En mayo de 2020 el CCN-CERT presentó esta nueva solución, un sistema automatizado de gestión de información y eventos de seguridad. Esta nueva herramienta recoge en una única plataforma toda la información existente sobre amenazas potenciales, permitiendo no solo reaccionar ante los ataques, sino adelantarse a ellos para remediarlos antes de que sucedan. La solución se une a GLORIA como posible SIEM a utilizar por las Administraciones Públicas.

In May 2020 the CCN-CERT presented this new solution, an automated information and security event management system. This new tool gathers in a single platform all the existing information about potential threats, allowing not only to react to attacks, but also to anticipate them in order to remedy them before they happen. The solution joins GLORIA as a possible SIEM to be used by Public Administrations.

5.4 Vigilancia
5.4 Surveillance

CARMEN

Solución desarrollada con el objetivo de identificar el compromiso de la red de una organización por parte de amenazas persistentes avanzadas (APT). En este sentido, constituye la primera capacidad española, basada en conocimiento y tecnología nacionales.

Solution developed with the aim of identifying the compromise of an organisation's network by advanced persistent threats (APT). In this sense, it is the first Spanish capability, based on national knowledge and technology.

CLAUDIA

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

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

microCLAUDIA

El CCN-CERT desarrolló en 2020 microCLAUDIA, una capacidad basada en el motor de su solución CLAUDIA que, mediante el despliegue de vacunas en equipos Windows, proporciona protección a organismos contra ransomware. Ese mismo año, se desarrollaron 60 vacunas para la protección de los equipos y la solución se desplegó en más de 88.000 equipos de 323 organismos, generando más de 10.000 alertas de seguridad.

In 2020, the CCN-CERT developed microCLAUDIA, a capability based on the engine of its CLAUDIA solution that, through the deployment of vaccines on Windows computers, provides protection to organisations against ransomware. That same year, 60 vaccines were developed for the protection of computers and the solution was deployed on more than 88,000 computers from 323 organisations, generating more than 10,000 security alerts.

+88.000
equipos
computers

323
organismos
organisations

+10.000
alertas de seguridad
security alerts

INFORME DE ACTIVIDADES _2020 - ACTIVITY REPORT _2020

5.5 Intercambio de información
5.5 Information exchange

El CCN-CERT, como Nodo de Intercambio de Información de Ciberincidentes en los Sistemas de Información de las Administraciones Públicas, ha desarrollado hasta el momento diversas soluciones que contribuyen a alcanzar el propósito mencionado.

The CCN-CERT, as the Information Exchange Node for Cyberincidents in Public Administration Information Systems, has so far developed several solutions that contribute to achieving the aforementioned purpose.

LUCÍA

Herramienta para la Gestión y Notificación de Ciberincidentes en las entidades del ámbito de aplicación del Esquema Nacional de Seguridad. Con ella se pretende mejorar la coordinación entre el CCN-CERT y los distintos organismos y organizaciones con las que colabora.

En 2020 un total de 260 organismos tenían instalado LUCÍA Central y 77 en formato federado, una cifra que es necesario incrementar de forma considerable de cara a 2021, dado que la experiencia ha demostrado que aquellos que utilizan la solución en esta última modalidad presentan mayor madurez en la resolución de incidentes.

Tool for the Management and Notification of Cyber Incidents in the entities within the scope of application of the National Security Framework. It aims to improve coordination between the CCN-CERT and the different bodies and organisations with which it collaborates.

In 2020, a total of 260 organisations had installed LUCÍA Central and 77 in federated format, a figure that needs to be increased considerably by 2021, given that experience has shown that those using the solution in federated format have greater maturity in incident resolution.

260
organismos con LUCÍA Central
organisations with LUCÍA Central

77
organismos en formato federado
organisations in federated format

REYES

Herramienta para agilizar los análisis de ciberincidentes y compartir información de ciberamenazas. A través de este portal centralizado de información puede realizarse cualquier investigación de forma rápida y sencilla, accediendo desde una única plataforma a la información más valiosa sobre ciberincidentes.

A final de 2020 se introdujeron en REYES más de 8.000 nuevos eventos, se crearon más de un millón de atributos, se registraron más de 55.000 consultas en la plataforma y se realizaron más de 1.500 nuevas investigaciones sobre ransomware. Además, las consultas realizadas se multiplicaron por dos con respecto al año anterior.

Tool to streamline the analysis of cyber incidents and share information on cyber threats. Through this centralized information platform, you can carry out any investigation quickly and easily, accessing from a single platform to the most valuable information on cyberincidents.

By the end of 2020, more than 8,000 new events were entered into REYES, more than one million attributes were created, more than 55,000 queries were logged on the platform, and more than 1,500 new ransomware investigations were conducted. In addition, the number of queries made doubled compared to the previous year.

+8.000
nuevos eventos
new events

+55.000
consultas
queries

+15.000
investigaciones sobre ransomware
ransomware investigations

6. Respuesta
6. Response

6.1 Centro de Operaciones de Ciberseguridad
6.1 Cybersecurity Operations Centre

Las Entidades Locales (EELL), al igual que el resto de Administraciones Públicas, tienen como objetivo crear las condiciones adecuadas para el desarrollo de nuevos servicios ligados a la evolución de la tecnología y promover e impulsar, de igual modo, su uso entre la ciudadanía y las empresas. Para ello, es esencial que lo hagan bajo un marco común de seguridad, el cual queda fijado en el Esquema Nacional de Seguridad (ENS).

En este sentido, el Centro Criptológico Nacional, a través de su Capacidad de Respuesta a incidentes de Seguridad de la Información (CCN-CERT) colabora activamente con las EELL para proteger sus sistemas, de forma que puedan desempeñar de forma segura el ejercicio de sus competencias de asistencia y cooperación económica y técnica. El apoyo que el CCN-CERT ofrece a estas entidades, ya sean Diputaciones, Cabildos, Consejos Insulares u órganos competentes equivalentes, así como Ayuntamientos de todas las dimensiones, se centra especialmente en conseguir que aquellas EELL con mayores dificultades se adecuen al ENS. La labor del CCN-CERT consiste, en esencia, en que las entidades apliquen las medidas necesarias para proteger sus sistemas e información, en cumplimiento de lo dispuesto en el Real Decreto 3/2010, de 8 de enero, y sean capaces de superar las auditorías relacionadas con esta materia.

Hasta la fecha, el CCN ha desempeñado una labor esencial en la protección de los sistemas informáticos de numerosos gobiernos autonómicos, como es el caso del Cabildo de Tenerife, el Principado de Asturias, el Gobierno de Navarra o la Comunidad Autónoma de la Región de Murcia, poniendo en marcha en las EELL un instrumento esencial para facilitar la adopción de las medidas oportunas que garanticen una defensa eficiente, así como la implantación de las herramientas o tecnologías más adecuadas para ello: los Centros Virtuales de Operaciones de Ciberseguridad (vSOC).

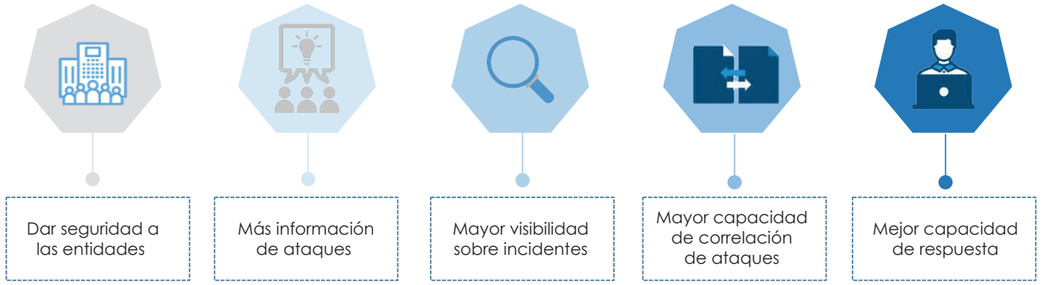
The Local Entities (EELL), like the rest of Public Administrations, aim to create the right conditions for the development of new services linked to the evolution of technology and to promote and encourage, in the same way, its use among citizens and companies. To this goal, it is essential that they do so under a common security framework, which is set out in the National Security Framework (ENS).

In this sense, the National Cryptologic Centre, through its Computer Emergency Response Team (CCN-CERT) actively collaborates with the EELLs to protect their systems, so that they can safely carry out their competences of economic and technical assistance and cooperation. The support that the CCN-CERT offers to these entities, whether they are Provincial Councils, Island Councils, Cabildos or equivalent competent bodies, as well as City Councils of all sizes, is especially focused on ensuring that those EELLs with greater difficulties adapt to the ENS. The work of the CCN-CERT consists, in essence, in ensuring that the entities apply the necessary measures to protect their systems and information, in compliance with the provisions of Royal Decree 3/2010, of 8 January, and that they are able to pass the audits related to this matter.

To date, the CCN has played an essential role in the protection of the computer systems of numerous autonomous governments, such as the Cabildo of Tenerife, the Principality of Asturias, the Government of Navarre or the Autonomous Community of the Region of Murcia, implementing in the EELLs an essential instrument to facilitate the adoption of appropriate measures to ensure an efficient defence, as well as the implementation of the most appropriate tools or technologies for this purpose: the Virtual Cybersecurity Operations Centres (vSOC).

Para implantar estos vSOC, el CCN-CERT sigue un modelo que, basado en la adecuación de las entidades al ENS, está integrado por cuatro grandes bloques de actuación: Plan de Adecuación del Sistema, implantación de medidas de seguridad, conformidad, y gestión continua de la seguridad.

In order to implement these vSOCs, the CCN-CERT follows a model that, based on the adaptation of the entities to the ENS, is made up of four main blocks of action: System Adaptation Plan, implementation of security measures, compliance and continuous security management.



Objetivos Virtual SOC (vSOC)
Virtual SOC (vSOC) objectives

7. Cultura de ciberseguridad
7. Cybersecurity Culture

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

The National Cryptologic Centre undertakes numerous actions aimed at promoting a culture of cybersecurity in Spain, aware of its importance in preventing a large part of the cyberthreats that affect society as a whole.

Por ello, a lo largo de 2020, y dado que se ha tratado de un año con especial vulnerabilidad frente a los ataques, no ha dejado de llevar a cabo numerosas iniciativas, todas ellas con el fin último de sensibilizar y concienciar a los españoles de los peligros y riesgos derivados del uso de las TIC.

For this reason, throughout 2020, and given that it has been a year of particular vulnerability to attacks, it has continued to carry out numerous initiatives, all with the ultimate aim of raising awareness and sensitizing Spaniards to the dangers and risks arising from the use of ICTs.

Foro Nacional de Ciberseguridad
National Cybersecurity Forum

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

The National Cybersecurity Forum, whose second vice-presidency is assigned to the CCN, was set up in 2020 with the aim of fostering the culture of cybersecurity, offering support to Industry and R&D&I and promoting training and talent, all through an environment of public-private collaboration and under the umbrella of the National Security Council.

FORO NACIONAL DE CIBERSEGURIDAD

Composición del Foro
Composition of the Forum

DSN

Presidencia / Presidency
Director del DSN y Vicepresidente del CNCS
Director of the DSN and Vice-President of the CNCS

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Vicepresidencia Primera / First Vice-Presidency
Directora del Instituto Nacional de Ciberseguridad
Director of the National Institute of Cybersecurity

CCN centro criptológico nacional

Vicepresidencia Segunda / Second Vice-Presidency
Subdirector del Centro Criptológico Nacional
Deputy Director of the National Cryptologic Centre

DSN

Secretaría / Secretary
Departamento de Seguridad Nacional
National Security Department

Vocalías permanentes / Permanent memberships
Un representante de cada uno de los miembros de la Comisión Permanente de Ciberseguridad
One representative of each of the members of the Standing Committee on Cybersecurity

Vocalías / Vocalities
Vocales representantes
Representative members

Para cumplir con sus objetivos principales, el Foro lleva a cabo diversas funciones:

- Proponer iniciativas al Consejo Nacional de Ciberseguridad.
- Analizar y estudiar propuestas.
- Contribuir a la valoración y análisis de los riesgos y amenazas.
- Apoyar la realización y evaluación de ejercicios de gestión de crisis.
- Contribuir a la identificación de las necesidades de la industria y de los centros de investigación.
- Colaborar en la realización de catálogos de recursos.
- Canalizar y formular propuestas sobre el marco regulatorio y normativo.
- Impulsar la realización proactiva de estudios e informes.
- Idear iniciativas tendentes a promover la cultura Nacional de Ciberseguridad.
- Apoyar la proyección y participación de España a nivel internacional y europeo en materia de ciberseguridad y ciberdefensa.

In order to fulfil its main objectives, the Forum carries out several functions:

- To propose initiatives to the National Cybersecurity Council.
- To analyse and study proposals.
- To contribute to the assessment and analysis of risks and hazards.
- To support the conduct and evaluation of crisis management exercises.
- To contribute to the identification of the needs of industry and research centres.
- To collaborate in the creation of resource catalogues.
- To channel and formulate proposals on the regulatory and normative framework.
- To promote proactive studies and reports.
- To devise initiatives aimed at promoting the National Cybersecurity culture.
- To support the projection and participation of Spain at international and European level in cybersecurity and cyberdefence.

Para llevar a cabo dichas funciones, se constituyeron un total de tres grupos de trabajo, aprobados por el Consejo Nacional de Ciberseguridad y en línea con sus objetivos principales:

To carry out these functions, a total of three working groups were set up, approved by the National Cybersecurity Council and in line with its main objectives:

Grupo de Trabajo de Cultura de Ciberseguridad

Cybersecurity Culture Working Group

Grupo de Trabajo de Impulso a la Industria y a la I+D+i

Working Group for the Promotion of Industry and R&D&I

Grupo de Trabajo de Formación, Capacitación y Talento

Training, Capacity Building and Talent Working Group

Informar y sensibilizar
Informing and raising awareness

Con el objetivo de cumplir con una de sus principales funciones, informar y sensibilizar a la sociedad acerca de la importancia de la ciberseguridad, el CCN mantiene una fuerte presencia tanto en medios de comunicación como en las principales redes sociales.

En este sentido, a lo largo de 2020 ha publicado un total de 105 comunicados en su portal web y elaborado 7 artículos para diversas revistas del sector: Aviador, Cuadernos de Seguridad, Red Seguridad, CSIRT Chile, RECEX, Seis I+S y Socinfo.

En cuanto a su actividad en redes sociales, el CCN ha continuado desempeñando una importante labor de difusión y ha aumentado sus iniciativas de concienciación y divulgación a través de estos canales. Ejemplo de ello es la creación, al comienzo de la pandemia, de un hilo en Twitter que, bajo los hashtag #NoTeinfectesConElMail y #CiberCOVID19, reunía todas las recomendaciones y consejos del CCN para hacer frente a los ciberriesgos derivados de la COVID-19.

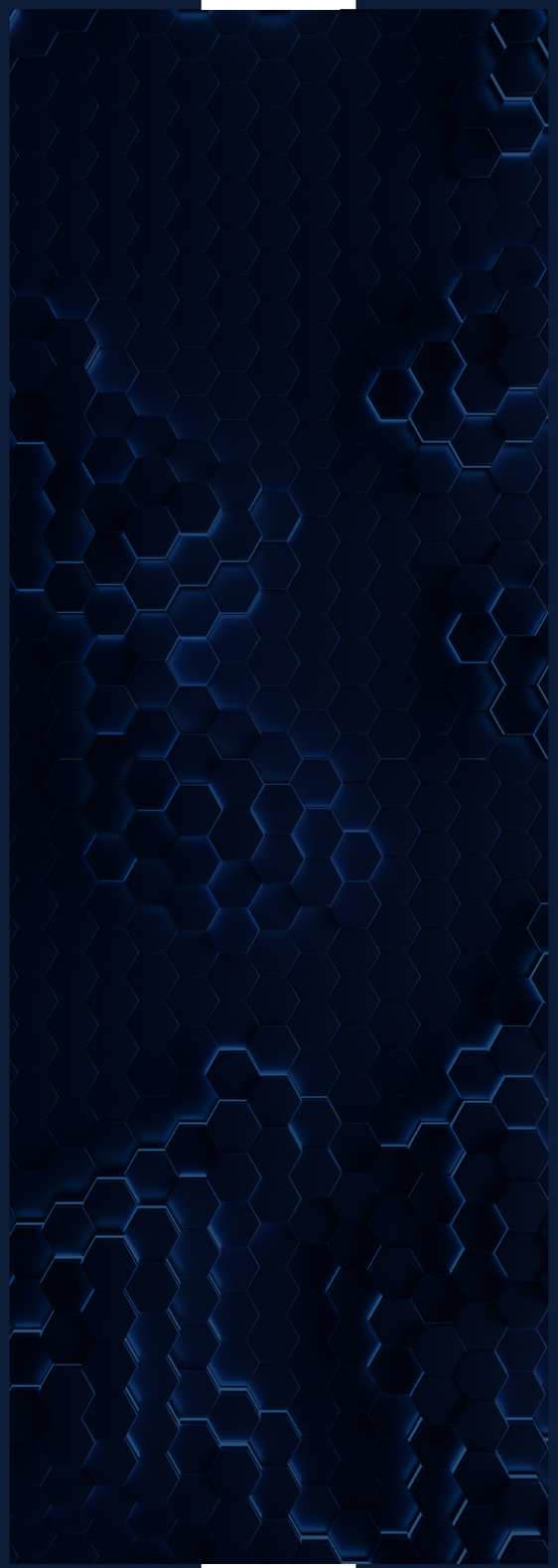
Como consecuencia de esta mayor actividad, todos los perfiles del CCN en redes sociales han atraído cada vez más público, siendo las cifras actuales las siguientes:

With the aim of fulfilling one of its main functions, to inform and raise awareness in society about the importance of cybersecurity, the CCN maintains a strong presence both in the media and in the main social networks.

In this sense, throughout 2020 it has published a total of 105 announcements on its website and has written 7 articles for various magazines in the sector: Aviador, Cuadernos de Seguridad, Red Seguridad, CSIRT Chile, RECEX, Seis I+S and Socinfo.

Regarding its activity on social networks, the CCN has continued to carry out important dissemination work and has increased its awareness-raising and dissemination initiatives through these channels. An example of this is the creation, at the beginning of the pandemic, of a thread on Twitter that, under the hashtag #NoTeinfectesConElMail and #CiberCOVID19, gathered all the recommendations and advice of the CCN to face the cyber risks derived from the COVID-19.

As a result of this increased activity, all CCN profiles on social networks have attracted more and more people, with the current figures being as follows:



LinkedIn

22.012
Seguidores
Followers

+7.686
Respecto a 2019
Compared to 2019

53%
Creció un
It grew by

Twitter

20.886
Seguidores
Followers

+6.534
Respecto a 2019
Compared to 2019

45%
Creció un
It grew by

YouTube

2.961
Suscriptores
Subscribers

+1.221
Respecto a 2019
Compared to 2019

70%
Creció un
It grew by

Eventos
Events

II Encuentro del Esquema Nacional de Seguridad
II Meeting of the National Security Framework

La segunda edición de este Encuentro, organizado el 24 de junio de 2020 por el CCN, en colaboración con el Ministerio de Asuntos Económicos y Transformación Digital y la Federación Española de Municipios y Provincias (FEMP), marcó un nuevo hito en la actividad del Organismo. Su celebración tuvo lugar a puerta cerrada y los más de 600 usuarios registrados pudieron seguir en directo, a través de VANESA, las ocho ponencias y cuatro talleres que, a cargo de 25 ponentes, conformaron el programa.

The second edition of this Meeting, organized on 24 June 2020 by the CCN, in collaboration with the Ministry of Economic Affairs and Digital Transformation and the Spanish Federation of Municipalities and Provinces (FEMP), marked a new milestone in the activity of the Centre. Its celebration took place behind closed doors and the more than 600 registered users were able to follow live, through VANESA, the eight presentations and four workshops that, by 25 speakers, made up the program.

La segunda edición de este Encuentro, organizado el 24 de junio de 2020 por el CCN, marcó un nuevo hito en la actividad del Organismo.

The second edition of this Meeting, organized on 24 June 2020 by the CCN, marked a new milestone in the activity of the Centre.

De izquierda a derecha: Carme Artigas (Secretaria de Estado de Digitalización e Inteligencia Artificial), Paz Esteban (Secretaria de Estado directora del CNI), Carlos Daniel Casares (Secretario General de la FEMP), y Juan Jesús Torres (Secretario General de Administración Digital)

From left to right: Carme Artigas (Secretary of State for Digitalisation and Artificial Intelligence), Paz Esteban (Secretary of State Director of the CNI), Carlos Daniel Casares (Secretary General of the FEMP), and Juan Jesús Torres (Secretary General for Digital Administration)

De izquierda a derecha: Juan Jesús Torres (Secretario General de Administración Digital), Carlos Galán (Asesor del CCN-CERT), y Javier Candau (Jefe del Departamento de ciberseguridad del Centro Criptológico Nacional)

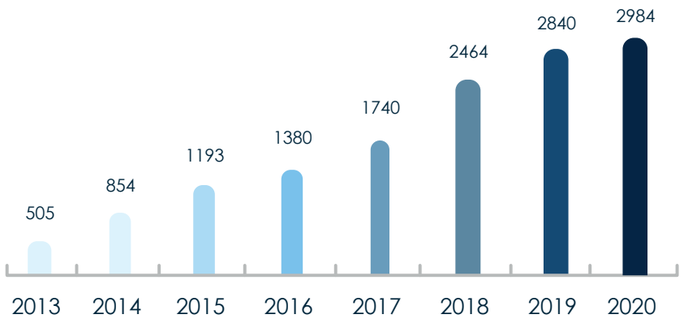
From left to right: Juan Jesús Torres (Secretary General for Digital Administration), Carlos Galán (CCN-CERT Advisor), and Javier Candau (Head of the Cybersecurity Department of the National Cryptologic Centre).

XIV Jornadas STIC CCN-CERT

XIV STIC CCN-CERT Conference

Las Jornadas STIC CCN-CERT del Centro Criptológico Nacional volvieron a demostrar en su decimocuarta edición ser el principal evento de ciberseguridad en España. A pesar de las circunstancias excepcionales del año 2020, que obligaron a celebrar el encuentro sin público y con retransmisión íntegra por streaming, congregó nuevamente a los principales agentes y profesionales del sector en nuestro país.

The STIC CCN-CERT Conference of the National Cryptologic Centre once again proved in its fourteenth edition to be the main cybersecurity event in Spain. Despite the exceptional circumstances of the year 2020, which forced the meeting to be held without an audience and with full streaming, it once again brought together the main agents and professionals of the sector in our country.



2020: 2.984

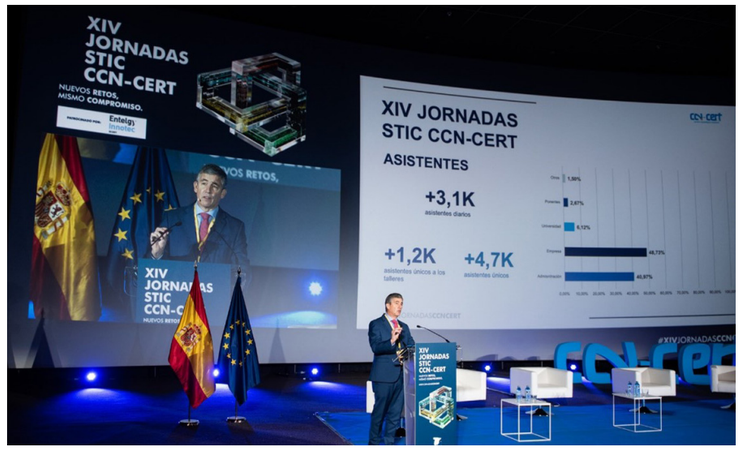
asistentes únicos / *attendees*

Celebrado entre los días 30 de noviembre y 4 de diciembre de 2020 y bajo el lema 'Nuevos retos, mismo compromiso', sus casi 3.000 asistentes pudieron disfrutar de más de 60 horas íntegras de retransmisión, con un protagonista claro en las ponencias: los ciberriesgos asociados a la pandemia de la COVID-19.

Held between 30 November and 4 December 2020 and under the slogan 'New challenges, same commitment', its almost 3,000 attendees were able to enjoy more than 60 full hours of broadcasting, with a clear protagonist in the presentations: the cyber risks associated with the COVID-19 pandemic.

XIV Jornadas STIC CCN-CERT

XIV STIC CCN-CERT Conference



Javier Candau (Jefe del Departamento de ciberseguridad del Centro Criptológico Nacional)

Javier Candau (Head of the Cybersecurity Department, National Cryptologic Centre)

Paz Esteban (Secretaria de Estado directora del CNI)

Paz Esteban (Secretary of State Director of the CNI)

8. Programas, grupos de trabajo y acuerdos de colaboración

8. Programmes, working groups and collaboration agreements

Nuevos acuerdos, convenios y grupos de trabajo

New agreements, conventions and working groups

Convenio de colaboración con INAP

Collaboration agreement with INAP

La secretaria de Estado Directora del CNI y del CCN, Dña. Paz Esteban, y el director del Instituto Nacional de Administración Pública (INAP), D. Mariano Fernández, firmaron en septiembre de 2020 un convenio de colaboración para impulsar la formación de empleados públicos en materia de seguridad de las Tecnologías de la Información y la Comunicación (TIC).

En concreto, en este convenio se estableció la organización, participación o colaboración conjunta en cursos, seminarios o itinerarios profesionales de seguridad y otras actividades similares de formación y/o sensibilización.

The Secretary of State Director of the CNI and the CCN, Ms. Paz Esteban, and the Director of the National Institute of Public Administration (INAP), Mr. Mariano Fernandez, signed in September 2020 a collaboration agreement to promote the training of public employees in the field of security of Information and Communication Technologies (ICT).

Specifically, this agreement established the joint organisation, participation or collaboration in courses, seminars or professional security itineraries and other similar training and/or awareness-raising activities.

INFORME DE ACTIVIDADES _2020 - ACTIVITY REPORT _2020

Acuerdo de colaboración con FEMP

Collaboration agreement with FEMP

El Centro Criptológico Nacional renovó en 2020 su acuerdo de colaboración con la Federación Española de Municipios y Provincias (FEMP). La firma de este convenio, que lleva vigente desde 2008 y ha sido actualizado a las circunstancias actuales, tuvo lugar en el marco del II Encuentro del Esquema Nacional de Seguridad. Con este acuerdo, ambas instituciones renovaron su compromiso con la ciberseguridad de la E-Administración y con el principal motor de esta: la confianza ciudadana.

The National Cryptologic Centre renewed in 2020 its collaboration agreement with the Spanish Federation of Municipalities and Provinces (FEMP). The signing of this agreement, which has been in force since 2008 and has been updated to the current circumstances, took place within the framework of the II Meeting of the National Security Framework. With this agreement, both institutions renewed their commitment to the cybersecurity of the E-Administration and its main driver: citizen trust.

Paz Esteban (Secretaria de Estado directora del CNI) y Carlos Daniel Casares (Secretario General de la FEMP)

Paz Esteban (Secretary of State Director of the CNI) and Carlos Daniel Casares (Secretary General of the FEMP).

Edita: Centro Criptológico Nacional
Edit: National Cryptologic Centre

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

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.11.11 12:20:15 +01'00'

centro criptológico nacional

centro criptológico nacional

CENTRO CRIPTOLÓGICO NACIONAL

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